Usable Cryptocurrency Systems

Dissertation

an der Fakultät für Mathematik, Informatik und Statistik
der Ludwig-Maximilians-Universität München

eingereicht von

MICHAEL FRÖHLICH

München, den 18.10.2022

Erstgutachter:	Prof. Dr. Albrecht Schmidt
Zweitgutachter:	Prof. Dr. Florian Alt
Drittgutachter:	Prof. Nigel Davies, Ph.D.

Tag der mündlichen Prüfung: xx.xx.2022

ABSTRACT

Since the introduction of Bitcoin in 2008 cryptocurrency and blockchain technology have drawn increasing attention from research and industry alike. The probably most visible evidence of the growing adoption of cryptocurrencies is the combined market capitalization which had reached over USD 2.9 trillion in November 2021. While the market capitalization remains subject to high volatility and has fallen since, the field has been growing steadily behind the scenes. Developer activity has been growing over the last decade and multiple projects which had been started to improve over the original design have reached maturity in recent years.

However, the introduction of new technologies is often accompanied by the emergence of equally new design challenges. Despite the technological progress over the past years, cryptocurrencies have earned a reputation of being hard to get started with and overall difficult to use. But what exactly are the aspects that make them difficult to use? How do users manage their cryptocurrency in practice? Which challenges do they need to overcome? And how can Human-Computer Interaction help overcome these challenges? In several studies, this dissertation addresses these questions and explores them through three different approaches:

(1) Cryptocurrency in Human-Computer Interaction: By systematically reviewing published Human-Computer Interaction research since the inception of Bitcoin, we organize the existing research effort and juxtapose it with the changing landscape of emerging technologies from practice to identify avenues for future research. Our results show that existing research has overwhelmingly focused on Bitcoin and Ethereum, while not addressing novel cryptocurrencies.

(2) Understanding User Behavior: By exploring user behavior through multiple lenses we shed light on real-world practices of users and the challenges they face. We explore security and privacy practices through a qualitative interview study and triangulate the results in a delphi-study with 25 experts. We conducted an interview study to understand a particularly relevant point for the adoption of cryptocurrency – we investigate challenges first-time users face. Our results show that many usability issues are not rooted in the technical aspects of blockchain technology and can be addressed through Human-Computer Interaction research.

(3) Improving Application Usability: By evaluating different approaches on how to aid the development of cryptocurrency applications we translate the findings of our empirical work into artifacts and put them to the test. Our results show that onboarding in mobile apps can improve perceived usability for first-time users under the right conditions, that Bitcoin Lightning can serve as a usable settlement layer for everyday transactions, that education can support the next generation of developers in building more useful applications, and that systems for rapid interface prototyping may speed up development efforts.

Collectively, the contribution of this dissertation centers around the ongoing discussion on how to build usable cryptocurrency systems. More precisely, this dissertation contributes (a) empirical studies that show how users manage their cryptocurrency in practice and which challenges they face in doing so and (b) constructive approaches attempting to support the development of cryptocurrency systems in the future. The work concludes by reflecting on the future role of Human-Computer Interaction research in the cryptocurrency and blockchain space.

ZUSAMMENFASSUNG

Seit der Einführung von Bitcoin im Jahr 2008 haben Kryptowährungen und die Blockchain-Technologie in der Forschung und der Industrie zunehmend an Aufmerksamkeit gewonnen. Der wohl sichtbarste Beweis für die wachsende Akzeptanz ist die kombinierte Marktkapitalisierung, die im November 2021 über 2,9 Milliarden USD erreicht hatte. Während die Marktkapitalisierung einer hohen Volatilität unterliegt und seitdem gesunken ist, ist das Feld hinter den Kulissen stetig gewachsen. Die Zahl aktiver Entwickler hat in den letzten zehn Jahren zugenommen, und zahlreiche Projekte, die zur Verbesserung der ursprünglichen Technologie begonnen wurden, haben die Marktreife erreicht.

Die Einführung neuer Technologien geht jedoch häufig mit dem Aufkommen ebenso neuer Designherausforderungen einher. Trotz des technologischen Fortschritts haben Kryptowährungen den Ruf erworben, schwer zugänglich und insgesamt schwierig zu bedienen zu sein. Doch was genau sind die Aspekte, die die Nutzung erschweren? Wie verwalten Nutzer ihre Kryptowährungen in der Praxis? Welche Herausforderungen müssen sie dabei bewältigen? Und wie kann die Mensch-Maschine-Interaktion helfen, diese Herausforderungen zu meistern? In mehreren Studien geht diese Dissertation diesen Fragen nach und untersucht sie durch drei verschiedene Linsen:

(1) Kryptowährungen in der Mensch-Computer-Interaktion: Durch eine systematischen Literaturanalyse der Mensch-Computer-Interaktion Forschung seit der Einführung von Bitcoin organisieren wir die bestehenden Forschungsanstrengungen und stellen sie der sich verändernden Landschaft aufkommenden Technologien gegenüber, um Wege für die zukünftige Forschung zu identifizieren. Unsere Ergebnisse zeigen, dass sich die bestehende Forschung überwiegend auf Bitcoin und Ethereum konzentriert hat, während sie sich nicht mit neuen Kryptowährungen befasst.

(2) Verständnis des Nutzerverhaltens: Durch die Erforschung des Nutzerverhaltens aus verschiedenen Blickwinkeln beleuchten wir die realen Praktiken der Nutzer und die Herausforderungen, denen sie sich dabei stellen. Wir untersuchen Sicherheitspraktiken durch eine qualitative Interviewstudie und triangulieren die Ergebnisse mit einer Delphi-Studie mit 25 Experten. Wir führen eine Nutzerstudie durch, um einen besonders relevanten Punkt für die Annahme von Kryptowährungen zu verstehen – die Herausforderungen, denen sich Erstnutzer gegenübersehen. Unsere Ergebnisse zeigen, dass viele Herausforderungen nicht in den technischen Aspekten der Blockchain-Technologie verwurzelt sind und mittels der Mensch-Computer-Interaktionsforschung adressiert werden können.

(3) Verbesserung der Benutzerfreundlichkeit von Anwendungen: Durch die Evaluierung verschiedener Ansätze zur Unterstützung der Entwicklung von Kryptowährungsanwendungen setzen wir die Erkenntnisse unserer empirischen Arbeit in Artefakte um. Unsere Ergebnisse zeigen, dass Onboarding in mobilen Apps die Benutzerfreundlichkeit für Erstnutzer unter den richtigen Bedingungen verbessern kann, dass Lehrkonzepte die nächste Generation von Entwicklern bei der Erstellung nützlicherer Anwendungen unterstützen kann und dass Systeme für schnelles Interface-Prototyping die Entwicklung beschleunigen können.

Zusammenfassend adressiert diese Dissertation die Frage, wie benutzbare Kryptowährungssysteme gebaut werden können: durch (a) empirische Studien, die zeigen, wie Benutzer ihre Kryptowährung in der Praxis verwalten und welche Herausforderungen sie dabei meistern müssen, und (b) durch konstruktive Ansätze, die versuchen, die Entwicklung von zukünftigen System zu verbessern. Die Arbeit schließt mit einer Reflexion über die zukünftige Rolle der Mensch-Computer-Interaktionsforschung im Kryptowährungs- und Blockchain-Bereich ab.

ACKNOWLEDGEMENT

I am grateful and humbled by the support I have received from so many over the past four years and want to use this opportunity to express my heartfelt appreciation.

I am grateful for the trust placed in me by my supervisors Prof. Albrecht Schmidt and Prof. Florian Alt. Your support from the very first day when I walked through the doors of the Cascada building to the current moment have made this dissertation an enriching experience that not only showed me how to conduct meaningful research, but also how to enjoy the process along the way. Your joint supervision left me room to explore projects at my own pace. You gave me the freedom to venture beyond the core topics presented in this dissertation and were always there to help whenever I asked for guidance and support. Putting trust in me despite my ample other responsibilities and interests made all the difference. Thank you for all of this. I would also like to thank the team at UniBW – Heike Renner, Sarah Prange, Yomna Abdelrahman, Yasmeen Abdrabou, Lukas Mecke, Radiah Rivu, Mariam Hassib, Sarah Delgado, Felix Dietz, Pascal Knierim, and Ken Pfeuffer – for welcoming me to your group. Seeing your research inspired me to strive for more myself! Thank you to everyone at the UniBW and LMU Media Informatics team from whom I could learn during the internal doctoral colloquia and winter schools. You showed me how to improve my research. A special thank you to Sarah Prange for being the first to welcome me at UniBW, for occasionally sharing your office, supervising theses, writing and publishing together.

Looking back, I am humbled by all the people I had the honor to work and co-author research with. Without you writing and publishing these papers would have been not only more challenging, but for sure a lot less fun. Thank you Philipp Hulm for showing iron determination and grit in acquiring our expert panel and making writing papers and proposals a joyful experience even when going long into the night. Thank you Ludwig Trotter for your perspective in positioning our literature review in the beginning and then helping me push it over the finishing line more than a year later. Thank you Franz Waltenberger, Jose Vega, Amelie Pahl, and Sergej Lotz for your help in running user studies, data collection, and sharpening our manuscripts, despite your full calendars. Thank you Charlotte Kobiella, Maurizio Wagenhaus, Benjamin Moser, and Felix Gutjahr for placing trust in me as your thesis supervisor and going the extra mile in publishing the research rooted in your theses with me.

Not all research projects of the past years are included in this dissertation. However, many of the projects not included have helped me improve and position subsequent work. Supervising theses and working together with talented, bright students was one of the most energizing aspects of conducting research that allowed me to look beyond my core research questions. While I am grateful for every student I have supervised, I want to thank Maurizio Wagenhaus, Charlotte Kobiella, Klaudia Guzij, Chandramohan Sudar, and Stefan Bielmeier for their exceptional commitment in working together. While working with each of you has been unique in many ways, you have all shown attention to detail while not missing the bigger picture and managed to be examples of grit and determination. I have learned a lot from our collaboration! All of this would not have been possible without the additional support of Prof. Isabell Welpe, Prof. Alexander Pretschner, Prof. Pramod Bhatotia, Prof. Wolfgang Kellerer, Prof. Klaus Diepold, Prof. Hana Milanov, and Prof. Reiner Braun. Thank you for your help in supervising these theses and IDPs. Thank you Prof. Hana Milanov, Prof. Isabell Welpe, Prof. Jörg Claussen, and Prof. Jelena Spanjol for sharing your experience and insight on how to manage life and work as a doctoral student during the internal doctoral seminars at CDTM.

I also want to express my sincere appreciation to Prof. Nikolaus Franke and the Institute for Entrepreneurship and Innovation at the Vienna University of Economics and Business. You welcomed me with open arms and enabled me to focus on my research during my stay in Vienna. Thank you Rudolf Domötör and Stephan Jung for introducing me to the Viennese startup ecosystem. Thank you Sophie Quach for showing me *Das Cafe*– the place where large parts of this dissertation were written. Thank you Peter Keinz, Stefan Bolzenius, Caroline Fabian, Jan Fell, Klaus Marhold, Shtefi Mladenovska, Tina Marie Monelyon, Benjamin Monsorno, Richard Olbrecht, Thomas Pannermayr, Jakob Pohlisch, Sophie Quach, Monique Schlömmer for welcoming me to E&I and sharing your research and teaching with me.

While this dissertation summarizes my scientific research output, my personal and professional growth over the past years has been shaped by much more than that. Without the support of family, friends, and colleagues this journey would have been indefinitely more challenging. I am grateful, because I have achieved this only by standing on your shoulders. I am lucky to have my parents Sabine Fröhlich and Robert Fröhlich on my side. In the hustle of everyday life it is easy to forget that my successes foot on the fundament that you have provided in so many ways. Your support means a lot. Thank you for always believing in me! Thank you Sabine Fröhlich for challenging my writing in this dissertation and the included publications. Your feedback was invaluable and helped me find the right words. Thank you Anna Fröhlich for being an inspiration on your own PhD journey and always a competition I hope to live up to. It has been inspiring to see you grow in work and life in the past years. Never stop. Thank you Gerhard Engleder for sharing the experiences and learnings from your own research journey, your career, and your management challenges.

Thank you Johann Nordhus-Westarp for the shared moments and projects ever since our very first encounter in Clemensstraße. You always bring a critical voice to the table not letting me get away with any excuses. You have grown into nothing less than a role model for determination, strong work attitude, and reflected leadership for me. But more than that, I want to thank you for being a great friend. Thank you Saad Bin Tariq, Kira Thuar, Philip Eller, and Esther Eller for the unforgettable visits to Berlin and Italy. The shared moments with you have helped me gain new perspectives on life and work. Thank you Michael Westbomke, Marco Djurisic, and Xaver Steigerwald for introducing me to Schafkopf. Thank you for the shared evenings, tolerating my ignorance of any and all implicit rules, the many *Böppel* I caused, and reminding me that joy can be found even in losing moments. Thank you Alexander Kremsmair for being an example of grit in pursuing your own research, our conversations far into the night, and the shared lazy moments in front of the TV. Thank you, Maximilian Wühr for always bringing joy into my life and setting an example of never being afraid to be yourself. You helped me to do the same. It is impressive to witness your journey at FINN and see how you grow with every challenge in front of you. Thank you Felix Krauth for showing me how to appreciate the randomness life has to offer and that summer evenings are best enjoyed with a cool drink and good friends. *In dubio Aperol!* Thank you Gesa Biermann for first making our office a little bit greener and now the world. Thank you Paul Schandelmaier and Justus Weiller for introducing me to Studentenküche and all the delicious meals that followed. Thank you Johannes Leitner for finally becoming flatmates in Vienna. Living together was eventful to say the least. It also reminded me why it is great to have you as a friend.

Finally, I want to express my sincere gratitude to the Center for Digital Technology and Management (CDTM). Being able to join CDTM, first as student and then as part of the management team, has without doubt changed the trajectory of my career and life. I have benefited tremendously from the program, the people, and the challenges I had to overcome. My experience here has taught me to

be a better man: To extend trust and respect first. To challenge my environment and myself and be ready to offer and ask for support if needed. To always be open for new ideas and proactively take responsibility in bringing positive change into the world. I will carry these values with me – wherever life takes me next. Thank you Robert Weindl for convincing me to apply back in 2015. I still remember the moment when the CDTM sticker on your MacBook caught my attention. Thank you Florian Lacher for bringing joy (and beer) to our time at Berkeley and convincing me to apply again in 2018. What might have been insignificant conversations for you, made all the difference for me. Without you I would not be here today. Thank you! It has been a growth journey ever since. Thank you to the students I had the honor to work with. I will always remember the classes of Spring 2019, Fall 2019, Spring 2020, Fall 2020, and Spring 2021 in a special place. Seeing you master the challenges within my courses made me proud then. Seeing you leave CDTM and embark on your careers as innovators makes me even prouder now. In this light, a special thank you to Carla Pregel-Hoderlein, Jose Vega, and Charlotte Kobiella for taking on one of the most rewarding jobs. It is great to see you join the management team and lift up the next generation of Centerlings.

More than anything else, the people you work with determine the quality of your professional life. And I am lucky and grateful to have worked next to a tremendous group of people: Patrick Bilic, Michael Chromik, Gesa Biermann, Tom Schelo, Philipp Hulm, Aaron Defort, Philipp Hofsommer, Theresa 'Tessa' Doppstadt, Elizaveta Felsche, Anna-Sophie Liebender-Luc, Amelie Pahl, Jose Vega, Carl-Pregel-Hoderlein, Felix Dörpmund, Vera Maria Eger, and Charlotte Kobiella. I am humbled that I got to call you my colleagues. Thank you for all the chances to learn from each other and grow together.

Working with you has been (mostly) awesome!

COLLABORATION STATEMENT

The publications on which this dissertation builds are the result of the collaboration with great people: my supervisors, fellow colleagues, and students. These publications would not have been possible without their support. I am grateful for their contributions which I acknowledge by using the scientific "we" throughout the text of this dissertation. In this statement I delineate my personal contribution to each project from the help I received.

All publications are the result of close collaboration with my supervisors Florian Alt and Albrecht Schmidt, who were involved from the early conceptualization to the final publication of each project.

Contribution of Students: Some publications included in this dissertation are rooted in Bachelor and Master theses supervised by me [P1, P3, P4, P7]. I was the main supervisor for each of them and determined the research topic, supervised the progress, and enabled their work with ample assistance. All theses projects were conducted in close cooperation with weekly or bi-weekly meetings. Decisions throughout the respective theses (e.g. regarding concepts, prototype features, study designs, evaluations) were made in coordination with me while specific steps (e.g. data collection, prototype implementation) were led by the respective students. In each of these cases, I was actively involved in the analysis of the data and took a leading role in the writing and editing of the paper as well as the publishing process.

Contribution of Colleagues: Other contributors were colleagues at the Center for Digital Technology and Management (CDTM) [P2, P5, P6, P8], fellow researchers from the University of Lancaster [P5], and from the Technical University of Munich (TUM) [P8]. In each of these cases, I took the leading role in all steps from conceiving the research question to publishing the final manuscript while my colleagues and co-authors supported in specific steps of the process (e.g. data collection, data analysis, writing).

Own Contribution: In all projects I took the leading role in determining the research question and the research design as well as writing, editing, and publishing the manuscript. In four projects I was leading data collection efforts [P2, P5, P6, P8] and in two projects I was supporting them [P3, P4]. In all projects I was heavily involved in the analysis of the data. In [P6] I was solely responsible for the implementation of the system, while in [P4] and in [P7] the prototype implementation was led by the respective student.

Table 1 provides a detailed clarification of the contributions of others to individual publications. Additionally, I clarify my co-authors and my own contribution in the publication summaries provided in Chapter 3.

Table 1: Clarification of the author's contribution to each included publication.

	Title	Contribution of Others
[P1]	Don't Lose Your Coin! Investigating Security Practices of Cryptocurrency Users (DIS'20)	Under my supervision Felix Gutjahr contributed to the design of the interview guideline and conducted the interviews as part of his Bachelor thesis.
[P2]	Under Pressure. A User-Centered Threat Model for Cryptocurrency Owners (ICBTA'21)	Philipp Hulm supported in the acquisition of the expert panel, the distribution of the delphi surveys, and in writing and revising the manuscript.
[P3]	Don't Stop Me Now! Exploring Challenges Of First-Time Cryptocurrency Users (DIS'21)	Under my supervision Maurizio Wagenhaus contributed to the design of the user study, he conducted the user study, supported in the analysis of the data, and the revision of the manuscript as part of his Master thesis.
[P4]	Is It Better With Onboarding? Improving First-Time Cryptocurrency App Experiences (DIS'21)	Under my supervision Charlotte Kobiella contributed to the design of the study, she conducted half of the interviews, designed the onboarding prototypes, conducted the user study, supported in the analysis of the data, and the revision of the manuscript as part of her Master thesis.
[P5]	Blockchain and Cryptocurrency in Human Computer Interaction: A Systematic Literature Review and Research Agenda (DIS'22)	Franz Waltenberger supported in writing sections 4.4 - 4.6 of the paper, the creation of the figures, and revision of the final manuscript. Ludwig Trotter supported in the design of the research approach to the literature review and revising the final manuscript. I also reused parts of a script written by Benjamin Moser as part of his Master thesis to automize keyword-search across all literature databases.
[P6]	Implementation and Evaluation of a Point-Of-Sale Payment System Using Bitcoin Lightning (NordiCHI'22)	Jose Vega supported in conducting the user study, during the analysis of the results, and in the revision of the manuscript.
[P7]	Supporting Interface Experimentation for Blockchain Applications (NordiCHI'22)	Under my supervision Benjamin Moser implemented the prototype and conducted the user study as part of his Master thesis.
[P8]	Prototyping with Blockchain: A Case Study for Teaching Blockchain Application Development at University (ICL'22)	Jose Vega, Amelie Pahl, and Sergej Lotz supported the positioning of the research question in joint discussions, the design and implementation of the course format and in writing and revising the manuscript. Isabell Welpe supported during the early idea generation for the course format and the revision of the manuscript.

Note. Florian Alt and Albrecht Schmidt were involved in every project from the early conceptualization to the final publication. For all publications I conceived the research question and research design, composed the manuscript, edited the final version, and led the publication process.

TABLE OF CONTENTS

1
Introduction

I am very intrigued by Bitcoin. It has all the signs. Paradigm shift, hackers love it, yet it is described as a toy. Just like microcomputers.

Paul Graham, Hacker News, 2013

1.1 Thesis Statement

Over the past decade cryptocurrencies have emerged from being a technical curiosity into a global phenomenon. The most visible indicator of the growing adoption is the combined market capitalization, which reached an all time high of over USD 2.9 trillion in November 2021 [25]. While market capitalization has been subject to volatility, the space has been steadily growing when looking at other indicators such as user activity [24], developer activity [35, 124], or social media activity [35].

For advocates, cryptocurrency and its underlying technology, blockchain, are viewed as enabling technology, often compared to the Internet [6, 24, 39, 87]. The open architecture of the Internet [82, 143] allowed for almost unrestricted participation which in turn fueled competition and innovation [143]. Driven by its open and decentralized architecture proponents of cryptocurrencies predict a similar effect on innovation of financial services that will ultimately increase financial inclusion [106, 122, 144]. More than that, the ability to digitally transfer ownership is seen by some as a fundamental paradigm-shift on which an entirely new class of internet applications can be realized [6]. The same way the proliferation of the internet drastically reduced transaction costs for information, cyptocurrencies and blockchain technology are expected to bring down the costs to transfer ownership [13] allowing people to build novel products and services. While many argue that the technology has the potential to disrupt current business models, financial systems, and organizations [6, 37, 38, 66, 133] this potential has yet to manifest itself.

Despite the space being characterized by a rapid pace of innovation there remain many challenges that need to be overcome. Current issues revolve around four themes: legality, scalability, usability, and acceptability [141]. Cryptocurrencies have been criticized to aid illicit activities [58, 136]. The speed and cost of transactions has for now remained behind those of centralized payment systems [141, 145] while being more complicated to use [3]. And against the backdrop of the fight against climate change the energy consumption of proof-of-work (PoW) blockchains has been a major point of discussion [34, 53, 130], with regulators going as far a proposing a complete ban within Europe [127]. However, these points of critique are not as black-and-white as they might seem at first glance. There are complex interdependent issues underlying them that are often misunderstood by examining them through the lens of any one discipline. For example, while country-level adoption of cryptocurrencies was shown to correlate with corruption [2], it is not clear that cryptocurrencies are the cause of said corruption. The stronger adoption of cryptocurrencies could equally be driven by the lower trust in formal institutions or less developed existing financial systems in these countries.

To address these interdependent challenges, a recent commentary in Nature puts forward nine focus points to move research on cryptocurrencies forward [141]: criminality, regulation, energy use, transaction speed, volatility, security, fee management, privacy, and education of users. Many of these points connect with core topics of Human-Computer Interaction research, echoing the calls from within our research community to engage with cryptocurrency and blockchain and to play an active role in shaping the use of these technologies [39, 40, 49]. However, these points also highlight the need for further research across disciplines. In doing so, they underline that cryptocurrencies, for now, remain a technology that is still under active development.

The growing adoption over the past decade cannot not hide the fact that cryptocurrencies have earned a reputation of being difficult to use (e.g. [3, 56, 147, 148]). The decentralized and pseudonymous nature of the technology raises both technical and social challenges, connected to long-standing issues in Human-Computer Interaction [39]. Key management has been recognized as a difficult task for the majority of users [41, 152]. With a complex underlying technology mental models often diverge from the technical reality [18, 90] opening the door for mistakes and exploitation. While being described as a "*trustless*" technology, interacting with pseudonymous entities raises socio-technical challenges [10] related to trust and collaboration [120, 121]. Collectively, these aspects impede users from adopting cryptocurrencies, reduce users' experience during use, and ultimately put them at risk of accidental loss or malicious attacks.

The research presented in this dissertation contributes to addressing these issues with the objective to better understand how we can build more usable cryptocurrency systems. Using the Technology Acceptance Model (TAM) as a framework to theorize about the adoption of cryptocurrency, we do so following three approaches: (1) We review the status quo of cryptocurrency research in Human-Computer Interaction; (2) we investigate user behavior, security practices and challenges; and (3) we explore constructive approaches to improve the usability and usefulness of cryptocurrency applications. Based on the combined results of the contributing publications we present a synopsis of our findings. We synthesize where current systems fall short, discuss arising design implications, and propose avenues for future research. In summary, the studies included in this dissertation collectively contribute to our understanding of how users interact with cryptocurrencies, which challenges they face while doing so, and how solutions to overcome them could look like.

1.2 Contributing Publications

The results of this cumulative dissertation have been published in individual publications before. This dissertation, therefore, serves as a summary of all projects to situate the results in the overall scientific discourse and to present a concluding reflection. The contributing publications are listed in chronological order in the reference list below.

Citations of these publications are marked with a "P" (e.g. [P4]). Seven out of the eight publications have been published as full papers at conferences [P1, P2, P3, P4, P5, P6, P8]. [P7] is an Extended Abstract. [P4] received an *Honourable Mention Award* at DIS '21. [P8] received a *Best Paper Award* at ICL '22.

The original publications are fully attached in *Appendix: Original Publications*.

Contributing Publications

[P1] Michael Froehlich, Felix Gutjahr, and Florian Alt. "Don't Lose Your Coin! Investigating Security Practices of Cryptocurrency Users". In: *Proceedings of the 2020 ACM Designing Interactive Systems Conference*. Association for Computing Machinery, 2020, pp. 1751–1763. DOI: 10.1145/3357236.3395535 (cited on pp. x, xi, 2, 6, 8–11, 15, 17, 20–22, 25, 26, 29–36, A 1).

[P2] Michael Froehlich, Philipp Hulm, and Florian Alt. "Under Pressure. A User-Centered Threat Model for Cryptocurrency Owners". In: *2021 4th International Conference on Blockchain Technology and Applications*. ICBTA 2021. Association for Computing Machinery, 2021, pp. 39–50. DOI: 10.1145/3510487.3510494 (cited on pp. x, xi, 2, 6, 8–11, 15, 17, 20, 21, 29, 30, 33, A 1).

[P3] Michael Froehlich, Maurizio Raphael Wagenhaus, Albrecht Schmidt, and Florian Alt. "Don't Stop Me Now! Exploring Challenges Of First-Time Cryptocurrency Users". In: *Designing Interactive Systems Conference 2021*. DIS '21. Association for Computing Machinery, 2021, pp. 138–148. DOI: 10.1145/3461778.3462071 (cited on pp. x, xi, 2, 6, 8–11, 15, 17, 20, 22, 24–26, 29–34, 36, A 1).

[P4] Michael Froehlich, Charlotte Kobiella, Albrecht Schmidt, and Florian Alt. "Is It Better With Onboarding? Improving First-Time Cryptocurrency App Experiences". In: *Designing Interactive Systems Conference 2021*. DIS '21. Association for Computing Machinery, 2021, pp. 78–89. DOI: 10.1145/3461778.3462047 (cited on pp. x, xi, 2, 6, 8, 10, 11, 17, 24, 25, 29, 31, 32, A 1).

[P5] Michael Froehlich, Franz Waltenberger, Ludwig Trotter, Florian Alt, and Albrecht Schmidt. "Blockchain and Cryptocurrency in Human Computer Interaction: A Systematic Literature Review and Research Agenda". In: *Designing Interactive Systems Conference*. DIS '22. Association for Computing Machinery, 2022, pp. 155–177. DOI: 10.1145/3532106.3533478 (cited on pp. x, xi, 2, 6, 7, 9–11, 13, 15–19, 26, 27, 29–36, A 1).

[P6] Michael Froehlich, Jose Vega, Florian Alt, and Albrecht Schmidt. "Implementation and Evaluation of a Point-Of-Sale Payment System Using Bitcoin Lightning". In: *ACM Nordic Human-Computer Interaction Conference (NordiCHI '22)*. NordiCHI '22. Association for Computing Machinery, 2022. DOI: 10.1145/10.1145/3546155.3546700 (cited on pp. x, xi, 2, 6, 8–11, 17, 26, 27, 29, 31, 34, A 1).

[P7] Michael Froehlich, Benjamin Moser, Florian Alt, and Albrecht Schmidt. "Supporting Interface Experimentation for Blockchain Applications". In: *Adjunct Proceedings of the 2022 Nordic Human-Computer Interaction Conference (NordiCHI Adjunct '22)*. NordiCHI Adjunct '22. Association for Computing Machinery, 2022. DOI: 10.1145/10.1145/3547522.3547676 (cited on pp. x, xi, 2, 6, 8–11, 17, 24, 27, 29, 31–33, A 1).

[P8] Michael Froehlich, Jose Vega, Amelie Pahl, Sergej Lotz, Florian Alt, Albrecht Schmidt, and Isabell Welpe. "Prototyping With Blockchain: A Case Study For Teaching Blockchain Application Development at University". In: *Learning in the Age of Digital and Green Transition - Proceedings of the 25th International Conference on Interactive Collaborative Learning (ICL2022)*. Springer International Publishing, 2022, p. 12 (cited on pp. x, xi, 2, 6, 9–11, 17, 24, 27–29, 31, 33, 35, A 1).

1.3 Dissertation Structure

The chapters in this dissertation are structured as follows. Chapter 1 begins by presenting the overall motivation for and relevance of the conducted research. It provides an overview of the included publications, the theoretical framework underlying the conducted studies, and presents our overall research approach. Chapter 2 details how the three guiding research questions for this dissertation were chosen, how they connect with each other and existing research. Chapter 3 briefly summarizes each of the included publications. Accompanied by a preview of the first page we explain the motivation,

approach, and findings under the larger umbrella of this dissertation and delineate the contribution of each individual author. Finally, Chapter 4 discusses the collective results of this dissertation. It provides a synthesis of the combined findings by discussing where cryptocurrency systems today fall short and what design implications arise from that. It reflects on the larger contribution of this dissertation in the context of the development of cryptocurrency technology over the past years and speculates about avenues for future work.

1.4 Theoretical Framework

Understanding which aspects influence the adoption of new information technologies is a central theme in Human-Computer Interaction research [60]. The Technology Acceptance Model (TAM) is often adopted as the theoretical framework through which to do so [31, 32]. Originally developed by Fred D. Davis in 1985 to empirically test the acceptance of end-user facing information systems [31], the model has since found widespread application in research [60, 93]. In the following, it lends itself as a valuable tool through which to examine the adoption of cryptocurrency technology and connect the contributions of the presented publications.

At its core, the Technology Acceptance Model suggests that two cognitive processes are crucial for users to form the intention to use a technology: their *perceived usefulness* and their *perceived ease-of-use*. The more useful and easy-to-use people perceive a technology, the more likely they are to form the intention to use it and eventually do so [31, 32]. More importantly, the model suggests that the manipulation of any external variables influences the intention to use only indirectly. Consequently, to accelerate the adoption of a technology one would need to increase the perceived usefulness and ease-of-use by manipulating relevant external variables [33]. Figure 1.1 illustrates this conceptual relationship.

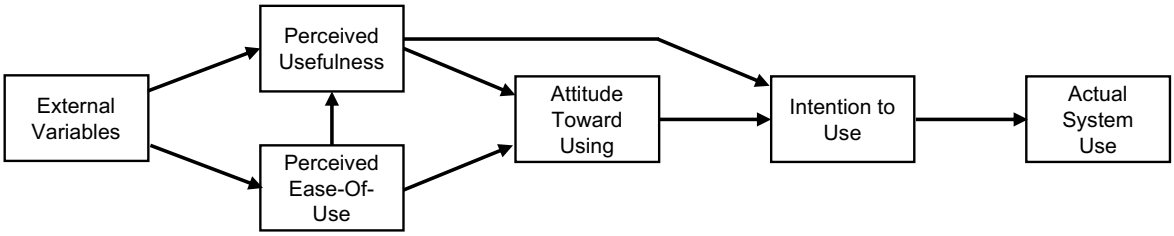


Figure 1.1: The original Technology Acceptance Model (TAM). (Figure adapted from [33], p. 4)

The original TAM does not elaborate which specific variables antecede perceived usefulness and perceived ease-of-use. As a consequence many studies have since evaluated and proposed different external variables [60, 93]. The most relevant extension regarding this dissertation, was the integration of *perceived risk* as equal antecedent to users' intention in the context of distributed e-commerce by Pavlou in 2003 [109], which has since found widespread adoption in research concerning the web [48]. While from today's perspective the comparison to e-commerce may seem far-fetched, the addition of perceived risk is motivated by "*the implicit uncertainty of the e-commerce environment*" ([109], p. 1). Information systems and Human-Computer Interaction research on cryptocurrencies reveal a similar uncertain environment [120, 121] and argue for the importance of perceived risk when

reasoning about cryptocurrencies [1, 48]. Hence, following this theoretical framework three variables are crucial to examine why users adopt cryptocurrency: perceived risk, perceived usefulness, and perceived ease-of-use.

Perceived Risk: Cryptocurrencies deal directly with monetary value. Security is therefore a necessary feature to avoid unauthorized access. Thus, cryptocurrency systems can only be usable in the long term if they provide the necessary security to mitigate risks that may otherwise lead to direct loss. As a consequence, it is to be expected that the more risks users perceive, the lower their intention to use the technology [48, 79, 109]. From research on usable security [5, 83] we know that building secure systems has implications on their usability and vice versa. For security features to be successful they need to be usable to the extent that users can routinely and automatically apply them [5, 119]. In other words, security and usability are dependent aspects of digital technologies. While security is of importance in the long term, security features often stand in the way of what users want to achieve in the moment [28]. For example, improving the security of cryptocurrency systems might decrease perceived risk, but at the same time also decrease the perceived ease-of-use. When interacting with cryptocurrencies in practice, users need to balance these competing objectives. Security features that are deployed without the appropriate understanding of how their users resolve the tensions between perceived risk and ease-of-use may therefore be ignored or circumvented by users in practice [44, 83]. Consequently, it is important to understand which risks exist surrounding the use of the technology, how users deal with security in practice, and which design challenges for building usable cryptocurrency systems arise from this.

Perceived Ease-Of-Use: The current lack of perceived usability documented in literature (e.g. [3, 62, 99, 147, 148]) indicates that the design of usable cryptocurrency applications is not well understood. This is problematic for several reasons: As the Technology Acceptance Model [31, 32] suggests, it may slow down adoption at large, potentially in areas where the technology could bring forward applications that are an improvement over existing solutions. While cryptocurrencies are not without problems today, this dissertation builds on the assumption that cryptocurrency technology will be beneficial for society in the long run. A high technical entry barrier can block users with low technology affinity from benefiting from participating and ultimately hinder inclusion. As documented incidents from other domains show, poor design can also directly cause errors that results in substantial damage [115]. With cryptocurrencies the potential negative impact of even minor user interface issues can be significant as it may lead to the direct loss of monetary value. Therefore it is crucial to directly investigate where the usability of cryptocurrency systems today falls short and what implications for design and research arise from that.

Perceived Usefulness: The Technology Acceptance Model emphasizes that ease-of-use alone is not sufficient to understand user adoption. A technology additionally needs to be perceived as useful [31, 32]. In simple words, it is necessary to understand the motivation of users to interact with cryptocurrencies and juxtapose it with whether using the systems lives up their expectations. Literature emphasizes that cryptocurrency systems should provide a genuine benefit over systems without blockchain technology [56] to be perceived as useful. However, this is where many applications fall short [137] as practitioners appear to struggle to answer the question for which use cases this is the case [85, 157]. To build not only usable but also useful cryptocurrency applications, it is therefore necessary to look beyond the end-user to the developer of cryptocurrency systems [48].

1.5 Research Approach

Grounded in the theoretical foundation of the Technology Acceptance Model, we summarize our overall research approach. The contributing publications can be structured along two dimensions: their thematic focus and their methodological approach. Figure 1.2 illustrates the relationship between publications.

Thematic Organization

The thematic axis organizes the contributing publications along the anteceding variables discussed in our theoretical framework. The primary focus of [P1] and [P2] lies in understanding **Security Practices** of users. By organizing the risks cryptocurrency users perceive and integrating them into a conceptual model in [P1] we directly contribute to the *perceived risk* variable. Motivated by these findings, [P2] systematically organizes the threat landscape from which these risks emerge.

The primary focus of [P3, P4] and [P6] lies on the **Usability** of cryptocurrency systems, directly relating to the *perceived ease-of-use* variable. [P1] identified a research gap in understanding novice users and motivated our work in [P3] focusing on challenges of first-time users. In [P4] we continue this work by exploring the design of onboarding as potential solution to increase the usability during initial use. [P6] then explores the usability of cryptocurrencies as means-of-payment at the example of Bitcoin Lightning. The motivation for this study originated from several sources: In [P1] users expressed interest in using cryptocurrency as payment more often. In [P3] slow transactions and high fees emerged as limiting factors for usability. Bitcoin Lightning claimed to address these issues, yet previous research had not explored newer cryptocurrencies and evaluated these claims [P5].

The primary focus of [P5, P7] and [P8] shifts the focus on **Developer Support**. In a systematic literature review [P5] summarizes and organizes the field for researchers and practitioners. Motivated by the lack of studies prototyping with cryptocurrencies other than Bitcoin and Ethereum, [P7] reasons that lowering the deverlopers' effort to experiment with different blockchains may increase usability in the future. Finally, [P8] consolidates the insights generated throughout this dissertation in an interdisciplinary university course aimed at teaching how to build both usable and useful applications, thus addressing the *perceived usefulness* variable.

Methodological Organization

The methodological axis comprises three categories: understanding the current **State of Research**, **Empirical** studies, and **Constructive** approaches. With a systematic literature review we attempt to capture and organize the existing research body on cryptocurrency and blockchain research in Human-Computer Interaction [P5]. The second methodological theme concerns creating a better understanding of *how users interact with cryptocurrency systems* and the arising implications thereof. The publications that fall under this theme [P1, P2, P3, P5] aim at creating generalizable knowledge about how cryptocurrencies are being used in practice. The third methodological theme concerns the exploration of solutions *to improve the usability of cryptocurrency systems* through prototyping, implementation, and evaluation. The publications that fall under this theme [P4, P6, P7, P8] produce original artifacts, test, and evaluate them. Although some of the projects underlying these publications were conceived in a non-linear and iterative way, to some degree, these themes can be viewed as subsequent steps in our research process. Earlier empirical work influenced and inspired the later development of artifacts.

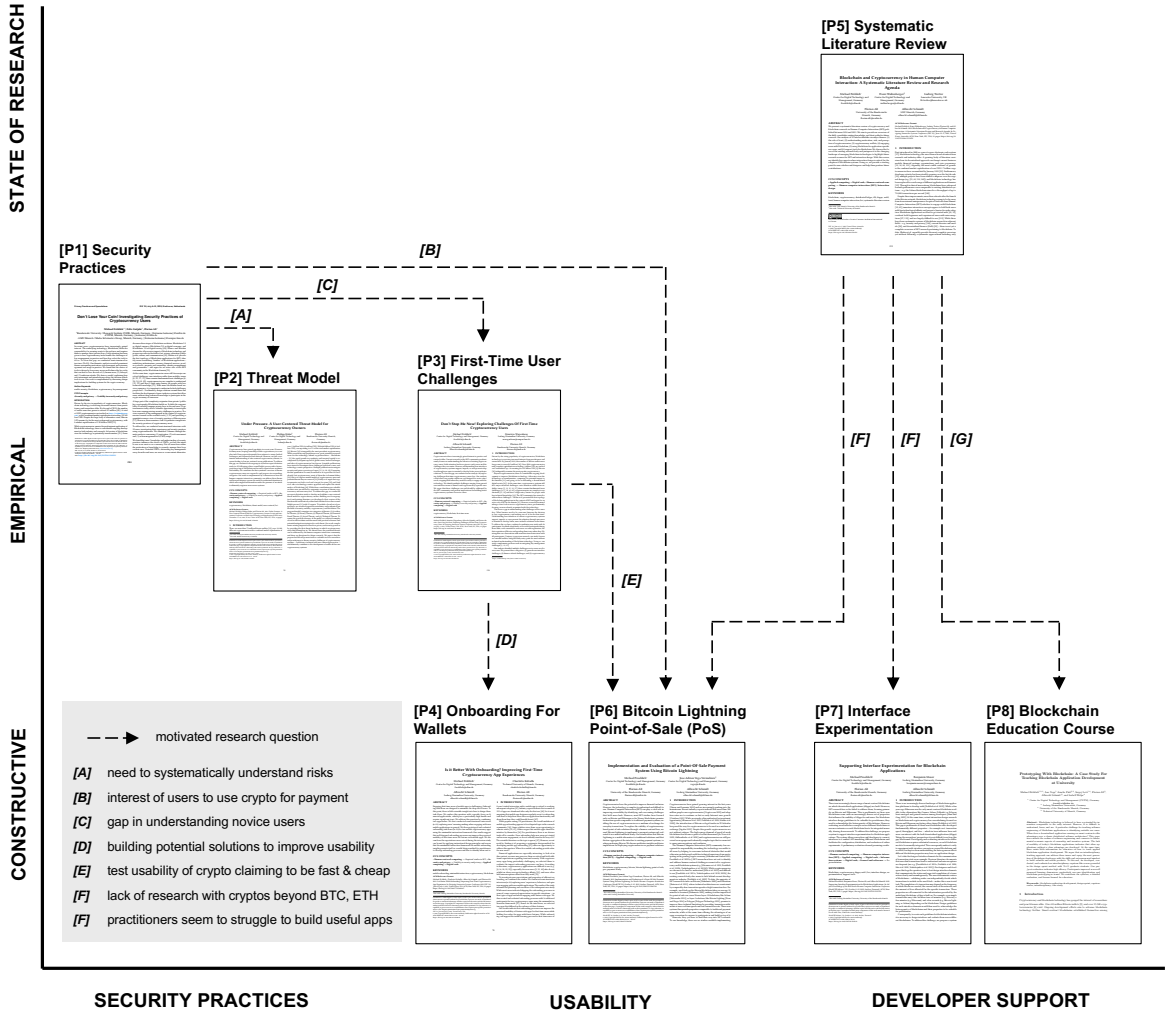


Figure 1.2: Methodological and thematic relationships between the contributing publications.

Research Methods

We employed a variety of research methods. The following section aims to provide an overview and brief rationale of the used methods. All studies contributing to this dissertation where conducted between 2019 and 2022. As a consequence of the global COVID-19 pandemic during this period, some of the studies and interviews were conducted virtually or used out-of-the-lab approaches to collect data [4]. We focused primarily on qualitative methods to understand what problems manifest themselves, explore their underlying causes, and prototype solutions.

Systematic Literature Review: All included publications are embedded in existing research through literature analyses. In [P5] our objective was to capture all relevant literature at the time of writing in a systematic and repeatable way. We were motivated to do so, since both practice and research on cryptocurrency had accelerated in recent years and believed that a well-written overview article could organize the field and help spark new research. Therefore, we followed the PRISMA framework [98] to identify relevant publications and qualitatively analyzed and summarize them.

Semi-Structured Interviews: We used semi-structured interviews as the primary method of data collection in [P1]. With [P1] our goal was deepen the understanding of how user interact with cryptocurrencies in practice. Therefore, we chose semi-structured interviews as they allowed us to investigate the phenomenon in depth while maintaining a balance between structure and flexibility [77]. The explorative character of the study revealed multiple new insights and motivated several of the subsequent studies. In addition, we also used interviews in combination with other methods to triangulate [111] the investigated phenomena in [P3, P4, P6].

Delphi Panel: [P1] revealed how perceived risks influence the behavior of cryptocurrency users. Building on these results, we wanted to build a comprehensive understanding of the threat landscape from which these perceived risks emerged. In a fast evolving space, we therefore selected an expert elicitation study as the appropriate method. The Delphi method [30] is well established in social sciences to lead a structured discussion with a panel of experts. In [P1] we used it in a three-round process with a heterogeneous panel of blockchain and security experts to develop and validate the model. Feedback during each round of the process was collected with questionnaires.

Focus Groups: All studies contributing to this theses were preceded by informal discussions with relevant stakeholders. For [P2] we conducted a formal focus group to discuss the initial idea of the threat model. We decided for a focus group, because we wanted observe whether a discussion between experts from different fields on the topic could lead to fruitful outcomes. The results from the focus groups strengthened the idea that the Delphi method would work.

Lab Studies: To understand the challenges of first-time users [P3] and evaluate the efficacy of onboarding to increase usability during initial use [P4] we conducted lab studies [77]. What is noteworthy about both studies is that they were conducted remotely [4] during the height of the COVID-19 pandemic. To collect data we provided detailed briefings to participants and utilized screen-recording features on mobile and desktop devices while participants used the *think-aloud* technique to share their thoughts [77]. In [P3] we additionally used the recordings to elicit further qualitative insights in interviews with participants after the tasks were completed. To ensure the generalizability of our observations, we included multiple wallets in both studies.

Field Studies: In [P6] we deployed the developed point-of-sale (PoS) system in an office-like setting at university and evaluated it in a field study. From previous studies we knew that users voiced their interest in using cryptocurrency not just as store of value, but also as a means of transaction. However, the limited availability of merchants accepting cryptocurrencies restricted options to conduct a study in the wild. By developing a point-of-sale system, we could deploy self-service terminals where participants could make purchases and observe users' behavior over several weeks. The data collecting during the field study comprised several mixed methods, including *think-aloud* data collection with recorded videos, *contextual inquiry*, *observations*, *weekly questionnaires* and *log analysis* [77].

Online Studies: In [P7] we evaluated the proposed approach in an online experiment on Amazons' Mechanical Turk platform. The goal of the study was to demonstrate the feasibility of running experiments with variable interface elements on the prototyped system. We therefore did not collect qualitative data, instead focusing on simulating how developers would be able to run an experiment on the developed platform. Participants were provided with task descriptions directly within the prototype. Data was collected with *questionnaires* before and after the tasks and via *log analysis* [77].

Prototyping and Artifacts: We contribute several artifacts. In [P4] we developed an interface prototype, which allowed us to quickly explore different approaches and improve the interface in several

iterations. In [P6] and [P7] we developed functional systems to deploy and test them under realistic conditions. [P6] comprised several components, with a mobile wallet constituting the core development effort whereas the prototype developed in [P7] was a web-based application. As consequence of the functional implementation of both prototypes, we could complement their evaluation with the collection of *log-data*.

Course Design: In [P8] we use the Design Sprint [69] as theoretical foundation to design a university course for usable and useful blockchain application development. While not directly situated within the typical contributions found in Human-Computer Interaction research, this project was motivated by insights from several studies [P2, P3, P5] all indicating that education about blockchain applications will be necessary to reduce existing misconceptions. By putting our focus on the next generation of developers and empowering them to identify useful use cases with user-centered methods, we hope to create compounding effects that eventually lead to better applications in the future.

Questionnaires: All studies were accompanied by questionnaires collecting structured data on demographics and, in some cases, additional qualitative information. For the pre/post evaluation of [P8] questionnaires were the primary method of data collection. We used several validated scales throughout our studies, including the Affinity of Technology Interaction scale (ATI) [8, 51], the User Experience Questionnaire (UEQ) [76], the System Usability Scale (SUS) [15], and blockchain specific items adapted from Abramova et al. [1].

Research Contribution

The publications included in this dissertation each contribute to the scientific conversation surrounding the usability of cryptocurrency systems. A recent essay by Oulasvirta and Hornbæk distinguishes Human-Computer Interaction problems into three subtypes: *empirical*, *conceptual*, and *constructive* [107]. The chronologically earlier publications in this dissertation contribute largely to the empirical side. Their contribution is "*aimed at creating or elaborating descriptions of real-world phenomena related to human use of computing.*" ([107], p. 3). The chronologically later publications shift their contribution increasingly to the constructive side. Their contribution is "*aimed at producing understanding about the construction of an interactive artifact for some purpose in human use of computing*" ([107], p. 3). Table 1.1 details the contributions of the included publications.

This dissertation's contributions can be organized along three research questions following the methodological axis. The individual questions will be developed in Chapter 2 in more detail.

With guidance of **RQ1** – "*What is the current state of blockchain and cryptocurrency research in the Human-Computer-Interaction domain?*" – this dissertation contributes an extensive analysis of the state of research through a systematic literature review. Based on the analysis of 99 publications identified from ACM, IEEE, and Springer we consolidate the existing research body into six common themes. The review serves as an overview of the current state of research for researchers and practitioners. In addition, it discusses current research gaps and proposes future research directions.

With guidance of **RQ2** – "*How do users interact with cryptocurrency systems and what implications arise from that?*" – this dissertation contributes new insights into the behavior of cryptocurrency users in practice. Based on the results of three empirical studies, we shed light on the challenges first-time users encounter [P3], the threat landscape they face [P2], and the security and privacy practices they deploy [P1]. From these observations we derive and contribute design implications for practitioners and research implications for open issues.

With guidance of **RQ3** – "*How can we build with and for cryptocurrency?*" – this dissertation contributes three prototypes of cryptocurrency systems and one approach to teaching applied blockchain application development. [P4] contributes and evaluates an interface prototype testing the efficacy of onboarding to improve perceived usability of wallets under different conditions. [P6] and [P7] present functional systems that build with and for cryptocurrency. After understanding the current state of research, conducting own inquiries into cryptocurrency use in practice, and building systems ourselves, [P8] consolidates and translates these findings into a university course teaching students how to build usable and useful cryptocurrency and blockchain applications.

Synopsis

In combination these studies have advanced the research conversation on usable cryptocurrency systems over the past years. We provide a synopsis of the cumulative findings of all publications below. A more detailed version can be found in Chapter 4.

Cryptocurrency user differ along the motivation to engage with cryptocurrency and their knowledge and motivation to deploy security measures [P1, 1]. Misconceptions are common among both experienced and inexperienced users [P1, P3], which exposes them to a range of threats exploiting these misconceptions [P2]. While key management is a challenge for most users [P1, 41], the broad range of usability issues originates only in parts from the underlying blockchain technology [P3, 148]. Current systems fall short for several other reasons: They overwhelm users with many new concepts at once and do not support their learning process [P3, P4, 56]. Getting started is further aggravated as many usability issues originate at the edge of established systems [P3, P6]. During use, free-market dynamics have resulted in general properties – e.g. volatility, uncertain and long transactions times, and expensive transaction fees – that make cryptocurrencies ill-suited for their original purpose as "*internet money*" [P3, P6]. As a result many users, within our European study context, do not see how cryptocurrencies offer a clear benefit over existing means of payment [P6].

From these results, several design implications for practitioners arise: With many usability issues not connected to the underlying technology, existing heuristics and human-centered methods are effective tools to build more usable cryptocurrency systems [P3, P8], which practitioner should make use of. They should understand their users and build their applications with a clear target group [P1] and use-case in mind to provide a clear benefit [P1, P8]. In building their applications they should aim to understand the learning process of their users and help them progress through it [P4, P5]. Beyond these design implications the research conducted over the course of this dissertation also showed that not all of the current issues can be solved with interface and interaction concepts. Education needs to be part of the solution to reduce misconceptions of users [P2, 141] and, in conjunction with the right support tools, to enable developers to build better products [P7, P8].

This dissertations also shows that Human-Computer Interaction research on cryptocurrencies still trails the developments in practice [P5]. This does not diminish the relevance of existing research, but highlights its importance. As practitioners bring forward many new concepts at an impressive rate, the Human-Computer Interaction community can provide tremendous value by clearing the fog and understanding which approaches work under which conditions. By doing so, future research may work towards a set of cryptocurrency specific guidelines that helps practitioners consistently solve many of the reoccurring questions [P2, P5]. To achieve this research on cryptocurrencies needs to move beyond the lab [P6], extend research on emerging cryptocurrencies [P5, P6, P7], and deepen the understanding of user groups and how the balance their needs [P1, P5].

Table 1.1: Overview of publications organized by research question, methods, and contribution type.

	Research Question	Methods	Contribution		
			Empirical	*Conceptual*	*Constructive*
RQ1: What is the current state of blockchain and cryptocurrency research in the Human-Computer-Interaction domain?					
[P5]	What is the state of blockchain and cryptocurrency research in the HCI?	• systematic literature review identifying 99 publications between 2014 and 2021	• organization of the current research body of blockchain in HCI	• synthesis of research gaps and future research avenues	–
RQ2: How do users interact with cryptocurrency systems and what implications arise from that?					
[P1]	What are security and privacy practices of established cryptocurrency users?	• semi-structured interviews (N=10) • thematic analysis	• qualitative accounts of cryptocurrency users' security practices	• a conceptual model integrating risk assessment, intended usage, and users' tool choice	• synthesis of design implications
[P2]	Which threats do cryptocurrency owners face and how can they be addressed?	• focus group (N=6) • delphi panel (N=25)	• systematic account of cryptocurrency threats	• a model organizing threats into six categories	–
[P3]	What challenges do first-time cryptocurrency users face?	• think-aloud study (N=34) • thematic analysis	• qualitative accounts how first-time users interact with cryptocurrencies	• classification of challenges of first-time cryptocurrency users	• synthesis of design implications
RQ3: How can the design of usable cryptocurrency applications be supported?					
[P4]	How can we support first-time users during their initial interaction with cryptocurrency apps?	• semi-structured interviews (N=16) • iterative interface development (N=16)	• analysis of users behavior and opinions on mobile onboarding • evaluation of onboarding protoypes	• discussion in which cases onboarding is beneficial	• implementation of onboarding prototypes for two mobile wallets
[P6]	How can cryptocurrency be used for everday payments?	• prototyping/ implementation • two-week long mixed-methods study (N=31)	• evaluation of system	• reference implementation and system architecture for cryptocurrency PoS system	• implementation of a Bitcoin Lightning PoS system
[P7]	How can we facilitate the development of usable cryptocurrency applications?	• prototyping/ implementation • online experiment (N=160)	• evaluation of developed system with a quantitative online experiment on mTurk	• proposition of a new method to evaluate blockchain interfaces	• implementation of a rapid experimentation system for cryptocurrency interfaces
[P8]	How can usable blockchain application development be taught at university?	• development of new course format • pre/post assessment of learning outcomes (N=11)	• evaluation educational impact of the course	• course curriculum • discussion of lessons-learned	• design of an interdisciplinary course for teaching blockchain application development

Notes: The contribution types follow Laudan's taxonomy [75] adapted for HCI by Oulasvirta and Hornbæk [107]. Publications are listed in order of presentation in this dissertation. The publications at the top focus on understanding user behavior and challenges. The publications towards the bottom of the table shift their focus increasingly towards building and testing constructive approaches.

2
Guiding Research Questions

The Web took off in all its glory because it was a royalty-free infrastructure . . . When I invented the Web, I didn't have to ask anyone's permission. Now, hundreds of millions of people are using it freely.

Sir Tim Berners-Lee, Web Foundation, 2017

After presenting the overall structure of this dissertation, this chapter develops the guiding research questions to which each of the included publications contribute.

2.1 Cryptocurrency and Human-Computer Interaction

Bitcoin was first introduced in 2008 in a whitepaper titled "*Bitcoin: A Peer-to-Peer Electronic Cash System*" [101]. Since then many new cryptocurrencies have been introduced to the market, developer activity has been steadily growing [35, 124], and new projects were started to improve the technical architecture underlying different cryptocurrencies and to serve different uses cases (e.g. [17, 67, 154, 158]). As of 2022, some of these new state-of-the-art blockchains claim to have a similar performance as existing distributed payment systems. For example, the Solana blockchain aims to reach a throughput of up to 710,000 transactions per second [158]. For comparison, Visa reported to have the capacity to manage up to 65,000 transactions per second in 2018 [145]. As a consequence of the evolving underlying blockchain technology, cryptocurrencies seem to have started to outgrow their original purpose as digital money. New use cases have started to emerge on top of the smart-contract infrastructure and gain traction: Decentralized finance (DeFi) [95], Decentralized Autonomous Organizations (DAOs) [150], and Non-Fungible Tokens (NFTs) [149] appear to be drawing in entirely new groups of users.

This decade characterized by fast-paced innovation raises the question how research has advanced at the same time. Taking a look at Human-Computer Interaction research seems particularly interesting given that cryptocurrencies have gained a reputation of being hard to use [56, 147, 148]. Both research [20, 99, 147] and practice [50, 57, 84] stress poor interaction concepts and bad usability to be major barriers for wider adoption. While scholars have called for the active engagement of the HCI community with cryptocurrency and blockchain in the past [39, 49], there has not been an effort to systematically consolidate the produced research findings.

While systematic literature reviews about cryptocurrency and blockchain have been published in adjacent fields – for example, in decentralized finance (DeFi) [95], current theories and models [61], and security and privacy [160] – there has not been an article organizing the collective research on cryptocurrency and blockchain in Human-Computer Interaction. Preceding the publication of [P5], the most complete overview of literature can be found in Elsden et al.'s article "*Making Sense of Blockchain Applications: A Typology for HCI*" [39]. Their paper focuses on the construction of a typology of blockchain applications considering application domains and distinguishing features.

However, their literature analysis does not follow a systematic process and included only literature up to 2018. In a field evolving at a rapid pace, we thus see the need for a systematic review of the Human-Computer Interaction literature to understand the past, present, and future of the field.

The first research question we pose is:

Research Question 1

"*What is the current state of blockchain and cryptocurrency research in the Human-Computer-Interaction domain?*"

2.2 Understanding User Behavior in Practice

As new technologies emerge, they are usually accompanied by novel design challenges. While they solve one problem, they also create other ones in different areas. Empirical research in Human-Computer Interaction [107, 153] aims to produce insight into the nature of problems that exist when users interact with new technologies. In HCI empirical contributions typically aim to either generate knowledge on how people use a system or about the people themselves [153].

Generating a research body of empirical knowledge about who interacts how with a new technology and which problems they encounter along the way is important for several reasons: Emerging technologies are often based on new design paradigms. How the technology actually works likely diverges from the mental model users have [18]. Designing user interfaces for new technologies also confronts designers with challenges that have not been solved previously. Poorly designed interfaces can lead to unexpected problems and, at the extreme, even contribute to catastrophic events [115]. The first step to avoid this and create the preconditions for building great user interfaces is thus to investigate and organize the design challenges that exist.

Cryptocurrencies are a relatively recent technology. While ideas about digital money have been discussed since the 1980s [22, 89, 91], cryptocurrencies have been around in their current form for just a little more than ten years [101]. Understanding who uses cryptocurrencies for what reasons, what works, and what does not through a human-centered lens is particularly important. Any mistake can ultimately lead to direct loss of monetary value and thus even minor problems can have substantial negative consequences for users.

From practitioner reports and the emerging research body we know that cryptocurrencies are perceived as hard to use (see e.g. [1, 73, 90, 147]). Accounts of lost [16, 73, 155] or stolen [58, 72, 73] cryptocurrencies are frequently reported news. There is an emerging body of research in Human-Computer Interaction that has started to explore how people use cryptocurrency in practice. Common themes surround the socio-technical role of trust in an arguably trustless system (e.g. [27, 70, 71, 120, 121, 146]), users' motivation, risk, and perception (e.g. [1, 54, 68, 73, 90, 146, 147]) as well as the usability of cryptocurrency wallets (e.g. [3, 56, 63, 65, 99, 148]).

However, there are still significant gaps in understanding how people use cryptocurrencies in practice. While first studies explored this question at a quantitative level [14, 73], deep understanding of typical problems and their causes are sparse and research attempting to fill this gap has only recently started to emerge [1, 148]. While threats are frequently mentioned in the public media, we know little

about the the context in which they occur and how they might be addressed. Given the sensitive nature of cryptocurrencies, users may hold additional expectations regarding trust and security. We also miss knowledge on how users balance the tensions arising from competing needs for usability, security, and privacy. In other words, we do not know enough about how people use cryptocurrency in practice and what problems they encounter while doing so. With Human-Computer Interaction being uniquely positioned to investigate and describe the real-world phenomena related to human use of cryptocurrencies, our second research question is:

Research Question 2
"*How do users interact with cryptocurrency systems and what implications arise from that?*"

2.3 Building Usable Cryptocurrency Applications

The human-centered design process [105] recognizes four essential steps to building products connected in a cyclic relationship: Idea Generation, Prototyping, Testing, and Observation.

Typically, new technologies have originated from controlled research environments, often universities, where idea generation, prototyping, and testing precede observations in the field. The maybe most prominent example following this path is the development of the Internet: Original ideas about a global communication network emerged at MIT in the early 1960s. The first concept for a computer network, ARPANET, was published in 1967. Funded by DARPA the development of ARPANET resulted in the first two computers being connected in 1969 between UCLA and Stanford university. The development of ARPANET continued for another two decades, driven by research, before the commercialization of the technology started in the late 1980s and public use of the internet as we know it today emerged [82].

In contrast, cryptocurrency technology follows a very different path. With the publication of the Bitcoin whitepaper in 2008 [101] the technology was released directly to the world and has been used in practice since then [103]. The development of the field until now has arguably been driven more by practice than by research. It was the growing usage in practice that then motivated scientific research to take interest in the phenomenon. Across different research communities, bibliometric analyses trace the first scientific publications back to as early as 2012 [94] with an increase in the number of publications after 2017 [47, 102, 129]. Research in Human-Computer Interaction has been published only from 2014 onwards [P5].

Given the availability of a real-world phenomenon to observe, most research on cryptocurrencies in our domain has so far been of empirical nature [P5]. For example, Sas and Khairuddin qualitatively explore trust and motivations of Bitcoin users [68, 120, 121], Abramova et al. shed light on different types of user groups based on their risk perception [1], and Voskobojnikov et al. investigate the user experience of cryptocurrency wallets [148]. Similarly, our own publications explore security and privacy [P1, P2] and challenges of first-time users [P3] from a user-centered perspective. These empirical studies contribute to a better understanding of the phenomena surrounding the technology. From their observations they often derive design implications or recommendations for various actors and use-cases. For example, Sas and Khairuddin argue for tools to support *Two-way Transactions*, *Reversible Transactions*, and *Materializing Trust* [120]. Abramova et al. argue for *different*

types of user profiles and *personalization* to better serve the needs of a heterogeneous user base [1]. Voskobojnikov et al. recommend that developers should *Mimic Existing Payment Systems*, *Allow Wallet Personalization*, and *Improve Users' Understanding of Cryptocurrencies* to increase the user experience of wallets [148].

While these recommendations grounded in observations of existing systems are a valuable starting point, we also need research actively designing, building, and evaluating prototypes to close the loop. At the moment, there remains a gap in studies using constructive approaches to build and evaluate cryptocurrency applications. While prototypes integrating blockchain to solve specific use cases have been published – e.g. conditional giving [138, 139], location-aware services [134, 135], or energy trading [36, 123] – there are hardly any artifact contributions for cryptocurreny in HCI (for a detailed discussion please refer to [P5]).

Without implementing the recommendations brought forward by empirical research and putting them to the test we therefore lack an essential part of the human-centered design process [105]. This leaves a gap in understanding the context under which these recommendations are useful and which trade-offs need to be considered when attempting to build usable cryptocurrency applications. Therefore, our third research question is:

Research Question 3
"*How can we build with and for cryptocurrency?*"

3
Publications

On the Internet, it's survival of the easiest. Give users a good experience and they're apt to turn into frequent and loyal customers. But it's easy to turn to another supplier in the face of even a minor hiccup. Only if a site is extremely easy to use will anybody bother staying around.

Jakob Nielsen

After developing the guiding research questions for this thesis, the following chapter outlines the individual contributing publications. All publications are summarized, accompanied by a preview of the first page, and a clarification of my personal contribution. The publications are ordered by the overarching research questions they aim to address. Table 3.1 provides an overview.

Table 3.1: Overview of publications contributing to this dissertation, used methods, and key outcomes.

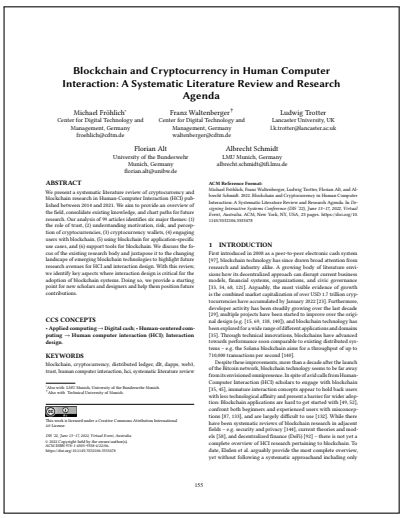
	Publication Title and Publishing Venue	Type	Method(s)	Key Outcome
A Review of Cryptocurrency Research in Human-Computer Interaction				
[P5]	"Blockchain and Cryptocurrency in Human Computer Interaction: A Systematic Literature Review and Research Agenda" in *DIS '22*	Full Paper (23 pages)	Systematic Literature Review (N=99)	Summary of extant literature, addressed research questions, and a discussion of promising future research avenues
Empirical Studies Exploring User Behavior				
[P1]	"Don't lose your coin! Investigating Security Practices of Cryptocurrency Users" in *DIS '20*	Full Paper (13 pages)	Semi-Structured Interviews (N=10), Thematic Analysis	Insight into user behavior, key risks that can lead to loss, a conceptual model how users balance these risks
[P2]	"Under Pressure. A User-Centered Threat Model for Cryptocurrency Owners" in *ICBTA '21*	Full Paper (12 pages)	Focus Group (N=6), Delphi Study (N=25)	A model providing an overview of user-centered threats and mitigation strategies
[P3]	"Don't Stop Me Now! Exploring Challenges Of First-Time Cryptocurrency Users" in *DIS '21*	Full Paper (11 pages)	Think-Aloud Study, Interviews, and Observation (N=34)	Challenges of first-time cryptocurrency users, and design implications for research and practice
Constructive Approaches Improving Application Usability				
[P4]	"Is It Better With Onboarding? Improving First-Time Cryptocurrency App Experiences" in *DIS '21*	Full Paper (12 pages)	Interview (N=16), Prototype Design and Evaluation (N=16)	Insight into how and when onboarding can improve the usability of cryptocurrency mobile apps
[P6]	"Implementation and Evaluation of a Point-Of-Sale Payment System Using Bitcoin Lightning" in *NordiCHI '22*	Full Paper (12 pages)	Prototype Development and Evaluation (N=31)	Reference implementation of a Bitcoin-Lightning based Point-Of-Sale system
[P7]	"Supporting Interface Experimentation for Blockchain Applications" in *NordiCHI '22*	Extended Abstract (5 pages)	Prototype Development, Experimental Evaluation (N=160)	Implementation of a prototype for conducting blockchain interface experiments
[P8]	"Prototyping with Blockchain: A Case Study For Teaching Blockchain Application Development at University" in *ICL '22*	Full Paper (12 pages)	Course Design and Survey-based Pre/Post Evaluation (N=11)	Insight into how to teach usable blockchain application development, a course syllabus, and evaluation of learning outcomes

3.1 A Review of Cryptocurrency Research in Human-Computer Interaction

Cryptocurrency and Blockchain technology were first introduced in 2008 with the publication of a whitepaper titled "*Bitcoin: A Peer-to-Peer Electronic Cash System*" by pseudonymous author Satoshi Nakamoto [101]. Since then both practice and research have increasingly taken interest in the technology. The objective of [P5] was to analyze the extant research body of cryptocurrency and blockchain studies in the Human-Computer Interaction field, provide an overview of addressed topics and synthesize promising avenues for future research, addressing the following research question:

RQ1: "*What is the current state of blockchain and cryptocurrency research in the Human-Computer-Interaction domain?*"

[P5] Blockchain and Cryptocurrency in Human Computer Interaction: A Systematic Literature Review and Research Agenda


Blockchain and Cryptocurrency in Human Computer Interaction: A Systematic Literature Review and Research Agenda

Michael Fröhlich, Center for Digital Technology and Management, Germany, froehlich@cdtm.de
Franz Waltenberger, Center for Digital Technology and Management, Germany, waltenberger@cdtm.de
Ludwig Trotter, Lancaster University, UK, l.k.trotter@lancaster.ac.uk
Florian Alt, University of the Bundeswehr Munich, Germany, florian.alt@unibw.de
Albrecht Schmidt, LMU Munich, Germany, albrecht.schmidt@ifi.lmu.de

ABSTRACT

We present a systematic literature review of cryptocurrency and blockchain research in Human-Computer Interaction (HCI) published between 2014 and 2021. We aim to provide an overview of the field, consolidate existing knowledge, and chart paths for future research. Our analysis of 99 articles identifies six major themes: (1) the role of trust, (2) understanding motivation, risk, and perception of cryptocurrencies, (3) cryptocurrency wallets, (4) engaging users with blockchain, (5) using blockchain for application-specific use cases, and (6) support tools for blockchain. We discuss the focus of the existing research body and juxtapose it to the changing landscape of emerging blockchain technologies to highlight future research avenues for HCI and interaction design. With this review, we identify key aspects where interaction design is critical for the adoption of blockchain systems. Doing so, we provide a starting point for new scholars and designers and help them position future contributions.

CCS CONCEPTS

• Applied computing → Digital cash. • Human-centered computing → Human computer interaction (HCI). Interaction design.

KEYWORDS

blockchain, cryptocurrency, distributed ledger, dlt, dapps, web3, trust, human computer interaction, hci, systematic literature review

ACM Reference Format:

1 INTRODUCTION

155

We conducted a systematic literature review including 99 articles published between 2014 and 2021. Our analysis identifies six major themes that have been addressed by Human-Computer Interaction research: (1) the role of trust, (2) understanding motivation, risk, and perception of cryptocurrencies, (3) cryptocurrency wallets, (4) engaging users with blockchain, (5) using blockchain for application-specific use cases, and (6) support tools for blockchain. Organized by these themes, figure 3.1 provides a visual overview of the Human-Computer Interaction research on cryptocurrency and blockchain that has been published between 2014 and 2021.

By juxtaposing the existing research body with the landscape of emerging blockchain technologies we discuss research avenues for HCI and interaction design moving forward. We identify research to (1) better understand blockchain users, (1) taking an active approach to designing wallets, (3) adopting new blockchains as design material, (4) engaging with web3 and decentralized applications, and (5) exploring digital identity as promising future directions.

Author Contributions: I determined the overall research question and research design together with Ludwig Trotter, Florian Alt, and Albrecht Schmidt. I managed the collection of relevant literature. To automize data collection during the initial keyword-search across all literature databases (ACM, IEEE, Springer) I reused a script written by Benjamin Moser during his Master thesis. I screened all 1413 publications and applied inclusion and exclusion criteria to narrow down the final 99 publications included in the review. I read and analyzed all publications and iteratively coded them along multiple dimensions. I determined the overarching structure of the manuscript. Franz Waltenberger and Ludwig Trotter supported in writing the manuscript and helped create the figures. All authors contributed feedback on the manuscript. I managed the final editing and publication process.

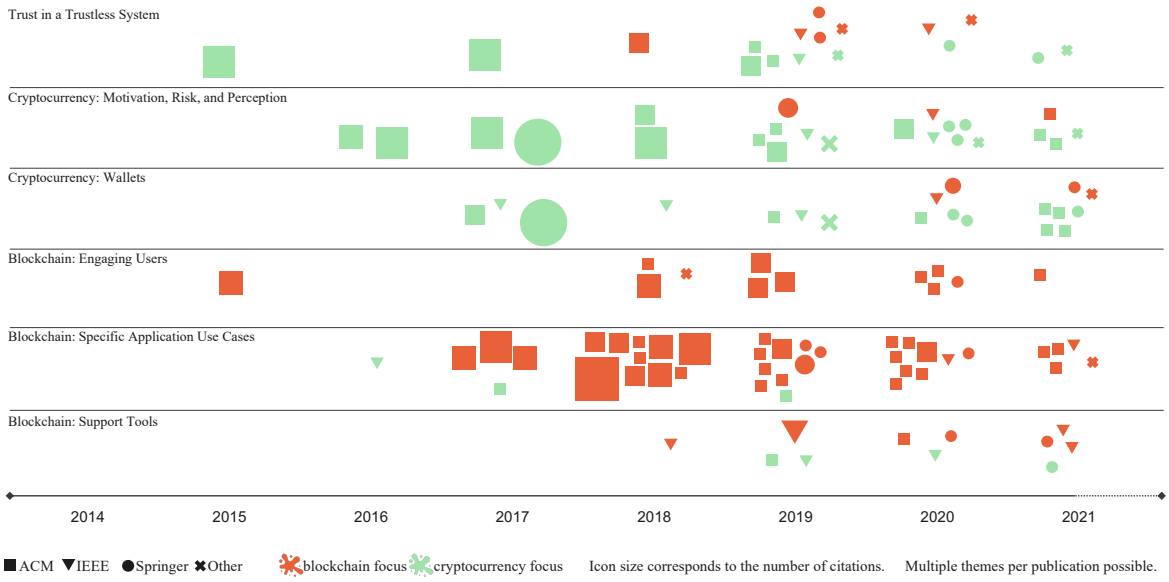


Figure 3.1: Overview of HCI research 2014 – 2021 by theme. (Originally published in [P5], p. 5)

3.2 Empirical Studies Exploring User Behavior

Following our review of the existing body of research, we present three publications aimed to improve our understanding of how users interact with cryptocurrencies in practice. First by looking into security and privacy practices [P1, P2] and then by zooming in on the challenges of new users [P3]. Collectively these publications address the second research question:

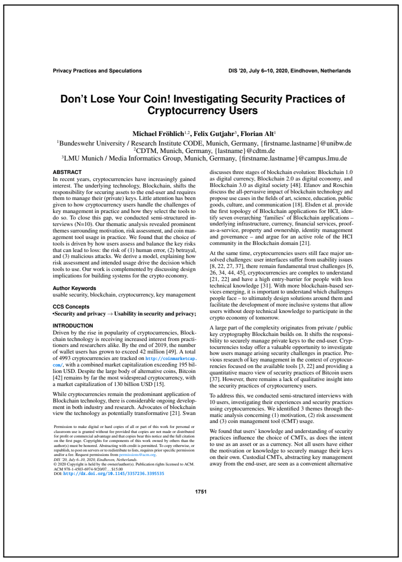
RQ2: "*How do users interact with cryptocurrency and blockchain systems and what implications arise from that?*"

In line with our theoretical framework discussed in Chapter 1, we identified security and privacy as particular relevant factors as they are essential elements of the technology. By focusing on challenges of first-time users we wanted to understand what factors reduce ease-of-use in beginners eyes. In the case of cryptocurrency the initial barrier to enter excludes people with less technical aptitude and we therefore wanted to address this particular gap in current research.

3.2.1 Security and Privacy

Early literature (e.g. [41, 73]) highlights security and privacy as substantial challenges for cryptocurrency users, often relating it back to challenges of key management. We wanted to gain a qualitative understanding of how security and privacy affect users in practice. We designed two studies to address this question. [P1] explores user behavior through deep qualitative interviews. Complementing the data collected directly from users, [P2] elicits security and privacy threats from an expert panel using the Delphi method [30]. Together they address the following research question: "*Which security and privacy challenges do cryptocurrency owners face?*"

[P1] Don't Lose your coin! Investigating Security Practices of Cryptocurrency Users


Privacy Practices and Speculations DIS '20, July 6–10, 2020, Eindhoven, Netherlands

Don't Lose Your Coin! Investigating Security Practices of Cryptocurrency Users

Michael Fröhlich[1,2], Felix Gutjahr[3], Florian Alt[1]
[1]Bundeswehr University / Research Institute CODE, Munich, Germany, {firstname.lastname}@unibw.de
[2]CDTM, Munich, Germany, {lastname}@cdtm.de
[3]LMU Munich / Media Informatics Group, Munich, Germany, {firstname.lastname}@campus.lmu.de

ABSTRACT
In recent years, cryptocurrencies have increasingly gained interest. The underlying technology, Blockchain, shifts the responsibility for securing assets to the end-user and requires them to manage their (private) keys. Little attention has been given to how cryptocurrency users handle the challenges of key management in practice and how they select the tools to do so. To close this gap, we conducted semi-structured interviews (N=10). Our thematic analysis revealed prominent themes surrounding motivation, risk assessment, and coin management tool usage in practice. We found that the choice of tools is driven by how users assess and balance the key risks that can lead to loss: the risk of (1) human error, (2) betrayal, and (3) malicious attacks. We derive a model, explaining how risk assessment and intended usage drive the decision which tools to use. Our work is complemented by discussing design implications for building systems for the crypto economy.

Author Keywords
usable security, blockchain, cryptocurrency, key management

CCS Concepts
•Security and privacy → Usability in security and privacy;

INTRODUCTION
Driven by the rise in popularity of cryptocurrencies, Blockchain technology is receiving increased interest from practitioners and researchers alike. By the end of 2019, the number of wallet users has grown to exceed 42 million [49]. A total of 4993 cryptocurrencies are tracked on http://coinmarketcap.com/, with a combined market capitalization exceeding 195 billion USD. Despite the large body of alternative coins, Bitcoin [42] remains by far the most widespread cryptocurrency, with a market capitalization of 130 billion USD [15].

While cryptocurrencies remain the predominant application of Blockchain technology, there is considerable ongoing development in both industry and research. Advocates of blockchain view the technology as potentially transformative [21]. Swan discusses three stages of blockchain evolution: Blockchain 1.0 as digital currency, Blockchain 2.0 as digital economy, and Blockchain 3.0 as digital society [48]. Efanov and Roschin discuss the all-pervasive impact of blockchain technology and propose use cases in the fields of art, science, education, public goods, culture, and communication [18]. Elsden et al. provide the first topology of Blockchain applications for HCI, identify seven overarching 'families' of Blockchain applications – underlying infrastructure, currency, financial services, proof-as-a-service, property and ownership, identity management and governance – and argue for an active role of the HCI community in the Blockchain domain [21].

At the same time, cryptocurrencies users still face major unsolved challenges: user interfaces suffer from usability issues [8, 22, 27, 37], there remain fundamental trust challenges [6, 26, 34, 44, 45], cryptocurrencies are complex to understand [21, 22] and have a high entry-barrier for people with less technical knowledge [31]. With more blockchain-based services emerging, it is important to understand which challenges people face – to ultimately design solutions around them and facilitate the development of more inclusive systems that allow users without deep technical knowledge to participate in the crypto economy of tomorrow.

A large part of the complexity originates from private / public key cryptography Blockchain builds on. It shifts the responsibility to securely manage private keys to the end-user. Cryptocurrencies today offer a valuable opportunity to investigate how users manage arising security challenges in practice. Previous research of key management in the context of cryptocurrencies focused on the available tools [3, 22] and providing a quantitative macro view of security practices of Bitcoin users [37]. However, there remains a lack of qualitative insight into the security practices of cryptocurrency users.

To address this, we conducted semi-structured interviews with 10 users, investigating their experiences and security practices using cryptocurrencies. We identified 3 themes through thematic analysis concerning (1) motivation, (2) risk assessment and (3) coin management tool (CMT) usage.

We found that users' knowledge and understanding of security practices influence the choice of CMTs, as does the intent to use as an asset or as a currency. Not all users have either the motivation or knowledge to securely manage their keys on their own. Custodial CMTs, abstracting key management away from the end-user, are seen as a convenient alternative

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
DIS '20, July 6–10, 2020, Eindhoven, Netherlands.
© 2020 Copyright is held by the owner/author(s). Publication rights licensed to ACM.
ACM 978-1-4503-6974-9/20/07...$15.00
DOI: http://dx.doi.org/10.1145/3357236.3395535

1751

Summary: Security and usability are often connected aspects of software systems. Our motivation for conducting this study was that previous literature mentioned security and privacy aspects of cryptocurrencies, like key management, as substantial challenges [41]. However, little was known about how users meet these challenges in practice. To close this gap, we conducted semi-structured interviews (N=10) with cryptocurrency users. The thematic analysis of the interviews identified themes surrounding motivation and risk assessment. We found that the choice of tools is driven by how users assess and balance the key risks that can lead to loss: the risk of (1) human error, (2) betrayal, and (3) malicious attacks. We derived a conceptual model, explaining how risk assessment and the intended use cases influence tool choice. We propose that cryptocurrency users are not a homogeneous group of people. Drawing from literature we propose to distinguish cryptocurrency users based on their attitudes towards security and privacy practices, which was later picked up and developed further by Voskobojnikov et al. [1, 146, 148]. Figure 3.2 illustrates how user choice between custodial and self-managed wallets

is influenced by their individual risk assessment and motivation and self-efficacy toward security. The paper closes by discussing the design implications that arise from the presented findings. Given the exploratory character of this paper, it motivated several of the subsequent research questions.

Author Contributions: I determined the overall research question, research design, and positioning within existing literature. Under my supervision, Felix Gutjahr conducted the user interviews as part of his Bachelor thesis and transcribed them. I independently conducted the thematic analysis based on the interview transcripts, wrote the paper, and managed the publication process. All authors contributed feedback on the manuscript. Florian Alt provided feedback throughout the process.

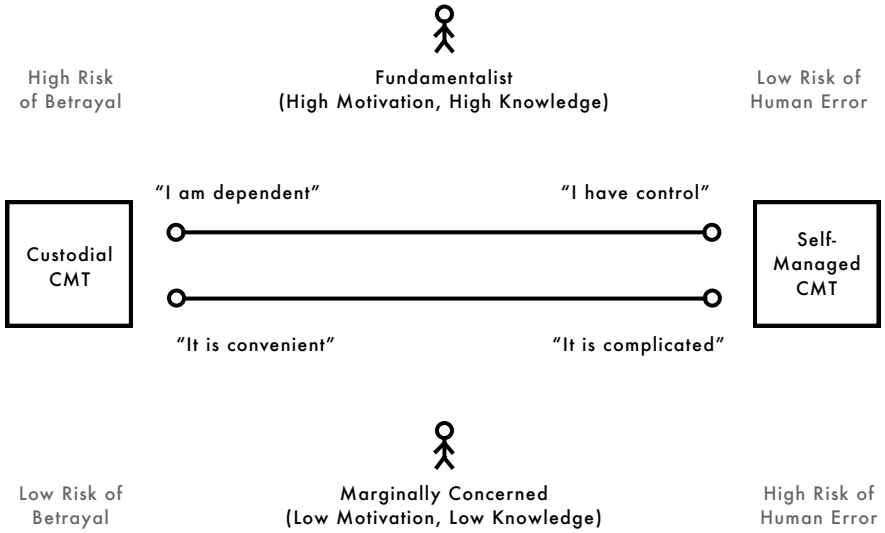


Figure 3.2: Conceptual model showing how security personas and individual risk assessment influence users' choice of Coin Management Tools (CMT). (Originally published in [P1], p. 8)

[P2] Under Pressure. A User-Centered Threat Model for Cryptocurrency Owners

Summary: Motivated by the relevance of individual risk assessment for user behavior, we wanted to understand what real-world threats exist and in how far they matched with perceived risks. The objective for this paper was to understand the landscape of threats cryptocurrency owners may face and understand potential approaches to deal with them. While technology-centric approaches to organize cryptocurrency and blockchain threats existed [113, 118], there was no systematic overview of threats end-users may face.


Under Pressure. A User-Centered Threat Model for Cryptocurrency Owners

To fill this gap, we conducted an expert elicitation study. Taking existing literature and a focus group as starting point, we conducted a three-round Delphi process [30] with 25 experts to systematically develop ans validate the model. To ensure a broad set of perspectives we recruited experts from industry and academia, from the fields of security, usability, cryptocurrency, and blockchain.

The final model identifies six categories of threats for end-users: (1) accidental threats, (2) privacy threats, (3) physical threats, (4) financial fraud threats, (5) social threats, and (6) technical threats. We additionally collected examples of real-world incidents and discussed the practical relevance and potential mitigation strategies.

Author Contributions: I determined the overall research question and research design, oversaw the collection of data from the Delphi panel, and the iterative creation of the threat model. I led writing the paper and its publication process. Philipp Hulm supported in the acquisition of the expert panel, the distribution of the survey, and in writing and revising the manuscript. Florian Alt provided feedback throughout the process, particularly at the conceptual phase and the manuscript revision.

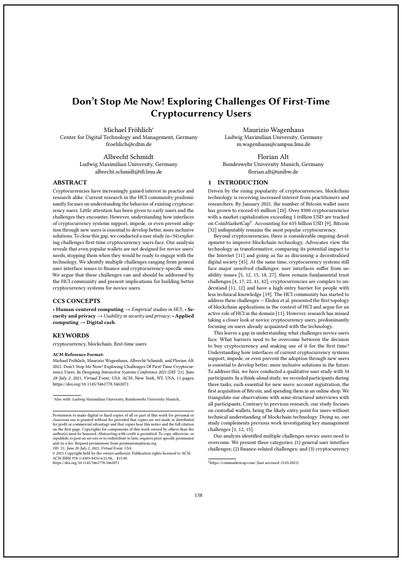
3.2.2 Challenges of New Users

Building on insights from our initial work [P1] and findings reported in literature [3, 54] we identified novice cryptocurrency users as a particular relevant group to look at, since challenges during initial use would likely have a high impact on subsequent adoption behavior. While existing research had often used inexperienced cryptocurrency users in their studies (e.g. [3, 54, 65, 99]), the field lacked a deeper understanding of which challenges users face during their first use and a framework to organize them. With [P3] we addressed this gap and identified challenges of first-time cryptocurrency users. The identified challenges and their categorization into *general challenges*, *finance-specific challenges*, and *cryptocurrency-specific challenges* was confirmed by research published around the same time by Voskobojnikov et al., who distinguish *general UX issues* and *domain-specific UX issues* [148] in a similiar manner after analysis of a large corpus of mobile app reviews. In summary, [P3] addresses the following research question: "*What challenges do users face when interacting with cryptocurrrency applications for the first time?*"

[P3] Don't Stop Me Now! Exploring Challenges Of First-Time Cryptocurrency Users

Summary: What barriers need to be overcome between the decision to buy cryptocurrency and making use of it for the first time? Understanding how interfaces of current cryptocurrency systems support, impede, or even prevent the adoption by new users is essential to develop better, more inclusive solutions in the future. This paper addresses this question by taking a dedicated look at how first-time cryptocurrency users interact with wallets. Being the likely entry point for users without previous experience of blockchain technology, our study focused on custodial wallets.

In a qualitative think-aloud user study with 34 participants we recorded participants during three tasks, each essential for new users: account registration, the first acquisition of Bitcoin, and spending them in an online shop. We triangulated [111] our observations with semi-structured interviews with all participants. To ensure the generalizability of our findings we included multiple wallets in our study.



Don't Stop Me Now! Exploring Challenges Of First-Time Cryptocurrency Users

Michael Fröhlich*
Center for Digital Technology and Management, Germany
froehlich@cdtm.de

Maurizio Wagenhaus
Ludwig Maximilian University, Germany
m.wagenhaus@campus.lmu.de

Albrecht Schmidt
Ludwig Maximilian University, Germany
albrecht.schmidt@ifi.lmu.de

Florian Alt
Bundeswehr University Munich, Germany
florian.alt@unibw.de

ABSTRACT

Cryptocurrencies have increasingly gained interest in practice and research alike. Current research in the HCI community predominantly focuses on understanding the behavior of existing cryptocurrency users. Little attention has been given to early users and the challenges they encounter. However, understanding how interfaces of cryptocurrency systems support, impede, or even prevent adoption through new users is essential to develop better, more inclusive solutions. To close this gap, we conducted a user study (n=34) exploring challenges first-time cryptocurrency users face. Our analysis reveals that even popular wallets are not designed for novice users' needs, stopping them when they would be ready to engage with the technology. We identify multiple challenges ranging from general user interface issues to finance and cryptocurrency-specific ones. We argue that these challenges can and should be addressed by the HCI community and present implications for building better cryptocurrency systems for novice users.

CCS CONCEPTS

• **Human-centered computing** → *Empirical studies in HCI*; • **Security and privacy** → *Usability in security and privacy*; • **Applied computing** → **Digital cash**.

KEYWORDS

cryptocurrency, blockchain, first-time users

ACM Reference Format:
Michael Fröhlich, Maurizio Wagenhaus, Albrecht Schmidt, and Florian Alt. 2021. Don't Stop Me Now! Exploring Challenges Of First-Time Cryptocurrency Users. In *Designing Interactive Systems Conference 2021 (DIS '21), June 28-July 2, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3461778.3462071

*Also with Ludwig Maximilian University, Bundeswehr University Munich,.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
DIS '21, June 28-July 2, 2021, Virtual Event, USA
© 2021 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-8476-6/21/06…$15.00
https://doi.org/10.1145/3461778.3462071

1 INTRODUCTION

Driven by the rising popularity of cryptocurrencies, blockchain technology is receiving increased interest from practitioners and researchers. By January 2021, the number of Bitcoin wallet users has grown to exceed 65 million [10]. Over 8300 cryptocurrencies with a market capitalization exceeding 1 trillion USD are tracked on CoinMarketCap[1]. Accounting for 635 billion USD [9], Bitcoin [32] indisputably remains the most popular cryptocurrency.

Beyond cryptocurrencies, there is considerable ongoing development to improve blockchain technology. Advocates view the technology as transformative, comparing its potential impact to the Internet [11] and going as far as discussing a decentralized digital society [45]. At the same time, cryptocurrency systems still face major unsolved challenges: user interfaces suffer from usability issues [5, 12, 15, 18, 27], there remain fundamental trust challenges [4, 17, 22, 41, 42], cryptocurrencies are complex to understand [11, 12] and have a high entry barrier for people with less technical knowledge [19]. The HCI community has started to address these challenges — Elsden et al. presented the first topology of blockchain applications in the context of HCI and argue for an active role of HCI in the domain [11]. However, research has missed taking a closer look at novice cryptocurrency users, predominantly focusing on users already acquainted with the technology.

This leaves a gap in understanding what challenges novice users face. What barriers need to be overcome between the decision to buy cryptocurrency and making use of it for the first time? Understanding how interfaces of current cryptocurrency systems support, impede, or even prevent the adoption through new users is essential to develop better, more inclusive solutions in the future. To address this, we have conducted a qualitative user study with 34 participants. In a think-aloud study, we recorded participants during three tasks, each essential for new users: account registration, the first acquisition of Bitcoin, and spending them in an online shop. We triangulate our observations with semi-structured interviews with all participants. Contrary to previous research, our study focuses on custodial wallets, being the likely entry point for users without technical understanding of blockchain technology. Doing so, our study complements previous work investigating key management challenges [1, 12, 15].

Our analysis identified multiple challenges novice users need to overcome. We present three categories: (1) general user interface challenges; (2) finance-related challenges; and (3) cryptocurrency

[1]https://coinmarketcap.com/ (last accessed 15.05.2021)

138

We identified multiple challenges novice users need to overcome and organized them into three categories: (1) general user interface challenges; (2) finance-related challenges; and (3) cryptocurrency-related challenges. To our surprise, most challenges are not rooted in technical constraints of blockchain technology and can, therefore, be addressed with HCI methods. Our discussion presents implications for research and practice.

Author Contributions: I determined the overall research question and research design. I enabled the study through close supervision and frequent discussions throughout conceptualization and data collection. Maurizio Wagenhaus conducted the user study and transcribed the collected data. Maurizio Wagenhaus and I equally contributed in the thematic analysis of the data. I led writing the paper and its publication process. Albrecht Schmidt and Florian Alt supported with their feedback from conceptualization to publication. All authors provided feedback for the revision of the manuscript.

3.3 Constructive Approaches Improving Application Usability

While the first two sections of this chapter focus on understanding the existing research body as well as user behavior in practice, the remaining publications in this dissertation explore how to translate these findings into action. They focus on the following research question:

RQ3: "*How can we build with and for cryptocurrency?*"

We addressed this research question from three perspectives. We investigated the potential benefits of onboarding for mobile cryptocurrency applications [P4], developed a functional system for point-of-sale transactions with Bitcoin Lightning [P8], and explored how future developers could be supported through enabling rapid interface experimentation [P7] and through novel education formats at university [P8]. These publications show that user-centered methods can improve the usability of cryptocurrency systems, that newer cryptocurrencies provide properties that enable use for everyday payments, and that interdisciplinary education may help developers build more useful applications. Doing so, the provide a foundation from which future work may map the larger design space beyond use cases as store of value and means of payment.

3.3.1 Onboarding of New Users

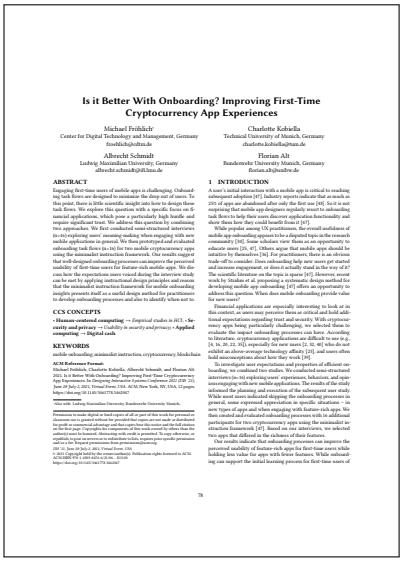
The initial experience users have when interacting with an app has a large influence on subsequent adoption [131]. 25% of apps are opened only one time [140] and within the first three days mobile apps lose 77% of their daily active users [23]. The first-time mobile app experience of cryptocurrency applications is therefore interesting when attempting to lower technological entry barriers. With cryptocurrency applications being challenging to get started with for new users [3, P3, 99], especially for those with below-average technology affinity [56], understanding how to improve the initial user experience of cryptocurrency apps could benefit the technology adoption.

Among practitioners, the question how to onboard new users to mobile apps has been of great interest [131]. However, while learnability has been a longstanding topic in the HCI community, the value of onboarding flows in mobile applications appears to be disputed among scholars [64]. While some view them as an opportunity to educate users [59, 131], others argue that mobile apps should be intuitive by themselves [80]. A recent studies with 60 experts in human-computer interactions confirms a large variance in the perceived usefulness of mobile app onboarding [64].

Overall, the scientific literature on how to design mobile application onboarding is sparse. While scholars evaluated onboarding for specific applications – e.g. a photo editing extension [52], a citizen science platform [19], gaming [110] and education [86] – the first systematic design method was presented by Strahm et al. in 2018: They characterized nascent practitioner guidance, discussed it in the context of the minimalist instruction theory [142], and proposed a context-free design method for creating onboarding processes for mobile applications [131].

While most previous practitioner resources have been comprised of rather general recommendations [131], Strahm et al.'s recent work provides an opportunity to look at onboarding experiences in a more systematic way. With [P4] we apply their methodological framework to cryptocurrency mobile apps. This allows us not only to explore how to improve first-time experience in this specific domain, but also offers an opportunity to address the following question through a more general lens: "*When does mobile onboarding provide value for new users?*"

[P4] Is it Better With Onboarding? Improving First-Time Cryptocurrency App Experiences


Is it Better With Onboarding? Improving First-Time Cryptocurrency App Experiences

Summary: In this paper, we explore the efficacy of onboarding for mobile cryptocurrency applications. The motivation for this paper arose from the empirical findings and observations of our preceding studies [P1, P3] and is the first attempt to design and evaluate solutions.

In this paper, we present the results of two studies: First, we explored users' experiences, behaviors, and opinions when engaging with new mobile applications through semi-structured interviews (n=16). The results of the study informed the planning and execution of the subsequent user study where we applied Strahm et al.'s minimalist instruction framework [131] to iteratively design and evaluate onboarding processes for two mobile cryptocurrency apps with differing levels of feature-richness. Our results indicate that onboarding processes can improve the perceived usability of feature-rich apps for first-time users while holding less value for apps with fewer features. In particular, with the developed onboarding the SUS score [15] of the feature-rich app increased from 57.5 to 78.8 while in the feature-low app it remained stable. We discuss how the expectations users voiced during the interview study can be met by applying instructional design principles and reason that the minimalist instruction framework for mobile onboarding presents itself as a useful design method for practitioners to develop onboarding processes.

Author Contributions: I determined the overall research question and research design. I enabled the study with close supervision and frequent discussions. Charlotte Kobiella and me conducted the interviews. Charlotte Kobiella designed the interfaces and evaluated them in the subsequent user study. I took the leading role in writing the paper and its subsequent publication process. Albrecht Schmidt and Florian Alt supported with their feedback from conceptualization to publication. All authors provided feedback for the revision of the manuscript.

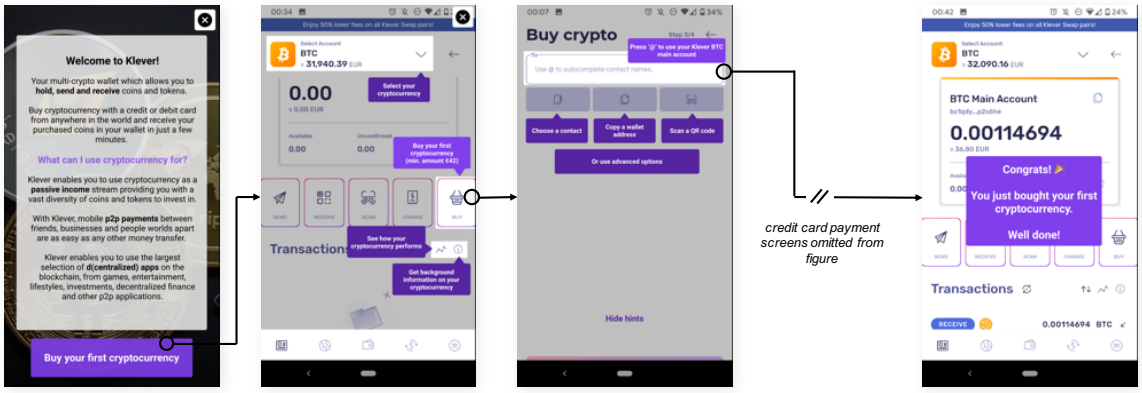
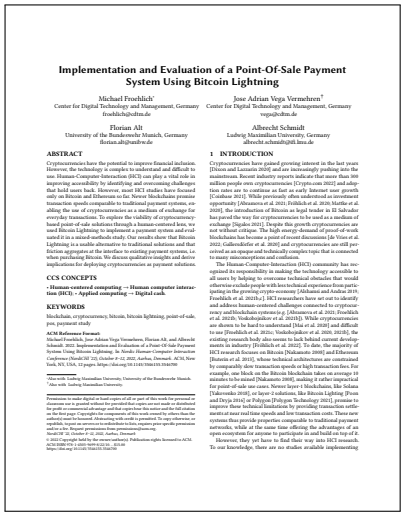


Figure 3.3: The interfaces of one prototyped onboarding process. (Originally published in [P4], p. 8)

3.3.2 Cryptocurrency for Everyday Payments

In its original white paper, Bitcoin was described as "*peer-to-peer electronic cash*" [101]. Despite the ongoing proliferation of Bitcoin as store of value over the past decade, it has not found much real-world application as means of transaction [P1, 73]. Part of the reason may be found in technical constraints. For example, Bitcoin is characterized by comparably slow transaction speeds. By design, mining one block takes on average 10 minutes. This makes it rather impractical to facilitate transactions in the real world, where goods and money would be exchanged at the same time. However, newer blockchains promise to overcome these technical limitations [P5]. For instance, Bitcoin Lightning promises "*near real time*" transactions [112] comparable to traditional payment networks. However, these claims have yet to be tested. Emerging empirical work indicates that while nodes within the Lightning network tend to behave in fair manner [159], payments also often fail [151]. This leaves the question whether Bitcoin Lightning can be a viable alternative to centralized systems, and taking a human-centered perspective, how it is perceived during use by end-users. With [P6] we address this gap and implement a functional point-of-sale system using Bitcoin Lightning as settlement layer. Doing so, we explore the question: "*Is Bitcoin Lightning a viable technology to facilitate everyday point-of-sale transactions?*"

[P6] Implementation and Evaluation of a Point-Of-Sale Payment System Using Bitcoin Lightning



Implementation and Evaluation of a Point-Of-Sale Payment System Using Bitcoin Lightning

Michael Froehlich*
Center for Digital Technology and Management, Germany
froehlich@cdtm.de

Jose Adrian Vega Vermehren*
Center for Digital Technology and Management, Germany
vega@cdtm.de

Florian Alt
University of the Bundeswehr Munich, Germany
florian.alt@unibw.de

Albrecht Schmidt
Ludwig Maximilian University, Germany
albrecht.schmidt@ifi.lmu.de

ABSTRACT

Cryptocurrencies have the potential to improve financial inclusion. However, the technology is complex to understand and difficult to use. Human-Computer Interaction (HCI) can play a vital role in improving accessibility by identifying and overcoming challenges that hold users back. However, most HCI studies have focused only on Bitcoin and Ethereum so far. Newer blockchains promise transaction speeds comparable to traditional payment systems, enabling the use of cryptocurrencies as a medium of exchange for everyday transactions. To explore the viability of cryptocurrency-based point-of-sale solutions through a human-centered lens, we used Bitcoin Lightning to implement a payment system and evaluated it in a mixed-methods study. Our results show that Bitcoin Lightning is a usable alternative to traditional solutions and that friction aggregates at the interface to existing payment systems, i.e. when purchasing Bitcoin. We discuss qualitative insights and derive implications for deploying cryptocurrencies as payment solutions.

CCS CONCEPTS

• Human-centered computing → Human computer interaction (HCI); • Applied computing → Digital cash.

KEYWORDS

blockchain, cryptocurrency, bitcoin, bitcoin lightning, point-of-sale, pos, payment study

ACM Reference Format:

Michael Froehlich, Jose Adrian Vega Vermehren, Florian Alt, and Albrecht Schmidt. 2022. Implementation and Evaluation of a Point-Of-Sale Payment System Using Bitcoin Lightning. In *Nordic Human-Computer Interaction Conference (NordiCHI '22), October 8–12, 2022, Aarhus, Denmark.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3546155.3546700

*Also with: Ludwig Maximilian University, University of the Bundeswehr Munich.
†Also with: Ludwig Maximilian University.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
NordiCHI '22, October 8–12, 2022, Aarhus, Denmark
© 2022 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-9699-0/22/10…$15.00
https://doi.org/10.1145/3546155.3546700

1 INTRODUCTION

Cryptocurrencies have gained growing interest in the last years [Dixon and Lannaio 2020] and are increasingly pushing into the mainstream. Recent industry reports indicate that more than 300 million people own cryptocurrencies [Crypto.com 2022] and adoption rates are to continue as fast as early Internet user growth [Coinbase 2021]. While previously often understood as investment opportunity [Abramova et al. 2021; Fröhlich et al. 2020; Hartlin et al. 2020], the introduction of Bitcoin as legal tender in El Salvador has paved the way for cryptocurrencies to be used as a medium of exchange [Sigalos 2021]. Despite this growth cryptocurrencies are not without critique. The high energy demand of proof-of-work blockchains has become a point of recent discussions [de Vries et al. 2022; Gallersdörfer et al. 2020] and cryptocurrencies are still perceived as an opaque and technically complex topic that is connected to many misconceptions and confusion.

The Human-Computer Interaction (HCI) community has recognized its responsibility in making the technology accessible to all users by helping to overcome technical obstacles that would otherwise exclude people with less technical experience from participating in the growing crypto-economy [Alkhatani and Andras 2019; Froehlich et al. 2019b,c]. HCI researchers have set out to identify and address human-centered challenges connected to cryptocurrency and blockchain systems (e.g. [Abramova et al. 2021; Froehlich et al. 2021b; Voshmgir et al. 2021b]). While cryptocurrencies are shown to be hard to understand [Mai et al. 2020] and difficult to use [Froehlich et al. 2021c; Voshmgir et al. 2020, 2021b], the majority of HCI research focuses on Bitcoin and Ethereum implementations in industry [Fröhlich et al. 2022]. To date, the majority of HCI research focuses on Bitcoin [Nakamoto 2008] and Ethereum [Buterin et al. 2013], whose technical architecture are constrained by comparably slow transaction speeds or high transaction fees. For example, one block on the Bitcoin blockchain takes on average 10 minutes to be mined [Nakamoto 2008], making it rather impractical for point-of-sale use cases. Newer layer-1 blockchains, like Solana [Yakovenko 2018], or layer-2 solutions, like Bitcoin Lighting [Poon and Dryja 2016], or Polygon [Polygon Technology 2021], promise to improve these technical limitations by providing transaction settlements of near real time speeds and low transaction costs. These new systems thus provide properties comparable to traditional payment networks, while at the same time offering the advantages of an open ecosystem for anyone to participate in and build on top of it.

However, they yet have to find their way into HCI research. To our knowledge, there are no studies available implementing

Summary: In this paper we describe a reference implementation for a point-of-sale system integrating Bitcoin Lightning as settlement layer. The motivation for this paper arose from the findings of our previous studies [P1, P3] and our literature review [P5]. While users articulated that they would like to use cryptocurrency to make purchases [P1], there was only little research exploring its viability as means of transaction. Since newer solutions, such as Bitcoin Lightning, offer faster transaction speeds and lower fees compared to Bitcoin [P5], facilitating everyday transactions would now be possible for merchants and consumers. However, there has not been research exploring whether the promises made by Bitcoin Lightning would actually hold in practice and how users would perceive using it. To address this, we implemented a point-of-sale system and deployed it in an office-like setting at university to evaluate it in a mixed-methods study over a period of two weeks. Our results show that users find it reasonably easy to make payments once their wallet is set up. However, the initial purchasing of Bitcoin and configuration of their wallet before is error-prone and cumbersome. We discuss the system's performance concerning ease-of-use, speed, transaction fees, and reliability and present implications for adoption of cryptocurrency based payment systems.

Author Contributions: I determined the overall research question and research design. I designed the system architecture and implemented the entire system. I led the user study, data collection, the analysis of the results, writing the paper and its subsequent publication process. Jose Vega supported in conducting the user study, in the analysis of the results, and the revision of the manuscript. Albrecht Schmidt and Florian Alt supported with their feedback from conceptualization to publication.

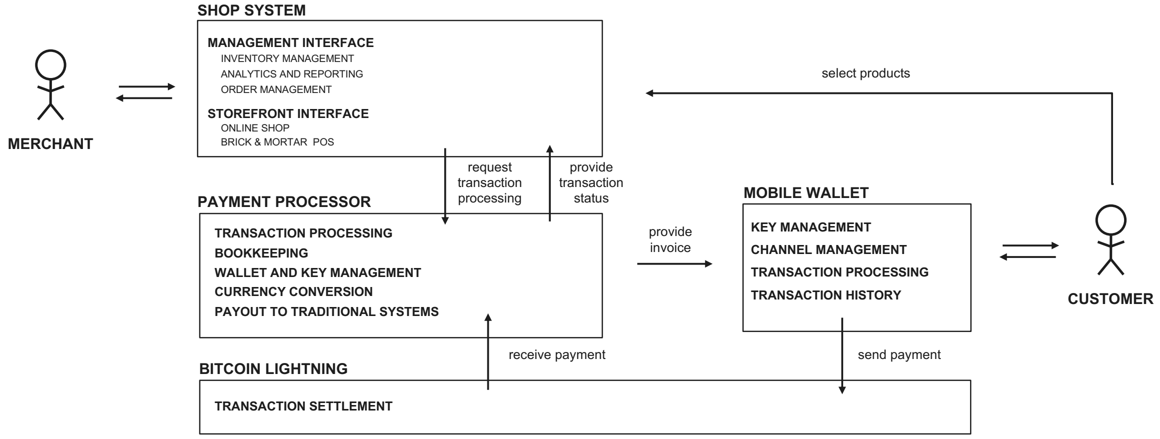


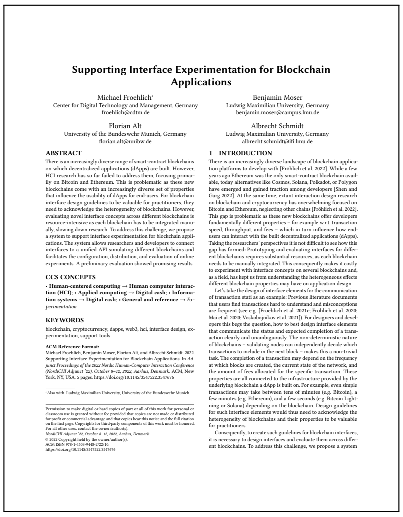
Figure 3.4: The subsystems of the proposed point-of-sale (PoS) system and their relationships to each other. (Originally published in [P6], p. 5)

3.3.3 Enabling Usable Blockchain Application Development

The final two approaches through which we explore how to facilitate the development of usable cryptocurrency applications shift the focus on the developer. Being essential for every software project, enabling developers to design for better usability could have compounding second-order effects for future applications. [P7] presents the implementation of a support system for developers of cryptocurrency and blockchain applications that enables rapid interface experimentation. [P8] explores how interdisciplinary education formats can be used to equip the next generation of developers with the necessary skills to develop useful blockchain applications. Together, [P7] and [P8] explore how developers can be supported during the design and development process of blockchain and cryptocurrency applications. They address the following research question: "*How can the development of usable blockchain applications be supported?*"

[P7] Supporting Interface Experimentation for Blockchain Applications

Summary: In this extended abstract we present a prototype that supports interface experimentation for blockchain applications. The system allows researchers and developers to connect interfaces to a unified API simulating different blockchains and facilitates the configuration, distribution, and evaluation of online experiments. The idea for this paper emerged as a result of the relative lack of HCI research on blockchains other than Bitcoin or Ethereum [P5]. To a certain degree, the contribution of this publication can be viewed as a methodological one. In essence, we wanted to make it easier for interface designers and researchers to experiment with different blockchains and accelerate their development and research workflows. We tested the feasibility of our approach by running a small experiment on mTurk (N=160). The findings, while generally positive, showed several points to improve the system.



Supporting Interface Experimentation for Blockchain Applications

Michael Froehlich*
Center for Digital Technology and Management, Germany
froehlich@cdtm.de

Benjamin Moser
Ludwig Maximilian University, Germany
benjamin.moser@campus.lmu.de

Florian Alt
University of the Bundeswehr Munich, Germany
florian.alt@unibw.de

Albrecht Schmidt
Ludwig Maximilian University, Germany
albrecht.schmidt@ifi.lmu.de

ABSTRACT

There is an increasingly diverse range of smart-contract blockchains on which decentralized applications (dApps) are built. However, HCI research has so far failed to address them, focusing primarily on Bitcoin and Ethereum. This is problematic as these new blockchains come with an increasingly diverse set of properties that influence the usability of dApps for end-users. For blockchain interface design guidelines to be valuable for practitioners, they need to acknowledge the heterogeneity of blockchains. However, evaluating novel interface concepts across different blockchains is resource-intensive as each blockchain has to be integrated manually, slowing down research. To address this challenge, we propose a system to support interface experimentation for blockchain applications. The system allows researchers and developers to connect interfaces to a unified API simulating different blockchains and facilitates the configuration, distribution, and evaluation of online experiments. A preliminary evaluation showed promising results.

CCS CONCEPTS

• **Human-centered computing → Human computer interaction (HCI)**; • **Applied computing → Digital cash**; • **Information systems → Digital cash**; • **General and reference →** *Experimentation.*

KEYWORDS

blockchain, cryptocurrency, dapps, web3, hci, interface design, experimentation, support tools

ACM Reference Format:
Michael Froehlich, Benjamin Moser, Florian Alt, and Albrecht Schmidt. 2022. Supporting Interface Experimentation for Blockchain Applications. In *Adjunct Proceedings of the 2022 Nordic Human-Computer Interaction Conference (NordiCHI Adjunct '22), October 8–12, 2022, Aarhus, Denmark.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3547522.3547676

*Also with Ludwig Maximilian University, University of the Bundeswehr Munich.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
NordiCHI Adjunct '22, October 8–12, 2022, Aarhus, Denmark
© 2022 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-9448-2/22/10.
https://doi.org/10.1145/3547522.3547676

1 INTRODUCTION

There is an increasingly diverse landscape of blockchain application platforms to develop with [Fröhlich et al. 2022]. While a few years ago Ethereum was the only smart-contract blockchain available, today alternatives like Cosmos, Solana, Polkadot, or Polygon have emerged and gained traction among developers [Shen and Garg 2022]. At the same time, extant interaction design research on blockchain and cryptocurrency has overwhelming focused on Bitcoin and Ethereum, neglecting other chains [Fröhlich et al. 2022]. This gap is problematic as these new blockchains offer developers fundamentally different properties – for example w.r.t. transaction speed, throughput, and fees – which in turn influence how end-users can interact with the built decentralized applications (dApps). Taking the researchers' perspectives it is not difficult to see how this gap has formed: Prototyping and evaluating interfaces for different blockchains requires substantial resources, as each blockchain needs to be manually integrated. This consequently makes it costly to experiment with interface concepts on several blockchains and, as a field, has kept us from understanding the heterogeneous effects different blockchain properties may have on application design.

Let's take the design of interface elements for the communication of transaction stati as an example: Previous literature documents that users find transactions hard to understand and misconceptions are frequent (see e.g. [Froehlich et al. 2021c; Fröhlich et al. 2020; Mai et al. 2020; Voskobojnikov et al. 2021]). For designers and developers this begs the question, how to best design interface elements that communicate the status and expected completion of a transaction clearly and unambiguously. The non-deterministic nature of blockchains – validating nodes can independently decide which transactions to include in the next block – makes this a non-trivial task. The completion of a transaction may depend on the frequency at which blocks are created, the current state of the network, and the amount of fees allocated for the specific transaction. These properties are all connected to the infrastructure provided by the underlying blockchain a dApp is built on. For example, even simple transactions may take between tens of minutes (e.g. Bitcoin), a few minutes (e.g. Ethereum), and a few seconds (e.g. Bitcoin Lightning or Solana) depending on the blockchain. Design guidelines for such interface elements would thus need to acknowledge the heterogeneity of blockchains and their properties to be valuable for practitioners.

Consequently, to create such guidelines for blockchain interfaces, it is necessary to design interfaces and evaluate them across different blockchains. To address this challenge, we propose a system

Author Contributions: I determined the overall research question and research design. I enabled the study through close supervision and frequent discussions throughout conceptualization, data collection, and analysis of the results. Benjamin Moser implemented the prototype, conducted the user study, and analyzed the results. I wrote the paper and led its subsequent publication process. Albrecht Schmidt and Florian Alt supported with their feedback from conceptualization to publication. All authors provided feedback for the revision of the manuscript.

[P8] Prototyping with Blockchain: A Case Study For Teaching Blockchain Application Development at University


Prototyping With Blockchain: A Case Study For Teaching Blockchain Application Development at University

Summary: In this paper we present an interdisciplinary blockchain application development course at university. We designed the curriculum based on our observation that many emerging blockchain applications fail to articulate what benefits arise from integrating a blockchain. Thus, our objective was to design a course that addresses this aspect by combining perspectives from different disciplines when evaluating blockchain use cases: technical feasibility (software engineering), value-creation (entrepreneurship), and user experience (human-computer-interaction). With this approach we hoped to enable participants to identify *useful* applications of blockchain technology, connecting back to second antecedent of the Technology Acceptance model [31, 32]. We used the Design Sprint [69] method as theoretical basis for creating the course. Our evaluation with N=11 students showed promising results: The course was well-perceived by participants and effective in improving participants ability to distinguish use cases (not) suited for the technology. We close the paper with lessons learned for educators.

Author Contributions: I determined the overall research question and research design, managed the data collection, and conducted the analysis of the results. I led writing the paper and its subsequent publication process. Jose Vega, Amelie Pahl, and Sergej Lotz supported the positioning of the research question through joint discussions, the execution of the course, and the revision of the manuscript. Albrecht Schmidt, Florian Alt, and Isabell Welpe supported with their feedback from conceptualization to publication.

Figure 3.5: Impressions of the conducted course format. (Originally published in [P8], p. 4)

4
Conclusion

Think of all the things people have envisioned and were told were impossible. Phones, cars, light bulbs, planes... the list goes on and on. The inventors and people with limitless minds found a way to make them happen.

Arnold Schwarzenegger

The overall goal of this dissertation was to advance our understanding of how to build usable cryptocurrency applications. Grounded in the eight publications this dissertation is composed of, it offers multiple contributions to this overarching question.

We started by consolidating and organizing the existing body of research following a systematic approach [P5]. We investigated user behavior in practice with a focus on privacy and security. From our observations we contribute a generalized description of cryptocurrency usage behavior and derive conceptual models to make these insights accessible to researchers and practitioners [P1, P2]. We explored challenges of first-time users through a qualitative evaluation of existing cryptocurrency wallets. We organize the identified challenges into three domains revealing the heterogeneity of causes for the lacking usability of current cryptocurrency wallets [P3]. Building on these results, we developed an interface prototype for onboarding new users to cryptocurrency wallets and evaluated its efficacy under different contextual circumstances. In doing so, we show that onboarding can be effective to reduce the entry barriers for users and contribute a discussion under which conditions this will be the case [P4]. Building on the insights from our previous studies and related work, we are the first to use Bitcoin Lightning as underlying settlement layer to implement a functional point-of-sale system. Our evaluation in a field study indicates that Bitcoin Lightning is becoming a viable alternative to proprietary transaction networks for small everyday transactions. Our study also reveals that much of the friction slowing the adoption of cryptocurrency as means of payment is likely situated at the transition points between existing financial systems and decentralized ones [P6]. Taking a step back, we shift our focus from the end-user to the developer. We implement a support system to enable cryptocurrency and blockchain developers to increase the speed at which they can test the usability of their application interfaces [P7]. Finally, we consolidate the knowledge accumulated throughout the publications of this dissertation into an interdisciplinary university course to educate and empower the next generation of developers to build usable and useful blockchain applications [P8].

Collectively these contributions have advanced the research conversation within the Human-Computer Interaction community on usable cryptocurrency systems over the past years. During the time the studies in this dissertation were conducted and published the larger cryptocurrency space has advanced as well: new cryptocurrencies have emerged, blockchain technologies have been improved, and new use-cases have attracted an increasingly diverse population of users. In this final chapter, we discuss key learnings of this dissertation, point to directions for future research, and reflect on the contributions against the backdrop of the changing landscape of cryptocurrency technology.

4.1 Discussion

The following section summarizes the cumulative learnings of this dissertation. As any aggregation of data comes at the cost of nuance, detailed discussions can be found in the individual publications.

How Users Interact With Cryptocurrency

Our empirical studies shed light on how users interact with cryptocurrencies in practice [P1, P3]. Most importantly, they highlight that cryptocurrency users are not one homogeneous group [P1, 1]. Users are interested in using cryptocurrency for different reasons. On a high level motivation can be grouped into either ideological, technological, or financial interest [P1]. At the individual level the specific motivation to engage with cryptocurrencies varies between people. While some do so to be at the forefront of technological innovation, some want to invest or protect their wealth from inflation, and others want to use it to make purchases [P1]. In line with contemporary research, our results show that in addition to their intended use, risk assessment, and perceived self-efficacy influence user behavior [P1, 1]. These results underline the relevance of perceived risk as preceding variable for technology acceptance [48, 109]. We identified three key risks users need to balance to avoid the loss of their cryptocurrency: the risk of human error, the risk of betrayal, and the risk of malicious attacks. Depending on how users assess these risks in relation to their own abilities to securely handle cryptocurrencies they will choose the tools to do so [P1]. While tech-savvy individuals may prefer to follow the "*not your key, not your crypto*" ethos, beginners may overall fare better to trust a custodial wallet provider to reduce their risk of loss through human error [P1, P3, P5]. Our expert panel further underscores the relevance of human errors as source of loss of cryptocurrencies [P2]. Missing or incomplete understanding of how the blockchain technology behind cryptocurrencies work are common [P1, 90] and put users at risk of accidental loss or malicious attacks [P1, P2]. In practice key management remains a point of struggle for both new and existing users [P1, 41]. While innovative concepts, such as mnemonics [108] or hierarchical deterministic key generation [156], have been introduced to reduce the burdens of key management, incorrect mental models [90, 148], missing knowledge about security practices [P1], or missing motivation [P1] limit their benefits. However, key management is not the sole source of usability issues of cryptocurrenies. Users perceive cryptocurrencies as difficult to use, even when passing key management on to custodial services [P3].

Where Today's Systems Fall Short

Our studies reveal that cryptocurrency applications today suffer from a range of usability issues. Their cause is only partly found in the technical constraints of the underlying blockchain technology.

New users are confronted with (too) many new concepts. Cryptocurrencies users face a steep learning curve along which they are confronted with many unfamiliar aspects within a short time that can easily feel overwhelming [P1, P3, 148]. Even before interacting with cryptocurrencies the first time, users need to answer several questions to move from intention to action [31, 32]: Where to buy cryptocurrencies? Which cryptocurrencies to acquire? How to do so? While the web has many resources to offer that address these questions, users struggle to find a starting point [56] since they first need to learn to discern which resources are trustworthy and which recommendations address their specific needs. The applications investigated in the included publications do not recognize the complexity of getting started with cryptocurrencies. Instead, their interfaces build on concepts from the finance or cryptocurrency domain that many users are not familiar with and consequently

exacerbate their use. Technical language and metaphors are confusing for users [P1, P3, 41, 147] and technology specific abstractions require users to update their mental models [P3]: What are addresses and how do they look like? How do fees work? What determines the speed and cost of transactions? How do you maintain basic security? Answering these questions is additionally complicated as there are subtle differences between cryptocurrencies [P7].

Friction accumulates at the edge to established systems. The initial use of cryptocurrency systems is further exacerbated since much of the friction originates at the edge to established systems [P3, P4, P6]. Our studies showed that Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) verification processes demanded by regulators are often only weakly integrated into the underlying products and increase the hurdles when first setting up an account [P3]. The primary goal of most users when first using crypotocurrency applications is to purchase cryptocurrency, yet instead they need to overcome a long and complicated setup process [P4]. Often cryptocurrencies have to be bought via third-party exchanges introducing additional unfamiliar elements and uncertainty [P3]. During our research it was not uncommon that users' bank and credit card providers blocked the purchase of cryptocurrency [P3, P6]. Making online purchases with Bitcoin proved difficult due to missing integration between wallet and merchant: Manual data entry was complicated and error-prone. Additionally, inconsistent exchange rates to fiat currency confused users and led to incorrect balances being transacted [P3]. While not being part of the presented studies, the reimbursement of participants' remaining wallet balances after our field study [P6] was similarly cumbersome.

Free-market dynamics complicate everyday use. While the rise of cryptocurrencies' market valuations and prices have made them attractive targets to invest in, they introduced hurdles for everyday use. The high valuation of Bitcoin and other cryptocurrencies have resulted in price points that are so low that they are difficult to handle for everyday purchases. For example, distinguishing between EUR 2 and EUR 20 is almost effortless. In contrast, spotting the difference between BTC 0.0000861 and BTC 0.000861 requires active concentration [P3, P6]. High volatility connected with uncertainty when transactions are going to be completed make it difficult to determine price points for purchases. As both users and merchants are used to thinking in fiat currencies, this leads to inconsistent exchange rates being used between merchants and users' wallets [P3]. The limited throughput of leading cryptocurrencies causes surging fee prices if demand is high [45], making small transactions expensive and economically unviable in many cases. Newer cryptocurrencies attempt to address some of these issues [P5, P6, P8]. However, as of now we lack the empirical evidence whether the proposed solutions are a viable alternative in practice [P5, P6].

Cryptocurrency systems fail to offer a clear benefit. Beyond being an investment vehicle cryptocurrency systems need to offer a benefit to users to incentivize everyday use. While some users voiced their excitement about using cryptocurrency to pay [P1], some argued that they do not see any advantages compared to established systems such as Paypal [P3, P6]. If there are trusted centralized payment providers in a region cryptocurrencies face an uphill battle against these market incumbents protected by network effects [96]. This also indicates that the perceived utility of cryptocurrencies may not only depend on their internal properties, but also the availability of alternatives [88]. In other words, when aiming to understand the adoption and perceived usefulness of cryptocurrencies through the lens of the Technology Acceptance Model [31, 32, 48], the surrounding cultural, geographic, and socioeconomic context should be considered as moderating variables. Participants in the presented payment studies [P3, P6] were situated primarily in Germany and surrounding central European nations, where alternative payment systems are well established and the limited options to pay with cryptocurrencies failed to provide a clear benefit. These results do not speak against the suitability of

cryptocurrency as means of payment in itself, but highlight the platform dynamics cryptocurrencies need to overcome to deliver a clear benefit.

Implications For the Design of Usable Cryptocurrency Systems

The results of this dissertation offer several implications for the design of usable cryptocurrency systems. Practitioners should follow established design guidelines, build products with a clear focus on target groups and use cases, and consider users' learning process in their application designs.

Make use of established design guidelines. A sizeable portion of usability issues with cryptocurrency applications is not caused by constraints of the underlying technology and can be addressed by adhering to established design guidelines and design practices [P3]. Multiple publications show that established methods such as usability walkthroughs can catch a lot of these general issues [P3, P5, 41, 42, 99, 148]. Our own studies show that user-centered design methods offer a promising methodological framework through which more usable applications can be realized [P4]. In very practical terms, this means that practitioners should familiarize themselves with interface heuristics [125] and follow a human-centered design process integrating iterative testing with users [105].

Build with a target group in mind. Cryptocurrency users are not one uniform group of people but meaningfully differ in their behavior [P1, 1]. Hence, practitioners should consider this heterogeneity in the design and development of applications to better meet the needs of the specific subgroups using them. In this dissertation we identified security knowledge and motivation as well as the resulting risk perception as relevant dimensions along which to segment user groups [P1] and point to the special challenges first-time cryptocurrency users face [P1, P3]. To build more usable cryptocurrency applications, practitioners should therefore first aim to understand the needs of the specific target groups for which they are building. Knowledge along which dimensions groups differ, will help to build products that balance the competing needs between security and convenience in alignment with users' preferences [P1].

Build with a use-case in mind. Users' motivations to engage with cryptocurrency have a direct influence on how they intend to use it [P1]. While cryptocurrencies have been primarily used as store of value [P1], alternative use cases are emerging [P5]. With fundamental properties that approach the performance of existing distributed systems new blockchains provide the technical platform to support an increasingly diverse set of use cases [P4, P5, P7]. These different use cases – store of value, everyday payments, DeFi, NFTs, DAOs, identity – will attract users with different needs [P5]. To maximize usability, practitioners should thus aim to build products with a specific use case in mind instead of building one-size-fits-all solutions [1]. Since users are willing to use several wallets in parallel [P1], this will help to build a competitive advantage over general purpose systems by providing more utility for the relevant target groups. Concentrating development efforts on one vertical will also allow for more resources to flow in the identification and integration of relevant adjacent services, which may help reduce the friction that accumulates at the edge of today's systems.

Support users' learning process. Cryptocurrency applications confront users with many new concepts at once, often overwhelming them [P3, 148]. Application onboarding can be one solution to focus users' attention to the relevant aspects and improve first-use usability [P4]. However, practitioners should consider how their applications can be designed to progressively onboard new users and support their learning process beyond first-use [P4]. Users' preferences between control and convenience may vary depending on their experience and motivation [P1]. For beginners default options

may reduce information overload and decision fatigue. With increasing experience and knowledge of how cryptocurrencies work, users may want to adjust and tweak settings (e.g. transaction fees) to their liking. Interfaces should aim to support the typical learning journey through which their users transition. In general, interfaces should aim for simplicity through useful abstraction and default parameters. Advanced configuration may be added through progressive disclosure [104], by providing user profiles [148], or options to personalize interfaces [1, 148]. Hybrid wallets that help users transition from custodial to self-managed ones as users progress have been suggested as another approach [P1, P5]. For this to be effective, practitioners should aim to understand the specific progression of their users' learning journey.

Lesson's Beyond Usability

Our results revealed several insights that transcend the core field of Human-Computer Interaction and underline the importance of contributions from multiple disciplines.

Education needs to be part of the solution. Some usability issues as well as arising mistakes and threats originate from users' mental model mismatching the technical reality. While some of these misconceptions are caused by ill-designed interfaces, others result from a wrong understanding of how the blockchain technology powering cryptocurrency works [P2, P3, 90, 148]. Issues rooted in such fundamental misconceptions will neither be resolved through technical innovation nor improved interface and interaction concepts. Instead, we need to find a way to educate users [141] and correct misconceptions in their mental models. The results of [P1] indicate that educational interventions can be effective. A particular challenge to this end will be education on secure key management, which remains a challenge for most users [P1, 41]. Closing this gap is not only important to improve usability and adoption of cryptocurrencies in the long run, but also to protect existing users from threats that exploit their misunderstanding [P2].

Empower developers to build usable and useful applications. One goal of this dissertation was to provide practitioners with actionable insights on how they can improve the usability of their systems. Most available research addresses this objective by focusing on how users interact with cryptocurrencies. However, to advance the adoption of cryptocurrencies not only ease-of-use but also the usefulness of applications is critical [31, 32]. As practitioners appear to struggle to identify relevant use cases [85, 157], our work shows that human-centered methods are effective to support them to this end [P8]. This requires to shift the research focus away from end-users to the developers of cryptocurrency systems. Could the poor usability of cryptocurrency applications [P3, 62, 148] at least in part be caused by a lack of methods and support tools for those building them? Based on our tentative findings [P7, P8], researching and creating supporting tools and methods to enable developers could be a promising approach to improve the usability and usefulness of cryptocurrency applications.

Research on cryptocurrency is trailing practice. Our literature review shows that Human-Computer Interaction research on cryptocurrency systems trails the development in practice [P5]. In parts the reason for this is that cryptocurrencies are arguably the first technology that has the economic incentives for its own future development embedded in itself. By improving the blockchain in which a developer is invested in, they improve the value of the platform itself, which is reflected in the future value of the cryptocurrency. As a consequence, there are many cryptocurrency applications available for users today. While in general, the usability of cryptocurrency apps is perceived as subpar [P3, 62, 148], there might be specific applications that provide a good usability and introduce promising interaction concepts. In this shifting landscape, the Human-Computer Interaction community can

provide value by focusing on cutting through the fog. Research can shed light on which approaches explored by practice are promising, develop these concepts further, and possibly formalize them in thoroughly tested guidelines for practitioners [P5].

4.2 Future Work

The contribution of this dissertation represents a step towards better understanding how to design for and with cryptocurrencies. However, there remain unanswered questions and unresolved challenges. Arguably, the rapid development of the larger cryptocurrency space has opened up more questions than this dissertation managed to address during the same time frame. The studies presented in this dissertation naturally face limitations, which are laid out in detail in the individual publications. Overall, the presented insights resulted from studies conducted in Europe. Studies in other geographical and political contexts may bring forward differences with regard to users behavior, motivation, or perceived utility. Given the limited proliferation of cryptocurrencies during the time the studies were conducted, most results originate from lab studies. While we are confident that the presented results are robust to generalize to in-the-wild use, further research is needed to confirm this assumption. Rooted in the presented findings, we therefore discuss how future Human-Computer Interaction research may overcome these limitations and address new questions that have emerged from the evolving cryptocurrency landscape.

Going Beyond The Lab

The projects presented in this dissertation started out in early 2019 [P1]. Since then cryptocurrencies have grown their user base and proliferated into new areas [24, P5, 57]. Future research should increasingly focus on moving beyond laboratory settings to explore cryptocurrency usage in the field. While this was not possible before, the growing adoption in different regions of the world offers up new possibilities. Several governments introduced Bitcoin as legal tender, most prominently El Salvador, yet little is known about the real experiences there [P6, 126]. This new empirical context offers unique opportunities to observe the everyday use of cryptocurrencies and may help overcome some of the limitations of existing research. This is particularly interesting as much of the friction connected to the use of cryptocurrencies appears to originate at the edge to established systems [P3, P6]. Areas where cryptocurrencies have been adopted at country-level would allow for prolonged observation in a context where paying with cryptocurrencies is the norm and could thus bring forward exciting new insights.

Extending Research to Emerging Cryptocurrencies

Bitcoin provided the foundational technology for cryptocurrencies [101]. Ethereum advanced the field by designing, deploying, and growing the first smart-contract platform [17]. Therefore, it is not surprising that both cryptocurrencies have been the overwhelming focus of studies in recent years [P5]. However, moving forward it will be important to extend research to the increasingly diverse set of cryptocurrencies that have reached maturity over the past years [P5, 57]. New smart contract cryptocurrencies provide improved features that exceed the performance of established cryptocurrencies and open up the designed space for new applications [55]. At the same time algorithmic stable coins [97] and Central Bank Digital Currencies (CBDC) [9] address and arguably solve the volatility

issue, opening a bridge to established financial systems. Exploring how these new cryptocurrencies fare against established ones will extend our understanding of cryptocurrencies as design material.

Exploring Web3 Use Cases

Driven by recent innovations in blockchain technology, cryptocurrencies have started to outgrow their original purpose as internet money and enable a set of new use cases. Dubbed *web3* [13, P5, P8] these applications typically run within the web browser and connect to an underlying blockchain via browser based wallets such as Metamask [81]. Bringing cryptocurrencies to the web opened up a broad and diverse set of use cases that have only been marginally explored by Human-Computer Interaction research to date [P5]: Decentralized Finance (DeFi) [95], Decentralized Autonomous Organizations (DAOs) [150], Non-Fungible Tokens (NFTs) [149], and identity service such as the Ethereum Name Service (ENS) [12] are just a few of them. We lack a systematic understanding of the design space surrounding these applications and poorly understand who is using these new applications for what reasons [P5]. We hypothesize that the characteristics of these new users differs from earlier users. At the same time, we expect that the discussed design implications are useful for practitioners in the context of these new domains.

Balancing User-Needs

Much of the diversity of different blockchains rising to the market can be attributed to different approaches addressing the so-called blockchain trilemma [29, P5, 100]. It refers to the theorem that the decentralization, security, and scalability of blockchain are dependent features. Changing either one of the three will require tradeoffs with regards of the others [29]. A recent example illustrating this interdependence can be found in the switch of Ethereum from Proof-Of-Work (PoW) to Proof-of-Stake (PoS). While designed to increase the scalability of the blockchain [43], it simultaneously raises concerns to be less resistant against censorship [78]. Such tradeoffs are not easy to make and will require sacrifices on some side. Ever so more important will it be to have a user-centered perspective contributing to the discussion to contextualize the consequences these decisions will have for users. Beyond contributing knowledge to architectural decisions, it will be equally relevant to understand how users balance competing needs in practice. For example, [P1] proposes a model to explain how the need for convenience and security may influence decision making of users. As use-cases evolve, this balance may shift and expose both new opportunities and risks to users.

Cryptocurrency-Specific Design Guidelines

All of these points flow together as they may ultimately contribute to establishing cryptocurrency specific guidelines to designing user interfaces [P5]. Such guidelines may provide a framework to help practitioners in building usable user interfaces for cryptocurrency applications. To establish such guidelines it will be necessary to better understand the dimensions along which cryptocurrencies meaningfully differ from each other. For example, does the average transaction speed make a difference for how users would like to be informed about transaction stati? If so, which thresholds can serve as signposts to assign cryptocurrencies into groups that should be treated differently with regards to their representation in interfaces. To move towards a consistent and helpful set of guidelines research, it will be neccessary to both zoom in on specific user interface elements relevant for cryptocurrencies while at the same time recognizing the heterogeneity of available cryptocurrencies.

4.3 Reflection

The cryptocurrency and blockchain space has seen rapid growth during the brief period of time in which this dissertation was written [24, 124]. Drawing from our own anecdotal experience, it was remarkably difficult to find and recruit existing cryptocurrency users for our first study in 2019 [P1]. During the past three years this has changed: The number of cryptocurrency users has grown to more than 100 million globally [24]. Figure 4.1 illustrates the ongoing adoption of cryptocurrencies by juxtaposing it with the historic growth of Internet users from 1990 to 2000.

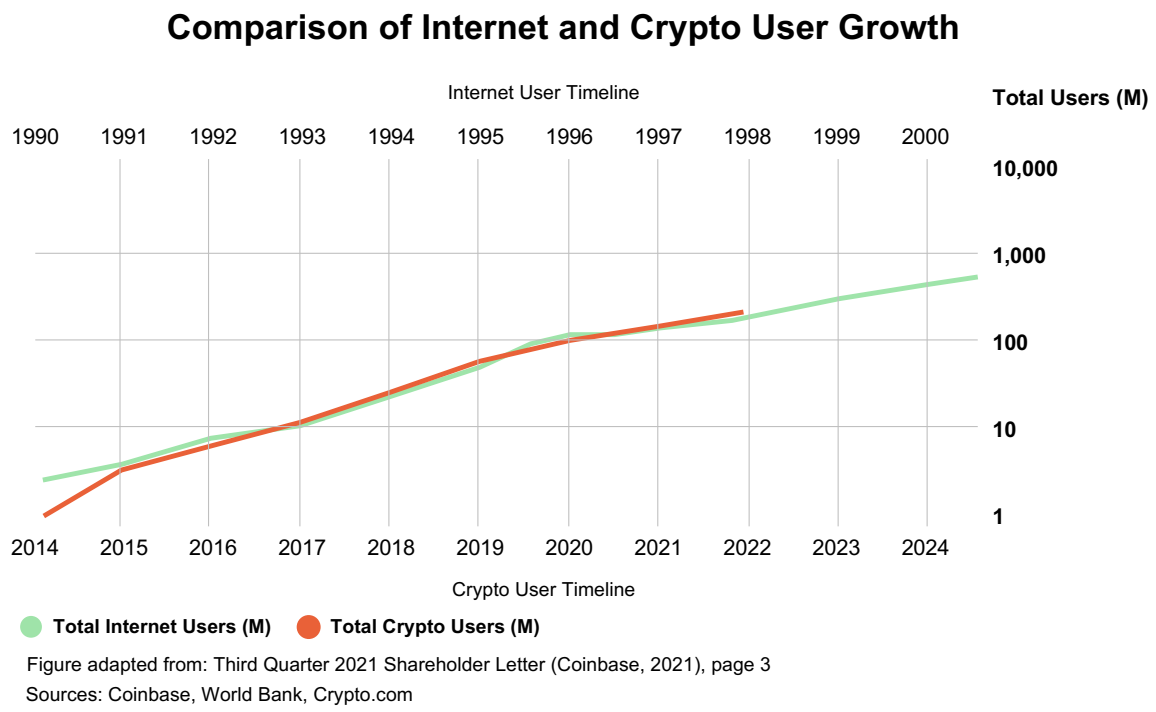


Figure 4.1: Comparison of Internet and crypto user growth. (Figure adapted from [24], p. 3)

The rising adoption shows that cryptocurrency and blockchain applications manage to increasingly satisfy the needs of a growing population of users and provide value for them. By means of comparison these numbers also indicate at a macro-level what the findings presented in this dissertation show at a user-level: Cryptocurrenies today are not a mature technology but one that is still under development. The technology is difficult to get started with, new terminology and interaction models are confusing for users, and transaction times are perceived as slow [P1, P3, P5].

Building on the comparison with the Internet in 1998, web usage then substantially differed in both usability and use-cases from today. Then the web was hard to get started with, confronted users with new concepts, and was slow: Connecting to the internet still required dial-up modems and download speeds were around 56kbps [114]. And, as the rise of Napster in 1999 showed, many regulatory issues at that time were unsolved [74]. Only over time, the technical infrastructure was improved, interaction models and design guidelines were developed, users' mental models adopted,

and legislation was introduced to settle disputes. This development led to more useful and usable applications being built on top of the Internet, which in turn resulted in more user growth and time being spent online [116].

Extrapolating from this analogy, cryptocurrencies find themselves in a somewhat comparable spot today. While the underlying infrastructure manages to support emerging use-cases, it is still evolving. The breath of different cryptocurrency and blockchain projects that have emerged over the past years and attracted substantial investments highlights that the field is still experimenting how to improve and overcome its existing limitations [26, 57]. As the recent downfall of Terra Luna showed [117], this experimentation will not proceed without some approaches failing. Ultimately only time will show which solutions will emerge successfully.

Reflecting on this larger development, the findings presented in this dissertation need to be viewed as a snapshot in time reflecting the usability of cryptocurrency applications in 2022. The results discussed in our publications point to many of the issues that require further research and development to enable more usable cryptocurrency applications in the future. The heterogeneity of challenges we found indicates that solutions to them will likely come from a variety of sources: technical innovations, design guidelines from within the HCI community, educational approaches, learning effects of users over time, and regulatory approaches. It further highlights the importance of the Human-Computer Interaction community to actively engage in the ongoing process of developing cryptocurrency technology by integrating the human-centered perspective into the discussion through both empirical, conceptual, and constructive approaches.

4.4 Concluding Remarks

The best way to predict the future is to create it.
Peter Drucker

History is littered with predictions about the success or demise of technologies that turned out to be spectacularly wrong (see e.g [128, 132]). While, with the power of hindsight, these past projections are an amusing reminder of the past, they also tell us that predicting the future is not an easy feat. History shows that extrapolating from today's use cases to predict which new applications may arise on top of emerging technologies is inherently difficult. When packet networks were developed in the 1960s [82] their creators probably did not think that one day their technology would enable instant video calls around the globe [116], web applications connecting billions of people [46], or robotic surgeries conducted by doctors in countries far apart [7, 11].

The public conversation surrounding cryptocurrencies today seems to be characterized by oscillating predictions about either their soon-to-expect spectacular downfall (e.g. [21]) or their breathtaking potential to challenge and overthrow existing financial systems (e.g. [92]). Reflecting on my learnings over the past four years, I believe a moderated view is more appropriate to foster a constructive discussion where the future of cryptocurrencies is headed. Cryptocurrencies today are rightfully criticized for many aspects along which they fall short: their usability, their environmental impact, their economic viability, and even their threat to established monetary systems. However, this criticism does not speak for the inadequacy of the technology itself but rather its early stage. There is the need for further research and development across disciplines. Only the interplay of technical, social,

and regulatory fields will move the space forward. As with any new technology, there are risks and opportunities that we just have started to understand. By practicing intellectual humility in exploring the tradeoffs surrounding the use of the technology, we will be able to shape cryptocurrencies to serve our society for the better.

I hope that the work presented in this dissertation contributes its humble part to this end and can serve as a foundation for future research and practice. If anything, it shows that the usability of cryptocurrencies is not fixed, but can be improved with user-centered methods: by better understanding users, working with them to prototype solutions, and iteratively testing and improving them. There are without doubt many questions and problems surrounding cryptocurrencies that are in need of answers moving forward. But if history has shown anything, then that there is no limit to human ingenuity. And while we cannot predict the future, we can proactively shape it.

List of Figures

List of Tables

REFERENCES

[1] Svetlana Abramova, Artemij Voskobojnikov, Konstantin Beznosov, and Rainer Böhme. "Bits Under the Mattress: Understanding Different Risk Perceptions and Security Behaviors of Crypto-Asset Users". In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. CHI '21. Association for Computing Machinery, 2021. DOI: 10.1145/3411764.3445679 (cited on pp. 5, 9, 10, 14–16, 20, 30, 32, 33).

[2] Marwa Alnasaa, Nikolay Gueorguiev, Jiro Honda, Eslem Imamoglu, Paolo Mauro, Keyra Primus, and Dmitriy Rozhkov. "Crypto, Corruption, and Capital Controls: Cross-Country Correlations". In: *Available at SSRN 4076356* (2022) (cited on p. 1).

[3] Abdulla Alshamsi and Prof. Peter Andras. "User perception of Bitcoin usability and security across novice users". In: *International Journal of Human-Computer Studies* 126 (2019), pp. 94–110. DOI: 10.1016/j.ijhcs.2019.02.004 (cited on pp. 1, 2, 5, 14, 22, 24).

[4] Florian Alt. "Out-of-the-Lab Research in Usable Security and Privacy". In: *Adjunct Proceedings of the 29th ACM Conference on User Modeling, Adaptation and Personalization*. Association for Computing Machinery, 2021, pp. 363–365 (cited on pp. 7, 8).

[5] Florian Alt and Emanuel von Zezschwitz. "Emerging Trends in Usable Security and Privacy". In: *i-com* 18.3 (2019), pp. 189–195. DOI: 10.1515/icom-2019-0019 (cited on p. 5).

[6] Marc Andreessen. Why Bitcoin Matters. 2014. URL: https://archive.nytimes.com/dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/ (visited on 07/18/2021) (cited on p. 1).

[7] Jumpei Arata, Hiroki Takahashi, Phongsaen Pitakwatchara, Shin'ichi Warisawa, Kazuo Tanoue, Kozo Konishi, Satoshi Ieiri, Shuji Shimizu, Naoki Nakashima, Koji Okamura, Yuichi Fujino, Yukihiro Ueda, Pornarong Chotiwan, Mamoru Mitsuishi, and Makoto Hashizume. "A remote surgery experiment between Japan and Thailand over Internet using a low latency CODEC system". In: *Proceedings 2007 IEEE International Conference on Robotics and Automation*. 2007, pp. 953–959. DOI: 10.1109/ROBOT.2007.363108 (cited on p. 37).

[8] Christiane Attig, Daniel Wessel, and Thomas Franke. "Assessing Personality Differences in Human-Technology Interaction: An Overview of Key Self-report Scales to Predict Successful Interaction". In: *HCI International 2017 – Posters' Extended Abstracts*. Ed. by Constantine Stephanidis. Springer International Publishing, 2017, pp. 19–29 (cited on p. 9).

[9] Raphael Auer, Jon Frost, Leonardo Gambacorta, Cyril Monnet, Tara Rice, and Hyun Song Shin. "Central Bank Digital Currencies: Motives, Economic Implications, and the Research Frontier". In: *Annual Review of Economics* 14.1 (2022), pp. 697–721. DOI: 10.1146/annurev-economics-051420-020324 (cited on p. 34).

[10] Andreas Auinger and René Riedl. “Blockchain and Trust: Refuting Some Widely-held Misconceptions”. In: *Proceedings of the International Conference on Information Systems - Bridging the Internet of People, Data, and Things, ICIS 2018, San Francisco, CA, USA, December 13-16, 2018*. 2018 (cited on p. 2).

[11] Patrick Barba, Joshua Stramiello, Emily K. Funk, Florian Richter, Michael C. Yip, and Ryan K. Orosco. “Remote telesurgery in humans: a systematic review”. In: *Surgical Endoscopy* 36.5 (2022), pp. 2771–2777. DOI: 10.1007/s00464-022-09074-4 (cited on p. 37).

[12] Davi Pedro Bauer. “Ethereum Name Service”. In: *Getting Started with Ethereum : A Step-by-Step Guide to Becoming a Blockchain Developer*. Apress, 2022, pp. 103–106. DOI: 10.1007/978-1-4842-8045-4_9 (cited on p. 35).

[13] Juan Benet. What Exactly is Web3? by Juan Benet at Web3 Summit 2018 (Video). 2018. URL: https://youtu.be/l44z35vabvA (visited on 02/11/2022) (cited on pp. 1, 35).

[14] Jeremiah Bohr and Masooda Bashir. “Who Uses Bitcoin? An exploration of the Bitcoin community”. In: *2014 Twelfth Annual International Conference on Privacy, Security and Trust*. 2014, pp. 94–101. DOI: 10.1109/PST.2014.6890928 (cited on p. 14).

[15] John Brooke. “SUS: a ’quick and dirty’ usability scale”. In: *Usability evaluation in industry* (1996), p. 189 (cited on pp. 9, 25).

[16] Michael Brown. The Top 5 Biggest Lost Bitcoin Fortunes (That We Know About). 2022. URL: https://www.cryptovantage.com/news/the-top-5-biggest-lost-bitcoin-fortunes-that-we-know-about/ (visited on 08/20/2022) (cited on p. 14).

[17] Vitalik Buterin et al. “Ethereum White Paper”. In: *GitHub Repository* 1 (2013), pp. 22–23 (cited on pp. 13, 34).

[18] John M. Carroll and Judith Reitman Olson. “Chapter 2 - Mental Models in Human-Computer Interaction”. In: *Handbook of Human-Computer Interaction*. Ed. by MARTIN HELANDER. North-Holland, 1988, pp. 45–65. DOI: 10.1016/B978-0-444-70536-5.50007-5 (cited on pp. 2, 14).

[19] Marina Cascaes Cardoso. “The Onboarding Effect: Leveraging User Engagement and Retention in Crowdsourcing Platforms”. In: *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. CHI EA ’17. Association for Computing Machinery, 2017, pp. 263–267. DOI: 10.1145/3027063.3027128 (cited on p. 24).

[20] Fran Casino, Thomas K. Dasaklis, and Constantinos Patsakis. “A systematic literature review of blockchain-based applications: Current status, classification and open issues”. In: *Telematics and Informatics* 36 (2019), pp. 55–81. DOI: 10.1016/j.tele.2018.11.006 (cited on p. 13).

[21] Orge Castellano. Why Bitcoin Is Doomed to Fail. 2018. URL: https://orge.medium.com/sorry-but-bitcoin-is-doomed-to-fail-heres-why-98d66d7f517f (visited on 08/20/2022) (cited on p. 37).

[22] David Chaum. “Blind Signatures for Untraceable Payments”. In: *Advances in Cryptology*. Ed. by David Chaum, Ronald L. Rivest, and Alan T. Sherman. Springer US, 1983, pp. 199–203 (cited on p. 14).

[23] Andrew Chen. New data shows losing 80% of mobile users is normal, and why the best apps do better. 2016. URL: https://andrewchen.co/new-data-shows-why-losing-80-of-your-mobile-users-is-normal-and-that-the-best-apps-do-much-better (visited on 01/31/2021) (cited on p. 24).

[24] Coinbase. Coinbase Third Quarter 2021 Shareholder Letter. 2021 (cited on pp. 1, 34, 36).

[25] Coinmarketcap. Total Cryptocurrency Market Cap. 2022. URL: https://coinmarketcap.com/charts/ (visited on 07/18/2021) (cited on p. 1).

[26] ConsenSys. Web 3 Report Q3 2021. ConsenSys. 2021. URL: https://consensys.net/reports/web3-report-q3-2021/ (visited on 02/11/2022) (cited on p. 37).

[27] Barnaby Craggs and Awais Rashid. "Trust Beyond Computation Alone: Human Aspects of Trust in Blockchain Technologies". In: *2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Society (ICSE-SEIS)*. 2019, pp. 21–30. DOI: 10.1109/ICSE-SEIS.2019.00011 (cited on p. 14).

[28] Lorrie Faith Cranor and Norbou Buchler. "Better Together: Usability and Security Go Hand in Hand". In: *IEEE Security & Privacy* 12.6 (2014), pp. 89–93. DOI: 10.1109/MSP.2014.109 (cited on p. 5).

[29] Cryptopedia Staff. The Blockchain Trilemma: Fast, Secure, and Scalable Networks. 2022. URL: https://www.gemini.com/cryptopedia/blockchain-trilemma-decentralization-scalability-definition (visited on 08/20/2022) (cited on p. 35).

[30] Norman Dalkey and Olaf Helmer. "An experimental application of the Delphi method to the use of experts". In: *Management science* 9.3 (1963), pp. 458–467 (cited on pp. 8, 20, 21).

[31] Fred D. Davis. "A technology acceptance model for empirically testing new end-user information systems: Theory and results". PhD thesis. Massachusetts Institute of Technology, 1985 (cited on pp. 4, 5, 28, 30, 31, 33).

[32] Fred D. Davis. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology". In: *MIS Quarterly* 13.3 (1989), pp. 319–340 (cited on pp. 4, 5, 28, 30, 31, 33).

[33] Fred D. Davis, Richard P. Bagozzi, and Paul R. Warshaw. "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models". In: *Management Science* 35.8 (1989), pp. 982–1003. DOI: 10.1287/mnsc.35.8.982 (cited on p. 4).

[34] Alex de Vries, Ulrich Gallersdörfer, Lena Klaaßen, and Christian Stoll. "Revisiting Bitcoin's carbon footprint". In: *Joule* 6.3 (2022), pp. 498–502. DOI: 10.1016/j.joule.2022.02.005 (cited on p. 1).

[35] Chris Dixon and Eddy Lazzarin. The Crypto Price-Innovation Cycle. Andreessen Horowitz. 2020. URL: https://a16z.com/2020/05/15/the-crypto-price-innovation-cycle/ (visited on 12/13/2021) (cited on pp. 1, 13).

[36] Susen Döbelt and Maria Kreußlein. "Peer-to-Peer Traded Energy: Prosumer and Consumer Focus Groups about a Self-consumption Community Scenario". In: *HCI International 2020 - Posters*. Ed. by Constantine Stephanidis and Margherita Antona. Communications in Computer and Information Science. Springer International Publishing, 2020, pp. 130–140. DOI: 10.1007/978-3-030-50726-8_17 (cited on p. 16).

[37] Dmitry Efanov and Pavel Roschin. “The all-pervasiveness of the blockchain technology”. In: *Procedia Computer Science* 123 (2018), pp. 116–121. DOI: 10.1016/j.procs.2018.01.019 (cited on p. 1).

[38] Chris Elsden, Inte Gloerich, Anne Spaa, John Vines, and Martijn de Waal. “Making the Blockchain Civic”. In: *Interactions* 26.2 (2019), pp. 60–65. DOI: 10.1145/3305364 (cited on p. 1).

[39] Chris Elsden, Arthi Manohar, Jo Briggs, Mike Harding, Chris Speed, and John Vines. “Making Sense of Blockchain Applications: A Typology for HCI”. In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, 2018, pp. 1–14. DOI: 10.1145/3173574.3174032 (cited on pp. 1, 2, 13).

[40] Chris Elsden, Bettina Nissen, Karim Jabbar, Reem Talhouk, Caitlin Lustig, Paul Dunphy, Chris Speed, and John Vines. “HCI for Blockchain: Studying, Designing, Critiquing and Envisioning Distributed Ledger Technologies”. In: *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*. CHI EA ’18. Association for Computing Machinery, 2018, pp. 1–8. DOI: 10.1145/3170427.3170602 (cited on p. 2).

[41] Shayan Eskandari, David Barrera, Elizabeth Stobert, and Jeremy Clark. “A First Look at the Usability of Bitcoin Key Management”. In: *Proceedings 2015 Workshop on Usable Security* (2015). DOI: 10.14722/usec.2015.23015 (cited on pp. 2, 10, 20, 30–33).

[42] Shayan Eskandari, Jeremy Clark, and Abdelwahab Hamou-Lhadj. “Buy Your Coffee with Bitcoin: Real-World Deployment of a Bitcoin Point of Sale Terminal”. In: *2016 Intl IEEE Conferences on Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*. 2016, pp. 382–389. DOI: 10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0073 (cited on p. 32).

[43] ethereum.org. The Merge. 2022. URL: https://ethereum.org/en/upgrades/merge/ (visited on 08/20/2022) (cited on p. 35).

[44] Michael Fagan and Mohammad Maifi Hasan Khan. “Why Do They Do What They Do?: A Study of What Motivates Users to (Not) Follow Computer Security Advice”. In: *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, 2016, pp. 59–75 (cited on p. 5).

[45] Youssef Faqir-Rhazoui, Miller-Janny Ariza-Garzón, Javier Arroyo, and Samer Hassan. “Effect of the Gas Price Surges on User Activity in the DAOs of the Ethereum Blockchain”. In: *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, 2021. DOI: 10.1145/3411763.3451755 (cited on p. 31).

[46] G. Fauville, M. Luo, A.C.M. Queiroz, J.N. Bailenson, and J. Hancock. “Zoom Exhaustion & Fatigue Scale”. In: *Computers in Human Behavior Reports* 4 (2021), p. 100119. DOI: 10.1016/j.chbr.2021.100119 (cited on p. 37).

[47] Ahmad Firdaus, Mohd Faizal Ab Razak, Ali Feizollah, Ibrahim Abaker Targio Hashem, Mohamad Hazim, and Nor Badrul Anuar. “The rise of blockchain: bibliometric analysis of blockchain study”. In: *Scientometrics* 120.3 (2019), pp. 1289–1331. DOI: 10.1007/s11192-019-03170-4 (cited on p. 15).

[48] Daniel Folkinshteyn and Mark Lennon. “Braving Bitcoin: A technology acceptance model (TAM) analysis”. In: *Journal of Information Technology Case and Application Research* 18.4 (2016), pp. 220–249. DOI: 10.1080/15228053.2016.1275242 (cited on pp. 4, 5, 30, 31).

[49] Marcus Foth. “The Promise of Blockchain Technology for Interaction Design”. In: *Proceedings of the 29th Australian Conference on Computer-Human Interaction*. OZCHI ’17. Association for Computing Machinery, 2017, pp. 513–517. DOI: 10.1145/3152771.3156168 (cited on pp. 2, 13).

[50] FIO Foundation. Blockchain Usability Report. 2018. URL: https://fioprotocol.io/blockchain-usability-report-2019 (visited on 09/20/2022) (cited on p. 13).

[51] Thomas Franke, Christiane Attig, and Daniel Wessel. “A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale”. In: *International Journal of Human–Computer Interaction* 35.6 (2019), pp. 456–467. DOI: 10.1080/10447318.2018.1456150 (cited on p. 9).

[52] C. Ailie Fraser, Mira Dontcheva, Holger Winnemöller, Sheryl Ehrlich, and Scott Klemmer. “DiscoverySpace: Suggesting Actions in Complex Software”. In: *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*. DIS ’16. Association for Computing Machinery, 2016, pp. 1221–1232. DOI: 10.1145/2901790.2901849 (cited on p. 24).

[53] Ulrich Gallersdörfer, Lena Klaaßen, and Christian Stoll. “Energy Consumption of Cryptocurrencies Beyond Bitcoin”. In: *Joule* 4.9 (2020), pp. 1843–1846. DOI: 10.1016/j.joule.2020.07.013 (cited on p. 1).

[54] Xianyi Gao, Gradeigh D. Clark, and Janne Lindqvist. “Of Two Minds, Multiple Addresses, and One Ledger: Characterizing Opinions, Knowledge, and Perceptions of Bitcoin Across Users and Non-Users”. In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. CHI ’16. Association for Computing Machinery, 2016, pp. 1656–1668. DOI: 10.1145/2858036.2858049 (cited on pp. 14, 22).

[55] Martin Garriga, Stefano Dalla Palma, Maxmiliano Arias, Alan De Renzis, Remo Pareschi, and Damian Andrew Tamburri. “Blockchain and cryptocurrencies: A classification and comparison of architecture drivers”. In: *Concurrency and Computation: Practice and Experience* 33.8 (2021), e5992. DOI: 10.1002/cpe.5992 (cited on p. 34).

[56] Leonhard Glomann, Maximilian Schmid, and Nika Kitajewa. “Improving the Blockchain User Experience - An Approach to Address Blockchain Mass Adoption Issues from a Human-Centred Perspective”. In: *Advances in Artificial Intelligence, Software and Systems Engineering*. Ed. by Tareq Ahram. Advances in Intelligent Systems and Computing. Springer International Publishing, 2020, pp. 608–616. DOI: 10.1007/978-3-030-20454-9_60 (cited on pp. 2, 5, 10, 13, 14, 24, 30).

[57] Kim Grauer, Will Kueshner, Ethan McMahon, and Henry Updegrave. The Chainalysis State of Web3 Report. 2022. URL: https://go.chainalysis.com/2022-web3-report.html (visited on 09/20/2022) (cited on pp. 13, 34, 37).

[58] Kim Grauer, Will Kueshner, and Henry Updegrave. The 2022 Crypto Crime Report. 2022. URL: https://go.chainalysis.com/2022-Crypto-Crime-Report.html (visited on 08/20/2022) (cited on pp. 1, 14).

[59] Aurora Harley. Instructional Overlays and Coach Marks for Mobile Apps. 2014. URL: https://www.nngroup.com/articles/mobile-instructional-overlay/ (visited on 01/11/2021) (cited on p. 24).

[60] Kasper Hornbæk and Morten Hertzum. "Technology Acceptance and User Experience: A Review of the Experiential Component in HCI". In: *ACM Trans. Comput.-Hum. Interact.* 24.5 (2017). DOI: 10.1145/3127358 (cited on p. 4).

[61] Huawei Huang, Wei Kong, Sicong Zhou, Zibin Zheng, and Song Guo. "A Survey of State-of-the-Art on Blockchains: Theories, Modelings, and Tools". In: *ACM Comput. Surv.* 54.2 (2021). DOI: 10.1145/3441692 (cited on p. 13).

[62] Johannes Huebner, Remo Manuel Frey, Christian Ammendola, Elgar Fleisch, and Alexander Ilic. "What People Like in Mobile Finance Apps: An Analysis of User Reviews". In: *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia*. MUM 2018. Association for Computing Machinery, 2018, pp. 293–304. DOI: 10.1145/3282894.3282895 (cited on pp. 5, 33).

[63] Hyeji Jang, Sung H. Han, Ju Hwan Kim, and Kimin Kwon. "Usability Evaluation for Cryptocurrency Exchange". In: *Convergence of Ergonomics and Design*. Ed. by Alma Maria Jennifer Gutierrez, Ravindra S. Goonetilleke, and Rex Aurellius C. Robielos. Advances in Intelligent Systems and Computing. Springer International Publishing, 2021, pp. 192–196. DOI: 10.1007/978-3-030-63335-6_20 (cited on p. 14).

[64] Ger Joyce, Mariana Lilley, Trevor Barker, and Amanda Jefferies. "Mobile application tutorials: perception of usefulness from an HCI expert perspective". In: *International Conference on Human-Computer Interaction*. Springer. 2016, pp. 302–308 (cited on p. 24).

[65] Ali Kazerani, Domenic Rosati, and Brian Lesser. "Determining the Usability of Bitcoin for Beginners Using Change Tip and Coinbase". In: *Proceedings of the 35th ACM International Conference on the Design of Communication*. SIGDOC '17. Association for Computing Machinery, 2017. DOI: 10.1145/3121113.3121125 (cited on pp. 14, 22).

[66] Denisa Reshef Kera, Petr Šourek, Mateusz Kraiński, Yair Reshef, Juan Manuel Corchado Rodríguez, and Iva Magdalena Knobloch. "Lithopia: Prototyping Blockchain Futures". In: *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. CHI EA '19. Association for Computing Machinery, 2019, pp. 1–6. DOI: 10.1145/3290607.3312896 (cited on p. 1).

[67] Evan Kereiakes, Marco Di Maggio Do Kwon, and Nicholas Platias. Terra money: Stability and adoption. 2019. URL: https://assets.website-files.com/611153e7af981472d8da199c/618b02d13e938ae1f8ad1e45_Terra_White_paper.pdf (visited on 09/20/2022) (cited on p. 13).

[68] Irni Eliana Khairuddin, Corina Sas, Sarah Clinch, and Nigel Davies. "Exploring Motivations for Bitcoin Technology Usage". In: *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. CHI EA '16. Association for Computing Machinery, 2016, pp. 2872–2878. DOI: 10.1145/2851581.2892500 (cited on pp. 14, 15).

[69] Jake Knapp, John Zeratsky, and Braden Kowitz. Sprint: How to solve big problems and test new ideas in just five days. Simon and Schuster, 2016 (cited on pp. 9, 28).

[70] Megan Knittel, Shelby Pitts, and Rick Wash. “"The Most Trustworthy Coin": How Ideological Tensions Drive Trust in Bitcoin”. In: *Proc. ACM Hum.-Comput. Interact.* 3.CSCW (2019). DOI: 10.1145/3359138 (cited on p. 14).

[71] Megan L. Knittel and Rick Wash. “How "True Bitcoiners" Work on Reddit to Maintain Bitcoin”. In: *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. CHI EA ’19. Association for Computing Machinery, 2019, pp. 1–6. DOI: 10.1145/3290607.3312969 (cited on p. 14).

[72] Jennifer Korn. Report: $1.9 billion stolen in crypto hacks so far this year. 2022. URL: https://edition.cnn.com/2022/08/16/tech/crypto-hack-rise-2022/index.html (visited on 08/20/2022) (cited on p. 14).

[73] Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer, and Edgar Weippl. “The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy”. In: *Financial Cryptography and Data Security*. Ed. by Jens Grossklags and Bart Preneel. Lecture Notes in Computer Science. Springer, 2017, pp. 555–580. DOI: 10.1007/978-3-662-54970-4_33 (cited on pp. 14, 20, 26).

[74] Raymond Shih Ray Ku. “The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology”. In: *The University of Chicago Law Review* 69.1 (2002). Full publication date: Winter, 2002, pp. 263–324. DOI: 10.2307/1600355 (cited on p. 36).

[75] Larry Laudan. Progress and its problems: Towards a theory of scientific growth. Vol. 282. Univ of California Press, 1978 (cited on p. 11).

[76] Bettina Laugwitz, Theo Held, and Martin Schrepp. “Construction and evaluation of a user experience questionnaire”. In: *Symposium of the Austrian HCI and usability engineering group*. Springer. 2008, pp. 63–76 (cited on p. 9).

[77] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. Research methods in human-computer interaction. Morgan Kaufmann, 2017 (cited on p. 8).

[78] Dylan Leclair and Sam Rule. The Ethereum Merge: Risks, Flaws and the Pitfalls of Centralization. 2022. URL: https://bitcoinmagazine.com/business/centralization-risks-and-flaws-of-ethereum-merge (visited on 08/20/2022) (cited on p. 35).

[79] Ming-Chi Lee. “Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit”. In: *Electronic Commerce Research and Applications* 8.3 (2009), pp. 130–141. DOI: 10.1016/j.elerap.2008.11.006 (cited on p. 5).

[80] Valentino Lee, Heather Schneider, and Robbie Schell. Mobile applications: architecture, design, and development. Prentice Hall PTR, 2004 (cited on p. 24).

[81] Wei-Meng Lee. “Using the MetaMask Chrome Extension”. In: *Beginning Ethereum Smart Contracts Programming: With Examples in Python, Solidity, and JavaScript*. Apress, 2019, pp. 93–126. DOI: 10.1007/978-1-4842-5086-0_5 (cited on p. 35).

[82] Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. “A Brief History of the Internet”. In: *SIGCOMM Comput. Commun. Rev.* 39.5 (2009), pp. 22–31. DOI: 10.1145/1629607.1629613 (cited on pp. 1, 15, 37).

[83] Markus Lennartsson, Joakim Kävrestad, and Marcus Nohlberg. “Exploring the meaning of usable security – a literature review”. In: *Information & Computer Security* 29.4 (2021), pp. 647–663. DOI: 10.1108/ICS-10-2020-0167 (cited on p. 5).

[84] Liberlion. Global Crypto Adoption: Between Profit and Usability. 2022. URL: https://adapulse.io/global-crypto-adoption-between-profit-and-usability/ (visited on 08/15/2022) (cited on p. 13).

[85] Sin Kuang Lo, Xiwei Xu, Yin Kia Chiam, and Qinghua Lu. “Evaluating Suitability of Applying Blockchain”. In: *2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS)*. 2017, pp. 158–161. DOI: 10.1109/ICECCS.2017.26 (cited on pp. 5, 33).

[86] Mark Lochrie, Glenn Matthys, Adrian Gradinar, Andy Dickinson, Onno Baudouin, and Paul Egglestone. “Co-Designing a Physical to Digital Experience for an Onboarding and Blended Learning Platform”. In: *Proceedings of the The 15th International Conference on Interaction Design and Children*. IDC ’16. Association for Computing Machinery, 2016, pp. 660–665. DOI: 10.1145/2930674.2936002 (cited on p. 24).

[87] Taylor Locke. Mark Cuban on blockchain: It’s like the early days of the internet when a lot of people thought we were crazy. 2021. URL: https://www.cnbc.com/2021/02/12/mark-cuban-compares-blockchain-crypto-to-early-days-of-the-internet.html (visited on 07/18/2021) (cited on p. 1).

[88] William J. Luther. “CRYPTOCURRENCIES, NETWORK EFFECTS, AND SWITCHING COSTS”. In: *Contemporary Economic Policy* 34.3 (2016), pp. 553–571. DOI: 10.1111/coep.12151 (cited on p. 31).

[89] Daniel C. Lynch and Leslie Lundquist. Digital Money: The New Era of Internet Commerce. John Wiley & Sons, Inc., 1996 (cited on p. 14).

[90] Alexandra Mai, Katharina Pfeffer, Matthias Gusenbauer, Edgar Weippl, and Katharina Krombholz. “User Mental Models of Cryptocurrency Systems - A Grounded Theory Approach”. In: *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, 2020, pp. 341–358 (cited on pp. 2, 14, 30, 33).

[91] Scott Mainwaring, Wendy March, and Bill Maurer. “From Meiwaku to Tokushita! Lessons for Digital Money Design from Japan”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’08. Association for Computing Machinery, 2008, pp. 21–24. DOI: 10.1145/1357054.1357058 (cited on p. 14).

[92] Ilia Maksimenka. DeFi is the future of banking that humanity deserves. 2021. URL: https://cointelegraph.com/news/defi-is-the-future-of-banking-that-humanity-deserves (visited on 08/20/2022) (cited on p. 37).

[93] Nikola Marangunić and Andrina Granić. “Technology acceptance model: a literature review from 1986 to 2013”. In: *Universal Access in the Information Society* 14.1 (2015), pp. 81–95. DOI: 10.1007/s10209-014-0348-1 (cited on p. 4).

[94] Ignasi Merediz-Solà and Aurelio F. Bariviera. “A bibliometric analysis of bitcoin scientific production”. In: *Research in International Business and Finance* 50 (2019), pp. 294–305. DOI: 10.1016/j.ribaf.2019.06.008 (cited on p. 15).

[95] Eva Meyer, Isabell M Welpe, and Philipp G Sandner. "Decentralized Finance—A systematic literature review and research directions". In: *Available at SSRN 4016497* (2021). DOI: 10.2139/ssrn.4016497 (cited on pp. 13, 35).

[96] Alistair Milne. "What is in it for us? Network effects and bank payment innovation". In: *Journal of Banking & Finance* 30.6 (2006). Frontiers in Payment and Settlement Systems, pp. 1613–1630. DOI: 10.1016/j.jbankfin.2005.09.006 (cited on p. 31).

[97] Makiko Mita, Kensuke Ito, Shohei Ohsawa, and Hideyuki Tanaka. "What is Stablecoin?: A Survey on Price Stabilization Mechanisms for Decentralized Payment Systems". In: *2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI)*. 2019, pp. 60–66. DOI: 10.1109/IIAI-AAI.2019.00023 (cited on p. 34).

[98] David Moher, Larissa Shamseer, Mike Clarke, Davina Ghersi, Alessandro Liberati, Mark Petticrew, Paul Shekelle, and Lesley A Stewart. "Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement". In: *Systematic reviews* 4.1 (2015), pp. 1–9 (cited on p. 7).

[99] Md Moniruzzaman, Farida Chowdhury, and Md Sadek Ferdous. "Examining Usability Issues in Blockchain-Based Cryptocurrency Wallets". In: *Cyber Security and Computer Science*. Ed. by Touhid Bhuiyan, Md. Mostafijur Rahman, and Md. Asraf Ali. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer International Publishing, 2020, pp. 631–643. DOI: 10.1007/978-3-030-52856-0_50 (cited on pp. 5, 13, 14, 22, 24, 32).

[100] Gianmaria Del Monte, Diego Pennino, and Maurizio Pizzonia. "Scaling Blockchains without Giving up Decentralization and Security: A Solution to the Blockchain Scalability Trilemma". In: *Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems*. CryBlock '20. Association for Computing Machinery, 2020, pp. 71–76. DOI: 10.1145/3410699.3413800 (cited on p. 35).

[101] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008. URL: https://bitcoin.org/bitcoin.pdf (visited on 09/20/2022) (cited on pp. 13–15, 18, 26, 34).

[102] Adeel Nasir, Kamran Shaukat, Kanwal Iqbal Khan, Ibrahim A. Hameed, Talha Mahboob Alam, and Suhuai Luo. "What is Core and What Future Holds for Blockchain Technologies and Cryptocurrencies: A Bibliometric Analysis". In: *IEEE Access* 9 (2021), pp. 989–1004. DOI: 10.1109/ACCESS.2020.3046931 (cited on p. 15).

[103] Pranav Nerurkar, Dhiren Patel, Yann Busnel, Romaric Ludinard, Saru Kumari, and Muhammad Khurram Khan. "Dissecting bitcoin blockchain: Empirical analysis of bitcoin network (2009–2020)". In: *Journal of Network and Computer Applications* 177 (2021), p. 102940. DOI: 10.1016/j.jnca.2020.102940 (cited on p. 15).

[104] Jakob Nielsen. Progressive Disclosure. 2006. URL: https://www.nngroup.com/articles/progressive-disclosure/ (visited on 08/11/2022) (cited on p. 33).

[105] Don Norman. The design of everyday things: Revised and expanded edition. Basic books, 2013 (cited on pp. 15, 16, 32).

[106] Alex Norta, Benjamin Leiding, and Alexi Lane. "Lowering Financial Inclusion Barriers with a Blockchain-Based Capital Transfer System". In: *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2019, pp. 319–324. DOI: 10.1109/INFCOMW.2019.8845177 (cited on p. 1).

[107] Antti Oulasvirta and Kasper Hornbæk. “HCI Research as Problem-Solving”. In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. CHI ’16. Association for Computing Machinery, 2016, pp. 4956–4967. DOI: 10.1145/2858036.2858283 (cited on pp. 9, 11, 14).

[108] Marek Palatinus, Pavlov Rusnak, Aaron Voisine, and Sean Bowe. BIP 39: Mnemonic code for generating deterministic keys. 2013. URL: https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki (visited on 09/20/2022) (cited on p. 30).

[109] Paul A. Pavlou. “Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model”. In: *International Journal of Electronic Commerce* 7.3 (2003), pp. 101–134. DOI: 10.1080/10864415.2003.11044275 (cited on pp. 4, 5, 30).

[110] Falko Weigert Petersen, Line Ebdrup Thomsen, Pejman Mirza-Babaei, and Anders Drachen. “Evaluating the Onboarding Phase of Free-ToPlay Mobile Games: A Mixed-Method Approach”. In: *Proceedings of the Annual Symposium on Computer-Human Interaction in Play*. CHI PLAY ’17. Association for Computing Machinery, 2017, pp. 377–388. DOI: 10.1145/3116595.3125499 (cited on p. 24).

[111] Ingrid Pettersson, Florian Lachner, Anna-Katharina Frison, Andreas Riener, and Andreas Butz. “A Bermuda Triangle? A Review of Method Application and Triangulation in User Experience Evaluation”. In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, 2018, pp. 1–16. DOI: 10.1145/3173574.3174035 (cited on pp. 8, 22).

[112] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments. 2016. URL: https://www.bitcoinlightning.com/wp-content/uploads/2018/03/lightning-network-paper.pdf (visited on 09/20/2022) (cited on p. 26).

[113] Eveshnie Reddy and Anthony Minnaar. “Cryptocurrency: a tool and target for cybercrime”. In: *Acta Criminologica: African Journal of Criminology & Victimology* 31.3 (2018), pp. 71–92 (cited on p. 21).

[114] Phillip Remaker. What was the Internet like in 1998? 2022. URL: https://www.quora.com/What-was-the-Internet-like-in-1998/answer/Phillip-Remaker (visited on 08/20/2022) (cited on p. 36).

[115] Axel Roesler. “Lessons from Three Mile Island: The Design of Interactions in a High-Stakes Environment”. In: *Visible Language* 43.2/3 (2009), p. 169 (cited on pp. 5, 14).

[116] Max Roser, Hannah Ritchie, and Esteban Ortiz-Ospina. Internet. 2015. URL: https://ourworldindata.org/internet (visited on 09/20/2022) (cited on p. 37).

[117] Qihong Ruan. “Systemic Risks in Financial Networks Under Strategic Attacks”. In: *Available at SSRN 4180984* (2022). DOI: 10.2139/ssrn.4180984 (cited on p. 37).

[118] Muhammad Saad, Jeffrey Spaulding, Laurent Njilla, Charles Kamhoua, Sachin Shetty, Dae-Hun Nyang, and Aziz Mohaisen. “Exploring the attack surface of blockchain: A systematic overview”. In: *arXiv preprint arXiv:1904.03487* (2019) (cited on p. 21).

[119] J.H. Saltzer and M.D. Schroeder. “The protection of information in computer systems”. In: *Proceedings of the IEEE* 63.9 (1975), pp. 1278–1308. DOI: 10.1109/PROC.1975.9939 (cited on p. 5).

[120] Corina Sas and Irni Eliana Khairuddin. “Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users”. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. CHI ’17. Association for Computing Machinery, 2017, pp. 6499–6510. DOI: 10.1145/3025453.3025886 (cited on pp. 2, 4, 14, 15).

[121] Corina Sas and Irni Eliana Khairuddin. “Exploring Trust in Bitcoin Technology: A Framework for HCI Research”. In: *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction*. OzCHI ’15. Association for Computing Machinery, 2015, pp. 338–342. DOI: 10.1145/2838739.2838821 (cited on pp. 2, 4, 14, 15).

[122] Brett Scott. How can cryptocurrency and blockchain technology play a role in building social and solidarity finance? UNRISD Working Paper 2016-1. 2016 (cited on p. 1).

[123] Sabrina Scuri, Gergana Tasheva, Luísa Barros, and Nuno Jardim Nunes. “An HCI Perspective on Distributed Ledger Technologies for Peer-to-Peer Energy Trading”. In: *Human-Computer Interaction – INTERACT 2019*. Ed. by David Lamas, Fernando Loizides, Lennart Nacke, Helen Petrie, Marco Winckler, and Panayiotis Zaphiris. Lecture Notes in Computer Science. Springer International Publishing, 2019, pp. 91–111. DOI: 10.1007/978-3-030-29387-1_6 (cited on p. 16).

[124] Maria Shen and Avichal Garg. Developer Report 2021. Electric Capital. 2022. URL: https://github.com/electric-capital/developer-reports/blob/master/dev_report_2021_updated_012622.pdf (visited on 02/11/2022) (cited on pp. 1, 13, 36).

[125] Ben Shneiderman, Catherine Plaisant, Maxine S Cohen, Steven Jacobs, Niklas Elmqvist, and Nicholas Diakopoulos. Designing the user interface: strategies for effective human-computer interaction. Pearson, 2016 (cited on p. 32).

[126] MacKenzie Sigalos. El Salvador looks to become the world’s first country to adopt bitcoin as legal tender. 2021. URL: https://www.cnbc.com/2021/06/05/el-salvador-becomes-the-first-country-to-adopt-bitcoin-as-legal-tender-.html (visited on 04/03/2022) (cited on p. 34).

[127] Sebastian Sinclair. EUs Crypto Bill in Monday Vote Without Proof-of-work Ban. 2022. URL: https://blockworks.co/eus-crypto-bill-mica-heads-to-a-monday-vote-without-proof-of-work-ban/ (visited on 07/20/2022) (cited on p. 1).

[128] Graham Singer and Julio Franco. In Hindsight... Tech Predictions and Quotes. 2021. URL: https://www.techspot.com/article/754-tech-predictions-and-quotes/ (visited on 08/20/2022) (cited on p. 37).

[129] Ana Sousa, Eva Calcada, Paula Rodrigues, and Ana Pinto Borges. “Cryptocurrency adoption: a systematic literature review and bibliometric analysis”. In: *EuroMed Journal of Business* 17.3 (2022), pp. 374–390. DOI: 10.1108/EMJB-01-2022-0003 (cited on p. 15).

[130] Christian Stoll, Lena Klaaßen, and Ulrich Gallersdörfer. “The Carbon Footprint of Bitcoin”. In: *Joule* 3.7 (2019), pp. 1647–1661. DOI: 10.1016/j.joule.2019.05.012 (cited on p. 1).

[131] Brendan Strahm, Colin M. Gray, and Mihaela Vorvoreanu. “Generating Mobile Application Onboarding Insights Through Minimalist Instruction”. In: *Proceedings of the 2018 Designing Interactive Systems Conference*. DIS ’18. Association for Computing Machinery, 2018, pp. 361–372. DOI: 10.1145/3196709.3196727 (cited on pp. 24, 25).

[132] Robert Strohmeyer. The 7 Worst Tech Predictions of All Time. 2009. URL: https://abcnews.go.com/Technology/PCWorld/story?id=6558231 (visited on 08/20/2022) (cited on p. 37).

[133] Melanie Swan. Blockchain: Blueprint for a New Economy. 1st. O'Reilly Media, Inc., 2015 (cited on p. 1).

[134] Ella Tallyn, Larissa Pschetz, Rory Gianni, Chris Speed, and Chris Elsden. "Exploring Machine Autonomy and Provenance Data in Coffee Consumption: A Field Study of Bitbarista". In: *Proc. ACM Hum.-Comput. Interact.* 2.CSCW (2018). DOI: 10.1145/3274439 (cited on p. 16).

[135] Ella Tallyn, Joe Revans, Evan Morgan, and Dave Murray-Rust. "GeoPact: Engaging Publics in Location-Aware Smart Contracts through Technological Assemblies". In: *Proceedings of the 2020 ACM Designing Interactive Systems Conference*. Association for Computing Machinery, 2020, pp. 799–811. DOI: 10.1145/3357236.3395583 (cited on p. 16).

[136] Fabian Maximilian Johannes Teichmann and Marie-Christin Falker. "Cryptocurrencies and financial crime: solutions from Liechtenstein". In: *Journal of Money Laundering Control* 24.4 (2021), pp. 775–788. DOI: 10.1108/JMLC-05-2020-0060 (cited on p. 1).

[137] Kyle Torpey. These DApps Don't Need a Blockchain. 2018. URL: https://coinjournal.net/news/these-dapps-dont-need-a-blockchain/ (cited on p. 5).

[138] Ludwig Trotter, Mike Harding, Chris Elsden, Nigel Davies, and Chris Speed. "A Mobile Platform for Event-Driven Donations Using Smart Contracts". In: *Proceedings of the 21st International Workshop on Mobile Computing Systems and Applications*. HotMobile '20. Association for Computing Machinery, 2020, p. 108. DOI: 10.1145/3376897.3379161 (cited on p. 16).

[139] Ludwig Trotter, Mike Harding, Peter Shaw, Nigel Davies, Chris Elsden, Chris Speed, John Vines, Aydin Abadi, and Josh Hallwright. "Smart Donations: Event-Driven Conditional Donations Using Smart Contracts On The Blockchain". In: *32nd Australian Conference on Human-Computer Interaction*. OzCHI '20. Association for Computing Machinery, 2020, pp. 546–557. DOI: 10.1145/3441000.3441014 (cited on p. 16).

[140] Inc. Upland Software. 21% of Users Abandon an App After One Use. 2021. URL: https://uplandsoftware.com/localytics/resources/blog/21-percent-of-users-abandon-apps-after-one-use (cited on p. 24).

[141] Andrew Urquhart and Brian Lucey. Crypto and digital currencies—nine research priorities. 2022. DOI: 10.1038/d41586-022-00927-5 (cited on pp. 1, 2, 10, 33).

[142] Hans Van der Meij. "Principles and heuristics for designing minimalist instruction". In: *Technical communication* 42.2 (1995), pp. 243–261 (cited on p. 24).

[143] Barbara Van Schewick. Internet architecture and innovation. Mit Press, 2012. DOI: 10.7551/mitpress/7580.001.0001 (cited on p. 1).

[144] Olusegun Vincent and Olaniyi Evans. "Can cryptocurrency, mobile phones, and internet herald sustainable financial sector development in emerging markets?" In: *Journal of Transnational Management* 24.3 (2019), pp. 259–279. DOI: 10.1080/15475778.2019.1633170 (cited on p. 1).

[145] Visa Inc. Visa Factsheet. 2018. URL: https://www.visa.co.uk/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf (visited on 07/18/2021) (cited on pp. 1, 13).

[146] Artemij Voskobojnikov, Svetlana Abramova, Konstantin Beznosov, and Rainer Boehme. "Non-Adoption of Crypto-Assets: Exploring the Role of Trust, Self-Efficacy, and Risk". In: *ECIS 2021 Research Papers* 9 (2021) (cited on pp. 14, 20).

[147] Artemij Voskobojnikov, Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. "Surviving the Cryptojungle: Perception and Management of Risk Among North American Cryptocurrency (Non)Users". In: *Financial Cryptography and Data Security*. Ed. by Joseph Bonneau and Nadia Heninger. Springer International Publishing, 2020, pp. 595–614 (cited on pp. 2, 5, 13, 14, 31).

[148] Artemij Voskobojnikov, Oliver Wiese, Masoud Mehrabi Koushki, Volker Roth, and Konstantin (Kosta) Beznosov. "The U in Crypto Stands for Usable: An Empirical Study of User Experience with Mobile Cryptocurrency Wallets". In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. CHI '21. Association for Computing Machinery, 2021. DOI: 10.1145/3411764.3445407 (cited on pp. 2, 5, 10, 13–16, 20, 22, 30, 32, 33).

[149] Qin Wang, Rujia Li, Qi Wang, and Shiping Chen. "Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges". In: *CoRR* abs/2105.07447 (2021). arXiv: 2105.07447 (cited on pp. 13, 35).

[150] Shuai Wang, Wenwen Ding, Juanjuan Li, Yong Yuan, Liwei Ouyang, and Fei-Yue Wang. "Decentralized Autonomous Organizations: Concept, Model, and Applications". In: *IEEE Transactions on Computational Social Systems* 6.5 (2019), pp. 870–878. DOI: 10.1109/TCSS.2019.2938190 (cited on pp. 13, 35).

[151] Finnegan Waugh and Ralph Holz. "An empirical study of availability and reliability properties of the Bitcoin Lightning Network". In: *CoRR* abs/2006.14358 (2020). arXiv: 2006.14358 (cited on p. 26).

[152] Alma Whitten and J. D. Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0". In: *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*. SSYM'99. USENIX Association, 1999, p. 14 (cited on p. 2).

[153] Jacob O. Wobbrock and Julie A. Kientz. "Research Contributions in Human-Computer Interaction". In: *Interactions* 23.3 (2016), pp. 38–44. DOI: 10.1145/2907069 (cited on p. 14).

[154] Gavin Wood. Polkadot: Vision for a heterogeneous multi-chain framework. 2016. URL: https://polkadot.network/PolkaDotPaper.pdf (visited on 09/20/2022) (cited on p. 13).

[155] Turner Wright. Crypto user who lost $163M in Bitcoin wants to deploy robot search party — Report. 2022. URL: https://cointelegraph.com/news/crypto-user-who-lost-163m-in-bitcoin-wants-to-deploy-robot-search-party-report (visited on 08/20/2022) (cited on p. 14).

[156] Pieter Wuille. BIP32: Hierarchical Deterministic Wallets. 2013. URL: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki (visited on 01/05/2020) (cited on p. 30).

[157] Karl Wüst and Arthur Gervais. “Do you Need a Blockchain?” In: *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. 2018, pp. 45–54. DOI: 10.1109/CVCBT.2018.00011 (cited on pp. 5, 33).

[158] Anatoly Yakovenko. Solana: A new architecture for a high performance blockchain v0. 8.13. 2018. URL: https://solana.com/solana-whitepaper.pdf (visited on 09/20/2022) (cited on p. 13).

[159] Philipp Zabka, Klaus-T. Foerster, Stefan Schmid, and Christian Decker. “Empirical evaluation of nodes and channels of the lightning network”. In: *Pervasive and Mobile Computing* (2022), p. 101584. DOI: 10.1016/j.pmcj.2022.101584 (cited on p. 26).

[160] Rui Zhang, Rui Xue, and Ling Liu. “Security and Privacy on Blockchain”. In: *ACM Comput. Surv.* 52.3 (2019). DOI: 10.1145/3316481 (cited on p. 13).

APPENDIX: ORIGINAL PUBLICATIONS

This appendix includes all contributing publications of this thesis in their original format without any modifications (except page numeration) in chronological order.

Don't Lose Your Coin! Investigating Security Practices of Cryptocurrency Users

Michael Fröhlich[1,2], **Felix Gutjahr**[3], **Florian Alt**[1]
[1]Bundeswehr University / Research Institute CODE, Munich, Germany, {firstname.lastname}@unibw.de
[2]CDTM, Munich, Germany, {lastname}@cdtm.de
[3]LMU Munich / Media Informatics Group, Munich, Germany, {firstname.lastname}@campus.lmu.de

ABSTRACT
In recent years, cryptocurrencies have increasingly gained interest. The underlying technology, Blockchain, shifts the responsibility for securing assets to the end-user and requires them to manage their (private) keys. Little attention has been given to how cryptocurrency users handle the challenges of key management in practice and how they select the tools to do so. To close this gap, we conducted semi-structured interviews (N=10). Our thematic analysis revealed prominent themes surrounding motivation, risk assessment, and coin management tool usage in practice. We found that the choice of tools is driven by how users assess and balance the key risks that can lead to loss: the risk of (1) human error, (2) betrayal, and (3) malicious attacks. We derive a model, explaining how risk assessment and intended usage drive the decision which tools to use. Our work is complemented by discussing design implications for building systems for the crypto economy.

Author Keywords
usable security, blockchain, cryptocurrency, key management

CCS Concepts
•**Security and privacy** → **Usability in security and privacy;**

INTRODUCTION
Driven by the rise in popularity of cryptocurrencies, Blockchain technology is receiving increased interest from practitioners and researchers alike. By the end of 2019, the number of wallet users has grown to exceed 42 million [49]. A total of 4993 cryptocurrencies are tracked on http://coinmarketcap.com/, with a combined market capitalization exceeding 195 billion USD. Despite the large body of alternative coins, Bitcoin [42] remains by far the most widespread cryptocurrency, with a market capitalization of 130 billion USD [15].

While cryptocurrencies remain the predominant application of Blockchain technology, there is considerable ongoing development in both industry and research. Advocates of blockchain view the technology as potentially transformative [21]. Swan discusses three stages of blockchain evolution: Blockchain 1.0 as digital currency, Blockchain 2.0 as digital economy, and Blockchain 3.0 as digital society [48]. Efanov and Roschin discuss the all-pervasive impact of blockchain technology and propose use cases in the fields of art, science, education, public goods, culture, and communication [18]. Elsden et al. provide the first topology of Blockchain applications for HCI, identify seven overarching 'families' of Blockchain applications – underlying infrastructure, currency, financial services, proof-as-a-service, property and ownership, identity management and governance – and argue for an active role of the HCI community in the Blockchain domain [21].

At the same time, cryptocurrencies users still face major unsolved challenges: user interfaces suffer from usability issues [8, 22, 27, 37], there remain fundamental trust challenges [6, 26, 34, 44, 45], cryptocurrencies are complex to understand [21, 22] and have a high entry-barrier for people with less technical knowledge [31]. With more blockchain-based services emerging, it is important to understand which challenges people face – to ultimately design solutions around them and facilitate the development of more inclusive systems that allow users without deep technical knowledge to participate in the crypto economy of tomorrow.

A large part of the complexity originates from private / public key cryptography Blockchain builds on. It shifts the responsibility to securely manage private keys to the end-user. Cryptocurrencies today offer a valuable opportunity to investigate how users manage arising security challenges in practice. Previous research of key management in the context of cryptocurrencies focused on the available tools [3, 22] and providing a quantitative macro view of security practices of Bitcoin users [37]. However, there remains a lack of qualitative insight into the security practices of cryptocurrency users.

To address this, we conducted semi-structured interviews with 10 users, investigating their experiences and security practices using cryptocurrencies. We identified 3 themes through thematic analysis concerning (1) motivation, (2) risk assessment and (3) coin management tool (CMT) usage.

We found that users' knowledge and understanding of security practices influence the choice of CMTs, as does the intent to use as an asset or as a currency. Not all users have either the motivation or knowledge to securely manage their keys on their own. Custodial CMTs, abstracting key management away from the end-user, are seen as a convenient alternative

DIS '20, July 6–10, 2020, Eindhoven, Netherlands.

ACM 978-1-4503-6974-9/20/07…$15.00
DOI: http://dx.doi.org/10.1145/3357236.3395535

to self-managed solutions for some, while others categorically advise against them. Those managing their keys themselves go to great length to secure their backups resorting to redundancy and also more traditional means, such as bank deposit boxes. Contrary to previous research, financial interest revealed itself to be the predominant motivator of users. This indicates that cryptocurrencies have started to move beyond the early adopters (who did so out of ideological and technological interest) to a broader audience (who does so out of utility). From our findings, we distill a model explaining how the dynamics can be used to better understand cryptocurrency users and explore design implications for research and practice.

Contribution Statement: The main contributions of this work are (1) a qualitative investigation of current cryptocurrency users' security practices; (2) a model explaining how risk assessment and intended usage influence users' tool choice; and (3) design implications for designing future systems.

BACKGROUND AND RELATED WORK

Our work draws from several strands of research, most notably research on blockchain applications from an HCI perspective as well as research on security and privacy practices of users.

Blockchain: Terms and Concepts

Bitcoin is a digital currency introduced by pseudonymous identity Satoshi Nakamoto in 2008 as 'a Peer-to-Peer Electronic Cash System' [42]. Bitcoin allocates units of value by maintaining a public distributed ledger of all transactions, making use of a technology known as Blockchain. This ledger is maintained by a decentralized network and makes use of a novel method to reach consensus on the valid state of the ledger, without the need for a trusted central authority. The transaction validation within the system is called mining. Participating actors compete for transaction fees and a reward for being the first to validate a block of transactions [34].

A critical component for this to work is private / public key cryptography. Bitcoin addresses are pseudonymous and derived from the public key of an account. To prove ownership, transactions are signed with the private key of the sending account to be accepted by the system. Knowledge of a private key grants access to the associated funds. Loss of a private key results in loss of access to those funds. Owning cryptocurrency in reality means, owning private keys to specific accounts on the public blockchain. Consequently, it is a critical task for users to maintain and secure these keys. This is done with cryptocurrency clients, commonly known as wallets [22].

Since the introduction of Bitcoin, a substantial number of alternative cryptocurrencies have been introduced. Bonneau et al. provide a first systematic exposition of these second-generation cryptocurrencies [10]. Initially, mining was the only way to obtain cryptocurrencies. Today, there are many exchanges that allow users to buy, sell, and exchange these cryptocurrencies. Some of these cryptocurrencies aim to provide additional functionality, enabling 'Smart Contracts' and ultimately 'Decentralized Autonomous Organizations (DAOs)'. Ethereum, one of the most advanced projects, aims to 'to provide a blockchain with a built-in fully fledged Turing-complete programming language' [14].

There is a growing body of research surrounding Blockchain technology, investigating the potential impact it could have on future use cases. Swan's discussion on the stages of blockchain development – Blockchain 1.0 as digital currency, Blockchain 2.0 as digital economy, and Blockchain 3.0 as digital society – is picked up by Elsden et al. and Efanov and Roschin [18, 21, 48]. In an aim to create the first topology of Blockchain applications for the HCI community, Elsden et al. cataloged over 200 applications of Blockchain and identified 7 overarching 'families': Underlying Infrastructure, Currency, Financial Services, Proof-As-A-Service, Property and Ownership, Identity Management and Governance. They base their topology on applications available or in development today and discuss specific use cases in depth, including examples [21]. Efanov an Roschin describe application use cases beyond currency and financial use i.e. in the fields of art, science, education, public goods, culture and communication and expand on M2M interactions in the context of the Internet of Things (IoT) and Digital Identity [18].

While the concept of a blockchain-based 'Digital Economy' may seem like in a distant future, the concept of a machine-to-machine (M2M) electrical market is already being explored [2, 47]. Wu et al. showed the feasibility of using smart contracts to manage the demand side of a grid by simulation [51].

Blockchain and HCI

There is an emerging body of research dealing with blockchain in HCI. Elsden et al. provide the first broader summary on Blockchain research in the HCI community [21].

Experiences and Motivation

Several publications report on the experiences and motivations of Bitcoin users [27, 36, 37, 44]. Sas and Khairuddin focused on Bitcoin-related practices in the context of a developing country at the example of Malaysian Bitcoin users [36, 44]. Gao interviewed both users and non-users of Bitcoin in the US [27]. Krombholz presents a survey of 990 Bitcoin users, complemented by interviews with frequent users [37].

While the motivation of users is reported in most instances, results are difficult to compare as there is no common taxonomy. Khairuddin et al. report the 'Oncoming Monetary Revolution', 'Empowerment Associated With the Use of a Decentralized Cryptocurrency' and 'Perceived (Material) Value' [36]. Later, Sas and Khairuddin reduce motivation to 'Economic Rationale', subsuming 'distrust in financial institutions', 'security' and 'speculation' [45]. Krombholz et al. identified 'Decentralized nature' and 'curiosity' as main motivators [37].

Trust an Values

Sas and Khairuddin further explore the role of trust in the context of Bitcoin, arguing for research into technological, social and institutional trust as well as stakeholder groups (miners, users, exchanges, merchants, governments) in the context of Bitcoin [44]. They identified 'the risk of insecure transactions' dealing with 'dishonest traders' as the main trust challenge for Bitcoin users [45] and further explore the trust challenges of miners [35]. Auinger and Riedl argue that Blockchain systems, such as Bitcoin, are not purely technical systems, but socio-technical systems and thus not trust-free technologies.

They propose a trust framework similar to the one by Sas and Khairuddin, with focus on the trust questions users have to consider when using, buying, selling and owning Bitcoin [6]. Lustig and Nardi explored the concept of algorithmic authority in Bitcoin online communities, identifying considerable variance in how participants viewed the cryptocurrency and what they valued it for. They concluded that trust in algorithms cannot entirely substitute trust in humans [39].

Key Management

Key management has been a topic of interest in usable security research since Whitten and Tygar first investigated the usability of PGP 5.0 in 1999, revealing significant challenges users faced with regards to key management [50]. More than 20 years later 'Johnny' has found his way into the title of many publications dealing with usable key management and email encryption as the topic remains unsolved [5].

Eskandri et al. present the first review of key management in the context of Bitcoin in 2015. They remark that users are challenged to ensure their keys be simultaneously accessible, resistant to digital theft and resilient to loss. While they conclude that Bitcoin key management shares fundamental challenges of key management in general, they emphasize their observations that 'developers in the Bitcoin ecosystem are making innovative attempts to solve decades-old problems of usable key management', calling for further investigation user- behavior [22].

Krombholz et al. report on practices of Bitcoin management. They found most users resort to a password-protected wallet. Users of web clients have less background knowledge and are less likely to have backed up their wallets. 22.5% of users had to face a loss of Bitcoin, half of which were attributed to self-induced errors. They conclude that managing Bitcoins remains a major challenge for users [37].

Bonneau et al. identified strategies developers of Bitcoin software deployed to mask the complexities of key management: keys stored on device, password protected wallets, offline storage, air-gapped and hardware storage and hosted wallets [10]. Eskandari et al. propose an evaluation framework for key management approaches [22]. Krombholz et al. propose a methodology to categorize wallets based on their degree of control over key management operations. They introduce the term Coin Management Tool (CMT) as a name, capturing the functionality Bitcoin clients offer, as the term 'wallet' was defined as a 'collection of private keys' originally [32, 37].

We build on the proposed categorization approaches and differentiate between **self-managed** and **custodial** CMTs. Self-Managed CMTs require the user to manage their keys. Custodial CMTs take over key management for end users.

User Attitudes Towards Security And Privacy

An important part of building secure systems is to understand how users actually engage with those. This holds true for cryptocurrency systems especially, given that they delegate security-related tasks to the end user. Security and privacy researchers have found that end users differ in their willingness to deploy and use tools to secure themselves [1, 9, 16]. Barth and De Jong describe the privacy paradox: While users claim to be concerned about their privacy, they undertake but little to protect it. They identify the risk-benefit calculation as major decision-making process and discuss it through the different lenses offered by the surveyed publications [7]. To better understand users, different measurement instruments have been proposed to assess the attitude of users toward privacy [13] and security [19, 20].

There have been also efforts to cluster users based on their attitude towards security and privacy and identify common types of users. Research from Westin [38] distinguishes three types of users: (1) The Marginally Concerned, (2) the Fundamentalists and the (3) Pragmatic Majority. However, these categories were shown to be bad predictors of user behavior. Dupree et al. extend Westin's model to 5 privacy personas that differ in their knowledge of and motivation toward security and privacy [17].

- Fundamentalists (High Knowledge, High Motivation)
- Lazy Experts (High Knowledge, Low Motivation)
- Technicians (Medium Knowledge, High Motivation)
- Amateurs (Medium Knowledge, Medium Motivation)
- Marginally Concerned (Low Knowledge, Low Motivation)

In the context of cryptocurrency it is interesting to consider that users may differ in the motivation and ability to protect themselves. Research indicates that cryptocurrency users are not a homogeneous group, but that their perceptions of security and risk differ substantially [37, 39].

Summary

From previous work, we can extract several learnings for the context of this paper. Blockchain and cryptocurrencies remain a complex topic to understand, primarily because they suffer from the same challenges as key management in general. Several accounts of Bitcoin users' experiences provide insight into their behavior and motivation, yet a thorough qualitative account of how they manage security challenges is missing. These reports have also come to age, exploring findings from 2016 and earlier, before the 'run on cryptocurrencies' in 2017 – this may have led to a different composition of cryptocurrency users as well as a change in their behavior today. The work of Dupree et al. shows that knowledge and motivation on how security differs between people, something worth also exploring among cryptocurrency users. Eskandari et al. emphasized the innovative approaches of developers in the Bitcoin ecosystem back in 2015. Five years later, we think it is worth looking at how users manage their cryptocurrency today.

METHOD

In this section, we describe our research approach, the apparatus of questions guiding the semi-structured interviews and the coding and analysis process.

Approach

We conducted semi-structured interviews via Skype[1] between September 4th and 28th, 2019. The interviews lasted between 37 and 54 minutes (in total 451 minutes), were conducted in German language, audio-recorded and fully transcribed.

[1] https://skype.com

Apparatus

The interviews explored the challenges users face when managing cryptocurrencies in practice. The question catalogue was derived based on a qualitative analysis of posts and discussion in online forums (reddit.com/r/bitcoin, bitcoin.stackexchange.com and blockchainjournal.news) dealing with challenges of managing cryptocurrencies securely, collected during August 2019. We inquired about the following topics during the interviews and probed deeper when interesting topics emerged.

- Cryptocurrency ownership: Which cryptocurrencies do you own? Why did you start to get involved with cryptocurrencies? How to you manage / use your cryptocurrencies?
- Wallet Usage: Which wallets do you use? How do you use them? Why did you decide for these wallets? Can you remember problems you encountered while using wallets?
- Backup Behavior: How do you approach backups in general? How do you store mnemonics? Can you remember a time, when you had to use your backup(s)? Do you think your backups are stored securely?
- Demographic Information: Age, Gender, Highest Finished Education, Affinity for Technology Interaction (ATI) scale [4, 25], self-assessed experience with Blockchain (5-item Likert scale)

Recruiting

For this study, we recruited 10 cryptocurrency users between 19 and 36 (mean 27.2) years old. Participants were recruited using local networks in Munich, Germany. An initial outreach to identify participants was shared via the local blockchain meetup group and a university Slack[2] channel. From initially 16 responses, 10 participants scheduled the interview.

Data Analysis

For data analysis, we used thematic analysis following the 6-step process described by Braun and Clark, using an inductive approach [11]. The initial data set consisted of the transcribed interviews. To freely explore and organize emerging codes and themes we performed the initial three steps with printed versions of the transcript, before digitizing the codes and themes in subsequent iterations. As themes started to emerge during the iterative process, we included the previously collected dataset of online discussion to validate the identified themes. Figure 1 provides a snapshot of the process.

FINDINGS

From 10 participants, 9 were male. 5 participants are students, 5 participants are employed or work in their own company. Their highest finished education are High School (2), Bachelor Degree (3), Masters Degree (5). Participants are all located in Germany and Switzerland and have 3 different nationalities: 8 German, 1 Swiss and 1 US American. 5 participants are from business administration related fields, 5 from IT-related fields. 5 participants have worked with Blockchain technology during their studies or current employment already.

[2] https://slack.com

Figure 1. We used thematic analysis to analyze data collected from interviews and from online forums. To freely explore the data sets the initial steps were performed with printed transcripts.

The Affinity for Technology Interaction (ATI) score describes a person's tendency to actively engage in intensive technology interaction, or to avoid it. A score of 6 represents a high affinity for technology interaction and a score of 1 the opposite. Our participants rank between 1.56 and 5.78 (mean 4.76), showing a broad range of scores among the interviewees. [4, 25].

The participants have between 2 and 6 years (mean 3.6) of experience with cryptocurrencies (two participants did not disclose their experience in years). We asked participants to self-select experience with cryptocurrencies on a Likert-Scale from 1-5. The self-assessments range from 1 to 5 (mean 3.8).

All participants owned cryptocurrencies themselves. 7 participants disclosed which cryptocurrencies they owned. The number of different crypocurrencies listed per participant varied between 2 and 15. All of them listed Bitcoin and Ethereum. We further asked participants to provide a valuation in Euros of their cryptocurrencies at the current point in time. 8 participants agreed to do so, providing estimates between EUR 50 and EUR 25.000 (mean EUR 10.534).

Through the interview process and subsequent analysis, prominent themes emerged surrounding motivation, risks, and tool usage. Interviewee statements are denoted with "P" and statements from users in online forums with "W". Interview statements (P) were translated into English. Statements from online forums (W) were re-written to preserve their privacy [24, 12].

Motivation

The motivation to engage with cryptocurrencies varies between participants, though all of them could be attributed to either (1) financial interest, (2) ideological interest or (3) technical interest. These motivators are not mutually exclusive and most interviewees are motivated by a combination of them.

Financial Interest

We found financial interest to be the most frequently mentioned motivator for why people engage with cryptocurrencies – 8 of the 10 mentioned it. P1 stated, "*I view it as an investment, i.e. I expect an increase in value.*" and P7 shared that he engaged with cryptocurrencies for "*speculation*". However, they are not just seen as an investment opportunity, but also as a means for value preservation. P4 stated that he asked himself, "*How can I make sure that I don't lose what I have earned?*".

While it sounds trivial that people are motivated by financial interest to engage with cryptocurrencies, this contradicts earlier findings by Krombholz et al. who identified the "*decentralized nature"* and *"simple curiosity"* as primary motivators [37].

Research indicates that cryptocurrencies are used primarily as an asset and not as currency [27, 30, 45]. Our analysis indicates the desire of practitioners to use it as a currency: P4 stated, "*I would like to use it on a day-to-day basis*" and P10, "*I would like to spend it in the real world*". However, practitioners agree that a lack of options to spend cryptocurrency is holding them back from doing so.

Ideological Interest

Some participants are motivated by ideology, i.e. the "decentralized nature" of cryptocurrencies. However, nobody mentioned ideological reasons as sole motivation. P2 stated, *"I do believe in the technology [. . .] but I also think the ideological idea behind the movement is very interesting. Thus, a mix of curiosity of ideology and technical and economic conviction."*. P4 added an interesting perspective by sharing, "*I am from Bulgaria. I know what could happen there. There was a hyper-inflation. The people lost their entire savings [. . .] I have been very sceptical about central banks since the financial crisis.*".

Krombholz et al. reported a similar case in their sample of qualitative interviews. For one participant, Bitcoin presented it as a secure alternative to receive money in Crimea during the Ukrainian-Russian conflict [37]. Similarly, a 2019 report on cryptocurrencies by the Dutch Bank ING surveying close to 15.000 people in 15 countries found that 61% of respondents from Turkey were most positive about the future of cryptocurrencies. In comparison, only 20% of participants from Germany and 31% from the US showed positive attitudes towards the future of cryptocurrencies [33]. The socio-political environment people find themselves in may have a significant impact on their motivation and intent to use cryptocurrencies.

Technological Interest

Curiosity in the technology was the third motivator we identified. P10 explained, "*[...] to try it out. To better understand the technology. And especially with Ethereum to play around with Smart Contracts*". P2 stated, "*I think it is exciting to be at the technological frontline*" and P8, "*Mainly technical interest. I started engaging with cryptos in practice. So, not just with cryptocurrencies but with fundamental blockchain and distributed ledger technology.*". These statements are in line with earlier findings. Krombolz et al. identified "curiosity" as the second strongest motivator in their sample [37].

Risk Assessment

Krombholz et al. found that 22.5% of their sample had lost cryptocurrencies. Of these incidents, 43.2% were account to the fault of the user, 26.5% to a hardware failure, 24.4% to a software failure and 18% to security breaches [37]. The questions on how to best secure crypto assets and minimize the risk of losing them are therefore vivid discussion points.

Our analysis identified three essential sources of risk that can lead to the loss of cryptocurrency. Users have to deal with the (1) Risk of Human Error, the (2) Risk of Betrayal and the (3) Risk of Malicious Attacks. Previous research by Sas and Kahiruddin interviewing 20 Malaysian Bitcoin users similarly identified risks with the specific focus on transactions: (R1) *Risks due to User's Challenges of Handling Passwords*, (R2) *Risks Due to Hackers' Malicious Attack*, (R3) *Risks due to Failure to Recover from Human Error of Malice*, (R4) *Risks from Dishonest Partner of a Transaction* [45]. Our definitions differ in that they are not limited to transactions, but apply to cryptocurrency usage in general. Risk of Human Error encompasses all risk rooted in user behavior, including R1 and R3. Risk of Trust includes all stakeholders involved directly or indirectly with buying, selling and managing cryptocurrencies. Risk of Malicious Attacks extended beyond the digital realm and the risk of physical attacks as well.

Risk of Human Error

The decentralized nature of cryptocurrencies does not only shift the control over assets but also the responsibility for securing them to the end-user. Mistakes made by users can, therefore, lead to the loss (of access) to the managed crypto assets. Practitioners are generally aware of this, as P10 put it, "*If you lost your private key, your are f*cked"*.

P2 was generally afraid to not adequately handle technology. He described his feeling when using his mnemonic recovery key: "*Whenever I do something with mnemonics, I have a weird feeling even though there is not much that can go wrong. It always feels just like there is this pressure, like, 'Oh God, if you do something wrong now, in the worst case everything is gone'. You cannot call anyone. You cannot reset anything.*".

There is a fear of forgetting critical information to access crypto assets, such as passwords, private keys or physical backup location: "*Memorization is not the best idea. I wrote my seed phrase on paper and now I can't remember where I hid it.*" (W1).

Finally, there are the fears of inadequately storing or losing critical information. Examples are losing the seed phrase, misspelling the seed phrase, selecting the wrong storage medium or location ultimately leading to breakdown or destruction of the stored information. On how to store backup phrases (mnemomics) P4 remarked: "*Paper is sort of safe until you think about what would happen if the apartment burnt down*".

Risk Betrayal

While blockchain enables trustless consensus, social trust between stakeholders is still necessary [6, 44, 45]: "*You always need a gateway into the decentral system. So there will always be someone*" (P3). Placing one's trust into a third party carries an inherent risk that this third party may not act according to expectations and ultimately betray one's trust. This risk is not necessarily unique to cryptocurrencies.

Custodial CMTs provide a way to participate in the crypto economy without the need to deal with key management. However, for this to work there is the need to trust the custody provider to handle one's keys. Some participants expressed distrust of these services, best captured by the phrase *"not your keys, not your crypto"* (P1, P2, P8, P10). This sentiment is rooted in a fear of placing trust in the wrong guardian. Using a centralized service to manage assets is for some in direct

conflict with the decentralized nature of blockchain technology. P8 said, *"Custodial wallets are pure fiction [. . .] If they are bankrupt or they want to betray you, they just take the real hardware wallet and run away*". However, this risk is not limited to custodial CMTs, but more generally applies to all third parties involved directly or indirectly with buying, selling and managing cryptocurrencies. P10 illustrated this point with the example of a cloud storage provider: "*If I put the private key of my decentral cryptocurrency into a Google Drive, I should expect that someone looks at it.*" , adding "*What if Google cooperates with the government and they hand out some data . . . Therefore, I would never store it in Cloud Storage.*".

Risk of Malicious Attack

Discussions regarding malicious attacks revolve around three core topics: the self-managed CMT getting compromised, the custodial CMT getting compromised, and physical attacks.

A common fear of users is that the self-managed CMT could get compromised, allowing attackers to gain access to their funds. Digital storage methods of keys and mnemonics are viewed as less secure than physical storage. W4 stated, *"Do not store mnemonics digitally - you are asking for hacker attacks."* and W3 confirmed, *"If you store your seed phrase digitally, you increase your attack surface enormously."*. As a result, some recommend the use of hardware wallets that are not connected to the internet and thus less susceptible to attacks. P1 said, "*In my opinion, hardware wallets take away the majority of errors users can make [. . .] In the end, my PC could be infested with 5 viruses but my private key would not be stolen.*". P10 shared this view, "*I can use hardware wallets on virus-infested computers without my money being stolen*".

W2 made an interesting point stating, *"I think those who can handle the complexity of cold storage and hardware wallets do so anyway. Because when it comes to security against external attackers, these solutions are more secure. However, when all causes of Bitcoin loss are considered, the probability of loss is more likely to be due to user errors than to device hacks."*. This notion is not unfounded – it coincides with the findings of Krombholz et al. that listed security breaches as the least common reason of Bitcoin loss. Bitcoin loss was caused by user mistakes twice as often as by security breaches [37].

Practitioners also fear that custodial CMTs, such as exchanges, are an attractive target for attackers. This fear is rooted in a rich history of incidents in the past, most notably the infamous hack of the at the time largest Bitcoin exchange mt.gox in 2014 during which Bitcoin worth USD 460 million were stolen [40, 41]. P1 concluded, "*We have seen it more than once that Exchanges were hacked or that the founders ran off with the funds of their customers*".

Malicious Attacks are not neccesarily confined to the digital realm. Physical attacks can take two forms: (1) theft of credentials and backups and (2) attacks on the owner forcing them to provide access to their CMT. W5 summarized his thoughts on theft as follows: *"I can imagine that in the future, a burglar will know exactly what to do if he opens a drawer (or safe) and finds a laminated piece of paper with a seed phrase on it. In 1950 a thief would not have bothered to find a plastic card with a bunch of numbers in a wallet. But by 1960, every criminal knew exactly how to use a credit card."*. With regards to robbery, P1 said, *"Even if I was kidnapped and tortured, I could never give away my private key."*. W11 suggests a different approach for the event of robbery, *"Put an amount large enough that a thief cannot resist, into your wallet without password and the rest into a password protected wallet."*.

Coin Management Tool (CMT) Usage

The choice of Coin Management Tools by practitioners emerged as the third theme. Our findings indicate that there is no "silver bullet", no "one-size-fits-all solution" that works for all users and use cases. Rather, practitioners use both self-managed and custodial CMTs in parallel. They store backups redundantly and are aware of the challenges current CMTs brings about.

Use of Multiple CMTs

More than half of the participants reported to use both self-managed and custodial CMTs. The reasons behind choosing to use either type are consistent between participants. Users opting to use self-managed CMTs emphasise that only ownership of the private keys ensures ownership of cryptocurrency. This mindset is captured by the commonly used phrase *"not your keys, not your crypto"* (P1, P2, P8, P10). Users of custodial platforms value the usability and convenience they provide. Asked for his motivation, P3 explained, "*Because it has a lot of convenience. Honestly, does one really need to know one's keys? Do I really need to have access to them?*". P7 further argued that using a custodial CMT is a feature, as he is not solely responsible in case of a problem. He said, *"Do I trust the producer of the hardware wallet that the system will work in the future? As with Coinbase, other people have interest in it. Meaning, if there are problems, there will be a solution. If my personal hardware wallet breaks down, there is only me who has an interest in it. Worst case there will be not solution and my money is gone."*.

Participants using both self-managed and custodial CMTs do so for different use cases. Custodial wallets are used for spending and acquiring cryptocurrencies, whereas self-managed CMTs, specifically HW wallets, are seen as long-term storage for larger sums. P4 explained, "*There is not necessarily the need for one perfect thing for everything [. . .] The safe securely back home and a wallet of third parties for everyday use*". P8 claimed to use custodial CMTs only for buying: "*I use custodial wallets only to buy cryptocurrencies*", as did P2: "*On Coinbase I only buy and sell and then send it directly to my ledger . . . except for smaller sums*". This approach is similar to what Eskandari et al. propose: keeping small ready-to-spend amounts in online wallets and larger sums in more secure and difficult to access storage [22].

CMTs are not necessarily digital, either. Examples are services by banks, offering to handle the investment and storage of cryptocurrencies. P6 mentioned, "*There are already several private banks here which offer good solutions. These would be the Bank von Tovel und Bank Frick, who have been doing this for a long time now*.".

Backups Stored Redundantly

Backup of the private keys or the seed phrases are well discussed topics. We found that redundant backup storage is common practice among all users with self-managed CMTs. Most users store backups in the form of mnemonics: 12 or 24 letter sentences that encode the seed phrase used to generate the master key of a wallet [52, 43]. They store multiple copies, in multiple locations and combine different methods to do so. P1 explained his rational for redundant locations as safeguard against environmental threats: "*In my opinion, the best protection against environmental damage is redundancy. This means to not store my keys at one location, but to create maybe two backups and store them at geographically different places.*". Using multiple locations is also commonly recommended in online forums. W8 for example recommended, "*The most reliable way to keep your seed/secret key safe is to have numerous instances in different locations, perhaps in various formats, and even better if the keys are split.*".

These comments suggest that most users store these backups redundantly to avoid accidental loss or destruction. This naturally increases the probability a third party could gain access. To mitigate this, users employ additional strategies. P2 stores his backup in a safe, "*The ones for my Ledger Nano S are lying in a safe*" and P8 splits his backup and stores the parts in two fireproof safes, "*[. . .] just splitting the key in two parts. And then physically transport it in two fireproof safes*". Some users combine digital solutions with offline storage. P2 stated he additionally stores his backups, "*Having it encrypted on my laptop, deposit box in a bank and additionally some metal box lying around somewhere at home*". Some tech-savvy participants resort to the use of encryption. W10 for example stated to use PGP: *"I encrypt the keys of my wallet with PGP and send an email to my own account and someone I trust. Voila."*.

The collected data indicates that for backup storage there is no one-size-fits-all solution as well, causing users to resort to a combination of them: "*Every storage technique has its shortcomings. The optimum is always to diversify*" (P10).

Awareness of Usability Challenges

Another characteristic of interviewees is their awareness and acknowledgement of current issues with cryptocurrencies.

Many users perceive dealing with key management as a burden and bad usability. This is in line with prior usable security research [22, 28, 29, 50]. Not having to deal with keys is perceived as better usability. P3 said, "*The best usage for me would be to never see a private key or public key again. Optimal usage would be as simple as N26 banking today*". For these users, custodial CMTs, which shield them from having to deal with key management, are convenient. P8 explained the advantage of custodial CMTs, "*The usability of such wallets is far better. Because it is easier. Because you do not have to take care of any key management.*". P7 is convinced that key management is not the best solution, "*At the same time, I do not believe that local management is the best solution for all people*". He added, "*I believe, there is a large customer group for whom it makes a lot of sense to trust a central entity instead of managing it themselves*". P8 concluded that there could be different groups of CMTs for different users, "*There may be several groups. The first group has exceptional usability. The middle group is maybe encrypted – here MetaMask is very successful, but requires a lot of knowledge. And then there are things like Hardware wallets that are much more technical and more secure, but less convenient*".

Self-managed CMTs largely expose the underlying technology, blockchain, to the user. P4 is convinced that security needs to be at a level where the majority of people can use it: "*There will not be something like absolute security as long as humans are involved [. . .] Rather, the point is how can we provide the best security for most people so that most people can use it*". Several users suggested forms of biometric authentification as one solution (P3, P4, P8, P9). P3 thought, "*Maybe a fingerprint or retina scan will suffice in the future*".

Established naming concepts are perceived as bad metaphors that do not translate well to the concepts behind them. This makes it difficult for new users to asses possible consequences of these concepts. P10 said, "*I think a wallet has nothing to do with a wallet in which I put my bills. It is rather a box where I put my keys. This was simply a poor choice of labeling to understand what it really does*." and continued, "*The choice of words regarding 'wallets' is wrong [. . .] Recovery phrase sounds nothing like something private. It does not imply that, if you lose it, all your crypto might be gone*". From evaluating 6 Bitcoin key management clients Eskandari et al. concluded that "tasks involving key management can be mired in complex metaphors and confusing abstractions" [22].

There is a high technical entry-barrier new users need to clear before starting with cryptocurrencies. The complexity of the topic and the required technical knowledge make it difficult to use self-managed CMTs and provide many pitfalls for new users (increasing the **Risk of Human Error).** P1 stated, "*Creating a wallet is quite complicated for someone doing it the first time. At this point nobody is aware of the consequences of what they are doing*". P10 argued, "*The best entry point is to engage with the topic on a technical level*" and further explained, "*As non-technical user one should know that from the mnemonic the private key is created and that it has to be treated even more confidential*". P8 feels onboarding needs to be improved, "*I think that onboarding has to be improved everywhere*". Also Glomann et al. identified "The Onboarding Challenge" as one of the problems slowing down mainstream adoption of blockchain-based systems [31].

THEORETICAL IMPLICATIONS

We discuss the implications of our findings for HCI research on cryptocurrencies and blockchain systems. These are mostly valid for cryptocurrency users, but may be valuable to understand users interacting with other blockchain technologies.

Our findings indicate that all users are aware of the importance of keeping their cryptocurrency secure. Their strategies on how to achieve this, however, differ. Some users opt for a strict "not your keys, not your crypto" strategy, using only self-managed solutions while others choose to delegate key management all together to a custodial service. Some users advocate for offline storage in hardware wallets, while others manage them on internet-connected devices or web-based systems.

In choosing their tools, users need to balance the different sources of risk – **Risk of Human Error, Risk of Betrayal, Risk of Malicious Attack**. This happens largely along two dimensions. Firstly, users need to decide between self-managed and custodial CMTs. Secondly, users need to decide between CMTs disconnected from or connected to the internet.

Self-Managed CMT vs Custodial CMT

The decision to choose either self-managed or custodial services translates to balancing the **Risk of Human Error** against the **Risk of Betrayal**. For every individual user, this balance is different as it is influenced by their attitude toward security. As both motivation and knowledge of how to deploy security mechanisms influence this balance, Dupree et al.'s model of Privacy Personas lends itself as a valuable tool. Figure 2 exhibits this tension by showing two Privacy Personas on opposite sides of the spectrum. To illustrate this point we chose the extreme positions of the Privacy Personas [17].

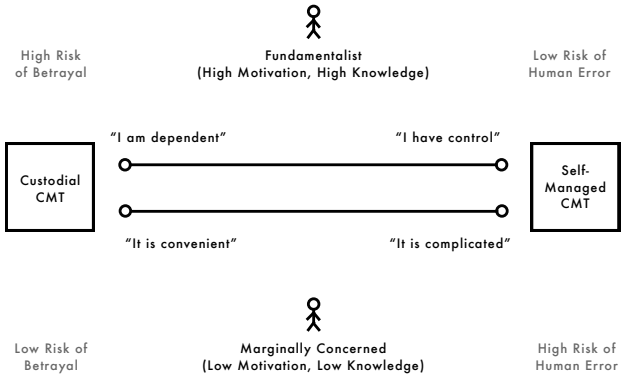


Figure 2. Motivation and Knowledge of security influences how users choose between self-managed and custodial CMTs.

Fundamentalists are characterized by a high motivation to and high knowledge of how to employ security. They value fine-grained access to security settings and generally view others as uneducated and insecure [17]. Consequently, they value the control over security self-managed CMTs offer. They know how to securely manage their keys and view it as unlikely that they will lose cryptocurrency through their own mistakes – they assess the **Risk of Human Error** to be low. From their perspective moving towards custodial CMTs is seen as giving up control and becoming dependent on a potentially insecure third party, ultimately increasing the **Risk of Betrayal**.

The Marginally Concerned have low motivation and knowledge about security concepts. They generally trust websites claiming to be secure. They know threats exist, but view it as unlikely that something will happen to them [17]. For them having to deal with key management is a burden. It is complicated. At best it is bad usability and at worst the source of mistakes that lead to the loss of their cryptocurrency. Custodial CMTs shield them from the technical complexity of key management and provide a familiar and convenient way to engage with cryptocurrencies. They trust the custodial service to provide better security than they could and assess the **Risk of Betrayal** as low. For them, moving from Custodial CMTs to Self-Managed CMTs is seen as a loss of convenience through additional complexity, increasing the **Risk of Human Error**.

Isolated CMT vs Connected CMT

The decision of whether to use a CMT isolated from or connected to the internet relates back to how users assess the **Risk of Malicious Attack**. To understand the decision process of users along this dimension, we review it through the lense of how cryptocurrency is being used. Previous research noted the dualism of cryptocurrencies – they are both an asset and a currency [27, 30, 45]. Assets and currencies exhibit different characteristics. The European Central Bank defines money as (1) a medium of exchange, (2) a store of value or (3) a unit of account to compare values of different goods or services [23]. Glaser et al. demarcate the use of Bitcoin as an asset from the use as a currency by whether users' intention is trade or a store of value [30]. Our findings indicate that this tension remains to exist. Users tend to use different strategies and tools next to each other to cope with the different use cases.

Figure 3 depicts how users' intention to use cryptocurrency as either asset (store of value) or currency (means to trade) influences their decision to use internet connected or isolated CMTs. Offline usage decreases the attack surface, but limits how fast users can access it.

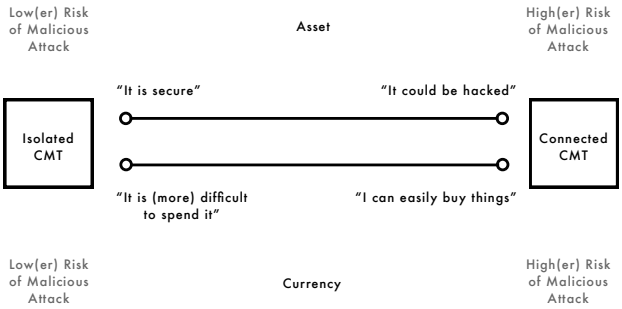


Figure 3. The intention to use cryptocurrencies as Assets or Currency influences decisions between online and offline CMTs.

We distinguish **Isolated CMT** and **Connected CMT** at each end of the spectrum. Connected CMTs are directly connected with the internet. Isolated CMTs are strictly disconnected from any network. These extremes define a scale on which any CMT can be placed based on how connected it is to the internet.

Managing cryptocurrencies with a connected CMT exposes it to potential digital attacks. Isolated CMTs are perceived to be more secure by users, as they decrease the attack surface. However, offline management limits how quickly users can spend cryptocurrencies. From the perspective of an asset – storing value over a long period of time – the time to access the funds is not as important as securing it from potential attackers. For the use as currency – to trade it for goods and services – the time needed to access them and complete a transaction is, however, crucial.

Depending on how users will use their cryptocurrencies, they will opt for isolated CMTs, connected CMTs or a combination.

A Model to Understand Coin Management Tool Usage

Understanding these fields of tension is important to develop better user-centric CMTs. We propose a conceptual model, which integrates these dimensions to enable researchers and practitioners to evaluate CMTs. Figure 4 depicts the model.

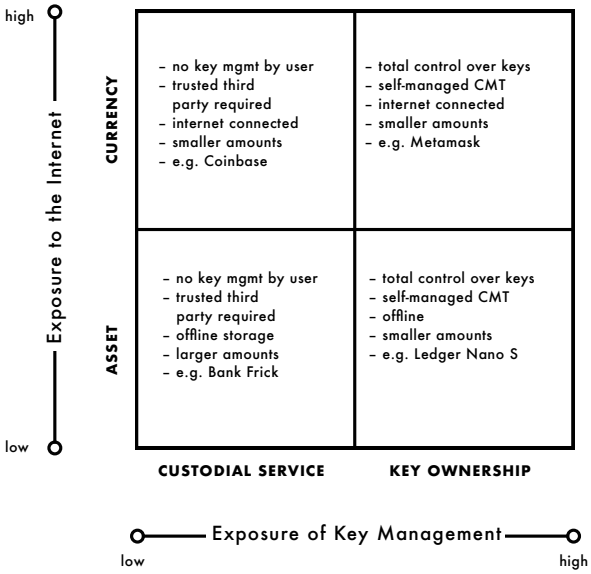


Figure 4. A model to explore how exposure to the internet and exposure of key management characterizes CMTs.

The vertical axis represents the degree to which the CMT is connected to the internet. The horizontal axis shows the degree to which public key cryptography is exposed to the end-user.

The key decision practitioners need to make with regards to how, i.e. with which tools, they want to participate in the crypto economy is dependent on how they assess the likelihood of the fundamental risks that can lead to a loss.

Different levels of key management enable control but also impose responsibility. Choosing between self-managed CMTs and custodial CMTs translates to balancing the **Risk of Human Error** against the **Risk of Betrayal** by a third party. Users with high motivation and knowledge about security mechanisms and key management will assess the risk to make mistakes themselves as low. Consequently, they see the usage of a custodial service as one that cause loss of control and independence. Users with low motivation and/or knowledge of key management will likely tend to choose a custodial CMT to abstract the key management away from them. For them, self-managed CMTs would reduce convenience and usability, while increasing the risk of loss through their own mistakes.

Choosing between connected and disconnected CMTs translates to the assessment of the **Risk of Malicious Attacks** by the practitioner. Managing one's crypto assets on an internet-enabled device, in the browser albeit, offers high mobility – that is the speed at which they can buy goods or sell their cryptocurrency. This naturally opens up an attack vector for potential malicious attackers. To reduce this attack surface, offline CMTs could be resorted to – at the cost of mobility. For example, storing one's hardware wallet in a bank safe may greatly reduce the attack surface, but limit the mobility of the assets to the time it takes to physically gain access through the processes of the bank. Depending on whether users' intent is value storage (use as an asset) or means of trade (currency), they are likely to choose a tool increasing mobility or security.

Each quadrant contains a short description of the features CMTs in this category would exhibit, including one example available today. These examples were chosen, because they were mentioned during the interviews and are explained below.

CMTs connected to the internet allow users to treat their cryptocurrencies as digital cash and use it to buy and sell goods. Metamask[3], for example is a wallet in the form of a browser-extension for the cryptocurrency Ethereum. It runs directly in the browser and allows websites to interact with by integrating the web3.js library. It stores keys password protected in the local browser, but requires users to protect and store the master private key of the wallet themselves.

Coinbase[4] is a web-based wallet and exchange that allows users to buy and sell a wide array of different cryptocurrencies. While also connected to the internet, it abstracts all key management tasks. Users can authenticate via familiar username/password and 2-factor authentication mechanism. Since the service takes over the key management, users need to trust that Coinbase does so with the necessary care.

Such custodial services also exist disconnected from the internet. The Liechtenstein based bank Bank Frick[5]offers custodial coin management through a traditional bank. Customers can delegate the acquisition and secure storage of cryptocurrencies entirely to the bank. The complete offline storage makes this method inapplicable for using cryptocurrencies to trade. However, it greatly reduces the attack surface through which potential attackers would gain access to them.

Users eager to maintain complete control over their keys without dependence on any third party may also opt out of offline storage methods. Besides, simple paper wallets, the Ledger Nano S[6] is a password protected hardware wallet enabling offline key management. The thumbdrive-sized device is supported by a wide range of digital wallets (mobile apps) and can be used to sign transactions for compatible cryptocurrencies.

DESIGN IMPLICATIONS

Based on the theoretical implications and our findings, we derive three design implications [46] for researchers and practitioners. CMTs should be developed with a clear target group in mind and focused on either the use as an asset or currency. Finally, a better understanding of cryptocurrency non-users is needed to address impediments and challenges that keep them from engaging with the technology.

Pick Your Target Group

The conversation around cryptocurrency security is largely led by tech-savvy people with high knowledge and motivation to deploy security. However, not all users have either the motivation or knowledge to securely manage cryptocurrencies on their own. Getting started with cryptocurrencies itself is perceived as a complicated process and key management remains a major challenge for non-technical users [31, 22].

[3] https://metamask.io
[4] https://www.coinbase.com
[5] https://www.bankfrick.li/en
[6] https://www.ledger.com

As the adoption of blockchain technology continues, it is important to design for inclusiveness. We argue that there is a need to lower the technological entry barrier to engage with the cryptocurrencies – and in extension, blockchain technology – to allow people without deep technical insight to participate in the crypto economy. Custodial CMTs (e.g. coinbase.com) are one product category where this already happens. At their example, one can see that people are willing to engage with the technology if they are provided with the right tools. Designers of CMT services should consider which audience they are building their product for and understand how balancing the **Risk of Human Error** and **Risk of Betrayal** influence their choice of tools.

Key management remains a challenge for users and current CMTs are either entirely self-managed or custodial. Using the proposed model, we hope that practitioners can go forward, envisioning hybrid CMTs that serve new audiences.

Design for Assets or for Currency

Cryptocurrencies exhibit a dualist nature, being both an asset and a currency. Depending on the reason users engage with the technology, different user needs should be considered. Developers should be aware that services for either assets or currencies have different requirements, especially regarding mobility and attack surface and design services accordingly.

Thinking through the lens of these different use cases should also be reflected in the communication towards users. Practitioners should aim to develop best practices specific for each use case and find meaningful analogies to convey them to non-technical users. For large investments emphasizing secure and redundant offline storage following a "not your keys, not your crypto" mindset is justified. Similarly to carrying cash in your pocket, smaller amounts of cryptocurrency can be managed with little downside risk in digital, custodial CMTs that allow for quick access when spending them.

As positive real-world example with focus on enabling spending of cryptocurrency in a currency-like way is the Lightning Network project[7], enabling real-time transactions of Bitcoin. The project decisively focuses on using cryptocurrency as a means to trade and makes use of metaphors taken from everyday life on their website to explain the technical concept behind it (last accessed April 18th 2020). They write, "*This is similar to how one makes many legal contracts with others, but one does not go to court every time a contract is made. [...] Only in the event of non-cooperation is the court involved – but with the blockchain, the result is deterministic.*"

Despite these efforts, cryptocurrencies today are, contrary to their name, predominantly used as an asset and not like a currency. Our findings indicate that this is not due to a lack of interest, but rather a lack of supply -– users would like to use them as currency, but cannot because of a lack of services accepting them. As technical limitations disappear, future research should investigate why merchants refrain from accepting cryptocurrency and explore how to "make cryptocurrencies as easy as online banking".

[7] https://lightning.network/

Seek Understanding of Non-Users

Arguably, the composition of cryptocurrency users has changed over the past 12 years. Current HCI research on cryptocurrencies is, however, primarily focused on practitioners. Findings from these studies ultimately help to understand and improve services for those that already use them. We argue that understanding why people are held back from engaging with cryptocurrencies in the first place is equally important to enabling more inclusive design.

The challenges non-users have to face might be very different from those that have become familiar with the terms and concepts. Glomann et al. stress the difficulty to find a "starting point" to learn basic concepts as one issue for potentially interested users [31]. Given the complexity of cryptocurrencies, it would be interesting to understand how novel users work around this issue and obtain their initial knowledge base.

The research community would further benefit from a deeper understanding of security and privacy behavior [17, 7] in the context of cryptocurrencies. Understanding how non-users attitudes towards privacy and security differ from those of current users would be valuable for researchers and practitioners alike.

Elsden et al. argue for the role of HCI in *Engaging Participants with Blockchain*, both for knowledge exchange and participatory design [21]. Future research should strive to include non-users in this process. Their perspective might lead to different types of applications, such as Gateway Services [21] mediating interactions with blockchain services, potentially opening them up to a broader audience overall.

CONCLUSION

This paper explores users' practices of engaging with cryptocurrencies and identifies prominent themes regarding motivation, risk assessment, and CMTs usage. We discuss how motivation and risk assessment influence CMT usage, introduce a conceptual model and derive design implications. While rooted in findings from CMT usage, we hope that this model provides a valuable lens through which HCI researchers and practitioners can view and understand user behavior in the wider area of emerging blockchain-based applications.

ACKNOWLEDGMENTS

This work was supported by the Deutsche Forschungsgemeinschaft (DFG) (grant no. 316457582 and 425869382).

REFERENCES

[1] Anne Adams and Martina Angela Sasse. 1999. Users Are Not the Enemy. *Commun. ACM* 42, 12 (Dec. 1999), 40–46. DOI:http://dx.doi.org/10.1145/322796.322806

[2] Amanda Ahl, Masaru Yarime, Kenji Tanaka, and Daishi Sagawa. 2019. Review of blockchain-based distributed energy: Implications for institutional development. *Renewable and Sustainable Energy Reviews* 107 (2019), 200 – 211. DOI:http://dx.doi.org/https://doi.org/10.1016/j.rser.2019.03.002

[3] E. Almutairi and S. Al-Megren. 2019. Usability and Security Analysis of the KeepKey Wallet. In *2019 IEEE International Conference on Blockchain and*

Cryptocurrency (ICBC). 149–153. DOI: http://dx.doi.org/10.1109/BLOC.2019.8751451

[4] Christiane Attig, Daniel Wessel, and Thomas Franke. 2017. Assessing Personality Differences in Human-Technology Interaction: An Overview of Key Self-report Scales to Predict Successful Interaction. In *HCI International 2017 – Posters' Extended Abstracts*, Constantine Stephanidis (Ed.). Springer International Publishing, Cham, 19–29.

[5] Erinn Atwater, Cecylia Bocovich, Urs Hengartner, Ed Lank, and Ian Goldberg. 2015. Leading Johnny to Water: Designing for Usability and Trust. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 69–88. https://www.usenix.org/conference/soups2015/proceedings/presentation/atwater

[6] Andreas Auinger and René Riedl. 2018. Blockchain and Trust: Refuting Some Widely-held Misconceptions. In *Proceedings of the International Conference on Information Systems - Bridging the Internet of People, Data, and Things, ICIS 2018, San Francisco, CA, USA, December 13-16, 2018*. https://aisel.aisnet.org/icis2018/crypto/Presentations/2

[7] Susanne Barth and Menno D.T. de Jong. 2017. The Privacy Paradox Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior A Systematic Literature Review. *Telemat. Inf.* 34, 7 (Nov. 2017), 1038–1058. DOI: http://dx.doi.org/10.1016/j.tele.2017.04.013

[8] Aaron W Baur, Julian Bühler, Markus Bick, and Charlotte S Bonorden. 2015. Cryptocurrencies as a disruption? empirical findings on user adoption and future potential of bitcoin and co. In *Conference on e-Business, e-Services and e-Society*. Springer, 63–80.

[9] Bettina Berendt, Oliver Günther, and Sarah Spiekermann. 2005. Privacy in E-Commerce: Stated Preferences vs. Actual Behavior. *Commun. ACM* 48, 4 (April 2005), 101–106. DOI: http://dx.doi.org/10.1145/1053291.1053295

[10] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A Kroll, and Edward W Felten. 2015. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In *IEEE Symposium on Security and Privacy*. http://www.ieee-security.org/TC/SP2015/papers-archived/6949a104.pdf

[11] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. DOI: http://dx.doi.org/10.1191/1478088706qp063oa

[12] Amy Bruckman. 2002. Studying the amateur artist: A perspective on disguising data collected in human subjects research on the Internet. *Ethics and Information Technology* 4, 3 (2002), 217–231. DOI: http://dx.doi.org/10.1023/A:1021316409277

[13] Tom Buchanan, Carina Paine, Adam N. Joinson, and Ulf-Dietrich Reips. 2007. Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology* 58, 2 (2007), 157–165. DOI:http://dx.doi.org/10.1002/asi.20459

[14] Vitalik Buterin. 2014. A Next-Generation Smart Contract and Decentralized Application Platform. (Sep 2014). Retrieved Jan 28, 2020 from https://github.com/ethereum/wiki/wiki/white-paper/

[15] Coinmarketcap. 2020. Top 100 Cryptocurrencies by Market Capitalization. (Jan 2020). Retrieved Jan 4, 2020 from https://coinmarketcap.com/

[16] Paul Dourish and Ken Anderson. 2006. Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. *Human–Computer Interaction* 21, 3 (2006), 319–342. DOI: http://dx.doi.org/10.1207/s15327051hci2103_2

[17] Janna Lynn Dupree, Richard Devries, Daniel M. Berry, and Edward Lank. 2016. Privacy Personas: Clustering Users via Attitudes and Behaviors toward Security Practices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. Association for Computing Machinery, New York, NY, USA, 5228–5239. DOI: http://dx.doi.org/10.1145/2858036.2858214

[18] Dmitry Efanov and Pavel Roschin. 2018. The all-pervasiveness of the blockchain technology. *Procedia Computer Science* 123 (2018), 116–121. DOI: http://dx.doi.org/10.1016/j.procs.2018.01.019

[19] Serge Egelman and Eyal Peer. 2015a. Predicting Privacy and Security Attitudes. *SIGCAS Comput. Soc.* 45, 1 (Feb. 2015), 22–28. DOI: http://dx.doi.org/10.1145/2738210.2738215

[20] Serge Egelman and Eyal Peer. 2015b. Scaling the security wall : Developing a security behavior intentions scale (SeBIS). *Conference on Human Factors in Computing Systems - Proceedings* 2015-April (2015), 2873–2882. DOI: http://dx.doi.org/10.1145/2702123.2702249

[21] Chris Elsden, Arthi Manohar, Jo Briggs, Mike Harding, Chris Speed, and John Vines. 2018. Making Sense of Blockchain Applications: A Typology for HCI. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. Association for Computing Machinery, New York, NY, USA, Article Paper 458, 14 pages. DOI: http://dx.doi.org/10.1145/3173574.3174032

[22] Shayan Eskandari, David Barrera, Elizabeth Stobert, and Jeremy Clark. 2015. A First Look at the Usability of Bitcoin Key Management. *Proceedings 2015 Workshop on Usable Security* (2015). DOI: http://dx.doi.org/10.14722/usec.2015.23015

[23] Europe Central Bank. 2012. *Virtual Currency Schemes*. 55 pages. http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[24] Casey Fiesler and Nicholas Proferes. 2018. "Participant" Perceptions of Twitter Research Ethics. *Social Media + Society* 4, 1 (2018), 2056305118763366. DOI: http://dx.doi.org/10.1177/2056305118763366

[25] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human–Computer Interaction* 35, 6 (2019), 456–467. DOI: http://dx.doi.org/10.1080/10447318.2018.1456150

[26] Andrea Gaggioli, Shayan Eskandari, Pietro Cipresso, and Edoardo Lozza. 2019. The Middleman Is Dead, Long Live the Middleman: The "Trust Factor" and the Psycho-Social Implications of Blockchain. *Frontiers in Blockchain* 2 (2019), 20. DOI: http://dx.doi.org/10.3389/fbloc.2019.00020

[27] Xianyi Gao, Gradeigh D. Clark, and Janne Lindqvist. 2016. Of Two Minds, Multiple Addresses, and One Ledger: Characterizing Opinions, Knowledge, and Perceptions of Bitcoin Across Users and Non-Users. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. Association for Computing Machinery, New York, NY, USA, 1656–1668. DOI: http://dx.doi.org/10.1145/2858036.2858049

[28] Simson L. Garfinkel, David Margrave, Jeffrey I. Schiller, Erik Nordlander, and Robert C. Miller. 2005. How to Make Secure Email Easier to Use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '05)*. Association for Computing Machinery, New York, NY, USA, 701–710. DOI: http://dx.doi.org/10.1145/1054972.1055069

[29] Shirley Gaw, Edward W. Felten, and Patricia Fernandez-Kelly. 2006. Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted Email. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06)*. Association for Computing Machinery, New York, NY, USA, 591–600. DOI:http://dx.doi.org/10.1145/1124772.1124862

[30] Florian Glaser, Kai Zimmermann, Martin Haferkorn, Moritz Christian Weber, and Michael Siering. 2014. Bitcoin - Asset or currency? Revealing users' hidden intentions. *ECIS 2014 Proceedings - 22nd European Conference on Information Systems* January (2014).

[31] Leonhard Glomann, Maximilian Schmid, and Nika Kitajewa. 2020. Improving the Blockchain User Experience - An Approach to Address Blockchain Mass Adoption Issues from a Human-Centred Perspective. In *Advances in Artificial Intelligence, Software and Systems Engineering*, Tareq Ahram (Ed.). Springer International Publishing, Cham, 608–616.

[32] Steven Goldfeder, Rosario Gennaro, Harry Kalodner, Joseph Bonneau, Joshua Kroll, Edward W. Felten, and Arvind Narayanan. 2015. Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme. (2015). http://www.cs.princeton.edu/~stevenag/threshold_sigs.pdf Accessed: 2015-07-13.

[33] ING Bank N.V. 2019. *ING From cash to crypto: the money revolution*. https://think.ing.com/uploads/reports/IIS

[34] Irni Eliana Khairuddin and Corina Sas. 2019a. An Exploration of Bitcoin Mining Practices: Miners' Trust Challenges and Motivations. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, Article Paper 629, 13 pages. DOI:http://dx.doi.org/10.1145/3290605.3300859

[35] Irni Eliana Khairuddin and Corina Sas. 2019b. An Exploration of Bitcoin Mining Practices: Miners' Trust Challenges and Motivations. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, Article Paper 629, 13 pages. DOI:http://dx.doi.org/10.1145/3290605.3300859

[36] Irni Eliana Khairuddin, Corina Sas, Sarah Clinch, and Nigel Davies. 2016. Exploring Motivations for Bitcoin Technology Usage. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)*. Association for Computing Machinery, New York, NY, USA, 2872–2878. DOI: http://dx.doi.org/10.1145/2851581.2892500

[37] Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer, and Edgar Weippl. 2017. The other side of the coin: User experiences with bitcoin security and privacy. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 9603 LNCS (2017), 555–580. DOI: http://dx.doi.org/10.1007/978-3-662-54970-4_33

[38] Ponnurangam Kumaraguru and Lf Cranor. 2005. Privacy indexes: A survey of westin's studies. *School of Computer Science, Carnegie Mellon University* Tech. rep., December (2005), 1–22.

[39] C. Lustig and B. Nardi. 2015. Algorithmic Authority: The Case of Bitcoin. In *2015 48th Hawaii International Conference on System Sciences*. 743–752. DOI: http://dx.doi.org/10.1109/HICSS.2015.95

[40] Patrick McCorry, Malte Möser, and Syed Taha Ali. 2018. Why Preventing a Cryptocurrency Exchange Heist Isn't Good Enough. In *Security Protocols XXVI*, Vashek Matyáš, Petr Švenda, Frank Stajano, Bruce Christianson, and Jonathan Anderson (Eds.). Springer International Publishing, Cham, 225–233.

[41] Aleksander Murko and Simon L. R. Vrhovec. 2019. Bitcoin Adoption: Scams and Anonymity May Not Matter but Trust into Bitcoin Security Does. In *Proceedings of the Third Central European Cybersecurity Conference (CECC 2019)*. Association

for Computing Machinery, New York, NY, USA, Article Article 15, 6 pages. DOI: http://dx.doi.org/10.1145/3360664.3360679

[42] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. *bitcoin.org* (2008).

[43] Sean Palatinus, Marek, Rusnak, Pavlov, Voisine, Aaron, Bowe. 2013. BIP 39: Mnemonic code for generating deterministic keys. (2013). https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

[44] Corina Sas and Irni Eliana Khairuddin. 2015. Exploring Trust in Bitcoin Technology: A Framework for HCI Research. In *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction (OzCHI '15)*. Association for Computing Machinery, New York, NY, USA, 338–342. DOI: http://dx.doi.org/10.1145/2838739.2838821

[45] Corina Sas and Irni Eliana Khairuddin. 2017. Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Association for Computing Machinery, New York, NY, USA, 6499–6510. DOI: http://dx.doi.org/10.1145/3025453.3025886

[46] Corina Sas, Steve Whittaker, Steven Dow, Jodi Forlizzi, and John Zimmerman. 2014. Generating Implications for Design through Design Research. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. Association for Computing Machinery, New York, NY, USA, 1971–1980. DOI: http://dx.doi.org/10.1145/2556288.2557357

[47] Janusz J. Sikorski, Joy Haughton, and Markus Kraft. 2017. Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Applied Energy* 195 (2017), 234 – 246. DOI:http://dx.doi.org/https://doi.org/10.1016/j.apenergy.2017.03.039

[48] Melanie Swan. 2015. *Blockchain: Blueprint for a New Economy* (1st ed.). O'Reilly Media, Inc.

[49] M. Szmigiera. 2019. Number of Blockchain wallet users worldwide from 3rd quarter 2016 to 3rd quarter 2019. (Oct 2019). Retrieved Jan 4, 2020 from https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/

[50] Alma Whitten and J. D. Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8 (SSYM'99)*. USENIX Association, USA, 14.

[51] X. Wu, B. Duan, Y. Yan, and Y. Zhong. 2017. M2M Blockchain: The Case of Demand Side Management of Smart Grid. In *2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS)*. 810–813. DOI: http://dx.doi.org/10.1109/ICPADS.2017.00113

[52] Pieter Wuille. 2013. BIP32: Hierarchical Deterministic Wallets. (2013). https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

Under Pressure. A User-Centered Threat Model for Cryptocurrency Owners

Michael Fröhlich*
Center for Digital Technology and Management, Germany
froehlich@cdtm.de

Philipp Hulm†
Center for Digital Technology and Management, Germany
hulm@cdtm.de

Florian Alt
Bundeswehr University Munich, Germany
florian.alt@unibw.de

ABSTRACT

Cryptocurrencies have gained popularity in recent years. However, for many users, keeping ownership of their cryptocurrency is a complex task. News reports frequently bear witness to scams, hacked exchanges, and fortunes beyond retrieval. However, we lack a systematic understanding of user-centered cryptocurrency threats, as causes leading to loss are scattered across publications. To address this gap, we conducted a focus group (n=6) and an expert elicitation study (n=25) following a three-round Delphi process with a heterogeneous group of blockchain and security experts from academia and industry. We contribute the first systematic overview of threats cryptocurrency users are exposed to and propose six overarching categories. Our work is complemented by a discussion on how the human-computer-interaction community can address these threats and how practitioners can use the model to understand situations in which users might find themselves under the pressure of an attack to ultimately engineer more secure systems.

CCS CONCEPTS

• **Human-centered computing** → *Empirical studies in HCI*; • **Security and privacy** → *Usability in security and privacy*; • **Applied computing** → **Digital cash**.

KEYWORDS

cryptocurrency, blockchain, threat model, user-centered, hci

ACM Reference Format:
Michael Fröhlich, Philipp Hulm, and Florian Alt. 2021. Under Pressure. A User-Centered Threat Model for Cryptocurrency Owners. In *2021 4th International Conference on Blockchain Technology and Applications (ICBTA 2021), December 17–19, 2021, Xi'an, China.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3510487.3510494

1 INTRODUCTION

There are more than 73 million Bitcoin wallets [12], over 10,000 different cryptocurrencies with a combined market capitalization of over 1.3 trillion USD (8.4 trillion CNY). With 640 billion USD (4.1 trillion CNY), corresponding to 47% of the total market capitalization [9], Bitcoin [36] is inarguably the most prevalent cryptocurrency. While researchers and practitioners see great potential in several areas for the technology behind cryptocurrencies – blockchain – [6], the rapid growth in popularity and invested capital is accompanied by frequent reports of global scams, hacked exchanges, and tales of cryptocurrencies lost forever. Scientific publications have started to investigate these challenges both from a user- and technology-centric perspective. Multiple publications investigate security and privacy practices of users [15, 16, 20, 29]. Presenting the first quantitative account, Krombholz et al. report that 22% have already lost cryptocurrency, most of them due to human failure [29]. Mai et al. explore mental models of cryptocurrency users and potential threats they are aware of [32]. Reddy et al. argue that cryptocurrencies are both a tool and a target for crime [39], and Saad et al. take a technology-centric approach and explore the attack surface of blockchain [40]. While these contributions are valuable on their own, we still lack a systematic overview of threats cryptocurrency end-users may face. To address this gap, we conducted an expert elicitation study to develop and validate a user-centered threat model for cryptocurrency owners. Building on a focus group (n=6) and existing literature, we developed a first version of the threat model and iteratively refined and validated it in a three-round Delphi process [11] with 25 experts. To include a broad set of perspectives, we recruited experts from industry and academia from the fields of security, usability, cryptocurrency, and blockchain. The proposed model comprises six categories of threats: (1) Accidental Threats, (2) Privacy Threats, (3) Physical Threats, (4) Financial Fraud Threats, (5) Social Threats, and (6) Technical Threats. To ensure the practical relevance of the model, we collected examples of real-world incidents and discussed both practical relevance and potential mitigation strategies for each threat. Our work complements existing empirical research on privacy and security practices by providing the first threat landscape in which cryptocurrency users find themselves in. We discuss how the presented threats can be addressed by the human-computer-interaction community and draw up directions for future research. We expect that the proposed model will present itself as a valuable tool for researchers and practitioners to discuss security challenges of cryptocurrency systems — both from a technical and user-centered perspective — and ultimately contribute to the development of usable and secure cryptocurrency systems.

*Also with Ludwig Maximilian University, Bundeswehr University Munich,.
†Also with Technical University of Munich,.

ICBTA 2021, December 17–19, 2021, Xi'an, China

ACM ISBN 978-1-4503-8746-0/21/12…$15.00
https://doi.org/10.1145/3510487.3510494

2 BACKGROUND

Our work builds on several strands of research, most notably from the field of usable information security and human-centered research on cryptocurrency applications.

2.1 Cryptocurrency and HCI

Blockchain has received much attention in recent years. In their ICBTA'18 survey paper, Chen et al. highlight cryptocurrency as the most active area blockchain finds application in, despite increasing interest in other areas [6]. With increasing adoption, the Human-Computer-Interaction (HCI) community has slowly started to take interest in research on cryptocurrency systems [13, 18, 19]. Elsden et al. present the first typology of blockchain applications for human-computer-interaction. They identify fundamental human challenges related to financialization, procedural trust, algorithmic governance, and the front-end interactions and call on the HCI community to address these topics to help link the design of blockchain applications with the lived experience of people [13]. Several studies have investigated the experiences of cryptocurrency users, primarily at the example of Bitcoin [20, 23, 27, 29, 41, 48]. Most research is of qualitative nature — one exception being a quantitative study with 990 Bitcoin users by Krombholz et al. who report that 22.5% of respondents had lost Bitcoins at least once. The majority of incidents was caused by user mistakes (43.2%), followed by hardware failure (25.6%), software failure (24.4%), and security breaches (18%). More recently, Abramova et al. provide empirical evidence of risk perceptions of 395 crypto-asset users [1]. Reports from industry are consistent with these findings. The Foundation for Interwallet Interoperability (FIO) surveyed 231 cryptocurrency users and report that 18% of respondents had lost cryptocurrency due to user errors in 2018; 6% fell victim to a phishing or man-in-the-middle attempt [17]. Given the high number of incidents caused by users, it is fair to assume that handling cryptocurrencies remains a complex task. While blockchain enables trustless transactions, cryptocurrency systems are arguably not purely technical but socio-technical systems that still require trust between actors [4]. The role of trust in the context of Bitcoin has been addressed from different directions [4, 21, 31, 41, 42]. Sas and Khairuddin find that the "risk of insecure transactions" dealing with "dishonest traders' are fundamental trust challenges for Bitcoin users. Hence, trust between actors is necessary for the adoption of cryptocurrencies systems [42]. This, however, opens the door for attackers exploiting ill-placed trust of users. A recent exploration of mental models of cryptocurrency users by Mai et al. reveals that misconceptions among users are common and provide a breeding ground for both user errors and security and privacy threats [32].

2.2 Threat Modeling

Threat Modeling is a security engineering practice concerned with the identification of possible threats to a system — regardless of whether they can be exploited — to develop realistic and meaningful security requirements. Threat models should be developed following a systematic approach to avoid that areas of the potential attack space are left uninvestigated [35]. Adam Shostack describes threat modeling as a 4-step process, each step aimed at answering a specific question [45]: (1) What are you building? (2) What can go wrong once it is built? (3) What should we do about those things that can go wrong? (4) Did you do a decent job of analysis?

The work presented in this paper focuses on questions (2), (3), and (4) — taking a systematic approach to enumerate existing threats, discussing possible mitigation strategies, and evaluating the resulting model with the help of experts. Between disciplines, there are different definitions of what constitutes a threat. Human errors have been recognized as a significant issue for information system security in general [24] and were shown to be especially relevant in the context of cryptocurrencies [28]. While the intuitive notion might be to presume an attacker's presence, we include accidental sources of risk. We do so building on the definitions by Im and Baskerville as well as the Internet Engineering Task Force (IETF), which defines threats as both intentional and accidental sources of risk [24, 44]. Threat modeling is typically approached in one of three ways: asset-centric, attacker-centric, or software-centric [38]. Different methods to organize threats have been proposed in literature. STRIDE organizes threats into six classes based on the type of attack: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation or Privileges [46]. PASTA provides an extensive risk-centric framework to threat modeling [47], more suited to larger corporations [38]. More recently, Potteiger et al. proposed a method to merge attack and software-centric threat modeling [38]. Almashaqbeh et al. argue that traditional threat modeling frameworks are not well-fitted to evaluate cryptocurrencies and propose ABC, a threat modeling framework focused specifically on cryptocurrencies [2]. The human factor in information security has been recognized for years [49] and previous work argued to consider humans as "*the most vulnerable part of the system*" [28]. While existing frameworks for threat modeling have proven valuable to analyze technical systems, they are less suited to understand threats end-users themselves are exposed to. To account for the socio-technical nature of cryptocurrency systems, a different approach is needed. Recent work by Anell et al. explores how end-users' perceptions of threats and countermeasures differ from experts'. They followed an inductive approach to move beyond technology or topic-specific understanding of users' perceptions of security measures and consider "*general threats that users face in the Internet ecosystem*" [3]. We build on their approach and consider such general user threats in this work. Myagmar et al. argue that a systematic threat modeling process is needed to ensure that the developers, not the attackers, discover vulnerabilities to exploit [35]. As a foundation for such a process, we argue that a general model of cryptocurrency threats is needed to help developers address them before attackers do.

2.3 Cryptocurrency Security and Threats

The security and potential threats of cryptocurrency and blockchain systems are an active subject of research in different domains. In their 2018 Blockchain Threat Report, McAfee leads with the statement "*Blockchain, a Revolutionary Basis for Decentralized Online Transaction, Carries Security Risks*". Their reports structures blockchain attacks into *Phishing*, *Malware*, *Implementation Vulnerabilities*, and *Technology Attacks*. They further highlight cryptocurrency exchanges as highly attractive targets for cybercriminals [33]. Reddy and Minnar discuss cryptocurrencies from the perspective

of criminology as both a tool and target for cybercrime and present five classes of attacks: *Hacking*, *Phishing*, *Malware*, *Cyber Extortion and Ransomware*, and *Scams and Ponzi Schemes*. Several publications investigate technical threats of cryptocurrency systems. Saad et al. take a technology-centric approach exploring the attack surface, attacks, and countermeasures of public blockchains [40]. In a similar fashion, Cheng et al. provide an overview of security threats and possible defense mechanisms of blockchain systems. They organize threats along different layers of the blockchain architecture: *Data Layer Threats*, *Network Layer Threats*, *Consensus Layer Threats*, *Incentive Layer Threats*, *Smart Contract Threats*, and *Application Threats* [7]. Fabian et al. list security/ privacy risks of cryptocurrency systems and potential technical measures against them. They complement their analysis with a survey of 125 active Bitcoin users, measuring awareness and adoption security and privacy practices. They report low adoption of most security measures and argue for increasing awareness and improving the usability of existing security measures to promote adoption [16]. Sayeed et al. focus their research on the classification of smart contract attacks and protections. They structure attacks in *Malicious Attacks*, *Weak Protocol*, *Defraud*, and *Application Bugs* and further outline common attack techniques and security analysis tools [43]. Market and price manipulation of cryptocurrencies is another area addressed by research. Gandal et al. showed that suspicious trading activity — likely by a single actor — drove the Bitcoin price from USD 150 to USD 1000 in 2013, concluding that cryptocurrency markets remain vulnerable to manipulation [22]. Common market manipulations in the cryptocurrency space are Pump & Dump schemes. Organized groups artificially inflate the price of a currency by coordinatedly spreading misinformation – often facilitated by social media – before selling their coins at the height of the course. Kamps and Kleinberg's analysis revealed 920 suspicious Pump & Dump events over a period of 20 days [26]. Mirtaheri et al. combine data from social media channels to detect Pump& Dump scams as they unfold and predict thei success [34]. This emerging body of research highlights the importance of understanding the threat landscape of cryptocurrencies. Previous work largely focuses on technical threats and market dynamics but misses out on user-centered threats such as human error and social engineering. To develop the model presented in this paper, we build on the existing literature on cryptocurrency threats and connect them to the users' lived experiences with cryptocurrencies. Thus, the results presented in this paper will help practitioners to consider user threats more comprehensively and aid the development of more secure and usable applications.

2.4 Summary

Drawing from previous research, we can extract insights guiding the research presented in this paper. Cryptocurrency systems are socio-technical systems that remain complex to use. Misconceptions among users are common, making them an attractive target for criminals, using a broad range of different attacks. Additionally, human error is a frequent reason for the loss of cryptocurrencies, even if no intentional attacker is present. The purpose of threat modeling is to systematically identify and organize threats so they can be addressed. However, existing research on blockchain security and threats focuses on technical aspects and does not consider the user as a central part of the system. Consequently, research currently lacks a comprehensive understanding of the threat landscape relevant for cryptocurrency users. With this work, we aim to close this gap and provide the first systematic account of threats cryptocurrency users might find themselves exposed to.

3 METHOD

We first conducted a focus group with six cryptocurrency and security experts to construct an overview of the relevant threat landscape. Building on the focus group and related literature, we developed the initial version of the threat model. We then conducted an expert elicitation study following a three-round Delphi process [8] with 25 experts to iteratively validate the model. Figure **??** provides an overview of our approach.

3.1 Participant Recruiting

We recruited experts from academia and industry from the fields of blockchain, cryptocurrency, usability, security, and software engineering. Participants were recruited using the professional network of the authors and public lists of validated European blockchain experts[1]. We specifically looked for experts who previously published peer-reviewed research articles in relevant fields or professionally worked with blockchain or cryptocurrency. We were rigorous not to accept experts not meeting at least one of these criteria, resulting in a panel of 25 experts for the Delphi study.

3.2 Focus Group

To obtain an initial understanding of the threat landscape for cryptocurrency users we carried out a 115-minute-long focus group with 6 experts. The workshop was conducted remotely using Zoom and Miro, a web-based collaborative board. Together with existing research, the discussion of the focus group built the foundation for the development of the initial version of the threat model.

3.3 Delphi Study

To iteratively validate the threat model, we used a three-round, survey-based Delphi process. The Delphi method is a well-established qualitative approach for achieving consensus among experts through an iteratively steered dialog [11, 25]. A panel size between 15 and 30 experts [8] with a total of three rounds [30] is recommended. Between August 19th and September 6th, 2020, we sent out three weekly questionnaires presenting the model. Experts were asked to provide their opinions within 5 days, after which their feedback was integrated into the next iteration. The updated model and the anonymized comments served as input for the subsequent round. To iterate and validate the model, experts were asked to provide their opinion along the following dimensions: (1) Soundness: Does the categorization make sense? (2) Completeness: Are threats missing? (3) Relevance: How relevant are the threats in practice? (4) Countermeasures: How can these threats be best addressed? In each round, we distributed the entire threat model. In addition to questions on the model in general, we followed the approach used by Emami et al. [14] and split the model into four buckets to ask for detailed feedback on the specific categories and threats while

[1] https://blockpool.eu/experts/ (last accessed 2021-06-29)

Figure 1: The threat model was developed in five steps. First, we conducted a focus group (n=6). Second, we combined the outcomes with existing research on cryptocurrency threats into the first version. Third, in steps 2-4, we used a three-round Delphi process (n=25) to validate and iterate the model before consolidating the collected information into a final step.

minimizing survey fatigue [5]. Experts were randomly assigned to one bucket in the first round and then rotated in the subsequent rounds to collect a broad set of opinions. At the end of each survey, we provided room for experts to voice their opinion on categories they were not assigned to in the respective round. In total, 25 experts participated in the study, of which 22, 23, and 20 filled out the survey in the respective rounds. After the third iteration the model was consolidated into its final version. No major changes were necessary in this last step.

3.4 Limitations

We conducted our research intending to provide a thorough record of threats relevant to cryptocurrency users. However, we cannot claim general exhaustiveness, as the field of cryptocurrency systems and their underlying technical implementation is constantly evolving. We limited the scope to threats relevant to end-users and applicable for cryptocurrencies in general. Threats related to specific technical implementations of cryptocurrencies are not covered. To assess potential vulnerabilities related to the consensus mechanism and infrastructure layer of specific cryptocurrencies, a case-by-case analysis is necessary. Through the conversations with the experts in our panel, we noticed additional risks of cryptocurrency ownership beyond the scope of our research — e.g. legal, regulatory, and governance risks — but are still worth considering by anyone thinking about dealing with cryptocurrencies.

4 RESULTS

This section presents a comprehensive overview of threats that affect cryptocurrency users. We propose six categories and describe threat agents, possible consequences, and countermeasures for each threat. We first provide a brief overview of threat categories, threat agents, and potential consequences and then describe each category.

4.1 Threat Model Overview

We propose the six categories of threats that are relevant for cryptocurrency users.

(1) **Accidental Threats**: Accidental threats describe risks due to human error or omission, unintended equipment malfunction, or natural disaster.
(2) **Privacy Threats**: Privacy threats affect the correlation of public transaction data and information from additional sources — i.e., social media, data leaks — to obtain personal data about the victim.
(3) **Physical Threats**: Physical threats concern attacks against people and their possessions — i.e., storage devices.
(4) **Financial Fraud Threats**: Financial fraud threats concern the systematic manipulation of cryptocurrency markets, emerging from their unregulated nature.
(5) **Social Threats**: Social threats exploit the social nature of humans, i.e., their trust in other people and organizations.
(6) **Technical Threats**: Threats arising from the technologies used to interact with cryptocurrency systems

4.1.1 Threat Agents. We build on the generic set of threat agents proposed by the Open Web Application Security Project (OWASP) [37]. The descriptions below are verbatim quotes from Adam Shostack's Threat Modeling: Designing for Security, pages 478 - 479 [45].

- **Non-Target Specific**: Non-Target Specific Threat Agents are computer viruses, worms, trojans, and logic bombs.
- **Employees**: Staff, contractors, operational/ maintenance personnel, or security guards annoyed with the company.
- **Organized Crime and Criminals**: Criminals target information that is of value to them, such as bank accounts, credit cards, or intellectual property that can be converted into money. Criminals will often make use of insiders to help them.
- **Corporations**: Corporations who are engaged in offensive information warfare or competitive intelligence. Partners and competitors come under this category.
- **Human (Unintentional)**: Accidents, carelessness
- **Human (Intentional)**: Insider, outsider
- **Natural**: e.g. flood, fire, lightning, meteor, earthquakes

4.1.2 Potential Consequences. The following list of potential consequences highlights the potential damages to the cryptocurrency users if the threats materialize. Not all consequences lead to loss of cryptocurrencies directly.

- **Disclosure of Personal Data**: Private data about the victim becomes available to the attacker.
- **Complete Loss of Cryptocurrency**: The victim loses access to their entire cryptocurrencies in their wallet.
- **Partial Loss of Cryptocurrency**: The victim partially loses access to their cryptocurrencies — i.e., one transaction.
- **Temporary Loss of Access**: The victim temporarily loses access to their cryptocurrency, or transactions are deferred.
- **Endangered Personal Health**: The health of the victim is endangered.
- **Loss of Reputation**: The reputation of the victim (pseudonymous / virtual / real identity) is damaged.
- **Reduction of Value**: The relative value of the victim's cryptocurrency is reduced — i.e. it is worth less.

4.2 Accidental Threats

Accidental threats describe risks due to human error or omission, unintended equipment malfunction, or natural disasters. Items in this category do not have an intentional attacker. We can distinguish the following threats:

4.2.1 Erroneous Recording of Access Credentials. Access credentials — i.e., passwords, mnemonics, private keys — are recorded incorrectly, rendering the wallet and the associated cryptocurrencies inaccessible at a later time.

- **Threat Agents**: Human, Unintentional
- **Consequences**: Complete Loss of Cryptocurrency
- **Countermeasures**: Access credentials — i.e., mnemonics — should be verified immediately after recording them. This process might also be supported through the design of applications that require such a check.

4.2.2 Loss of Access Credentials. Access credentials — i.e., passwords, private keys, mnemonics, and other forms of backups — are recorded correctly but stored inadequately, ultimately being lost. Inadequate storage includes not storing access credentials, failing to consider hardware breakdown or catastrophes. We can distinguish the following sub-forms:

- **Forgetting Access Credentials**: Access credentials — i.e. wallet passwords, cold wallet pins – are not noted down and forgotten over time. This includes forgetting the location of a storage device if stored in a 'secret' place.
- **Accidental Destruction**: Access credentials are destroyed by accident by the users — i.e., overwriting a wallet.dat file, formatting a hard drive, or throwing the storage medium away.
- **Equipment Breakdown**: The hardware on which the access credentials are stored breaks down due to a technical failure, without accessible secondary backups in place.
- **Destructive Catastrophes**: Access credentials are lost due to natural catastrophes or 'acts of god' — i.e. fire, flooding, meteors.

All sub-forms of this threat share the following characteristics:

- **Threat Agents**: Human (Unintentional), Natural
- **Consequences**: Complete Loss of Cryptocurrency
- **Countermeasures**:
  - Novice users without the technical knowledge or motivation to deal with key management can resort to trustworthy custodial platforms that allow account recovery mechanisms through, e.g., government-issued identification.
  - Users comfortable with key management should backup their keys in a redundant manner. Digital backups should be stored on physically different devices, and analog backups should be stored in spatially different locations. Backups should be secured through access control — e.g., device passwords, bank deposit boxes. If physical access control is not available, a mnemonic can be split into three pieces so that two pieces suffice to recover the key.
  - For professional users handling large sums, advanced infrastructure (hardware security modules, multi-signature-based quorum controls, etc) might be a viable option. Utilizing third-party providers for advanced governance and/or insurance might provide additional security; e.g. Ledger's Vault platform or Coinbase Custody.

4.2.3 Erroneous Transaction. Erroneous Transactions are slips when executing a transaction. Colloquially they are also known as *Fat Finger* or *Gold Finger Transactions*. We distinguish the following sub-forms:

- **Misspelled Address**: Entering an incorrect but valid receiver address. The transaction is sent to a burned or foreign address without any way to reverse it.
- **Misspelled Amount**: Entering an incorrect amount. More than intended is sent to the destination address.
- **Misspelled Fees**: Entering incorrect transaction fees. Fees are awarded to the miner with no way to recover them.

All sub-forms of this threat share the following characteristics:

- **Threat Agents**: Human (Unintentional)
- **Consequences**: Partial Loss of Cryptocurrency
- **Countermeasures**:
  - Users should compare every transaction thoroughly before committing them.
  - Developers should design user interfaces to make it easy to catch fat finger transactions. Developers should (1) make it easy to compare addresses, (2) warn about high transactions (compared to the transaction history of the user), and (3) warn about unreasonably high transaction fees.

4.3 Privacy Threats

Pseudonymity or anonymity are central features to popular cryptocurrencies. Privacy threats affect the correlation of public transaction data and information from additional sources — i.e., social media, data leaks — to obtain personal data about the victim. The exploitation of privacy threats on their own does not directly lead to the loss of cryptocurrency but might enable further attacks. Within this category, we can distinguish and define the following threats:

4.3.1 De-Anonymisation. De- Anonymisation describes the analysis of existing digital artifacts — transactions, social media, etc. — in an effort to find the virtual or real-world identity of a person or company owning cryptocurrencies. For example, attackers might learn about the amount of the cryptocurrency, correlated wallets, and all the victim's past transactions. This information could be used as a stepping stone to launch further attacks.

- **Threat Agents**: Organized Crime and Criminals
- **Consequences**: Disclosure of Personal Data
- **Countermeasures**: Users can mitigate the risk of De-Anonymisation by (1) not publishing cryptocurrency addresses on the internet, (2) using cryptocurrencies that offer privacy-by-design (e.g., Monero, Zcash), or (3) using mixing services (e.g., Wasabi). However, to avoid De-Anonymisation completely, users need to acquire a thorough technical understanding of the privacy properties different cryptocurrencies offer.

4.3.2 Dusting Attack. A dusting attack involves unsolicitedly sending negligibly small amounts of cryptocurrency to a large pool of cryptocurrency addresses. By observing subsequent transactions on how these unspent transactions outputs (UTXOs) are combined, the attacker can correlate different wallet addresses controlled by one user. The goal of a dusting attack is to eventually link the dusted addresses to the owner's identity.

- **Threat Agents**: Organized Crime and Criminals, Corporations
- **Consequences**: Disclosure of Personal Data
- **Countermeasures**: Victims of a dusting attack can either freeze the UTXOs received as part of the dusting attack or transfer all non-dusted UTXOs to a completely new wallet. Defense against dusting attacks requires substantial awareness of one's account balances. Most users should be fine accepting the risk.

4.3.3 Tainted Coin Attack. An attacker in possession of cryptocurrencies obtained through criminal activity knowingly transfers these tainted coins to a victim to correlate the victim and their wallet addresses with the crime.

As a result, the victim's existing coins in their wallets could become less fungible — i.e., certain exchanges do not accept them anymore — and the victim themselves might become subject to a criminal investigation.

- **Threat Agents**: Organized Crime and Criminals
- **Consequences**: Loss of Reputation, Partial Loss
- **Countermeasures**: As the attack requires knowledge about the victim, keeping user information private is critical. Once affected, tainted coins can be sent back to the sender or mixing services may be used to clean tainted coins.

4.3.4 Identity Theft. Know-Your-Customer (KYC) policies require custodial exchanges to inquire about the real-world identity of customers. The information a victim discloses to the exchange or third-party KYC provider is a valuable target for attackers that could be resold, utilized to launch targeted attacks, or used to assume the victim's identity.

- **Threat Agents**: Organized Crime and Criminals, Human (Intentional)
- **Consequences**: Disclosure of Personal Data
- **Countermeasures**:
  - Instead of using centralized exchanges, cryptocurrency can be bought via P2P exchanges that do not require users to undergo a KYC process.
  - For centralized exchanges, reducing the amount of information shared — e.g., using a drivers' license instead of an ID — can lower the risk exposure.

4.4 Physical Threats

Physical threats concern potential attacks against people and their possessions — i.e., storage devices, laptops, data centers. Threats under this category have an intentional attacker and are not unique to cryptocurrency users.

Criminals have targeted wealthy individuals before Bitcoin existed. However, they are relevant because people known to own cryptocurrencies have been increasingly targeted for exactly that reason. Within this category, we can distinguish the following threats:

4.4.1 Theft. Theft of physical items — i.e., laptop, mnemonic codes — with the aim to get access to cryptocurrencies. Theft can either be a crime of opportunity or targeting a specific user.

- **Threat Agents**: Organized Crime and Criminals, Human (Intentional)
- **Consequences**: Complete Loss of Cryptocurrency
- **Countermeasures**:
  - As with any valuable goods and holding valid for all privacy threats listed within this category, physical access protection will provide a first layer of defense.
  - Backups stored in the form of mnemonics can be secured by a passphrase to prevent illegitimate access to the assets. This method is commonly referred to as 'the 25th word'.
  - Storing the backup mnemonics as separate parts - where a subset is sufficient to recover the full backup - in different locations can help distribute the risk.
  - For digital storage devices, access protection through mechanisms like disk encryption is advisable. Upon theft of such an item, transferring funds to a newly created wallet can offer additional protection.

4.4.2 Vandalism. Vandalism refers here to the purposeful destruction of a victim's computer system and/or physical backups of their access credentials to render their cryptocurrencies inaccessible.

- **Threat Agents**: Organized Crime and Criminals, Human (Intentional), Human (Unintentional)
- **Consequences**: Complete Loss of Cryptocurrency, Loss of Reputation
- **Countermeasures**:
  - Novice users with small funds and limited technical knowledge may resort to custodial wallets or exchanges.
  - Advanced users comfortable with key management can resort to redundant systems and backups.

4.4.3 Extortion. Extortion refers here to using threats or force to the disadvantage of the victim, coercing them to pay the attacker off with cryptocurrency.

- **Threat Agents**: Organized Crime and Criminals, Human (Intentional)
- **Consequences**: Complete Loss of Cryptocurrency, Endangered Personal Health
- **Countermeasures**: By having a decoy wallet with a limited set of funds in it, owners can distribute their risk. Some wallets provide this feature — the popular hardware wallet Ledger allows users to set up wallets with two valid PINs, each unlocking a different account behind it.

4.4.4 Abduction. The abduction of a person – oftentimes targeting publicly known cryptocurrency owners – to demand ransom for their release.

- **Threat Agents**: Organized Crime and Criminals, Human (Intentional
- **Consequences**: Complete Loss of Cryptocurrency, Endangered Personal Health
- **Countermeasures**: Insurance against abduction (and other physical risks mentioned before) might be a complementary option for wealthy users to reduce the potential financial risk.

4.5 Financial Fraud Threats

Financial fraud threats concern the systematic manipulation of cryptocurrency markets, emerging from their unregulated nature. If exploited financial fraud threats do not necessarily result in a loss of cryptocurrencies but in a loss of value for the victim. These

threats are risks of any unregulated free market. Other financial markets like the stock market are also vulnerable, but regulatory bodies outlaw these practices. In this category, we distinguish the following threats:

4.5.1 Pump & Dump. Pump and Dump schemes work by artificially increasing the price of a cryptocurrency while at the same time creating excitement on social media as prices surge. Once enough victims buy into the surging cryptocurrency, the attackers sell their shares, causing the prices to drop.

- **Threat Agents**: Organized Crime and Criminals
- **Consequences**: Reduction of Value
- **Countermeasures**:
  - Speculative trading in unregulated markets comes with the inherent risk that organized groups manipulate the market to their favor. As individual user, investments into cryptocurrencies should be long-term and technology-focused. Users who engage in speculative trading would do best to inform themselves thoroughly about the involved risks. This mitigation strategy generally applies all further financial threats below.
  - To avoid falling victim to Pump & Dump schemes, users should be aware of them and avoid panic buy or sell actions.

4.5.2 Short & Distort. Short and Distort schemes work by artificially causing a price drop by spreading negative rumors on social media. Attackers earn profits by 'shorting' the cryptocurrency prior to the attack.

- **Threat Agents**: Organized Crime and Criminals
- **Consequences**: Reduction of Value
- **Countermeasures**: *see Pump & Dump countermeasures*

4.5.3 Short/Long Hunting. Exchanges with large amounts of assets could buy/ sell themselves to create price jumps that in turn trigger short/long positions to liquidate. Exchanges would know which prices will trigger liquidations and would have the financial incentive to do so, as they earn on trading fees.

- **Threat Agents**: Organized Crime and Criminals, Corporations
- **Consequences**: Reduction of Value
- **Countermeasures**: Avoid centralized exchanges and speculative trading.

4.5.4 Rinse & Repeat. Whales — entities that control a significant amount of a specific cryptocurrency — can use their assets to cause sudden price jumps. A common tactic of whales is to cause a price drop by creating sale orders below market price, indicating falling prices and triggering panic sales. Once prices are low, the whale buys back the cryptocurrency at a profit.

- **Threat Agents**: Human (Intentional), Corporations, Organized Crime and Criminals
- **Consequences**: Reduction of Value
- **Countermeasures**: Avoiding speculative trading (see above)

4.5.5 Fake Walls. The aforementioned whales can also create a large buy or sell orders, building a 'wall' that causes the price to rise or fall. Other users follow the trend and issue even higher/ lower buy/sell orders. However, right after creating the orders, the whale simply cancels them and fulfills the higher/ lower orders placed by the victims.

- **Threat Agents**: Human (Intentional), Corporations, Organized Crime and Criminals
- **Consequences**: Reduction of Value
- **Countermeasures**: Avoiding speculative trading (see above)

4.5.6 Insider Trading. Without regulatory protection in place, insiders may use their access to privileged non-public information to their advantage. For example, employees of major exchanges or token creators can use information about a future listing on a popular exchange to benefit from the increase of the price following the public announcement.

- **Threat Agents**: Human (Intentional), Corporations
- **Consequences**: Reduction of Value

4.6 Social Threats

Social threats exploit victims' trust. We differentiate between Social Engineering, using psychological manipulation to convince people to perform actions or disclose confidential information, and the Platform Risk, putting trust into a third party that misuses the trust placed in them. Within this category, we distinguish the following threats:

4.6.1 Scams. We define 'Scams' as all forms of threats that trick the user into committing resources — fiat money, cryptocurrency — to a fraudulent cause. Within this threat, we distinguish the following sub-forms:

- **Fraudulent Exchange (Exit Scam)**: Fraudulent Exchange Scams refer to exchanges/ custodial wallets that are created with the aim to steal the user's cryptocurrencies at a later point.
- **Fraudulent Cryptocurrency Scam**: Fraudulent Cryptocurrency Scams convince a large number of victims to invest in the alleged cryptocurrency based on fraudulent promises. Examples are (1) Ponzi Schemes, (2) Pyramid Schemes, (3) Fake ICOs, (4) Fake Cryptocurrencies named after existing companies or projects.
- **Transaction Scam**: Transaction Scams trick the victim into sending cryptocurrencies while never providing the promised service in return. Examples of transactions scams are (1) fake token sales from private people, (2) local bitcoin sales, and (3) malicious merchants who never deliver the promised goods.
- **Impersonation Giveaway Scam**: Impersonation Giveaway Scams trick the victim by making them believe a famous/rich entity gives away cryptocurrency for free. The victim is convinced to send cryptocurrency to the attacker's address, believing the sent amount is being transferred back with a premium.
- **Blackmail Scam**: A scam making the user believe the attacker has sensitive information about the victim — i.e., browser history, video of the victim watching porn — which they will release unless the victim pays a ransom. This kind of scam is often combined with personal information about the victim to make the threat more believable.

All sub-forms share the following threat characteristics:

- **Threat Agents**: Organized Crime and Criminals
- **Consequences**: Complete Loss of Cryptocurrency, Loss of Reputation
- **Countermeasures**:
  - Education of users on how to assess the legitimacy of claims and common types of social engineering threats.

A 23

- Avoiding offers that are 'Too Good To Be True' or require to complete an action under (time) pressure. If in doubt, users should consult a trusted person and make use of a four-eye principle.
- Browser extensions like EtherAddressLookup can provide additional protection by offering warnings when browsing to potential fraudulent websites.

4.6.2 Phishing Attacks. We define 'Phishing Attacks' as all forms of threats that trick the user into revealing sensitive information, e.g., passwords or private keys, to the attacker. Attackers use lookalike copies, e.g., of exchanges, to trick the user into revealing their access credentials to take over their original account. Attackers likely deploy established phishing strategies to do so. Within this threat, we distinguish the following sub-forms:

- **E-Mail Phishing**: Attackers sending emails, impersonating a trustworthy source with the goal of stealing personal information from the victim. E-Mail phishing might redirect users to phishing websites, trick them into revealing their keys or mnemonics or download manipulated wallet software.
- **Ad Phishing**: Attackers use ads on search engines and/or social media to redirect the victim to a phishing site.
- **Social Media Phishing**: Direct messages on social media channels (i.e., Twitter, Facebook) or private forums (i.e., Slack, Telegram) redirecting the victim to a phishing site.
- **Voice Phishing**: Voice phishing refers to phishing through social engineering attacks via phone. Oftentimes attackers impersonate global brands and trusted agencies such as Microsoft or the IRS (US Tax office).
- **SMS Phishing (SMiShing)**: Attackers using mobile phone text messages (SMS) to lure victims into immediate action, such as downloading mobile malware, visiting a malicious website, or calling a fraudulent phone number.
- **Spear-Phishing**: Targeted Phishing of individual cryptocurrency owners with the aim to gain control of their cryptocurrencies using any of the above methods.

All sub-forms share the following threat characteristics:

- **Threat Agents**: Organized Crime and Criminals, Non-Target Specific
- **Consequences**: Complete Loss, Disclosure of Personal Data
- **Countermeasures**:
  - General skepticism towards any communication from platforms that were not initiated by the users, together with education of users on how to assess the legitimacy of claims, build a first step to mitigate social threats.
  - As mentioned before, trustworthy browser extensions can provide additional protection.
  - For custodial exchanges, users should ensure to access the platform directly via their URL - avoiding detours via links, search engines, or social networks - and to have two-factor-authentication with a secure passphrase in place.
  - For users comfortable handling their own keys, cold storage solutions provide additional security.

4.6.3 Platform Risk. Platform risk refers to centralized platforms — i.e., exchanges or custodial wallets — not following local laws and regulations and restricting individuals from accessing, sending, or receiving cryptocurrencies. Centralize services could decide to (1) close or block an account, (2) restrict the ability to send transactions, (3) restrict the ability of other users on the platform to send transactions to an address, or (4) remove access to the keys of a specific account.

- **Threat Agents**: Corporations, Employees
- **Consequences**: Complete Loss of Cryptocurrency, Temporary Loss of Cryptocurrency, Disclosure of Personal Data
- **Countermeasures**: Users should not rely on one single platform, backup and own the keys to their cryptocurrencies.

4.7 Technical Threats

Threats arising from the technologies used to interact with cryptocurrency systems. We focus on threats in the application layer, those that affect how the user interacts with the system, and purposefully exclude threats in the underlying infrastructure layer, consensus layer, or threats specific to certain cryptocurrency implementations. Within this category, we distinguish the following threats:

4.7.1 Malware. Malware refers to malicious computer software. In the context of cryptocurrency threats, it refers to software that runs on the victim's system without their knowledge to gain access to their asset/ cryptocurrencies. Within this threat, we can distinguish the following sub-forms:

- **Wallet/ Key Extraction Malware**: Wallet/ Key Extraction malware steals the private keys directly or the wallet repository — i.e., 'wallet.dat' file — for later encryption from the victim's system.
- **Transaction Manipulation Malware**: Transaction Manipulation Malware manipulates single transactions to redirect them to the addresses under the control of the attacker – i.e., a 'Clipboard Hijacker' malware listening for cryptocurrency addresses to be copied and replacing them with the attacker's address.
- **Credential Extraction Malware**: Credential Extraction Malware steals access credentials of the user — i.e. a keylogger listening for password entry on Coinbase or other websites.
- **Ransomware:** Ransomware encrypts the victim's data — i.e., their wallet — and demands ransom for decrypting it.

All sub-forms share the following threat characteristics:

- **Threat Agents**: Organized Crime and Criminals, Non-Target Specific
- **Consequences**: Complete Loss of Cryptocurrency, Disclosure of Personal Data
- **Countermeasures**:
  - For custodial wallets, two-factor authentication can provide additional security in case a device is compromised.
  - For software wallets on internet-connected devices (hot wallets), users should make sure to use a secure passphrase.
  - Increasingly large funds, especially when stored for a long time, should be moved to cold wallets.
  - Wallets should be backed up in a separate secure way, i.e., not on the same device.
  - Transactions should be checked carefully for their correctness before submitting them. Developers of wallets should make it easy for users to perform these checks (e.g., compare addresses, sent amount).

4.7.2 Fraudulent Client Applications. Fraudulent Client Applications pretend to perform services for users but secretly manipulate the output to the advantage of the attacker. Within this threat, we distinguish the following sub-forms:

- **Fraudulent Key/Wallet Generator**: A Fraudulent Key/Wallet Generator is a piece of hardware or software that creates a wallet for the user while at the same time providing the attacker access to the private keys, e.g., by pre-computing them. The victim believes only they are in possession of the private keys, while the attackers could at any time access the cryptocurrencies the user stores in this wallet.
- **Fraudulent Wallet**: A Fraudulent Wallet software pretends to be a secure client software to manage the cryptocurrency of the victim. A Fraudulent Wallet may (1) send the private keys to the attacker once the user imports an existing wallet or (2) manipulate transactions sent by the users behind the scenes.
- **Fraudulent QR Code Generator/ Scanner**: A Fraudulent QR Code Generator/ Scanner manipulates the encoded receiver address, replacing the original address with the attackers.

All sub-forms share the following threat characteristics:

- **Threat Agents**: Organized Crime and Criminals, Non-Target Specific
- **Consequences**: Complete Loss of Cryptocurrency, Disclosure of Personal Data
- **Countermeasures**:
  - Users should inform themselves whether a wallet software appears to be trustworthy before using it.
  - Wallet software should be downloaded only from trusted sources and be verified for integrity.
  - QR Codes should only be scanned or generated using the trusted wallets directly, not via third-party applications.

4.7.3 Attacks on Third-Party Services. Attacks on Third-Party Services do not target the user's devices but services they may rely on. Within this threat, we distinguish the following sub-forms:

- **Online Exchange Hack**: Attackers compromising a cryptocurrency exchange or custodial wallet that manages the cryptocurrencies of the user resulting in either (1) temporal inaccessibility of the cryptocurrencies (e.g., DOS attack), (2) partial loss of the cryptocurrencies managed by the exchange, or (3) complete loss of the managed cryptocurrencies. A successful attack on an exchange is often accompanied by the affected exchange filing for bankruptcy, making it increasingly difficult for users to regain the funds.
- **Block Explorer Manipulation**: Manipulation of block explorer platforms providing an interface to check the state of a blockchain (e.g., Etherscan). Victims using the block explorer can be deceived to believe a transaction has happened when it actually hasn't, being a steppingstone in a coordinated attack.
- **SIM Swapping Attacks**: Attackers port the victim's telephone number to their own SIM card by manipulating the telecom provider. Often used as part of an account-takeover attempt to break two-factor-authentication.

All sub-forms share the following threat characteristics:

- **Threat Agents**: Organized Crime and Criminals, Non-Target Specific
- **Consequences**: Complete Loss of Cryptocurrency, Disclosure of Personal Data
- **Countermeasures**:
  - Before using an exchange, users should inform themselves about the security measures they have in place. Large exchanges have started to adopt insurance policies that cover the loss of customer funds.
  - Web-based block explorers should best be accessed via TLS connections, and users should pay attention to valid certificates. In critical situations, checking transactions via different block explorers might help to spot manipulation.
  - Users can mitigate SIM Swapping attacks by securing their telecom account with a secure password. Alternatively, to using short messages as two-factor-authentication, they could change to authenticator apps.

4.7.4 Smart Contract Threats. Smart Contract Threats concern risks that arise from interactions with smart contracts. Users might not be aware that they are dealing with a smart contract — e.g., when cryptocurrencies are, in fact, ERC20 tokens implemented on the Ethereum blockchain. Within this threat, we can distinguish the following sub-forms:

- **Backdoor for Admin**: A deliberate backdoor in the smart contract that allows privileged users of the smart contract to withdraw funds. Oftentimes, this functionality is hidden through clever use of programming side effects that are not immediately detected when inspecting the code.
- **Honeypot Contracts**: A honeypot is a smart contract that pretends to leak its funds to an arbitrary user (victim), provided that the user sends additional funds to it. However, the funds provided by the user will be trapped, and only the honeypot creator (attacker) will be able to retrieve them.
- **Unintended Smart Contract Vulnerabilities**: Smart contracts might contain technical vulnerabilities which may (1) allow attackers to gain access to the contract's funds or (2) cause unexpected behavior leading to the loss of the contract's funds. Classifying common smart contract vulnerabilities is an active field — i.e. https://dasp.co/.

All sub-forms share the following threat characteristics:

- **Threat Agents**: Organized Crime and Criminals, Human (Intentional), Human (Unintentional)
- **Consequences**: Partial Loss of Cryptocurrency
- **Countermeasures**:
  - Upfront checking that the smart contract has undergone a white-glove security audit (security-review) by a reputable security firm.
  - Upfront checking whether the verified source code of the contract can be found on a platform — e.g., Etherscan for Ethereum Smart Contracts — and double-checking the code by the user.

4.7.5 Transaction Attacks. Transaction Attacks concern the manipulation of transactions on the blockchain itself. The provided list addresses the most common threats and does not claim exhaustiveness. Within this threat, we distinguish the following sub-forms:

- **Majority Attack (51% Attack)**: The attacker gains control over the majority of the resources limiting the consensus mechanism,

allowing them to manipulate past transactions. These attacks become more feasible the less popular the targeted cryptocurrency is.

- **Double Spending**: An attacker broadcasts a transaction to the blockchain — convincing the victim that the transaction was issued — following up with a second transaction with higher transaction fees which transfers the same funds to a different address under the attacker's control, causing the first transaction to fail. The second transaction 'overtakes' the original one.
- **Flood Attack**: The attacker issues a large number of transactions, flooding the backlog of transactions waiting to be confirmed (mempool) and delaying other transactions from being confirmed. For the end-user, this results in unexpected long waiting times.
- **Other Base Layer Attacks**: Depending on the implementation of specific cryptocurrencies, there are several additional threats targeting the consensus layer, infrastructure layer (e.g., DDoS attacks, NTP attacks), or network layer (e.g., routing and partitioning attacks). These threats deserve a thorough investigation on their own, which is outside of this project's scope. We point to recent research addressing this topic [7, 10, 40].

All sub-forms share the following threat characteristics:

- **Threat Agents**: Organized Crime and Criminals, Human (Intentional)
- **Consequences**: Partial Loss of Cryptocurrency, Temporary Loss of Cryptocurrency
- **Countermeasures**:
  - Avoiding investment in unknown cryptocurrencies.
  - Waiting for the recommended number of confirmations after a transaction was included in the blockchain before considering it as successfully sent.

5 DISCUSSION

We discuss the implications of our findings for usable security research on cryptocurrency systems. While these implications are valid primarily for cryptocurrencies, they may offer valuable insights to understanding the threat landscape users face when interacting with emerging blockchain applications in general. We summarize our findings, discuss the relevance to the proposed model, and propose design and research challenges for the HCI community.

5.1 Summary

Our results indicate that cryptocurrency users find themselves under the pressure of a broad and diverse range of threats. While previous work has focused on the technical security of blockchain systems, many of the threats users face are not of technical nature but exploit users' misconceptions or gullibility. To create both usable and secure applications, researchers and developers need to acknowledge the socio-technical nature of cryptocurrencies and account for the many threats not rooted on a technical level.

Understanding which threats exist is imperative to address them. The model presented in this paper provides the first overview of threats relevant to end-users. For researchers, it can serve as a foundation to understanding the threat landscape, enabling a discussion on how to address it through human-centered research. For practitioners building user-facing cryptocurrency systems, we see twofold application: First, it can be used as a tool to evaluate how existing applications support or impede users in recognizing potential threats. Second, it can be used as starting point to an application specific threat modeling process to ensure completeness.

5.2 Relevance

We collected reports of incidents for all threats presented and queried the expert panel for their assessment. In the third round of the study, experts rated the practical relevance of each threat category on a five-point Likert scale. From their responses, we calculated a score by coding the answers as [-2, -1, 0, 1, 2], and averaging their sums by the number of answers, resulting in a score between -2 (not at all relevant) and 2 (highly relevant). Table 1 shows the calculated scores. All categories received positive scores, indicating their practical relevance in the eyes of our panel. The scores are also reflected in the qualitative responses of participants. On the topic of Privacy Threats, one participant pointed out that anonymity and consequently privacy are not inherent elements of cryptocurrencies. Future regulatory developments might push back on anonymity, and cryptocurrencies connected to the identity of users might even be advantageous in some aspects. While these are certainly interesting aspects for research — i.e., understanding how the omission of anonymity would change user behavior — we argue for the inclusion of Privacy Threats in the model. As the overwhelming majority of today's cryptocurrencies is designed to be pseudonymous or anonymous, privacy remains an active subject of research and concern of cryptocurrency users in practice.

In a similar fashion, Physical Threats deserve inclusion in the model. While any wealthy individual can become an attractive target for criminals, we have found several incidents where cryptocurrency owners were specifically targeted. Thus, the reason for including these threats in the model is not because they are unique but because they are relevant for cryptocurrency users. We think practitioners and developers should know that these threats have evolved and exist in the cryptocurrency space — only then can they think about whether and how they should be addressed.

Table 1: The relevance scores (-2=not at all relevant, 2=highly relevant) for each threat category. All categories are considered relevant by the expert panel, with Privacy and Physical Threats less strongly compared to the other categories.

Accidental Threats	1.60
Privacy Threats	0.75
Physical Threats	0.35
Financial Fraud Threats	1.45
Social Threats	1.45
Technical Threats	1.65

5.3 Design Challenges and Future Work

In this paper, we presented a first look at potential countermeasures to deal with threats. However, it is unclear how useful these countermeasures are in practice. We hypothesize that high interaction costs or the necessity of detailed technical knowledge are barriers to adoption. There is a unique role for the HCI community to explore these questions and contribute to mitigating threats for cryptocurrency users by making security and privacy measures

more accessible. We draw up three directions for future research centering around effectively educating users, building assistive systems, and improving the usability of existing systems through the development of design guidelines.

5.3.1 Educating Users. Education has been a longstanding research area in the HCI community. Teaching users about the threat landscape and providing advice on dealing with them is a first step to prevent threats from materializing. While many threats rooted in misjudgment can be addressed this way, it is unclear how to best achieve this, especially given the complex nature of cryptocurrencies. Arguably, it is not realistic to expect users to read a scientific publication before engaging with cryptocurrencies. As of now, we know little about which methods work, and there remain many questions relevant for HCI: Which information is crucial to avoid misconceptions? How effective are digital onboarding processes to convey knowledge and affect behavior? How do novel approaches such as Coinbase's Earn program perform to this end? We call upon researchers to explore methods to efficiently educate users on relevant threats and how to avoid them.

5.3.2 Assistive Systems. Beyond education, assistive systems might prove an effective tool to bridge the gap between awareness and behavior by supporting users in recognizing and avoiding threats. First examples can already be found in practice. ETHProtect monitors Ethereum addresses involved in fraudulent activity. We have little understanding of how well these systems work for end-users. HCI research could contribute by investigating how to make these solutions accessible to a broad range of users. Moving assistive systems closer to the place where users might face threats might be a key step to increasing adoption and could help stop threats arising from misjudgment. Additionally, the development of novel assistive systems can be addressed by HCI. Potential future directions might concern privacy communicating interfaces, intelligent user interfaces detecting potential attacks from market data, or users' physiological reactions. HCI research can play a valuable role in exploring which assistive technologies provide effective protection and are also accepted by users. In this context, a specifically interesting question is how far such systems should protect users from their own misjudgment by restricting their ability to interact with cryptocurrencies.

5.3.3 User Interface Guidelines. Researchers should further pursue the development of guidelines for designing secure and usable cryptocurrency interfaces. Effective guidelines may help developers to translate theoretical findings into secure user interfaces. Such guidelines could be developed, building on established interface design theory and best practice examples found in existing cryptocurrency systems. Pursuing research in this direction will require a thorough look at aspects for cryptocurrencies that, to our knowledge, have not been considered by HCI so far. How can users be motivated to back up their keys securely? How usable are hardware wallets? How can we make it easier for users to compare cryptocurrency transactions? How could a usable multi-sig wallet be implemented? Addressing these questions will benefit many smaller aspects along the way. A particular challenge in designing these guidelines will be to balance the trade-off between complexity and security under the consideration of different types of users.

6 CONCLUSION

This paper presents the first systematic overview of threats cryptocurrency owners have to face, proposing an organization into six overarching categories: Accidental Threats, Privacy Threats, Physical Threats, Financial Fraud Threats, Social Threats, and Technical Threats. The proposed model was iteratively validated following a three-round Delphi process with 25 experts. Results suggest it to be a valuable tool for researchers and practitioners to inform future research on cryptocurrency systems. We argue that finding countermeasures to these threats needs to go beyond the technical dimension and follow a user-centered approach. To this end, we call upon the HCI community to take this threat landscape as a stimulus to investigate how more secure and more usable interfaces for cryptocurrency systems can be developed to ultimately reduce the pressure of threats under which cryptocurrency users may find themselves.

ACKNOWLEDGMENTS

This work was supported by the Deutsche Forschungsgemeinschaft (DFG) (grant no. 316457582 and 425869382). We thank the team from https://condens.io/ for supporting us with their qualitative research analysis tool — it helped us make sense of the heap of data in front of us.

REFERENCES

[1] Svetlana Abramova, Artemij Voskobojnikov, Konstantin Beznosov, and Rainer Böhme. 2021. *Bits Under the Mattress: Understanding Different Risk Perceptions and Security Behaviors of Crypto-Asset Users.* Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411764.3445679

[2] Ghada Almashaqbeh, Allison Bishop, and Justin Cappos. 2019. ABC: a cryptocurrency-focused threat modeling framework. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS).* IEEE, 859–864.

[3] Simon Anell, Lea Gröber, and Katharina Krombholz. 2020. End User and Expert Perceptions of Threats and Potential Countermeasures. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (2020).

[4] Andreas Auinger and René Riedl. 2018. Blockchain and Trust: Refuting Some Widely-held Misconceptions. In *Proceedings of the International Conference on Information Systems - Bridging the Internet of People, Data, and Things, ICIS 2018, San Francisco, CA, USA, December 13-16, 2018.* https://aisel.aisnet.org/icis2018/crypto/Presentations/2

[5] Kristen Backor, Saar Golde, and Norman Nie. 2007. Estimating survey fatigue in time use study. In *international association for time use research conference. Washington, DC.* Citeseer.

[6] Wubing Chen, Zhiying Xu, Shuyu Shi, Yang Zhao, and Jun Zhao. 2018. A Survey of Blockchain Applications in Different Domains. In *Proceedings of the 2018 International Conference on Blockchain Technology and Application* (Xi'an, China) *(ICBTA 2018).* Association for Computing Machinery, New York, NY, USA, 17–21. https://doi.org/10.1145/3301403.3301407

[7] Jieren Cheng, Luyi Xie, Xiangyan Tang, Naixue Xiong, and Boyi Liu. 2020. A survey of security threats and defense on Blockchain. *Multimedia Tools and Applications* (2020), 1–30.

[8] Mark J Clayton. 1997. Delphi: a technique to harness expert opinion for critical decision-making tasks in education. *Educational psychology* 17, 4 (1997), 373–386.

[9] Coinmarketcap. 2021. *Top 100 Cryptocurrencies by Market Capitalization.* Retrieved June 28, 2021 from https://coinmarketcap.com/

[10] Mauro Conti, E Sandeep Kumar, Chhagan Lal, and Sushmita Ruj. 2018. A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys & Tutorials* 20, 4 (2018), 3416–3452.

[11] Norman Dalkey and Olaf Helmer. 1963. An experimental application of the Delphi method to the use of experts. *Management science* 9, 3 (1963), 458–467.

[12] Raynor de Best. 2021. *Number of Blockchain wallet users worldwide from November 2011 to June 14, 2021.* Retrieved June 28, 2021 from https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/

[13] Chris Elsden, Arthi Manohar, Jo Briggs, Mike Harding, Chris Speed, and John Vines. 2018. Making Sense of Blockchain Applications: A Typology for HCI. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*

(Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, Article 458, 14 pages. https://doi.org/10.1145/3173574.3174032

[14] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the Experts: What Should Be on an IoT Privacy and Security Label? *arXiv preprint arXiv:2002.04631* (2020).

[15] Shayan Eskandari, David Barrera, Elizabeth Stobert, and Jeremy Clark. 2015. A First Look at the Usability of Bitcoin Key Management. *Proceedings 2015 Workshop on Usable Security* (2015). https://doi.org/10.14722/usec.2015.23015

[16] Benjamin Fabian, Tatiana Ermakova, Jonas Krah, Ephan Lando, and Nima Ahrary. 2018. Adoption of security and privacy measures in bitcoin–stated and actual behavior. *Available at SSRN 3184130* (2018).

[17] Foundation for Interwallet Operability. 2019. Blockchain Usability Report. (2019), 19.

[18] Michael Froehlich, Charlotte Kobiella, Albrecht Schmidt, and Florian Alt. 2021. *Is It Better With Onboarding? Improving First-Time Cryptocurrency App Experiences*. Association for Computing Machinery, New York, NY, USA, 78–89. https://doi.org/10.1145/3461778.3462047

[19] Michael Froehlich, Maurizio Raphael Wagenhaus, Albrecht Schmidt, and Florian Alt. 2021. *Don't Stop Me Now! Exploring Challenges Of First-Time Cryptocurrency Users*. Association for Computing Machinery, New York, NY, USA, 138–148. https://doi.org/10.1145/3461778.3462071

[20] Michael Fröhlich, Felix Gutjahr, and Florian Alt. 2020. Don't Lose Your Coin! Investigating Security Practices of Cryptocurrency Users. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference* (Eindhoven, Netherlands) *(DIS '20)*. Association for Computing Machinery, New York, NY, USA, 1751–1763. https://doi.org/10.1145/3357236.3395535

[21] Andrea Gaggioli, Shayan Eskandari, Pietro Cipresso, and Edoardo Lozza. 2019. The Middleman Is Dead, Long Live the Middleman: The" Trust Factor" and the Psycho-Social Implications of Blockchain. *Frontiers Blockchain* 2 (2019), 20.

[22] Neil Gandal, JT Hamrick, Tyler Moore, and Tali Oberman. 2018. Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics* 95 (2018), 86–96.

[23] Xianyi Gao, Gradeigh D. Clark, and Janne Lindqvist. 2016. Of Two Minds, Multiple Addresses, and One Ledger: Characterizing Opinions, Knowledge, and Perceptions of Bitcoin Across Users and Non-Users. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 1656–1668. https://doi.org/10.1145/2858036.2858049

[24] Ghi Paul Im and Richard L Baskerville. 2005. A longitudinal study of information system threat categories: the enduring problem of human error. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems* 36, 4 (2005), 68–79.

[25] William Jones, Robert Capra, Anne Diekema, Jaime Teevan, Manuel Pérez-Quiñones, Jesse David Dinneen, and Bradley Hemminger. 2015. "For telling" the present: Using the delphi method to understand personal information management practices. *Conference on Human Factors in Computing Systems - Proceedings* 2015-April (2015), 3513–3522.

[26] Josh Kamps and Bennett Kleinberg. 2018. To the moon: defining and detecting cryptocurrency pump-and-dumps. *Crime Science* 7, 1 (2018), 18.

[27] Irni Eliana Khairuddin, Corina Sas, Sarah Clinch, and Nigel Davies. 2016. Exploring Motivations for Bitcoin Technology Usage. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI EA '16)*. Association for Computing Machinery, New York, NY, USA, 2872–2878. https://doi.org/10.1145/2851581.2892500

[28] Katharina Krombholz, Heidelinde Hobel, Markus Huber, and Edgar Weippl. 2015. Advanced social engineering attacks. *Journal of Information Security and Applications* 22 (2015), 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

[29] Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer, and Edgar Weippl. 2017. The other side of the coin: User experiences with bitcoin security and privacy. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 9603 LNCS (2017), 555–580. https://doi.org/10.1007/978-3-662-54970-4_33

[30] Barbara Ludwig. 1997. Predicting the future: Have you considered using the Delphi methodology. *Journal of extension* 35, 5 (1997), 1–4.

[31] C. Lustig and B. Nardi. 2015. Algorithmic Authority: The Case of Bitcoin. In *2015 48th Hawaii International Conference on System Sciences*. 743–752. https://doi.org/10.1109/HICSS.2015.95

[32] A. Mai, K. Pfeffer, M. Gusenbauer, E. Weippl, and K. Krombholz. 2020. User Mental Models of Cryptocurrency Systems - A Grounded Theory Approach. *Symposium on Usable Privacy and Security (SOUPS) 2020* (2020).

[33] Charles McFarland, Tim Hux, Eric Wuehler, and Sean Campbell. 2018. Blockchain Threat Report. *McAfee: Cryptojacking* (2018).

[34] Mehrnoosh Mirtaheri, Sami Abu-El-Haija, Fred Morstatter, Greg Ver Steeg, and Aram Galstyan. 2019. Identifying and analyzing cryptocurrency manipulations in social media. *arXiv preprint arXiv:1902.03110* (2019).

[35] Suvda Myagmar, Adam J Lee, and William Yurcik. 2005. Threat modeling as a basis for security requirements. In *Symposium on requirements engineering for information security (SREIS)*, Vol. 2005. Citeseer, 1–8.

[36] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. *bitcoin.org* (2008).

[37] OWASP.org. [n.d.]. *Category: Attack*. Technical Report. https://www.owasp.org/index.php/Category:Attack

[38] Bradley Potteiger, Goncalo Martins, and Xenofon Koutsoukos. 2016. Software and Attack Centric Integrated Threat Modeling for Quantitative Risk Assessment. In *Proceedings of the Symposium and Bootcamp on the Science of Security* (Pittsburgh, Pennsylvania) *(HotSos '16)*. Association for Computing Machinery, New York, NY, USA, 99–108. https://doi.org/10.1145/2898375.2898390

[39] Eveshnie Reddy and Anthony Minnaar. 2018. Cryptocurrency: a tool and target for cybercrime. *Acta Criminologica: African Journal of Criminology & Victimology* 31, 3 (2018), 71–92.

[40] Muhammad Saad, Jeffrey Spaulding, Laurent Njilla, Charles Kamhoua, Sachin Shetty, DaeHun Nyang, and Aziz Mohaisen. 2019. Exploring the attack surface of blockchain: A systematic overview. *arXiv preprint arXiv:1904.03487* (2019).

[41] Corina Sas and Irni Eliana Khairuddin. 2015. Exploring Trust in Bitcoin Technology: A Framework for HCI Research. In *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction* (Parkville, VIC, Australia) *(OzCHI '15)*. Association for Computing Machinery, New York, NY, USA, 338–342. https://doi.org/10.1145/2838739.2838821

[42] Corina Sas and Irni Eliana Khairuddin. 2017. Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 6499–6510. https://doi.org/10.1145/3025453.3025886

[43] Sarwar Sayeed, Hector Marco-Gisbert, and Tom Caira. 2020. Smart Contract: Attacks and Protections. *IEEE Access* 8 (2020), 24416–24427.

[44] R. Shirey. 2007. *Internet Security Glossary, Version 2*. RFC 4949. RFC Editor. https://tools.ietf.org/rfc/rfc4949.txt

[45] Adam Shostack. 2014. *Threat modeling: Designing for security*. John Wiley & Sons.

[46] Frank Swiderski and Window Snyder. [n.d.]. Threat Modeling, 2004.

[47] Tony UcedaVelez and Marco M Morana. 2015. *Risk centric threat modeling*. Wiley Online Library.

[48] Artemij Voskobojnikov, Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. 2020. Surviving the Cryptojungle: Perception and Management of Risk Among North American Cryptocurrency (Non)Users. In *Financial Cryptography and Data Security*, Joseph Bonneau and Nadia Heninger (Eds.). Springer International Publishing, Cham, 595–614.

[49] M. E. Zurko. 2005. User-centered security: stepping up to the grand challenge. In *21st Annual Computer Security Applications Conference (ACSAC'05)*. 14 pp.–202.

Don't Stop Me Now! Exploring Challenges Of First-Time Cryptocurrency Users

Michael Fröhlich*
Center for Digital Technology and Management, Germany
froehlich@cdtm.de

Maurizio Wagenhaus
Ludwig Maximilian University, Germany
m.wagenhaus@campus.lmu.de

Albrecht Schmidt
Ludwig Maximilian University, Germany
albrecht.schmidt@ifi.lmu.de

Florian Alt
Bundeswehr University Munich, Germany
florian.alt@unibw.de

ABSTRACT

Cryptocurrencies have increasingly gained interest in practice and research alike. Current research in the HCI community predominantly focuses on understanding the behavior of existing cryptocurrency users. Little attention has been given to early users and the challenges they encounter. However, understanding how interfaces of cryptocurrency systems support, impede, or even prevent adoption through new users is essential to develop better, more inclusive solutions. To close this gap, we conducted a user study (n=34) exploring challenges first-time cryptocurrency users face. Our analysis reveals that even popular wallets are not designed for novice users' needs, stopping them when they would be ready to engage with the technology. We identify multiple challenges ranging from general user interface issues to finance and cryptocurrency-specific ones. We argue that these challenges can and should be addressed by the HCI community and present implications for building better cryptocurrency systems for novice users.

CCS CONCEPTS

• **Human-centered computing** → *Empirical studies in HCI*; • **Security and privacy** → *Usability in security and privacy*; • **Applied computing** → **Digital cash**.

KEYWORDS

cryptocurrency, blockchain, first-time users

ACM Reference Format:
Michael Fröhlich, Maurizio Wagenhaus, Albrecht Schmidt, and Florian Alt. 2021. Don't Stop Me Now! Exploring Challenges Of First-Time Cryptocurrency Users. In *Designing Interactive Systems Conference 2021 (DIS '21), June 28-July 2, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3461778.3462071

*Also with Ludwig Maximilian University, Bundeswehr University Munich,.

DIS '21, June 28-July 2, 2021, Virtual Event, USA

ACM ISBN 978-1-4503-8476-6/21/06…$15.00
https://doi.org/10.1145/3461778.3462071

1 INTRODUCTION

Driven by the rising popularity of cryptocurrencies, blockchain technology is receiving increased interest from practitioners and researchers. By January 2021, the number of Bitcoin wallet users has grown to exceed 65 million [10]. Over 8300 cryptocurrencies with a market capitalization exceeding 1 trillion USD are tracked on CoinMarketCap[1]. Accounting for 635 billion USD [9], Bitcoin [32] indisputably remains the most popular cryptocurrency.

Beyond cryptocurrencies, there is considerable ongoing development to improve blockchain technology. Advocates view the technology as transformative, comparing its potential impact to the Internet [11] and going as far as discussing a decentralized digital society [45]. At the same time, cryptocurrency systems still face major unsolved challenges: user interfaces suffer from usability issues [5, 12, 15, 18, 27], there remain fundamental trust challenges [4, 17, 22, 41, 42], cryptocurrencies are complex to understand [11, 12] and have a high entry barrier for people with less technical knowledge [19]. The HCI community has started to address these challenges — Elsden et al. presented the first topology of blockchain applications in the context of HCI and argue for an active role of HCI in the domain [11]. However, research has missed taking a closer look at novice cryptocurrency users, predominantly focusing on users already acquainted with the technology.

This leaves a gap in understanding what challenges novice users face. What barriers need to be overcome between the decision to buy cryptocurrency and making use of it for the first time? Understanding how interfaces of current cryptocurrency systems support, impede, or even prevent the adoption through new users is essential to develop better, more inclusive solutions in the future. To address this, we have conducted a qualitative user study with 34 participants. In a think-aloud study, we recorded participants during three tasks, each essential for new users: account registration, the first acquisition of Bitcoin, and spending them in an online shop. We triangulate our observations with semi-structured interviews with all participants. Contrary to previous research, our study focuses on custodial wallets, being the likely entry point for users without technical understanding of blockchain technology. Doing so, our study complements previous work investigating key management challenges [1, 12, 15].

Our analysis identified multiple challenges novice users need to overcome. We present three categories: (1) general user interface challenges; (2) finance-related challenges; and (3) cryptocurrency

[1]https://coinmarketcap.com/ (last accessed 15.05.2021)

challenges. Surprisingly, most challenges are not rooted in technical constraints of blockchain technology and can, therefore, be addressed with HCI methods. We discuss why the considered wallets are not designed with novice users in mind and present implications for HCI researchers and practitioners on how to address open challenges, to ultimately build systems better equipped to address the needs of novice users.

Contribution Statement. The main contributions of this work are (1) a qualitative investigation (n=34) of how first-time users interact with cryptocurrencies; (2) a classification of challenges users face in the process; and (3) implications for building cryptocurrency systems for novice users.

2 BACKGROUND

Our work builds on several strands of research, most notably research on blockchain and cryptocurrency applications from an HCI perspective.

2.1 Cryptocurrencies and HCI

Since the inception of Bitcoin in 2008 as "Peer-to-Peer Electronic Cash System" [32], cryptocurrencies have seen increasing rates of adoption, with recent studies reporting rates as high as 11% in Germany [8] and 18% in Turkey [39]. Likewise, cryptocurrencies have become a topic of interest in the HCI community.

Elsden et al. review existing research on blockchain applications and highlight that many of the core conceptual challenges related to long-standing issues in HCI research. They call on the HCI community to investigate the fundamental human challenges connected to blockchain technology [11]. Several publications have explored motivations of cryptocurrency users [15, 18, 23, 27, 41] with Financial Interest, Ideological Interest or Technological Interest [15] emerging as main reasons to engage with the technology. Users perceive cryptocurrencies to fulfill all functions of money [30], would like to use them as a means of payment, but criticize the lack of opportunity to do so [15].

Furthermore, previous work shows that the usability of cryptocurrency applications remains problematic [2, 5, 12, 15, 18, 27, 31]. Cryptocurrencies are difficult to understand and misconceptions are common. Mai et al. explored mental models of both cryptocurrency users and non-users and identified misconceptions in regard to keys, fees, and anonymity [29]. These misconceptions increase the risk of user errors: Krombholz et al. presented the first quantitative study of cryptocurrency users (n=990) and reported that 22.5% had lost cryptocurrencies in the past, most commonly through self-induced errors. Industry reports confirm these findings: In 2018, 18% of cryptocurrency users reported having lost cryptocurrencies due to user errors [13]. Security practices, especially key management, have been identified as core usability issues by past research [12, 15, 26, 29]. Eskandari et al. presented a first look at key management, remarking that users are challenged to keep keys simultaneously resilient to loss, resistant to digital theft, and accessible [12]. Krombholz et al. suggest categorizing wallets based on the control over key management they offer [27]. In their DIS'20 paper Froehlich et al. distinguish between self-managed and custodial wallets – wallets that hide key management aspects from the user, but require trust in the intermediary — and highlight the latter as an alternative for users with less technical affinity. They argue that users' decisions to choose a custodial or self-managed wallet is implicitly mediated by their risk assessment. Users less knowledgeable and motivated in their security skills would be inclined to choose custodial wallets over self-managed ones because they perceive the risk of making a mistake themselves higher than the risk of suffering betrayal from a third party [15].

With a considerable amount of users engaging with custodial wallets[2] and the apparent benefit of a lower technical entry barrier to foster financial inclusion, we were surprised to not find any HCI studies (beyond a Kazerani et al. with two participants [21]) focusing on custodial wallets. We think this gap is worth addressing. Recent work by Huebner et al. suggests cryptocurrency applications suffer from issues beyond key management. Their analysis of over 300.000 app store reviews revealed that both "user interfaces" and "the signup experience" of blockchain apps are rated worse than those of comparable finance applications [20].

2.2 Novice Users

While the importance of understanding novice users' needs is well established in the HCI community [33, 35], there seems to be no universally agreed-on definition. For the scope of this paper, we, therefore, refer to novice users as *"users who previously have not interacted or owned cryptocurrencies"*. While previous research in the field of cryptocurrencies to date has focused predominantly on established users, there is a small but emerging body of work investigating novice users [2, 16, 18, 21, 31].

Early work by Gao et al. characterizing the perception of Bitcoin across users and non-users with an interview study found that non-users expected that they would not be able to use cryptocurrencies without understanding the technology [18]. Kazerani et al. presented an exploratory study investigating the usability of Bitcoin with two novice users at the example of ChangeTip and Coinbase. Despite having just two participants, their study is worth mentioning, because they are, to our knowledge, the first to provide qualitative evidence that custodial wallets are hard to use [21]. More recently, Moniruzzaman et al. performed a cognitive walkthrough of five self-managed cryptocurrency wallets with five experts "*simulating the evaluation from the eye of a novice user*". They compare desktop and mobile wallets of different cryptocurrencies (Bitcoin, Ethereum, Ripple) and find high variations in error rates between different apps, overall concluding that current wallets lack usability for novice users [31].

Alshamsi and Andras presented the most comprehensive approach to date and were the first to include novice users directly. They quantitatively compared the perceived usability and security between Bitcoin and credit/debit cards with an in-between study setup with 22 novice cryptocurrency users and 33 established credit/debit card users. They report significantly worse perceptions of Bitcoin along the dimensions of Learnability, Efficiency, Help, Security, and Satisfaction. They highlight the relation between perceived usability and perceived security, arguing that the good usability of credit/debit cards positively influenced security

[2] Coinbase self-reports 43 million users (Jan 2021). See https://www.coinbase.com/about (last accessed 15.05.2021)

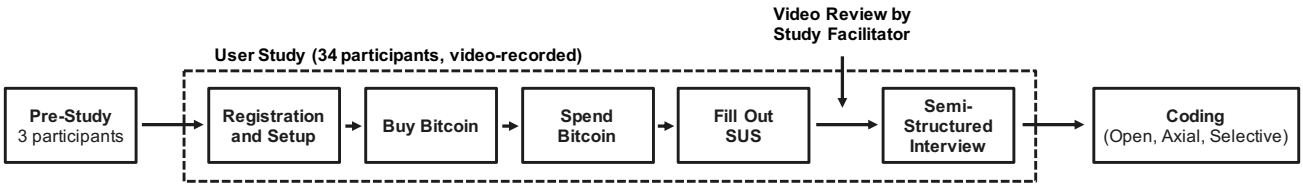


Figure 1: A visualization of our research approach. The user study was comprised of three tasks (1) Registration and Setup, (2) Buying Bitcoin, and (3) Spending Bitcoin. Afterward, participants were interviewed using retrospective probing. Data analysis followed an inductive approach, coding over several rounds.

perception. In contrast, Bitcoin's comparably poorer usability negatively influenced its security perception. Based on their findings, they discuss tradeoffs between usability and security and provide first suggestions on how to improve user interfaces for cryptocurrency systems. They conclude that Bitcoin as a payment system still faces major challenges and call for research on educating users, understanding users' challenges and mental models, and exploring how usable interfaces for novices can be designed [2]. With their findings rooted in a quantitative comparison study between one self-managed cryptocurrency app and credit card usage, we complement their work by contributing a qualitative think-out-aloud study providing the first in-depth exploration of novice users' challenges across three representative wallets on both mobile and desktop devices.

2.3 Summary

In the context of this paper, we can build on several learnings from previous work. Cryptocurrencies are complex to understand and misconceptions between users' mental models and the actual technical workings of the systems are common. Key management has been recognized as a challenge for users and addressed extensively by previous research. Custodial wallets offer an option to engage with cryptocurrencies without dealing with the details of key management, however, they require trust in the intermediary. While already widely used, we lack research on challenges users face with custodial wallets. First work exploring novice users' usability perception of Bitcoin indicates the need for further research. This work addresses these open questions and takes a closer look at the challenges that first-time cryptocurrency users are confronted with and how to overcome them.

3 METHOD

In this section, we describe our research approach, the sample of participants, the setup of the user study, and the analysis process.

3.1 Approach

We conducted a user study in English language between May 16th and September 9th, 2020, lasting between 12 and 102 minutes per participant (total 1195 minutes, average 39 minutes). Due to COVID-19, the user study was conducted remotely. Participants were instructed to think aloud and record their screens and audio — if necessary they received help setting up the recording software. After completing the study, users rated the usability of the tested wallets and shared their experiences in an interview. Prior to the study, we pre-tested our approach (n=3), resulting in minor adjustments of the instructions. As sensitive personal information had to be entered during registration, we obtained approval from the ethics board of our university (ID: EK-MIS-2020-018). Participants received EUR 30 or equivalent as compensation.

3.2 Participants

We recruited 34 people via social media and local networks in Munich, Germany. Participants qualified if they expressed interest to own cryptocurrency and reported not having done so in the past. 44 people indicated initial interest, of which 41 qualified. 6 people withdrew before starting and one participant from South Africa could not properly use the tested apps due to geographical restrictions. All participants resided in Europe – Germany (22), Austria (5), Denmark (2), Romania (2), Portugal (1), Sweden (1), United Kingdom (1). In the following, only the remaining 34 participants who started the user study are considered. 31 of them finished the entire study, resulting in a completion rate of 91%.

Table 1: The participants' demographics (n=34). The sample shows a slightly above average ATI scores, equal distribution between genders, is relatively young and well educated.

Demographic	Participants (%)
Gender	
Male	17 (50%)
Female	17 (50%)
Age	
20 – 24	5 (15%)
25 – 29	22 (65%)
30 – 39	4 (12%)
40 – 49	0 (0%)
50 – 59	3 (9%)
Highest Completed Education	
High School	5 (15%)
Bachelor Degree	14 (41%)
Master Degree	14 (41%)
PHD or Higher	1 (3%)
Annual Household Income in EUR	
15k or less	12 (35%)
15k – 30k	10 (29%)
30k – 45k	4 (12%)
45k – 60k	4 (12%)
60k or more	4 (12%)
ATI Scale	
1 – 1.99	1 (3%)
2 – 2.99	4 (12%)
3 – 3.99	11 (32%)
4 – 4.99	16 (47%)
5 – 6	2 (6%)

Table 1 shows the demographics of the participants. Our sample is gender-balanced with an average age of 28.73 years and an average annual household income between EUR 25,294 and EUR 49,411. In comparison, previous quantitative work found the sample of cryptocurrency users to be predominantly male (85%) with an average age of 28.56 years [27]. As for household income, we could not identify comparable data, but think it is worth to be reported in the context of cryptocurrencies. The Affinity for Technology Interaction (ATI) score describes a person's tendency to engage in or avoid technology interaction (6=high affinity, 1=low affinity). Our participants rank between 1.78 and 5.56 (mean 3.89) showing a broad range among the sample, slightly above average compared to the German population [3, 14, 47].

With women arguably making up half the potential user group, we think it is important not to marginalize them in the investigation of usability issues. We did not notice any gender differences during our study and are confident that our findings are representative of first-time cryptocurrency users.

3.3 Apparatus

The user study explored the challenges first-time users face when first interacting with cryptocurrencies. To reduce tool bias, we selected three wallets: Bitpanda[3], Coinbase[4], and TenX[5].

The wallets were chosen because they met several selection criteria: They were (1) custodial wallets, (2) implemented features to buy and send cryptocurrency, (3) offered both iOS and Android clients, and (4) had positive app store ratings (see table 2). Only Bitpanda and Coinbase offered a web application for desktop devices. Figure **??** shows the main screen of the tested wallets.

We reasoned that in a natural situation users would decide on whether to register an account on a mobile or desktop device. We, therefore, kept the decision which form factor to use to the participants and randomly assigned them to one of the three wallets according to their choice[6].

Table 2: The mobile app ratings (August 24th 2020) and the number of participants per wallet completing the study.

Wallet	Ratings (1=worst, 5=best)		Participants	
	App Store	Play Store	Mobile	Desktop
BitPanda	4.4	4.5	6	7
Coinbase	4.5	3.7	6	6
TenX	4.4	4.5	6	-

The user study was composed of three tasks, structured around the activities of (1) creating an account, (2) purchasing cryptocurrency, and (3) spending cryptocurrency. We chose these tasks because they arguably represent the first steps users want to take when engaging with a cryptocurrency wallet for the first time. Previous work investigating self-managed wallets used similar tasks [2, 31], but did not include purchasing of cryptocurrencies.

[3]http://bitpanda.com/ (last accessed 15.05.2021)
[4]https://coinbase.com/ (last accessed 15.05.2021)
[5]https://tenx.tech/ (last accessed 15.05.2021)
[6]We included both desktop and mobile devices to identify overarching challenges when engaging with cryptocurrencies. We acknowledge that desktop and mobile devices are different form-factors that deserve independent examination in future research.

We deliberately kept the task instructions to a minimum to allow participants to explore the wallet functionality themselves but advised them to ask for help if they got stuck. 16 out of 34 participants requested help at least once during the study. 3 out of 34 participants canceled the study (no common pattern). Each participant was instructed to

(1) Setup an account with the select application
(2) Purchase Bitcoin worth EUR 20
(3) Spend a maximum of EUR 15 in Bitcoin for a gift card or donation using Bitrefill[7] or BitPay[8]

After completion of all tasks, participants filled out a questionnaire to rate the usability of the tested wallets using the System Usability Scale (SUS) [7]. At last, an interview was conducted remotely via WhereBy[9] and recorded with the consent of participants. During the interview, challenging situations identified in the video recordings were addressed using retrospective probing [6].

3.4 Data Analysis

Data analysis followed an inductive approach using the think aloud and interview transcripts as data sets. To obtain an initial understanding, we used open and axial coding. During the initial open coding, two researchers independently coded the first 15 protocols. In a second step, we discussed the emerged codes and their relations to categorize them into higher-level axial codes. After agreeing on a final set of categories, focusing on challenges users encounter, two researchers used the agreed-upon codebook to selectively code the data set of the first 10 participants. We report an inter-rater reliability with an average Krippendorff's alpha of 0.87, indicating a high degree of agreement between coders [25].

Table 3: The inter-rater reliability (Krippendorff's Alpha) for the first 10 interviews.

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
0,96	0,90	0,94	0,82	1,00	0,96	0,90	0,78	0,68	0,72

Table 3 shows Krippendorff's alpha broken down to the participants' levels. Conflicts between coders occurred mostly due to ambiguous statements — i.e. statements that addressed several issues at once — and could be resolved in a joint review. The remaining interviews were coded by only one of the two researchers.

3.5 Limitations

We recognize that this study setup faces limitations regarding the generalizability of the results. First, the three selected wallets might not be entirely representative for all custodial wallets. By choosing well-rated ones, we reason that these applications are comparably well suited to identify challenges related to cryptocurrencies and not app design in general. Second, the think-aloud method puts participants in an unusual situation, potentially influencing behavior, and cannot capture issues users are not aware of [37]. We address this through method-triangulation with retrospective probing [6]. Third, all participants of the study were situated in Europe. Different cryptocurrency regulations in other jurisdictions might impact the experience of users in ways not observed.

[7]https://bitrefill.com/ (last accessed 15.05.2021)
[8]https://bitpay.com/ (last accessed 15.05.2021)
[9]https://whereby.com/ (last accessed 15.05.2021)

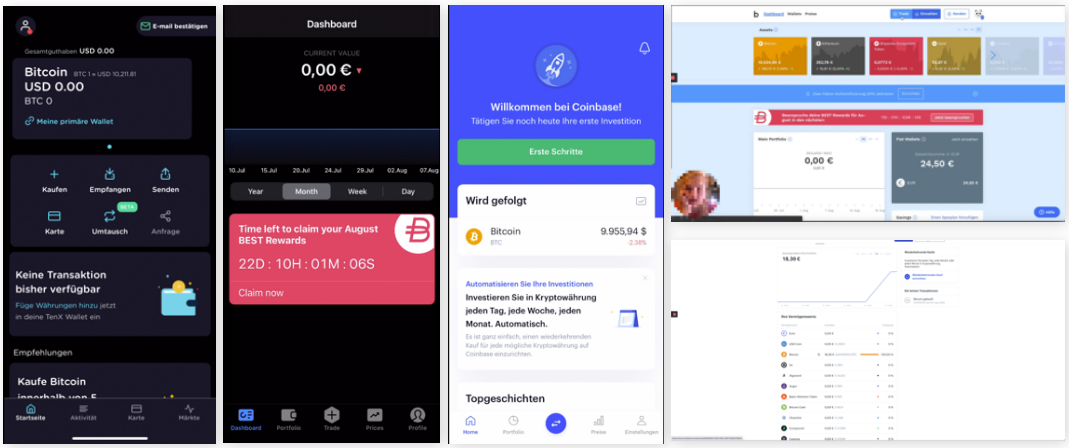


Figure 2: Screenshots of the first screen of each of the tested wallets (a full set of screenshots can be found in the supplementary material). From Left to right: TenX Mobile, BitPanda Mobile, Coinbase Mobile, Bitpanda Web, Coinbase Web.

4 FINDINGS

Our analysis reveals several challenges novice users have to overcome when interacting with cryptocurrency systems. The collected SUS ratings confirm these observations, showing that participants did not perceive the wallets to be usable. Table 4 depicts the scores and their corresponding US letter grades (A+ to F) [43] for both mobile and desktop versions. With the exception of TenX[10], the wallets rated well below the overall average SUS score in general (68) [43], the average SUS score of mass-market consumer software (74) [28], and the average SUS score for mobile apps (77) [24]. With a SUS score of 80 being the industrial goal [28], the perceived usability of the tested apps lacks considerably for novice users — emphasizing the need to further examine the usability of wallet applications.

Table 4: The resulting SUS scores per wallet. In parentheses the corresponding letter grades are shown.

Wallet	Ratings (max 100.0)	
	Mobile	Desktop
BitPanda	49.6 (F)	51.3 (F)
Coinbase	48.0 (F)	55.8 (D)
TenX	70.0 (C)	-

We organize the identified challenges into three overarching categories. Challenges in the first two categories are not exclusive to cryptocurrencies but relevant for developing a complete understanding of why users are struggling with custodial wallets today. Our intention behind reporting these challenges is to provide guidance for practitioners on how to address them.

(1) **User Interface Challenges:** This category subsumes challenges originating from the design of the user interface.
(2) **Finance Challenges:** This category subsumes challenges connected to the financial services offered in the application.
(3) **Cryptocurrency Challenges:** This category subsumes challenges tightly linked to core cryptocurrency concepts.

[10]While we cannot provide a definite answer to the comparably better SUS of TenX, we reason that the mobile-first design approach led to a simpler user-interface, more suited for novice users.

4.1 User Interface Challenges

We observed a set of common usability issues resulting from poor interface design across all three wallets. These findings may shed light on why user interfaces of blockchain mobile apps were found to be perceived worse than other categories of finance apps [20].

4.1.1 User Interfaces Are Not Optimized For Novice Users. User Interfaces offer rich functionality, overloading new users with information without adequately emphasizing the primary actions the user is looking for. At the same time the system status is only poorly reflected in the user interface and critical information for new users – i.e. account verification status — is hidden in setting menus.

Ambiguous System Status. To interact with a system, users generally need to answer two questions: (1) "What is the state of the system?", and (2) "How can they change it?" [48]. Users struggled to understand the system status in two situations specifically: the account verification status and which features were accessible. Especially the out-of-sync account verification status resulted in a cumbersome experience for users. Unclear about whether the verification was initiated, some users started the process a second time, even though their documents were already being processed. In several instances, users needed to manually sign out and in of their accounts for the new status to take effect, even after receiving an email confirmation about the success of the verification. In two wallets, unverified users could access the main interface of the application, without having the necessary authorization to interact with it. Instead, interactions resulted in error messages, often shown only after a few steps into the interaction.

Primary Actions Are Difficult to Access. Users opening a cryptocurrency application for the first time have a limited set of actions they want to complete: Finish their account setup, purchase cryptocurrency and potentially send a first transaction. All wallets had feature-rich user interfaces with high information density, designed for advanced users. Novice users, however, struggled to make sense of the information, find orientation, and locate the features they

needed. The most striking example of this was the account verification. Being an essential step it should be easily accessible. Instead, two wallets placed it in the settings menu, leaving users clueless where to find it. Another complicating issue concerned the purchasing flow to cryptocurrencies. One wallet required an intermediary step to deposit money into a "Euro Wallet" before users could buy cryptocurrency; directly purchasing cryptocurrency was not possible. This interim step increased interaction cost and consistently startled users — they tried to buy Bitcoin first until, by trial-and-error, they figured out they have to deposit Euros first.

4.1.2 General Issues. We encountered several additional usability issues during the study. Many of these are specific to the interface design of single wallets – e.g. unlabeled buttons or ambiguous iconography. We think that two issues are worth mentioning as they occurred across all three wallets.

Poor Error Messages. Novice users, likely to make mistakes during the initial exploration, are dependent on error messages that support their learning. However, participants were consistently confronted with error messages failing to do so: they were poorly constructed, contained finance-related or technical terms, and lacked actionable advice to support recovery. Application of established guidelines, namely that error messages should be explicit, human-readable, polite, precise, and contain constructive advice, could greatly benefit the experience of novice users [36].

Localization Issues. All three wallets exhibited a lack of localization, specifically poor, partial, or no translation at all. Additionally, one wallet did not accept the non-ascii character in the registration form, resulting in P15 having to find a workaround for the character "ß" in their name. While all participants in our sample were proficient in English, many people around the world are not, seriously limiting accessibility for those. For users struggling to learn the vocabulary that comes with cryptocurrencies inaccurate and faulty translations may further hinder their progress. Beyond accessibility, developers should provide professional localization out of self-interest. Users that encountered poor or partial translations noted the "*unprofessional*" impressions it left on them.

4.2 Finance Challenges

Our analysis revealed several finance-related challenges. These challenges arise from aspects every finance app needs to deal with. We found that the verification process is a major cause of frustration for first-time users and payment methods — though essential for cryptocurrency apps — frequently do not work as expected.

4.2.1 The Extended Account Verification Introduces Friction. Regulations require financial institutions to verify the identity of their customers. We observed the extended verification process to be one of the major causes for errors and frustration of participants during the study, confirming earlier findings [20].

Inadequate Explanations: The extended verification process is most commonly denoted as "Account Verification" and covers two aspects: anti-money-laundering (AML) and know-your-customer (KYC) regulations. The latter requires users to disclose the real identity, including personal information such as their national ID and address of residency. However, the necessity behind this process is only sparsely explained to users, often with rather technical and sparse descriptions, e.g. "Due to anti-money laundering policies". More detailed information provided behind a link is ignored by the vast majority of users. This results in misconceptions and negative sentiment on the users' side. For example, P12 assumed the data was collected for "*customer research and profiling*". P20 felt anxious about providing such personal data "*Does one really need to enter all this information ... This is scary*" and P27 thought the wallet expected them to "*be a fraudster*". In comparison, users with knowledge about the purpose of this extended verification process — e.g. through experience with other finance or ride-sharing apps — accepted the process and did not further question it.

Weak KYC Framework Integration: For identity verification, all wallets used third-party providers. Weakly integrated provider frameworks, as we observed in one wallet, break with the familiarity of the app and interrupt the overall user experience. Participants were confused by the new interface, increasingly so when different KYC providers were selected, seemingly at random, when the process was restarted. For example, P19 assumed to be the victim of a scam: "*It was a different one than the first time. I thought, "Oh my god, somebody hacked it and now he is taking all my information!"*. The weak integration was additionally frustrating for users who had to restart the process as it did not retain the state of already submitted documents.

Error-Prone KYC Process: This proved especially relevant, as KYC processes were likely to fail. 14 participants had to restart the verification process at least once, resulting in frustration: P21 vented, "*This is real crap!*" and P27 complained, "*I am going crazy with this!*". There were several issues leading to cancellation:

- **Policy Issues:** Policy issues arise from rules the wallet and KYC provider agreed on. For example, some types of national IDs were not accepted. In another instance, P19 registered their wallet account with only the first section of their hyphenated name, which was not accepted by the KYC provider and could only be changed by contacting the customer support of the wallet.
- **Document Issues:** Several users started the verification before preparing all documents and subsequently had to cancel it. While IDs were generally available, several users had to look for a utility bill to confirm their address.
- **Submission Issues:** In some instances, users had their documents not in the right format for the device they were using. P7 exported a PDF utility bill from an app on his smartphone, but could not select a PDF on the mobile interface. After several attempts, the participant sent the PDF to his computer, printed it, and scanned the printout using the camera dialogue of the verification process. Similarly, users on desktop devices had to switch to their smartphones to scan their IDs.
- **Connection Issues:** We observed several users struggling with network connection issues — either the KYC process would not start or abort abruptly.
- **Technical Issues:** Finally, we saw a variety of different technical issues, ranging from camera issues to browser compatibility issues to generic error messages.

4.2.2 Payment Methods Introduce Friction. Payment methods were an additional source of frustration for participants. We observed several underlying reasons: first, some users are anxious because they deal with money; second, payment methods used to buy Bitcoin did not work; and third, the status of the deposited money was not clearly communicated to users right away.

Dealing With Money Makes Users Nervous: We observed that some participants were increasingly cautious and nervous because they were dealing with money. While a soft observation, we think this is relevant as it indicates that some users might interact quite differently with finance-related systems compared to other categories. P20 stated "*With money, I am always extra cautious*" and P8 expressed clear expectations "*This is about money, not buttons!*". Consequently, users are anxious about making mistakes, especially given that they are not used to the interface of the new application. P4 expressed this insecurity when checking transaction details multiple times before finally submitting, saying "*It seemed like an important button that might initiate a transaction. I was unsure about what would happen if I entered a too high amount.*".

Payment Methods Are Likely To Fail: While essential to a cryptocurrency, payment methods proved challenging for many users — 10 participants needed to initiate the payment process at least twice. Several participants explicitly expressed disappointment that they could not pay via PayPal; most other participants chose debit/credit cards as their payment option. The most common reason for failure was a missing 3DSecure support of the credit card. However, in several instances, the reason for failure remained unclear. P26 got stuck on an infinite loading screen; P1 was redirected to a white screen without any content; for several users, credit card payment failed without any explanation. P31 summarizes her experience with, "*This is super complicated! It seems as if they don't even want me to buy Bitcoin!*"

Alternative Payment Options Offer Worse Experience: Alternative payment options, i.e. bank transfer, were used by only few participants and offered a worse experience than credit/debit cards. Users generally selected them only after credit/debit cards did not work. First, users generally expected their cryptocurrency or deposited Euros to be available immediately after the purchase and were often surprised if it was not the case. While deposit times were communicated by wallets, they were not visible enough for users, who just skipped over them. After completing their transaction with SOFORT Überweisung, P8 proclaimed, "*I think I am a proud owner of Bitcoin now... or not.*", only to later realize their mistake. Ambiguous or unclear presentation of the deposited money led to misconceptions of users: with no indication of the deposit, users were anxious it might have failed. With an ambiguous visualization, not emphasizing the *pending* status, users believed it had worked in an instant.

4.3 Cryptocurrency Challenges

Cryptocurrencies remain hard to deal with, even when taking key management out of the equation. We found several issues that participants found consistently challenging.

4.3.1 Dealing With Cryptocurrency Requires Mental Effort. Dealing with cryptocurrencies is hard. We observed several reasons why this is the case.

Users Mentally Convert Cryptocurrency To Fiat. We observed that novice users *think in the currency of their country of residence*: When purchasing or spending Bitcoin, users consistently resorted back to using their home currency. Wallet interfaces acknowledge this behavior to a certain extent. For example, the overall account balance is shown primarily in the fiat currency. Interfaces for sending Bitcoin proved more difficult to handle. Several users did not enter the purchase amount in Bitcoin as requested by the merchant but in Euros. This behavior can be problematic when the entered amount is interpreted as Bitcoin and users fail to notice — sending 15 Bitcoin by accident would be a quite costly mistake.

Different Exchange Rates Confuse Users. Due to the decentralized and volatile nature of cryptocurrencies, wallets and merchants frequently use different exchange rates. This caused over- or underpayments as users entered requested purchase amounts, not in Bitcoin but fiat currency, and used a toggle to convert to Bitcoin. Having calculated with the exchange rate of the wallet, the amount of Bitcoin sent did not match the one requested by the merchant.

Sub-comma Amounts Are Hard To Deal With. Handling small subcomma amounts when sending transactions proved challenging. Our observations indicate that dealing with amounts — e.g. sending *0.0015664788* Bitcoin compared to *15* Euro — increases effort for users. Users avoided manually entering values and instead used Copy&Paste. However, due to different localization of the decimal separator ("." vs ",") the input fields frequently rejected the pasted values. Manual entry required users to switch back and forth between the merchant and wallet interface multiple times: first, to enter the value, then to check it. User interfaces only accepting six decimal places even though Bitcoin extends to 8, lead to further confusion among users.

4.3.2 Fees Are Unexpected, Intransparent And Complicated. Networks fees are an essential part of how cryptocurrencies work as they incentivize miners to validate transactions. Previous work has recognized fees as a source of misconception for users [29]. Our findings add a dimension to it. Not just network fees are complicated to understand, but also platform fees introduced by the wallets. Users need to be aware of five types:

(1) **Deposit Fees** are charged by the wallet when users deposit money.
(2) **Exchange Fees** are charged by the wallet when users exchange currencies.
(3) **Withdrawal Fees** are charged by the wallet when users withdraw money. (not present in our study)
(4) **Merchant Fees** are added by the merchant on top of the purchase price of an item.
(5) **Network Fees** are added to a cryptocurrency transaction to incentive miners.

Users criticized the lack of clear explanations regarding fees. When asked after the study, the majority had little to no understanding of what fees were paid for and to whom they were paid. Consequently, users were surprised by the amount of fees paid during the

study. P8 complained, "*This is exorbitantly overpriced!*". On average, fees amounted to 2.15 EUR, with one participant paying a total of EUR 10.20 in fees during the study. This was caused by automatically calculated network fees amounting to 9.35 EUR, showing the downside of using heuristics for fee calculation [29]. A positive counter-example here was the wallet of TenX, which charged a flat fee of EUR 0.82 per cryptocurrency purchase.

Mental Model: What You See is What You Pay. We observed another aspect concerning Network Fees worth reporting. Users did not expect to pay fees when sending a transaction to the merchant. They expected the price tag of a product to be the final checkout value without any fees added — to buy a product priced 15 Euros, one pays 15 Euros. This hints towards the mental model of users: when buying products, European consumers are used to what-you-see-is-what-you-pay type prices.

4.3.3 Transaction States Are Intransparent. Cryptocurrency transactions undergo several steps before completion. They are published to the network, are validated and added to the blockchain, and finally considered valid only after a certain number of blocks — in the case of Bitcoin 6 — were added subsequently. Generally, novice users lack this technical understanding. Most participants believed that Bitcoin transactions would be in real-time and felt that waiting times were long and not sufficiently communicated. However, user interfaces displayed the status of transactions in ways that presumed this knowledge — i.e. "pending", "1 confirmation", "2 confirmations", ..., "confirmed", leading to confusion among users. Additionally, the states of transactions were displayed differently between the merchant and wallet, causing confusion about whether the transaction had actually succeeded. The merchant displayed transactions the moment they were published, yet not included in a mined block — users assumed the transaction was completed. Contrary, the wallet displayed the transaction as pending and neither was the purchased good, i.e. the voucher, delivered to the user's inbox.

4.3.4 The Payment Process Is Manual And Complicated. Users perceived the payment process as manual and complicated. Most expected that paying with cryptocurrency would be "*as easy as with PayPal*". Instead, they faced a manual process.

Missing Guidance For Novice Users. Upon completion of the checkout process users were presented with the requested purchase amount and a Bitcoin address to which they should send it. The checkout screens missed any further instructions for beginners. Additionally, the used language assumed knowledge of cryptocurrency-specific concepts. However, terms like "wallet" or "address" had ambiguous meanings for novice users. Confirming previous observations [2], several users did not recognize the address. P3 tried to enter the URL of the merchant's website, the Invoice ID, and the email address before considering the actual Bitcoin address. P15 did not think of their cryptocurrency app when reading "wallet", opening Apple's Wallet app on their iPhone instead.

Poor Checkout Process Integration Between Merchants And Wallets. The manual nature of the checkout process manifested in the missing integration between merchants and wallets. While merchants provided a QR Code and an "Open in Wallet" button intended to serve as shortcuts, they did not work. Both encoded a link in a URI-like format — "bitcoin:38Ap73vjNae5SaUBJXVS46muvRKk6Cikgf ?amount=0.020685". In the majority of cases, they failed to work. The link failed for any web-based wallets on desktop devices and only one mobile app responded. However, instead of processing the encoded parameters, it only opened the main screen of the app. Additionally, QR codes were hardly used. Except for one participant, users remained on one device throughout the checkout process. Scanning the QR Code when it is displayed on a desktop device would require an additional device switch users were not willing to make. Scanning the QR Code with the smartphone, it is displayed on is simply not possible.

Manual Payment Process Increases User Workload And Errors. Resulting from the lack of guidance and missing shortcuts, the payment process proved error-prone. Users had to manually switch between apps, locate the right functionalities to send transactions, and copy addresses and amounts between them. This lead to increased workload, frustration, and errors among users. Within the wallet apps, users struggled to locate the functionality to send a transaction. Copying the value from one app to another was perceived as a manual process that also lead to errors. Overall, 9 participants did not send the right amount of Bitcoin to the merchant.

5 DISCUSSION

Our results show that state-of-the-art cryptocurrency applications fail to address the needs of novice users. Many challenges do not arise from the underlying constraints of blockchain technology. Thus, developers may already improve their applications' usability significantly by applying existing guidelines such as Shneiderman's Golden Rules, or Nielsen's Usability Heuristics [34, 44]. Challenges specific to cryptocurrencies may prove more difficult to tackle. In the following, we present design implications for practitioners and highlight open questions for HCI research. Future work may build on these findings to develop guidelines on how to develop cryptocurrency wallets for beginners.

5.1 User Interfaces For Novice Users

Interfaces built for experts increase entry barriers and the likelihood of mistakes for new users. Previous research recommends adapting cryptocurrency tools to the risk perception of users [15], to diverging mental models [29], or to implement different interfaces for experts and novices [2]. We complement these recommendations with concrete suggestions on how to improve interfaces for novice users.

5.1.1 Present Relevant System Status and Interactions. Clearly and unambiguously communicating the status of a system to users is key to helping them bridge the gulf of evaluation; making important interactions easy to find also helps to overcome the gulf of execution [48]. Current wallets fail to adequately do so for new users as they present too much irrelevant information in domain-specific language, inadvertently hiding relevant information. Developers need to focus on making essential features easy to access [2], specifically system states and interactions related to account verification, buying cryptocurrency, and sending transactions.

5.1.2 Support Users' Learning Experience. Cryptocurrencies are a complicated topic to understand. Even established users frequently have incomplete or incorrect mental models [29]. Adaptive user interfaces and carefully crafted onboarding experiences could support users' learning experiences, gradually guiding them towards a more complete and correct understanding. Future research should investigate which information is crucial for users to form a functional mental model [38] of cryptocurrencies and how to translate it into user interfaces. To identify adequate ways, we encourage researchers to explore strategies deployed in the wild and involve users in the design process of new ones.

5.2 A Frictionless Signup Experience

The extended registration process is a major cause for frustration among novice users. Being required by regulation, reducing friction is crucial to avoid users abandoning applications before they unlock their full functionality. From our observations, we present implications for practitioners. The many issues related to the extended signup process indicate that this area could greatly benefit from HCI research. With increasing regulation, digital identity verification will become more prevalent as well. Understanding how to better design these could benefit applications in domains beyond cryptocurrencies, such as finance, micro-mobility, and e-government.

5.2.1 Inform Users First. KYC processes require users to disclose significant personal information. Often users do not know why the information is collected. It is crucial to clearly communicate the purpose behind inquiring about this information before the start of the process. Hyperlinks similar to "Terms and Conditions" notices should be avoided as users commonly ignore them [40]. Instead, explanations should be placed prominently, in such a way that users notice and read them. For compliance reasons the original legal texts may still be required to be linked, but the initial explanation should be written in a friendly manner and avoid technical or legal jargon when informing the user.

5.2.2 Eat the Biggest Frog First. Giving users access to the main interface before the extended verification process was completed resulted in an increased mental workload of users. Instead of clear guidance, now they had to find a way to start the verification process amidst the many features they could see, yet not use. Mark Twain is quoted to have said "*If it's your job to eat a frog, it's best to do it first thing in the morning. And if it's your job to eat two frogs, it's best to eat the biggest one first*". Given the unwanted friction and legal "must-have" quality of the extended signup process, it is fair to label it as a "frog", a big one in fact. Apps should guide the user through this process first, keep them informed about their progress, and only then present the full interface.

5.2.3 Provide An Integrated KYC Experience. Identity verification is commonly provided by third-party providers. "Lazy" integration of their frameworks breaks the user experience, causes confusion, and may lead to the cancellation of the process. Developers should aim for full control of the user experience during the verification process, including design language, the internal status of the verification process, and information — i.e. in the form of notifications — directed towards the user. Well-designed KYC processes should give users the feeling that they never leave the original application.

5.2.4 Expect Interruptions and Device Switches. Verification processes are likely to be canceled by users because they do not have the right documents ready, have connection issues, or face other technical difficulties on their device. Developers should account for this behavior and anticipate interruptions and device switches by the user. Each step of the process should, therefore, be stored and synchronized across devices, so users can seamlessly continue after interruptions.

5.3 Transparent Fees

While previous work addressed users' understanding of network fees [29], we find that the fees charged by custodial cryptocurrency platforms are equally difficult to understand. From this, we derive two implications.

5.3.1 Comprehensible Platform Fees. Platform fees should be communicated to users with utmost clarity. HCI can help design interfaces to this end, but there is a limit to how well complicated fee schemes can be explained. Wallets should aim to implement simple and consistent fee schemes, reducing the types of different fees. Easily comprehensible fees will avoid surprises, reduce frustration, and increase the long-term experience for users. We understand that such decisions are integral to the business models of companies developing wallets. High fees and a poor user experience will, however, only open the door for competition in the long term. Looking beyond cryptocurrencies, emerging brokerage startups have managed to simplify the traditionally complicated fee structure while staying profitable — e.g. digital brokerage platform TradeRepublic[11] offers a flat 1-Euro-Per-Trade fee. There is no reason why centralized cryptocurrency exchanges should not be able to do so as well.

5.3.2 Efficient Network Fee Visualization. Network fees are essential to how cryptocurrencies function, yet hard to understand for novice users. Mai et al. suggest heuristically pre-computed network fees labeled with easy-to-understand terms — i.e. "slow", "default", or "fast" [29]. We suggest additional features. In line with Nielsen's Help and Documentation heuristic [34], interfaces should explain the purpose of network fees in proximity to where they are shown. Explanations should avoid technical jargon, instead of focusing on users' tasks and how fees will influence the outcome — i.e. how fast the transactions will be completed. Presenting information aligned with users' mental models is key to making it easily interpretable: How many minutes does a "slow" transaction take? When will the transaction be completed? The same applies to communicating the cost of a transaction — presenting it in fiat currency or as a percentage of the overall transaction value might increase comprehension: distinguishing between 0.5 EUR and 5.0 EUR, or 1% and 10% requires little effort, compared to spotting the difference between 0.00004779 BTC and 0.0004779 BTC. As these small sub-comma values are prone to errors, interfaces for transactions should provide smart warning mechanisms [2] — e.g. based on fees typical of a specific cryptocurrency or the ratio between the fee and the transaction value. Smart warning mechanisms would further provide protection against both accidental user errors, so-called "Fat Finger Transactions", and errors in the heuristic fee calculation.

[11] https://traderepublic.com/

5.4 A Seamless Checkout Process

For establishing cryptocurrencies as a viable tool for online payment, much work remains to be done. Previous research recognizes the availability of merchants accepting cryptocurrencies [15], slow transaction times [2] and trust issues [41, 42] as open challenges. Our findings suggest that the manual payment process is another major challenge. Users expect a checkout process "*as easy as PayPal*" — current solutions however are manual, demand high interaction cost from users, and are prone to error.

5.4.1 Provide Adequate Guidance and Shortcuts. Merchant interfaces lacked guidance along the checkout process and used language that was easily misinterpreted ("wallet", "address") by novice users. Merchants should provide guiding explanations in plain language in the context of the checkout process to support users to correct misconceptions. While shortcuts (QR Codes, hyperlinks) between merchants and wallets promise to remove much friction from the process, adoption and interoperability lack behind. Wallets and merchants should work on establishing standards to transfer the wallet address and the transaction value automatically, reducing both interaction costs and the risk of "fat finger" mistakes. There remain several open questions to be addressed by HCI research. While shortcuts reduce manual work, they are also susceptible to attacks [26]. We encourage researchers to explore how methods to compare transaction data – e.g. [46] – can be implemented in the context of cryptocurrencies. Furthermore, it is unclear how transaction states should be presented. Current cryptocurrency systems have not yet developed a common understanding, resulting in ambiguous, confusing approaches. HCI research should explore how transaction states can best be displayed; how to communicate the necessary information, without presuming knowledge of the underlying technology.

5.4.2 As Easy As PayPal. While the recommendations above allow for an iterative improvement of the current checkout process, future research should explore how cryptocurrency payments can become truly frictionless. Many properties of Bitcoin — long alphanumerical addresses, high valuations, and high volatility, slow transactions — are difficult to handle and are not well suited for real-time purchases. Practitioners have noticed and addressed these issues through new solutions: the Ethereum Name System provides a DNS-like abstraction layer for cryptocurrency addresses; so-called Stable Coins aim to reduce volatility; and the Bitcoin Lightning Network enables real-time point-of-sale transactions. These and other technical improvements each solve important issues on their own. Most HCI research on cryptocurrencies today evolves around Bitcoin. Future research should explore how these new technologies can be integrated to enable truly seamless payments with cryptocurrencies.

6 CONCLUSION

This paper explores the interaction of first-time cryptocurrency users with custodial wallets. Our analysis reveals numerous challenges novice users need to overcome to engage with the technology, most prominently user interfaces designed for experts, a painstaking registration experience, and a manual and error-prone checkout process for paying with cryptocurrencies. Presenting the first investigation into custodial wallets, we reason that some of the identified challenges might be relevant in the larger context of finance apps. Rooted in these findings, we present design implications for practitioners and discuss how these challenges can be addressed by HCI researchers and practitioners. We think, moving towards usable cryptocurrency applications is an attainable goal and hope our work provides a valuable resource to direct future research on how cryptocurrencies can be made accessible to a broader range of people.

ACKNOWLEDGMENTS

This work was supported by the Deutsche Forschungsgemeinschaft (DFG) (grant no. 316457582 and 425869382). We thank the team from https://condens.io/ for supporting us with their qualitative research analysis tool — it helped us make sense of the heap of data in front of us.

REFERENCES

[1] Amanda Ahl, Masaru Yarime, Kenji Tanaka, and Daishi Sagawa. 2019. Review of blockchain-based distributed energy: Implications for institutional development. *Renewable and Sustainable Energy Reviews* 107 (2019), 200 – 211. https://doi.org/10.1016/j.rser.2019.03.002

[2] Abdulla Alshamsi and Prof. Peter Andras. 2019. User perception of Bitcoin usability and security across novice users. *International Journal of Human-Computer Studies* 126 (2019), 94 – 110. https://doi.org/10.1016/j.ijhcs.2019.02.004

[3] Christiane Attig, Daniel Wessel, and Thomas Franke. 2017. Assessing Personality Differences in Human-Technology Interaction: An Overview of Key Self-report Scales to Predict Successful Interaction. In *HCI International 2017 – Posters' Extended Abstracts*, Constantine Stephanidis (Ed.). Springer International Publishing, Cham, 19–29.

[4] Andreas Auinger and René Riedl. 2018. Blockchain and Trust: Refuting Some Widely-held Misconceptions. In *Proceedings of the International Conference on Information Systems - Bridging the Internet of People, Data, and Things, ICIS 2018, San Francisco, CA, USA, December 13-16, 2018.* https://aisel.aisnet.org/icis2018/crypto/Presentations/2

[5] Aaron W Baur, Julian Bühler, Markus Bick, and Charlotte S Bonorden. 2015. Cryptocurrencies as a disruption? empirical findings on user adoption and future potential of bitcoin and co. In *Conference on e-Business, e-Services and e-Society*. Springer, 63–80.

[6] Julie H Birns, Kristen A Joffre, Jonathan F Leclerc, and Christine Andrews Paulsen. 2002. Getting the Whole Picture: Collecting Usability Data Using Two Methods—-Concurrent Think Aloud and Retrospective Probing. In *Proceedings of UPA Conference*. Citeseer, 8–12.

[7] John Brooke. 1996. SUS: a 'quick and dirty' usability scale. *Usability evaluation in industry* (1996), 189.

[8] Karoline Busse, Mohammad Tahaei, Katharina Krombholz, Emanuel von Zezschwitz, Matthew Smith, Jing Tian, and Wenyuan Xu. [n.d.]. Cash, Cards or Cryptocurrencies? A Study of Payment Culture in Four Countries. ([n. d.]).

[9] Coinmarketcap. 2021. *Top 100 Cryptocurrencies by Market Capitalization.* Retrieved Jan 30, 2021 from https://coinmarketcap.com/

[10] Raynor de Best. 2021. *Number of Blockchain wallet users worldwide from November 2011 to January 24, 2021.* Retrieved Jan 30, 2021 from https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/

[11] Chris Elsden, Arthi Manohar, Jo Briggs, Mike Harding, Chris Speed, and John Vines. 2018. Making Sense of Blockchain Applications: A Typology for HCI. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, Article 458, 14 pages. https://doi.org/10.1145/3173574.3174032

[12] Shayan Eskandari, David Barrera, Elizabeth Stobert, and Jeremy Clark. 2015. A First Look at the Usability of Bitcoin Key Management. *Proceedings 2015 Workshop on Usable Security* (2015). https://doi.org/10.14722/usec.2015.23015

[13] Foundation for Interwallet Operability. 2019. Blockchain Usability Report. (2019), 19.

[14] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human–Computer Interaction* 35, 6 (2019), 456–467. https://doi.org/10.1080/10447318.2018.1456150 arXiv:https://doi.org/10.1080/10447318.2018.1456150

[15] Michael Fröhlich, Felix Gutjahr, and Florian Alt. 2020. Don't Lose Your Coin! Investigating Security Practices of Cryptocurrency Users. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference* (Eindhoven, Netherlands)

(DIS '20). Association for Computing Machinery, New York, NY, USA, 1751–1763. https://doi.org/10.1145/3357236.3395535

[16] Michael Fröhlich, Charlotte Kobiella, Albrecht Schmidt, and Florian Alt. 2021. Is it Better With Onboarding? Improving First-Time Cryptocurrency App Experiences. In *Proceedings of the 2021 ACM Designing Interactive Systems Conference* (Virtual Event, USA) *(DIS '21)*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3461778.3462047

[17] Andrea Gaggioli, Shayan Eskandari, Pietro Cipresso, and Edoardo Lozza. 2019. The Middleman Is Dead, Long Live the Middleman: The "Trust Factor" and the Psycho-Social Implications of Blockchain. *Frontiers in Blockchain* 2 (2019), 20. https://doi.org/10.3389/fbloc.2019.00020

[18] Xianyi Gao, Gradeigh D. Clark, and Janne Lindqvist. 2016. Of Two Minds, Multiple Addresses, and One Ledger: Characterizing Opinions, Knowledge, and Perceptions of Bitcoin Across Users and Non-Users. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 1656–1668. https://doi.org/10.1145/2858036.2858049

[19] Leonhard Glomann, Maximilian Schmid, and Nika Kitajewa. 2020. Improving the Blockchain User Experience - An Approach to Address Blockchain Mass Adoption Issues from a Human-Centred Perspective. In *Advances in Artificial Intelligence, Software and Systems Engineering*, Tareq Ahram (Ed.). Springer International Publishing, Cham, 608–616.

[20] Johannes Huebner, Remo Manuel Frey, Christian Ammendola, Elgar Fleisch, and Alexander Ilic. 2018. What People Like in Mobile Finance Apps: An Analysis of User Reviews. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia* (Cairo, Egypt) *(MUM 2018)*. Association for Computing Machinery, New York, NY, USA, 293–304. https://doi.org/10.1145/3282894.3282895

[21] Ali Kazerani, Domenic Rosati, and Brian Lesser. 2017. Determining the usability of bitcoin for beginners using change tip and coinbase. In *Proceedings of the 35th ACM International Conference on the Design of Communication*. 1–5.

[22] Irni Eliana Khairuddin and Corina Sas. 2019. An Exploration of Bitcoin Mining Practices: Miners' Trust Challenges and Motivations. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, Article 629, 13 pages. https://doi.org/10.1145/3290605.3300859

[23] Irni Eliana Khairuddin, Corina Sas, Sarah Clinch, and Nigel Davies. 2016. Exploring Motivations for Bitcoin Technology Usage. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI EA '16)*. Association for Computing Machinery, New York, NY, USA, 2872–2878. https://doi.org/10.1145/2851581.2892500

[24] Philip Kortum and Mary Sorber. 2015. Measuring the usability of mobile applications for phones and tablets. *International Journal of Human-Computer Interaction* 31, 8 (2015), 518–529.

[25] Klaus Krippendorff. 2018. *Content analysis: An introduction to its methodology*. Sage publications.

[26] Katharina Krombholz, Peter Frühwirt, Peter Kieseberg, Ioannis Kapsalis, Markus Huber, and Edgar Weippl. 2014. QR code security: A survey of attacks and challenges for usable security. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 79–90.

[27] Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer, and Edgar Weippl. 2017. The other side of the coin: User experiences with bitcoin security and privacy. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 9603 LNCS (2017), 555–580. https://doi.org/10.1007/978-3-662-54970-4_33

[28] James R Lewis. 2018. The system usability scale: past, present, and future. *International Journal of Human–Computer Interaction* 34, 7 (2018), 577–590.

[29] Alexandra Mai, Katharina Pfeffer, Matthias Gusenbauer, Edgar Weippl, and Katharina Krombholz. 2020. User Mental Models of Cryptocurrency Systems-A Grounded Theory Approach. (2020).

[30] Jens Mattke, Christian Maier, and Lea Reis. 2020. Is Cryptocurrency Money? Three Empirical Studies Analyzing Medium of Exchange, Store of Value and Unit of Account. In *Proceedings of the 2020 on Computers and People Research Conference* (Nuremberg, Germany) *(SIGMIS-CPR'20)*. Association for Computing Machinery, New York, NY, USA, 26–35. https://doi.org/10.1145/3378539.3393859

[31] Md Moniruzzaman, Farida Chowdhury, and Md Sadek Ferdous. 2020. Examining Usability Issues in Blockchain-Based Cryptocurrency Wallets. In *Cyber Security and Computer Science*. Springer International Publishing, 631–643. https://doi.org/10.1007/978-3-030-52856-0_50

[32] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. *bitcoin.org* (2008).

[33] Jakob Nielsen. 1994. *Usability engineering*. Morgan Kaufmann.

[34] Jakob Nielsen. 1995. 10 usability heuristics for user interface design. *Nielsen Norman Group* 1, 1 (1995).

[35] Jakob Nielsen. 2000. Novice vs. expert users. *Nielsen Norman Group* 1 (2000).

[36] Jakob Nielsen. 2001. Error message guidelines. *Nielsen Norman Group* 24 (2001).

[37] Jakob Nielsen. 2012. Thinking aloud: The# 1 usability tool. *Nielsen Norman Group* 16 (2012).

[38] Donald A Norman. 1983. Some observations on mental models. *Mental models* 7, 112 (1983), 7–14.

[39] ING Bank N.V. 2018. *Cracking the code on cryptocurrency: Bitcoin buy-in across Europe, the USA and Australia*. https://think.ing.com/uploads/reports/ING_International_Survey_Mobile_Banking_2018.pdf

[40] Jonathan A Obar and Anne Oeldorf-Hirsch. 2020. The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society* 23, 1 (2020), 128–147.

[41] Corina Sas and Irni Eliana Khairuddin. 2015. Exploring Trust in Bitcoin Technology: A Framework for HCI Research. In *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction* (Parkville, VIC, Australia) *(OzCHI '15)*. Association for Computing Machinery, New York, NY, USA, 338–342. https://doi.org/10.1145/2838739.2838821

[42] Corina Sas and Irni Eliana Khairuddin. 2017. Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 6499–6510. https://doi.org/10.1145/3025453.3025886

[43] Jeff Sauro and James R Lewis. 2016. *Quantifying the user experience: Practical statistics for user research*. Morgan Kaufmann.

[44] Ben Shneiderman. 1986. Eight golden rules of interface design. *Disponible en* (1986), 172.

[45] Melanie Swan. 2015. *Blockchain: Blueprint for a New Economy* (1st ed.). O'Reilly Media, Inc.

[46] Joshua Tan, Lujo Bauer, Joseph Bonneau, Lorrie Faith Cranor, Jeremy Thomas, and Blase Ur. 2017. Can Unicorns Help Users Compare Crypto Key Fingerprints?. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 3787–3798. https://doi.org/10.1145/3025453.3025733

[47] Daniel Wessel, Moreen Heine, Christiane Attig, and Thomas Franke. 2020. Affinity for Technology Interaction and Fields of Study: Implications for Human-Centered Design of Applications for Public Administration. In *Proceedings of the Conference on Mensch Und Computer*. Association for Computing Machinery, New York, NY, USA, 383–386. https://doi.org/10.1145/3404983.3410020

[48] K Whitenton. 2018. The Two UX Gulfs: Evaluation and Execution. *Nielsen Norman Group Technical Report* (2018).

Is it Better With Onboarding? Improving First-Time Cryptocurrency App Experiences

Michael Fröhlich*
Center for Digital Technology and Management, Germany
froehlich@cdtm.de

Charlotte Kobiella
Technical University of Munich, Germany
charlotte.kobiella@tum.de

Albrecht Schmidt
Ludwig Maximilian University, Germany
albrecht.schmidt@ifi.lmu.de

Florian Alt
Bundeswehr University Munich, Germany
florian.alt@unibw.de

ABSTRACT

Engaging first-time users of mobile apps is challenging. Onboarding task flows are designed to minimize the drop out of users. To this point, there is little scientific insight into how to design these task flows. We explore this question with a specific focus on financial applications, which pose a particularly high hurdle and require significant trust. We address this question by combining two approaches. We first conducted semi-structured interviews (n=16) exploring users' meaning-making when engaging with new mobile applications in general. We then prototyped and evaluated onboarding task flows (n=16) for two mobile cryptocurrency apps using the minimalist instruction framework. Our results suggest that well-designed onboarding processes can improve the perceived usability of first-time users for feature-rich mobile apps. We discuss how the expectations users voiced during the interview study can be met by applying instructional design principles and reason that the minimalist instruction framework for mobile onboarding insights presents itself as a useful design method for practitioners to develop onboarding processes and also to identify when not to.

CCS CONCEPTS

• **Human-centered computing** → *Empirical studies in HCI*; • **Security and privacy** → *Usability in security and privacy*; • **Applied computing** → **Digital cash**.

KEYWORDS

mobile onboarding, minimalist instruction, cryptocurrency, blockchain

ACM Reference Format:
Michael Fröhlich, Charlotte Kobiella, Albrecht Schmidt, and Florian Alt. 2021. Is it Better With Onboarding? Improving First-Time Cryptocurrency App Experiences. In *Designing Interactive Systems Conference 2021 (DIS '21), June 28-July 2, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3461778.3462047

*Also with Ludwig Maximilian University, Bundeswehr University Munich,.

DIS '21, June 28-July 2, 2021, Virtual Event, USA

ACM ISBN 978-1-4503-8476-6/21/06…$15.00
https://doi.org/10.1145/3461778.3462047

1 INTRODUCTION

A user's initial interaction with a mobile app is critical to reaching subsequent adoption [47]. Industry reports indicate that as much as 25% of apps are abandoned after only the first use [48]. So it is not surprising that mobile app designers regularly resort to onboarding task flows to help their users discover application functionality and show them how they could benefit from it [47].

While popular among UX practitioners, the overall usefulness of mobile app onboarding appears to be a disputed topic in the research community [30]. Some scholars view them as an opportunity to educate users [25, 47], Others argue that mobile apps should be intuitive by themselves [36]. For practitioners, there is an obvious trade-off to consider: Does onboarding help new users get started and increase engagement, or does it actually stand in the way of it? The scientific literature on the topic is sparse [47]. However, recent work by Strahm et al. proposing a systematic design method for developing mobile app onboarding [47] offers an opportunity to address this question. When does mobile onboarding provide value for new users?

Financial applications are especially interesting to look at in this context, as users may perceive them as critical and hold additional expectations regarding trust and security. With cryptocurrency apps being particularly challenging, we selected them to evaluate the impact onboarding processes can have. According to literature, cryptocurrency applications are difficult to use (e.g., [4, 16, 20, 22, 35]), especially for new users [2, 32, 40] who do not exhibit an above-average technology affinity [23], and users often hold misconceptions about how they work [39].

To investigate user expectations and properties of efficient onboarding, we combined two studies. We conducted semi-structured interviews (n=16) exploring users' experiences, behaviors, and opinions engaging with new mobile applications. The results of the study informed the planning and execution of the subsequent user study. While most users indicated skipping the onboarding processes in general, some expressed appreciation in specific situations – in new types of apps and when engaging with feature-rich apps. We then created and evaluated onboarding processes with 16 additional participants for two cryptocurrency apps using the minimalist instruction framework [47]. Based on our interviews, we selected two apps that differed in the richness of their features.

Our results indicate that onboarding processes can improve the perceived usability of feature-rich apps for first-time users while holding less value for apps with fewer features. While onboarding can support the initial learning process for first-time users of

feature-rich apps, we reason that it does not substitute usable app design in the long term. Minimalist instruction principles align with users' expectations of good onboarding in mobile applications and provide a solid theoretical basis for designers. Presenting the first study deploying Strahm et al.'s method to generate design insights, we discuss its usefulness and how it can be used by practitioners not only to design onboarding processes but also to decide when an onboarding process is not appropriate.

Contribution Statement. The contributions of this work are threefold: (1) We report and characterize users' opinions and behaviors related to onboarding processes and discuss these parallel to minimalist instruction theory. (2) We developed and evaluated onboarding processes for two cryptocurrency apps and discuss under which conditions they are helpful. (3) We present the first evaluation of the minimalist instruction framework for mobile onboarding insights in a different domain, showing it to be a valuable design method. We conclude by discussing how our findings on financial apps generalize for other use cases.

2 BACKGROUND

Framing our research, we first draw on the literature on mobile application onboarding and then introduce the state of cryptocurrency wallets.

2.1 Onboarding For Mobile Applications

The term *"onboarding"* has its roots in human resources, where it refers to the process of efficiently integrating a new hire into an organization [19]. The purpose of onboarding in the context of mobile applications can be understood analogously. Strahm et al. define the onboarding process as *"a key aspect of the user experience that allows users to discover application functionality in a timely manner and identify how this functionality might allow them to achieve their personal goals"*. In practice, this can take different forms. For example, instructional texts and media, just-in-time hints, or interactive tutorials are common [47].

Onboarding new users to mobile apps has been of great interest among practitioners [47]. It is not surprising to see why: 25% of apps are opened just once [48] and mobile apps lose 77% of daily active users within the first three days [10]. While learnability has been a longstanding topic in the HCI community, the value of onboarding seems to be disputed among scholars [30]. Joyce et al. theorize that the historical ineffectiveness of printed documentation and online help may have caused this sentiment. While their results do not support this theory, their survey shows a wide range of perceived usefulness among 60 HCI experts [30]. Unfortunately, no qualitative insight underpins these assessments.

Overall the scientific literature on mobile application onboarding is sparse. Some scholars applied onboarding to specific application domains such as a photo editing extension [18], a citizen science platform [9], gaming [44] and education [38].

The first systematic investigation into the topic was presented by Strahm et al. at DIS' 2018: They characterized nascent practitioner guidance, discussed it in the context of the minimalist instruction theory, and proposed a context-free design method for creating onboarding processes for mobile applications [47]. While most practitioner resources are comprised of rather general recommendations, they highlight a few exceptions providing more substantial guidelines [26, 28] and relate them to Van der Meij's and Caroll's minimalist instruction principles and heuristics [49].

Based on the surveyed practitioner literature, they emphasize focusing on the user journey during the design process and identifying the *aha! moment* and a *quick win* [28] as two critical steps during onboarding. The *aha! moment* refers to the moment in which users first realize how the application can benefit them personally. To guide users towards that moment, it is recommended to explain the application's purpose and provide an emotional reason to be interested. The *quick win* refers to a meaningful yet easily attainable benefit that new users can achieve in their first session, thereby providing closure and a positive conclusion [47]. Allowing users to make tangible progress early engages them in a learning process and provides confidence and control [47, 49].

The core contribution of their paper is the development and evaluation of a research-informed design method for generating insights for mobile onboarding. The method is grounded in the theory of minimalist instruction [49] and engages users in an interactive set of design and evaluation activities. Mediated interaction with a prototype is combined with structured mini-interviews to extract design insights by leveraging users' meaning-making process. The results of their evaluation using a low-fidelity educational application indicate that the method supports the elicitation of design insights to create onboarding processes. While they strongly argue for the value the method provides, they acknowledge the need for future work, specifically regarding evaluations in different domains and contexts [47].

Overall, scientific literature on mobile app onboarding is sparse. Yet, Strahm et al.'s recent work provides an opportunity to look at onboarding experiences systematically. Our interview study addresses the lack of qualitative insight into how users perceive onboarding processes in mobile apps. Our user study builds on Strahm et al.'s proposed design method to develop and evaluate onboarding processes, and we discuss how the method could be extended. Doing so, we are the first to apply and report on the method.

2.2 Cryptocurrency and HCI

More than a decade ago, Bitcoin [41] was introduced as the first cryptocurrency. Since then, more than 8,000 alternative cryptocurrencies have come forward [11]. Often overshadowed by rising valuations, the cryptocurrency space has also been steadily growing in terms of social media traction, developer engagement, and startup activity [14]. Recent investments by traditional institutional investors into Bitcoin further indicate a growing acceptance of cryptocurrencies in the public eye [31]. With PayPal aiming to enable its 361 million users [12] and 26 million merchants to buy, sell, and hold cryptocurrencies in 2021 [24], the adoption will likely increase.

These developments indicate progress in the ongoing adoption. However, work remains to be done. Cryptocurrency applications are still difficult to use (e.g., [4, 16, 20, 22, 29, 35]), especially for new users [2, 32, 40] who do not exhibit an above-average technology affinity [23]. Cryptocurrencies are difficult to understand, and both

users and non-users often have misconceptions [39]. Key management poses a major usability challenge, [16] and self-induced errors are a common source of loss [35]. Custodial wallets seem to offer an alternative for users with less technical knowledge by taking care of key management aspects for the user but require users' trust in the custodial service [20]. Even though they re-introduce a new intermediary, custodial wallets appear to be widely used, either as a gateway service or a permanent alternative to self-managed wallets [6]. However, key management does not appear to be the only issue cryptocurrency apps suffer from. Recent research has shown that "blockchain apps" are overall rated worse than comparable finance applications [27] and in a qualitative investigation we find that custodial wallets are difficult to use for first-time cryptocurrency users [21]. Glomann et al. identified one potential reason for this in the "*Onboarding Challenge*" – the initial challenge of gathering the basic knowledge of using a service or product [23].

While the HCI community has started to recognize its crucial role in improving the design of blockchain applications [15] and several publications brought forward the first recommendations related to cryptocurrency applications [2, 20, 23], we lack studies that prototype and evaluate solutions. For a technology believed to *"democratize"* financial services [45] and discussed for its potential to foster financial inclusion [42] for 1.7 billion unbanked people [13] worldwide, the initial entry barrier is problematic. It potentially marginalizes people without deep technical understanding from participating in the crypto economy (e.g., decentralized lending markets) and could contribute to a new form of second- and third-level digital divide [46]. For cryptocurrencies to truly become the currency of the internet – the currency of "nowhere and everywhere" – it is necessary to break down entry barriers so everyone can participate.

Motivated by the potential impact, the open issues, and scholars calling for more participatory design in the space [15], we think cryptocurrency apps are a fitting subject for our study.

3 METHOD

We conducted two studies: First, an interview study with 16 participants to better understand users' behavior and opinions regarding onboarding in mobile applications. Second, we conducted a user study with additional 16 participants to design and evaluate an onboarding experience for two selected cryptocurrency wallets following the minimalist instruction framework proposed by Strahm et al. [47]. The goal of the interview study was to understand users' behavior and expectations regarding onboarding experiences in mobile apps. The understanding developed during the interview study informed the design of the subsequent user study, specifically the focus on a domain novel to participants and the comparison between a simple and complex app. Both studies were held in English and conducted remotely via Zoom[1]. The interview study was fully transcribed for analysis.

3.1 Participants

For the interview study, we recruited 16 people in Germany and Austria. Participants qualified if they owned and used a smartphone.

[1]https://zoom.us/ (last accessed 15.05.2021)

For the user study, we recruited 16 additional participants. Participants from the first study were excluded from the second one. Since Strahm et al.'s framework is designed to elicit design insights for onboarding, we made sure that participants of the second study had not used any of the two apps before and represented a fitting target group. For both studies, we aimed to recruit participants from different age groups.

Table 1: The participants' demographics for both studies (n_1=16 and n_2=16). Both samples show relatively young and well educated participants.

Demographic	Interview Study	User Study
Gender		
Male	10 (63%)	9 (56%)
Female	6 (38%)	7 (44%)
Age		
	35.5	28.1
20 – 29	4 (25%)	12 (75%)
30 – 39	8 (50%)	2 (13%)
40 – 49	1 (6%)	2 (13%)
50 – 59	3 (19%)	0 (0%)
Highest Completed Education		
High School	4 (25%)	3 (19%)
Bachelor Degree	0 (0%)	8 (50%)
Master Degree	10 (63%)	5 (31%)
PHD or Higher	2 (13%)	0 (0%)
Own Cryptocurrencies		
Yes	2 (13%)	3 (19%)
No	14 (88%)	13 (81%)
ATI Scale		
	3.95	4.46
1 – 1.99	0 (0%)	0 (0%)
2 – 2.99	3 (19%)	1 (6%)
3 – 3.99	4 (25%)	3 (19%)
4 – 4.99	7 (44%)	5 (31%)
5 – 6.00	2 (13%)	7 (44%)

Table 1 shows the demographics of the sample. Our sample skews towards male participants with an average age of 35.5 years in the interview study and 28.1 years in the user study. In comparison, previous quantitative work found the sample of cryptocurrency users to be predominantly male (85%), with an average age of 28.56 [35]. The Affinity for Technology Interaction (ATI) score describes a person's tendency to engage in or avoid technology interaction (6=high affinity, 1=low affinity) [3, 17]. Our sample – interview study (min: 2.33, max: 5.11, mean: 3.95), user study (min: 2.00, max: 5.56, mean: 4.46) – ranks slightly above average compared to the general German population (mean: 3.61) [50]. Looking at the highest completed education, we recognize that our sample of the interview study, with 63% of participants having completed a Master's degree, is not representative of the wider population. We did not notice any differences concerning formal education during the study and think that our findings hold despite this limitation. Future work may address this with a similar experiment covering a wider range of the population.

3.2 Apparatus

The interview study first explored how users typically engage with new mobile applications. During these semi-structured interviews, we focused on the following topics and probed deeper when interesting points emerged. The full questions catalog can be found in the supplementary material.

- Initial behavior when interacting with mobile applications
- Problem-solving in mobile applications
- Experience with onboarding in mobile applications
- Experience and expectations regarding mobile apps dealing with finances

In the user study, we engaged participants in an iterative set of design and evaluation activities to generate design insights, which were then used to develop onboarding processes for two selected cryptocurrency wallets. We selected two existing mobile cryptocurrency wallets – TenX[2] and Klever[3] – to base our prototypes on. We chose TenX because of its focused feature set and Klever because of its rich feature set. Figure **??** illustrates the difference between the two apps. Data collection for the user study was centered around participants' interaction with detailed recreations of the apps as interactive, high-fidelity prototypes. This approach allowed us to later integrate the developed onboarding processes.

3.3 Procedure

For the user study, we applied the minimalist instruction framework proposed by Strahm et al [47]. The method's purpose is to generate design insights by engaging with participants' meaning-making process during prototype interaction. We followed the recommendation to involve 4 participants per session [47]. For both apps, we conducted (1) an initial session without any onboarding, (2) analyzed the collected data to develop the onboarding, and (3) conducted a second session with 4 new participants to evaluate the efficacy of the mobile app with the onboarding experience. Both the initial and evaluation session followed the same protocol (cf. Figure **??**). A short entry and exit interview captured the expectations and opinions of participants. In the entry interview, participants were asked for their expectations and which tasks they would like to accomplish with the app. In the exit interview, they were asked for their favorite part of the app and explained the app to their former self before the start of the user study. The researcher moderated the interaction with the prototype: Participants were asked two questions addressing their next action and expectations, performed the action, and were asked two questions probing for their reaction to the app's behavior. After each step, the researcher noted participants' responses on a card. After the exit interview, participants filled out the System Usability Scale (SUS) [5]. While originally described as a "quick-and-dirty" scale to evaluate the usability of a system, the SUS has been widely used and proven to be a reliable tool to measure perceived usability [37].

3.4 Data Analysis

We coded salient statements based on the transcribed interviews and used affinity diagramming to cluster salient topics from the user interviews [43]. Data analysis of the interview study was completed before and informed the subsequent user study. The analysis of the artifacts collected during the user study was conducted iteratively after each session and only considered data from the respective session. The data set consisted of the collected responses recorded on the cards and salient observations from the video recordings. The goal of the analysis was to review the app exploration and extract common patterns in participants' meaning-making processes. Following the method by Strahm et al., we focused on identifying moments of realization (*aha! moments*) and moments of closure (*quick wins*) [47] common among participants.

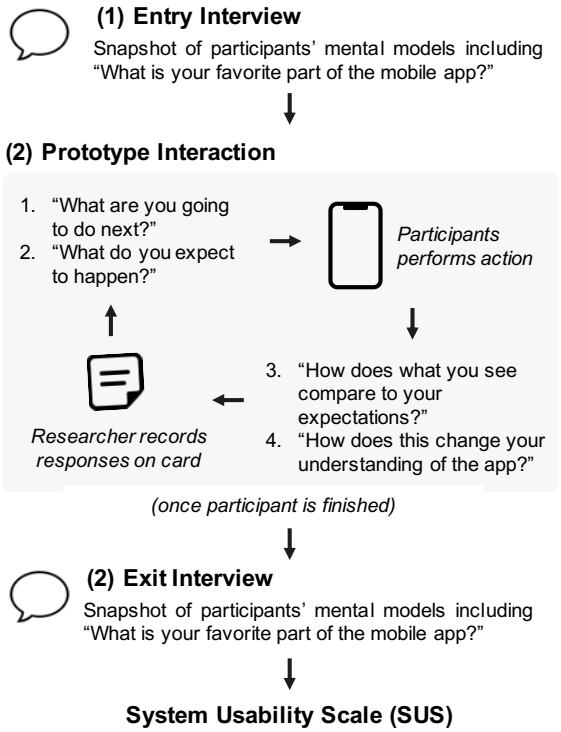


Figure 1: Process for conducting the sessions with participants: After a short entry interview, the participant interacts with the prototype following a strict routine: First, expressing their expectations; second, interacting with the prototype; third, reflecting on the app's behavior. Answers are recorded by the researchers on cards. Once the participant is finished, they reflected on their experience in a short exit interview. Filling out the system usability scale (SUS) concludes the process. *(adapted from Figure 3, Strahm et al. [47])*

4 INTERVIEW STUDY

The purpose of the interview study was to understand the experiences and opinions of users regarding mobile app onboarding, as we could not find any study on the topic in the literature. Through the interview process and subsequent analysis, topics emerged characterizing users' interaction with new apps, their experience, and expectations regarding mobile app onboarding.

[2]https://tenx.tech/ (last accessed 15.05.2021)
[3]https://klever.io/ (last accessed 15.05.2021)

4.1 Interaction With New Apps

During our interview, we explored users' behavior when engaging with new mobile applications.

New App Discovery: Participants in our sample report to install new apps between "*once a year*" (P3) and "*every second week*" (P4). These numbers are in line with industry reports [33]. While some report discovering new apps through advertisements, newspapers, or magazines, finding new apps is an intentional, need-driven process for most participants. P10 explains, "*I am not the guy who is in the app store and is looking for some new apps because he is bored or something. But I only install apps when there is a need*". P12 uses the app store to identify suited apps quickly, "*I have a special use case [...] and I would then just enter into the search bar in the app store and see if there's any reasonable search results*", while P2 reads recommendations upfront to understand the apps they download fully, "*I think I carefully choose which apps I download on my phone. [...] I try to read recommendations and other statements about the app before*". Sometimes apps are known by users through their social or work context. P10 mentions Zoom as an example from work, "*When I installed Zoom, I did know that I can do some calls*". Word-of-mouth recommendations of friends and family seem to be an additional important source for some users. P5 recalls, "*I think usually it is another person telling me about an app. And so, yes, I'm getting informed by talking to someone else*".

Install Decision: Users deploy different strategies to decide whether to install an app. While some perform a background check before installing apps, others are quick to install new apps, try them, and abandon them if unsuited. P3 explains, "*I want to know, who is working behind this app? How do they use the information?*", whereas P11 states, "*If I find something interesting, I would rather install it*".

Participants report to include app store ratings and comments, data privacy, and permissions, the price, as well as reports found on the internet and recommendations of friends and family into their decision process. P6 elaborates, "*I would ask friends if they use it [...] or I check the reviews if people use it and if they're happy with it. Yeah, that's pretty much it*".

Initial Behavior: Participants in our sample reported surprisingly consistent behavior when first engaging with newly installed mobile apps. Users engage in an unstructured exploration, navigating through all screens and trying out features. The fact that all participants reported the same approach was an unexpected finding, as we assumed that users would deploy different strategies. P9 explains, "*I'm curious [...] I want to try everything what I can do with the new app*". They expect to be able to use the app without any further explanation. P4 clarifies, "*For me a smartphone app should be self-explaining. There should be no manual needed for proper usage of this app*". This initial exploration phase is decisive for users' decision to engage with the app. P7 explains, "*I try basically out everything that it's got just to see what I can do with the app. And then yeah, I just think if I should use it or not*". If the purpose behind an app and the benefit for the user is not clear, users are quick to look for alternatives, abandon or uninstall the app. While P8 reflects, "*The thing is, not every app can keep me using it for a longer time...*", P16 takes a more active approach, "*There's not a lot of mercy involved. If it's not solving my problem, it's gone*".

Problem Handling: When facing problems while interacting with new apps, users deploy different strategies. For non-essential tasks uninstalling the app is common, indicating a low tolerance for errors, if users have alternatives to using a specific app. P11 illustrates, "*If I really get stuck, and it's not something that I have to do, I uninstall the app*". Participants reported several further strategies dealing with problems. We elicited five strategies from the interviews: Trial and Error, Ask Friends and Family, Search Engines, FAQs, and to Contact Support.

- Trial and Error: The initial reaction of most users when getting stuck is to try to resolve the issue themselves by trial and error. Participants report searching for alternative ways, restarting the process, restarting the app, or waiting for some time before trying again. P11 explains, "*Just leave it and go back, come back to it after like 30 minutes and try again. It's trial and error all the time [...] I've learned that sometimes you have to give technology some time to adapt*".
- Ask Friends and Family: When unable to resolve the problem on their own, users resort to help from their social environment. P12 says, "*If I already got stuck, my wisdom is exhausted, then I would just call somebody who should be knowledgeable*". P5 often asks her sons for help, "*I asked one of my sons, for instance, because they are more used to using apps*".
- Search Engines: Another strategy mentioned by the several participants is to verbalize the issue and use a search engine to find solutions. P4 explains, "*I usually google. Most of the time you find answers in internet forums. And most of the time, another person had already a similar problem. And then you find the solution on the internet, usually*". P11 specifies what they would search for, "*(I would search for) the name of the app and then try to sort of summarize the problem*".
- FAQ: Looking for FAQ sections on the developer's website directly was mentioned by participants with both positive and negative perceptions. While P11 says they would go to the FAQ section first, "*I'd go to FAQs first*", P1 tries to avoid them, "*Often there is a Q&A section, but I don't want to go to the Q&A section and search for my problem*".
- Contact Support: As a last resort, some users contact the support to help resolve the issue. Experiences and opinions when contacting support were split in our sample. P7 recalls, "*I hate calling a support line. And I'm just waiting 15 minutes listening to their stupid music. For me that is a point where I say "Okay, I'll never use this app again"*". In comparison, P14 prefers calls, "*I would rather like to call somebody. I don't like like typing the error, the problem, what I have into a smartphone, where the screen is so tiny*".

Users may deploy combinations of these strategies to overcome a problem. P3 illustrates their approach, "*First, I try to find it on my own [...] checking it with Google, trying to find it out myself. And the last thing is to ask my son*". We find it noteworthy that participants' answers in our sample consistently indicate that users do not expect to find help within a mobile app. P10 recalls, "*I didn't even think about a help section in the app, to be honest. I've never looked up anything in a help section, in any app*".

A 45

4.2 Onboarding Experiences and Opinions

We explored past experiences, user behavior, and opinions.

Experiences and Behavior: Most participants could recall one or several situations where they were confronted with onboarding. While some participants were quick to dismiss onboarding processes and report they would just skip through them, others noted they would carefully read them. P13 on the one side of the spectrum says, "*The truth is that when something like this happens, I always close it as fast as possible*". P5 recounts more moderate behavior, "*It also depends on how complicated the whole thing is. I mean, if it's not difficult, I'm just swiping through it and I don't want to waste too much time on those kinds of introduction. I'd like to just discover it myself, on my own*". In contrast, P3 sees onboarding processes as complementary to the subsequent exploration of the app, "*I read it, try to understand it, and then do it myself*", and P9 associates a positive feeling with them, "*It makes me feel more comfortable with the whole "How does it look like?". So I see it and I know what I can do with this app in a very quick way*". Some participants reported specific situations. Experiences with onboarding were perceived positively when users were interacting with feature-rich apps in new domains. For example, P4 explained in great detail how the onboarding of an advanced photography app helped them, "*I was not familiar with more complicated photography apps, where you can change lenses and focus settings, and so on. So it was quite helpful. So because it was a really new field for me*". P4 contrasted this with messenger apps, for which they thought onboarding to be unnecessary, "*If it is just like another messenger app – so I'm quite familiar with those things. So I just click further, further, further*". Statements by other participants underline this perception: newspaper apps, cooking apps, translation apps were mentioned as examples of familiar or simplistic apps, which did not need onboarding.

Expectations and Opinions: To elicit expectations for useful onboarding processes, we asked participants for positive and negative experiences and probed deeper into why they perceived the situations as such. For example, P4 describes their idea of annoying onboarding as follows, "*To make it really annoying, put a lot of information on it. So that I really have to scroll up and down until I find this "skip" and "further" button and do this 5, 6, 7 times. [...] And if it's really useless information. So if we start with the welcome screen telling me that this is now a messenger app and I can use it for chat. Yeah, of course I can use it for chatting*". Users expect onboarding processes to be short, skippable, focused, integrated, and lightweight.

- Short: Onboarding processes should not take up much time. Answers on the maximum acceptable time ranged from 1 minute to 10 minutes, with most answers between 1 and 3 minutes. P4, for example, says, "*Five short pages, so time-wise it shouldn't be more than 2 minutes or maybe 3 minutes*".
- Skippable: If users are not interested, they should be provided with an option to skip onboarding. P13 illustrates this point, "*I prefer when there is a little cross right away, but sometimes you have to swipe through them and there's like four or five screens. But as soon as it's longer, or more, I'm just like, Oh, my God, what do you want from me?*".
- Focused: Onboarding processes should focus on the most relevant features of the app. Obvious information, as well as further educational background information, should not be part of it. P8 elaborates, "*I think they should give you an overview with bullet points [...] but not too much information and then you can choose what interests you*".
- Integrated: Onboarding processes should be integrated into the app and not feel like a separated part from it. They "*should be supporting, but should not get in the way*" (P12).
- Lightweight: Onboarding processes should feel lightweight. Text- and information-heavy processes are perceived negatively. Information should be presented at bullet point level with the support of media. P7 states, "*I think good onboarding is just like a few pictures, a few short sentences, but that's it*".

Some participants expressed their desire to have no onboarding at all – instead, they expect apps to be intuitive and self-explanatory. P16 states, "*I would like to have no information because I think the user interface should be more or less self-explaining. If it's a good one, I don't need any explanations, then I will see through the design of the app what I can and what I can't do*". P12 also summarizes their expectations that developers should identify the need for onboarding through user testing, "*If there's certain relevant information that is not easy to be discovered without any explanations. In those cases, I would appreciate onboarding. But that's a very generic statement. It really depends. And I think it is very much with the developers to understand and also to test maybe with users in better versions whether they're struggling*".

5 ONBOARDING DESIGN

To test the impact of onboarding in a realistic setting, we selected two cryptocurrency apps. Based on our interview study, we hypothesized that onboarding would provide more value for users when (a) added to apps with novel context than apps users are familiar with and (b) when added to feature-rich apps compared to apps with fewer features. We further expected that cryptocurrencies are a sufficiently new domain for most users so that onboarding could provide value. We selected TenX (few features) and Klever (feature-rich) as examples and recreated both apps as high-fidelity prototypes. Figure **??** depicts the differences between the two apps.

5.1 Design Insights For Cryptocurrency Apps

The first step of the user study was designed to understand users' meaning-making process and generate design insights. The moderated interaction with the prototypes led to the following design insights. Statements from participants during the user study are denoted with a prefixed "U" (e.g., U1).

(1) Before interacting with the prototype, participants' expectations regarding features differed only slightly among the sample. All participants expected to have an overview of available cryptocurrencies, trendlines, and a way to purchase cryptocurrencies. Some users expected additional features. U4 explained, *"I would expect to have an overview of different cryptocurrencies, what the value is in different real currencies, and also to be able to buy them, maybe to sell them, to trade them into other currencies, to have like a whole stock market kind of situation"*.

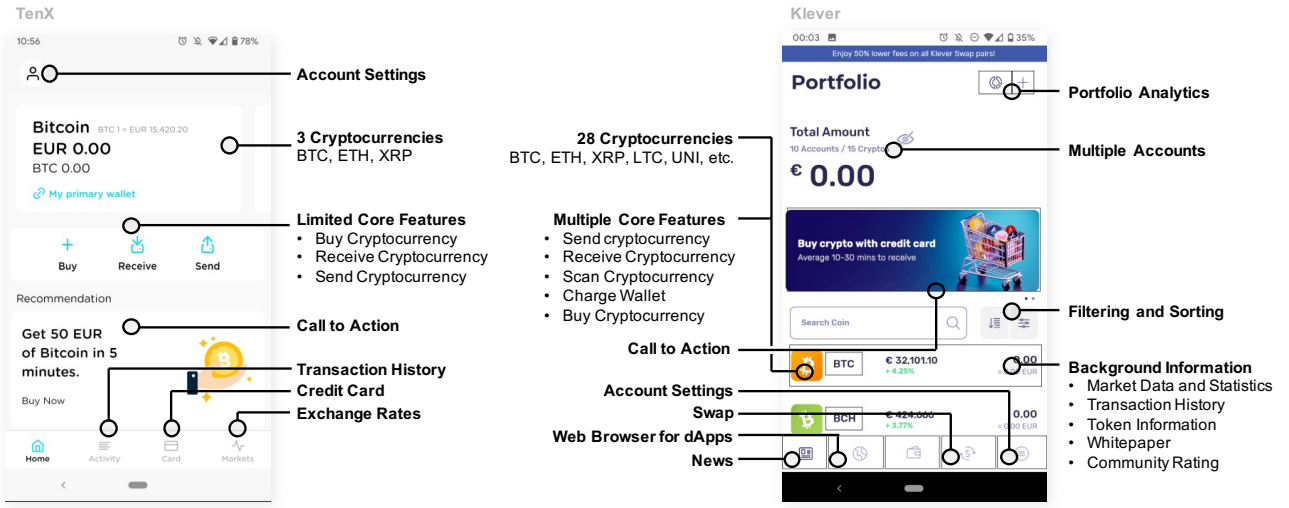


Figure 2: The initial screen after opening the TenX (left) and Klever (right) mobile apps. TenX offers a limited set of features and cryptocurrencies. Klever provides a wide range of features and cryptocurrencies.

(2) Users expect a portfolio overview and the value of their own portfolio to be easily accessible on the main screen. U6 noted, *"The main thing I instantly need is the information there on the top. That is my total amount, how much I own, and how many cryptocurrencies I own. So that's, that's very good"*.

(3) All participants initiated the buying process during the prototype exploration. In the intro interview, most users stated they would need to inform themselves extensively before investing in cryptocurrency. After the buying process, most users were surprised that they could buy cryptocurrency easily. U8 reflected, *"It shows me that it's really easy to buy it. [...] It makes it more transparent that it's also only a way of having a currency. Because to me, it was a bit of a bubble"*.

(4) Users primarily expected cryptocurrencies to be used as an investment. Features to send currency to friends or receive it from them came as a surprise for some. U4 elaborated, *"I have some recent experience with Trade Republic. I looked at the app quickly, and it looked very similar. So maybe I already have a little bit of an image in mind about general trading apps. I mean, this is just normal stocks, not cryptocurrency, but I expected it to be similar to that. And it looks really similar. So this is what I expected. [...] And then you can also [...] exchange cryptocurrency between your friends, which I think is also nice. I didn't think about that"*.

(5) Participants struggled to understand some concepts specific to cryptocurrencies, such as buying fractions of coins, abbreviations of the different coins and tokens, and the fees associated with buying cryptocurrency. U8 said, *"I didn't know that I could also buy parts of crypto"*.

During the user study, participants explored similar features in both apps. However, we observed some differences. Participants were faster in the prototype based on TenX (mean: 26 minutes) than in the one based on Klever (mean: 46 minutes). The duration is also reflective of the misconceptions users had during prototype exploration. When asked in the exit interview whether an onboarding process would have supported them, participants using TenX were rather doubtful as they perceived it as intuitive already. U3 said, *"It's good that it doesn't have too many buttons or too many options to choose from. Because I think this is what makes it easy to handle. [...] Just looking at this app, I can say for me, it's intuitive. And I would know what to do if I want to buy bitcoins"*. Taking the buying process as an example, we reason that the linear user interface of the TenX prototype provided clearer guidance for participants. In comparison, the Klever prototype offers configuration options at each step that give the user more control but also complicate beginners" meaning-making process.

5.2 Developing Onboarding

We used the compiled cards, recorded videos, and the transcribed recordings of participants as a basis for our analysis. Our primary goal was to identify an *aha! moment* shared among participants that could then be used to guide users to a first *quick win*. While participants named a wide range of features when asked for their favorite part in the app, we found the task flows visualized with the cards combined with the recordings to be a valuable combination to develop a deeper understanding of participants' behavior. During our analysis, the buying process emerged as a shared *aha! moment* guiding users to a *quick win* – completing their first cryptocurrency purchase and becoming cryptocurrency owners. We identified the buying process as particularly suited for several reasons. First, all participants expected to buy cryptocurrencies and went through the process during their exploration. Second, most participants expected buying cryptocurrencies to be more difficult. Third, we observed that participants started to reflect on the personal utility of cryptocurrencies after completing the buying process.
Based on our analysis, we developed an onboarding process for both prototypes leveraging the identified design insights and minimalist

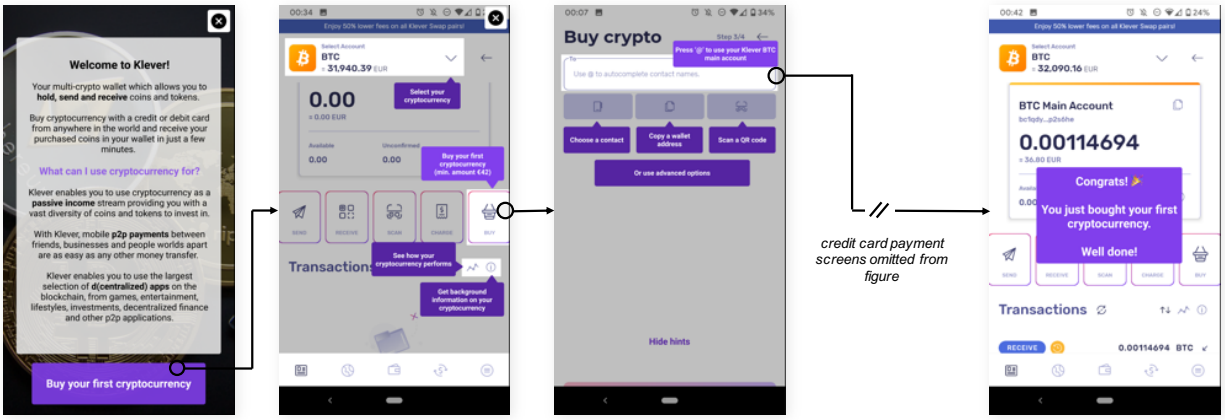


Figure 3: The screens of the prototyped onboarding process for the Klever app. After a brief explanation of the app's purpose and benefits, coach marks guide users through their *aha! moment* to the *quick win* of purchasing cryptocurrency.

instruction principles. Figure **??** shows the main screens adapted for the prototype based on Klever. We used a similar structure for the onboarding process in the TenX prototype. We decided to use coach marks to guide users through the buying process, reasoning that the onboarding would remain short, increase focus, and support the natural exploration process while not "getting in the way".

During the design, we applied the minimalist instruction principles – choose and action-oriented approach, anchor the tool in the task domain, support error recognition & recovery, and support reading to do, study & locate [49]. We included a welcome screen to each onboarding task flow to provide users with the app's purpose and features, as suggested by Strahm et al. [47]. Following the action-oriented approach, we directed participants directly to the screen on which they could initiate the buying process. While this was already the default screen for TenX, we skipped one screen for Klever. With this structure, we could provide an immediate opportunity to act without hindering the app exploration by the participants. Based on the elicited design insights, we clarified points of misunderstanding (i.e., abbreviations, vocabulary, currency fractions) while also supporting the user's experimentation. During the buying process, help buttons would further aid the user's error recognition and recovery. To provide closure and a distinct end to the onboarding process, we included a celebratory message after the successful purchase.

5.3 Impact of Onboarding

In a final step, we repeated the study with the implemented onboarding processes to evaluate its impact on participants' meaning-making. We strictly followed the same procedure with 4 new participants for both apps. We assess that onboarding supported participants' meaning-making process. For TenX, we found little changed compared to the first iteration. U14, a participant of the TenX user study, expressed, *"It was quite intuitive. You could just select how much bitcoin you want, add your credit card details and information [...] and then it does the rest for you. [...] So for me, it doesn't really need an onboarding"*. For Klever, we observed reduced misconceptions and quicker exploration of the app:

(1) All four participants understood from the information overlay that they could buy frictions of cryptocurrencies. U11 reflected, *"From the info screen before we know that 42 euros is the minimum which I can invest. So 42 euros equals to 0.001 whatever bitcoins. Okay, then I will invest 42 euros"*.
(2) Two users pointed out that Klever made them feel comfortable in the buying process as they knew where to inform themselves first. When asked to explain Klever to their former self at the beginning of the session, U10 answered, *"Klever gives you the ability to get an overview of all the coins available and their key figures, and then make kind of like, educated or informed decisions to buy coins"*.
(3) During the buying process, all four users were able to identify their main account as their wallet. One user could make the connection to set up different accounts for different cryptocurrencies. U11 observed, *"I directly understood that I need an account for every cryptocurrency without having an (additional) info screen [...] which is really good"*.
(4) When asked whether using the app made them more comfortable to try cryptocurrency apps, users commented on the ease of the buying process: *"buying crypto is a very complicated thing in my mind, but that [the buying process] was really easy"* (U12).

In addition to our qualitative analysis, we recorded the duration of each app exploration and surveyed participants for the perceived usability using the SUS [5, 37] after the prototype interaction from participants. Table 2 provides an overview of these measures. For context, the average SUS score of mass-market consumer software (74) [37], for mobile apps (77) [34], with a SUS score of 80 being the industry goal [37].

Table 2: Overview of SUS scores and average time needed for app exploration for both apps with and without onboarding.

	TenX		Klever	
	normal	onboarding	normal	onboarding
SUS	83.1	77.5	57.5	78.8
Duration	26 min	15 min	46 min	30 min

In the case of Klever, the addition of onboarding led to improvements in both duration and usability. Question item 10, "I needed to learn a lot of things before I could get going with this system", improved from an average score of 3.00 before onboarding to 1.50 after onboarding (with 1=strongly disagree and 5=strongly agree). In the case of TenX, the addition of onboarding had a less pronounced effect – participants needed less time, but the SUS score dropped slightly. These results are in line with the qualitative observations and analysis of the generated artifacts.

6 DISCUSSION

We have presented the results of our interview study and explored the design of onboarding in the context of cryptocurrency apps. Our results suggest that onboarding can support users in the initial exploration of mobile apps and that design insights for onboarding can be successfully elicited with the used method. In the following, we summarize our findings and discuss opportunities and open questions related to designing onboarding processes for mobile applications that can be generalized from our studies. While we do not claim relevancy for all domains, we believe the findings presented hold value for designers of mobile apps in general.

6.1 Efficacy of Onboarding for Mobile Applications

The results of our interview and user studies suggest that onboarding is not a silver bullet. Given this, the question is, under which conditions does onboarding provide value? We hypothesized from the interview study that novelty of context and complexity of mobile apps could be relevant factors. Our user study data indicates that onboarding supports users in their first interaction when added to complicated apps. The implications for apps with fewer features are less conclusive. In the case of TenX, the onboarding did improve the duration of the study but reduced perceived usability. Comments by participants testing TenX (both without and with onboarding) document their perception that they would not have needed the onboarding. Overall, this suggests that the novelty of context might be less relevant for the value of onboarding compared to a mobile app's complexity. In our study, we operationalized complexity as the number of features a mobile app provides and ignored other sources of complexity (i.e., novel interaction methods). Future research might look into which further sources of complexity could require onboarding.

Features of good onboarding: Strahm et al. were the first to connect Minimalist Instruction Theory [7, 8] to onboarding experiences in mobile applications. Our interview study extends the body of knowledge with an empirical account of user experiences and opinions related to onboarding experiences. The reported aspects of good onboarding – short, skippable, focused, lightweight, integrated – overlap with Minimalist Instruction Theory and confirm its applicability to mobile applications. We discuss our findings in the context of Van der Meij's and Caroll's minimalist instruction principles [49], and argue that minimalist instruction theory is well-suited to guide the design of onboarding experiences for mobile applications.

Principle 1: Choose an action-oriented approach. The first principle argues that meaningful action is necessary for effective learning [47, 49]. Strahm et al. connect this principle to their concept of the *quick win*, which allows users to progress toward a short-term goal [47]. This principle is also reflected in participants' expectations that onboarding in mobile applications should be *integrated* and *skippable*. Simply spoken, onboarding should not get into the way of users' desire to explore and respect users' approach to their exploration.

Principle 2: Anchor the tool in the task domain. The second principle advocates designing instructional activities as real tasks. The organization of the instruction should reflect a real task, and learners should be provided a relevant reward [49]. This principle is reflective of participants' expectations for *focused* onboarding. Onboarding should focus on few relevant features and guide users to make tangible progress towards them.

Principle 3: Support Error Recognition and Recovery. The third principle emphasized preventing mistakes whenever possible and provide on-the-spot error information if that is not possible [49]. During the initial app exploration, users are likely to hold misconceptions, and it is reasonable to expect that some will run into errors because of that. Users reported different error recovery strategies during our interview study. With hardly anyone expecting to receive in-app help for problems, we argue it is still important for designers to provide accurate error information. Users are likely to resort to search engines, FAQs, or friends or family to help them resolve the issue in case trial and error fails them. Being able to articulate the problem at hand is equally crucial for each of them.

Principle 4: Support reading to do, study, and locate. The fourth principle reminds designers to be brief and provide closure for chapters [49]. This closely relates to the concept of the *quick win* [47] and also aligns with users' expectations for *short* and *lightweight* onboarding experiences.

These principles proved to help guide the development of our onboarding processes. We used coach marks as they would allow for an action-oriented exploration while not getting in the way. We guided users through the real buying process, thereby anchoring the onboarding in the task domain. We tried to avoid errors by guiding users through a highlighted default path but provided an explanation for additional configuration options in case users deviated from it. We aimed for a short process, providing closure with the successful purchase of cryptocurrency.

Informational content should not be part of onboarding: During our interview study, participants clearly expressed that onboarding "*should not get in the way*". While it might be tempting to include educational information in an onboarding process, we reason practitioners would do better not to do so. Informational content, often presented in the form of tutorial cards, is not actionable and tends to get in the way of the user's desire to explore the app. Information that goes beyond the app's usage – in the addressed case, for example, *How do cryptocurrencies work?* – are likely explored by users outside of the app.

6.2 Reflections on Strahm's Framework for Onboarding Design Insights

Our experience showed that the framework proposed by Strahm et al. could be successfully used to generate design insights in the context of financial applications using high-fidelity interactive prototypes. Overall, we perceived the method to be a valuable framework aiding the design process of onboarding experiences. The moderated interaction with the prototype allowed users to reflect on their behavior while generating artifacts for the subsequent design process. Some participants even commented positively on the nature of the process. During the analysis part, the insights recorded on cards allowed us to reconstruct the task flow of different users and compare their differences and similarities. While providing structure to the sequence of steps, valuable insights emerged only in combination with video recordings and transcriptions of the user study. In the case of TenX, we observed that the generated design insights also indicate when onboarding might not be necessary or appropriate. During both iterations of the user study with the TenX prototype, participants raised doubts on whether onboarding would improve their understanding of the app.

Improvements and Extensions: From our experience in applying Strahm et al.'s procedure to develop two onboarding processes, we derive suggestions on how to adapt the procedure in the future.

(1) We found adding the System Usability Scale [5] after completing the prototype interaction a valuable addition to evaluate the impact of the prototyped onboarding. This modification adds little overhead to the procedure but provides a reliable quantified measure complementing the qualitative observations for evaluation.
(2) We also reported the duration of the prototype exploration (measured post hoc). We followed the rationale that the duration would demonstrate the difference between the two tested prototypes – i.e., the longer duration in the more feature-rich app demonstrated that users had more difficulty during their exploration. We argue that for evaluation of the efficacy of the onboarding, it is less suited, as researchers administering the study could (potentially unconsciously) influence it.
(3) One practical downside in reporting our results was the missing name of the method Strahm et al. proposed. While Minimalist Instruction Theory informs the creation of the onboarding prototypes, the design method focuses on eliciting users' meaning-making process. For designers, it might be helpful to have a dedicated name for the protocol itself (see figure **??**), as it might be used to generate design insights for different ends than onboarding. We humbly suggest *Iterative Moderated Exploration Framework (IMEF)* as a suitable name.

Future research: From our interviews, we found that the initial familiarization with mobile apps happens in an unstructured exploration – simply said, by clicking through all screens. While the moderated exploration is valuable for designers to understand users' meaning-making processes, it is an open point for future research to investigate whether participants would act the same way when exploring the app independently.

An additional avenue for further research would be the long-term impact of onboarding on usability perception and engagement. Is the onboarding effect a one-time improvement, or can successful onboarding interventions achieve increased engagement in the long term? In a similar light, it would be interesting to understand onboarding beyond first-time use. With feature-rich apps such as Klever, it is not realistic to onboard users to all features at once. How would the procedure need to be adopted to elicit valuable design insights for established users? How would users react to such onboarding? And which impact would it have?

6.3 Modeling App Installation as Intentional Process

From our interviews, we draw on the observation that the decision to install a new app appears to be an intentional process in most cases. Users reported that they would inform themselves with the help of online resources and reach out to friends and family to decide on whether to install certain apps. In the same notion, some participants mentioned during the interviews in our user study that they would learn more about cryptocurrencies before engaging with an app outside of the study setting. This indicates that when users first engage with a cryptocurrency app, they have already started the knowledge gathering process beforehand. Presumably, not all app installations are that intentional. Apps that serve an immediate need – i.e., public transport apps, translation apps, games – are likely installed without extensive research beforehand. Nevertheless, modeling the decision leading up to an app installation as an intentional process could extend our current understanding of user behavior and open up new avenues for research – i.e., how to guide users to trustworthy and factual sources.

In the context of cryptocurrencies, we hypothesize that users form the intention to engage with the technology over an extended period before they first download an app and buy cryptocurrencies. Future research in the area of cryptocurrency (and likewise in different domains) should investigate how users engage in the exploration, gather knowledge and form the intent to engage with a topic or not. Planned Behavior Theory [1] might provide a theoretical starting point for research in this direction.

7 CONCLUSION

In this paper, we have explored the impact of onboarding processes at the example of two prototypical cryptocurrency apps. We complemented the design and evaluation with a preceding interview study with 16 participants characterizing experiences and opinions regarding mobile app onboarding in general. Our findings indicate that mobile app onboarding improves usability for first-time users of feature-rich apps but might not do so for simpler ones. We discuss the results of both studies in the broader context of minimalist instruction principles, concluding that they are aligned to users' expectations regarding onboarding and thus represent a valuable set of guidelines for designers of mobile apps.

ACKNOWLEDGMENTS

This work was supported by the Deutsche Forschungsgemeinschaft (DFG) (grant no. 316457582 and 425869382).

REFERENCES

[1] Icek Ajzen. 1991. The theory of planned behavior. *Organizational behavior and human decision processes* 50, 2 (1991), 179–211.

[2] Abdulla Alshamsi and Prof. Peter Andras. 2019. User perception of Bitcoin usability and security across novice users. *International Journal of Human-Computer Studies* 126 (2019), 94 – 110. https://doi.org/10.1016/j.ijhcs.2019.02.004

[3] Christiane Attig, Daniel Wessel, and Thomas Franke. 2017. Assessing Personality Differences in Human-Technology Interaction: An Overview of Key Self-report Scales to Predict Successful Interaction. In *HCI International 2017 – Posters' Extended Abstracts*, Constantine Stephanidis (Ed.). Springer International Publishing, Cham, 19–29.

[4] Aaron W Baur, Julian Bühler, Markus Bick, and Charlotte S Bonorden. 2015. Cryptocurrencies as a disruption? empirical findings on user adoption and future potential of bitcoin and co. In *Conference on e-Business, e-Services and e-Society*. Springer, 63–80.

[5] John Brooke. 1996. SUS: a 'quick and dirty' usability scale. *Usability evaluation in industry* (1996), 189.

[6] BuyBitcoinOnline. 2020. *How Many People Own Bitcoin?* Retrieved Jan 31, 2021 from https://www.buybitcoinworldwide.com/how-many-bitcoin-users/

[7] John Carroll. 2014. Creating Minimalist Instruction. *International Journal of Designs for Learning* 5, 2 (Nov. 2014). https://doi.org/10.14434/ijdl.v5i2.12887

[8] John M Carroll. 1990. *The Nurnberg funnel: Designing minimalist instruction for practical computer skill.* MIT press.

[9] Marina Cascaes Cardoso. 2017. The Onboarding Effect: Leveraging User Engagement and Retention in Crowdsourcing Platforms. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI EA '17)*. Association for Computing Machinery, New York, NY, USA, 263–267. https://doi.org/10.1145/3027063.3027128

[10] Andrew Chen. 2016. *New data shows losing 80% of mobile users is normal, and why the best apps do better.* Retrieved Jan 31, 2021 from https://andrewchen.co/new-data-shows-why-losing-80-of-your-mobile-users-is-normal-and-that-the-best-apps-do-much-better

[11] Coinmarketcap. 2020. *Top 100 Cryptocurrencies by Market Capitalization.* Retrieved Dec 30, 2020 from https://coinmarketcap.com/

[12] Raynor de Best. 2020. *Active PayPal accounts worldwide 2010-2020, by quarter.* Retrieved Jan 02, 2021 from https://www.statista.com/statistics/218493/paypals-total-active-registered-accounts-from-2010/

[13] Asli Demirguc-Kunt, Leora Klapper, Dorothe Singer, Saniya Ansar, and Jake Hess. 2018. *The Global Findex Database 2017: Measuring financial inclusion and the fintech revolution.* The World Bank.

[14] Chris Dixon and Eddy Lazzarin. 2020. *The Crypto Price-Innovation Cycle.* Retrieved Jan 02, 2021 from https://a16z.com/2020/05/15/the-crypto-price-innovation-cycle/

[15] Chris Elsden, Arthi Manohar, Jo Briggs, Mike Harding, Chris Speed, and John Vines. 2018. Making Sense of Blockchain Applications: A Typology for HCI. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, Article 458, 14 pages. https://doi.org/10.1145/3173574.3174032

[16] Shayan Eskandari, David Barrera, Elizabeth Stobert, and Jeremy Clark. 2015. A First Look at the Usability of Bitcoin Key Management. *Proceedings 2015 Workshop on Usable Security* (2015). https://doi.org/10.14722/usec.2015.23015

[17] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human–Computer Interaction* 35, 6 (2019), 456–467. https://doi.org/10.1080/10447318.2018.1456150 arXiv:https://doi.org/10.1080/10447318.2018.1456150

[18] C. Ailie Fraser, Mira Dontcheva, Holger Winnemöller, Sheryl Ehrlich, and Scott Klemmer. 2016. DiscoverySpace: Suggesting Actions in Complex Software. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems* (Brisbane, QLD, Australia) *(DIS '16)*. Association for Computing Machinery, New York, NY, USA, 1221–1232. https://doi.org/10.1145/2901790.2901849

[19] S Frear. 2007. Comprehensive onboarding, traction to engagement in 90 days. *Washington, DC: Human Capital Institute* (2007).

[20] Michael Fröhlich, Felix Gutjahr, and Florian Alt. 2020. Don't Lose Your Coin! Investigating Security Practices of Cryptocurrency Users. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference* (Eindhoven, Netherlands) *(DIS '20)*. Association for Computing Machinery, New York, NY, USA, 1751–1763. https://doi.org/10.1145/3357236.3395535

[21] Michael Fröhlich, Maurizio Wagenhaus, Albrecht Schmidt, and Florian Alt. 2021. Don't Stop Me Now! Exploring Challenges Of First-Time Cryptocurrency Users. In *Proceedings of the 2021 ACM Designing Interactive Systems Conference* (Virtual Event, USA) *(DIS '21)*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3461778.3462071

[22] Xianyi Gao, Gradeigh D. Clark, and Janne Lindqvist. 2016. Of Two Minds, Multiple Addresses, and One Ledger: Characterizing Opinions, Knowledge, and Perceptions of Bitcoin Across Users and Non-Users. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 1656–1668. https://doi.org/10.1145/2858036.2858049

[23] Leonhard Glomann, Maximilian Schmid, and Nika Kitajewa. 2020. Improving the Blockchain User Experience - An Approach to Address Blockchain Mass Adoption Issues from a Human-Centred Perspective. In *Advances in Artificial Intelligence, Software and Systems Engineering*, Tareq Ahram (Ed.). Springer International Publishing, Cham, 608–616.

[24] Aaron Gould and Josh Criscoe. 2020. *PayPal Launches New Service Enabling Users to Buy, Hold and Sell Cryptocurrency.* Retrieved Jan 02, 2021 from https://newsroom.paypal-corp.com/2020-10-21-PayPal-Launches-New-Service-Enabling-Users-to-Buy-Hold-and-Sell-Cryptocurrency

[25] Aurora Harley. 2014. *Instructional Overlays and Coach Marks for Mobile Apps.* Retrieved Jan 11, 2021 from https://www.nngroup.com/articles/mobile-instructional-overlay/

[26] Krystal Higgins. 2015. *Engaging new users: Guided interaction.* Retrieved Jan 11, 2021 from https://www.kryshiggins.com/guided-interaction/

[27] Johannes Huebner, Remo Manuel Frey, Christian Ammendola, Elgar Fleisch, and Alexander Ilic. 2018. What People Like in Mobile Finance Apps: An Analysis of User Reviews. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia* (Cairo, Egypt) *(MUM 2018)*. Association for Computing Machinery, New York, NY, USA, 293–304. https://doi.org/10.1145/3282894.3282895

[28] Samuel Hulick. 2014. *The elements of user onboarding.* Retrieved Jan 31, 2021 from https://www.useronboard.com/training/

[29] H. Jang, S. H. Han, and J. H. Kim. 2020. User Perspectives on Blockchain Technology: User-Centered Evaluation and Design Strategies for DApps. *IEEE Access* 8 (2020), 226213–226223. https://doi.org/10.1109/ACCESS.2020.3042822

[30] Ger Joyce, Mariana Lilley, Trevor Barker, and Amanda Jefferies. 2016. Mobile application tutorials: perception of usefulness from an HCI expert perspective. In *International Conference on Human-Computer Interaction*. Springer, 302–308.

[31] Izabella Kaminska. 2020. *2020: The year bitcoin went institutional.* Retrieved Jan 02, 2021 from https://www.ft.com/content/0a6507e9-d3f4-4319-bffb-eb915260e388

[32] Ali Kazerani, Domenic Rosati, and Brian Lesser. 2017. Determining the usability of bitcoin for beginners using change tip and coinbase. In *Proceedings of the 35th ACM International Conference on the Design of Communication*. 1–5.

[33] J.P. McElyea Kelly Pedotto, Vivey Chen. 2017. *The 2017 U.S. Mobile App Report.* Retrieved Feb 7, 2021 from https://www.comscore.com/layout/set/popup/Request/Presentations/2017/The-2017-US-Mobile-App-Report?c=12

[34] Philip Kortum and Mary Sorber. 2015. Measuring the usability of mobile applications for phones and tablets. *International Journal of Human-Computer Interaction* 31, 8 (2015), 518–529.

[35] Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer, and Edgar Weippl. 2017. The other side of the coin: User experiences with bitcoin security and privacy. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 9603 LNCS (2017), 555–580. https://doi.org/10.1007/978-3-662-54970-4_33

[36] Valentino Lee, Heather Schneider, and Robbie Schell. 2004. *Mobile applications: architecture, design, and development.* Prentice Hall PTR.

[37] James R Lewis. 2018. The system usability scale: past, present, and future. *International Journal of Human–Computer Interaction* 34, 7 (2018), 577–590.

[38] Mark Lochrie, Glenn Matthys, Adrian Gradinar, Andy Dickinson, Onno Baudouin, and Paul Egglestone. 2016. Co-Designing a Physical to Digital Experience for an Onboarding and Blended Learning Platform. In *Proceedings of the The 15th International Conference on Interaction Design and Children* (Manchester, United Kingdom) *(IDC '16)*. Association for Computing Machinery, New York, NY, USA, 660–665. https://doi.org/10.1145/2930674.2936002

[39] Alexandra Mai, Katharina Pfeffer, Matthias Gusenbauer, Edgar Weippl, and Katharina Krombholz. 2020. User Mental Models of Cryptocurrency Systems-A Grounded Theory Approach. (2020).

[40] Md Moniruzzaman, Farida Chowdhury, and Md Sadek Ferdous. 2020. Examining Usability Issues in Blockchain-Based Cryptocurrency Wallets. In *Cyber Security and Computer Science*. Springer International Publishing, 631–643. https://doi.org/10.1007/978-3-030-52856-0_50

[41] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. *bitcoin.org* (2008).

[42] Jan Ohnesorge. 2018. *A primer on blockchain technology and its potential for financial inclusion.* Discussion Paper 2/2018. Bonn. https://doi.org/10.23661/dp2.2018

[43] Kara Pernice. 2018. *Affinity Diagramming for Collaboratively Sorting UX Findings and Design Ideas.* Retrieved Feb 7, 2021 from https://www.nngroup.com/articles/affinity-diagram/

[44] Falko Weigert Petersen, Line Ebdrup Thomsen, Pejman Mirza-Babaei, and Anders Drachen. 2017. Evaluating the Onboarding Phase of Free-ToPlay Mobile Games: A Mixed-Method Approach. In *Proceedings of the Annual Symposium on Computer-Human Interaction in Play* (Amsterdam, The Netherlands) *(CHI PLAY '17)*. Association for Computing Machinery, New York, NY, USA, 377–388. https://doi.org/10.1145/3116595.3125499

[45] Jonathan Rohr and Aaron Wright. 2018. Blockchain-based token sales, initial coin offerings, and the democratization of public capital markets. *Hastings LJ* 70

(2018), 463.
[46] Anique Scheerder, Alexander van Deursen, and Jan van Dijk. 2017. Determinants of Internet skills, uses and outcomes. A systematic review of the second- and third-level digital divide. *Telematics and Informatics* 34, 8 (2017), 1607 – 1624. https://doi.org/10.1016/j.tele.2017.07.007
[47] Brendan Strahm, Colin M. Gray, and Mihaela Vorvoreanu. 2018. Generating Mobile Application Onboarding Insights Through Minimalist Instruction. In *Proceedings of the 2018 Designing Interactive Systems Conference* (Hong Kong, China) *(DIS '18)*. Association for Computing Machinery, New York, NY, USA, 361–372. https://doi.org/10.1145/3196709.3196727
[48] Inc. Upland Software. 2021. *21% of Users Abandon an App After One Use.* Retrieved Jan 31, 2021 from https://uplandsoftware.com/localytics/resources/blog/21-percent-of-users-abandon-apps-after-one-use
[49] Hans Van der Meij. 1995. Principles and heuristics for designing minimalist instruction. *Technical communication* 42, 2 (1995), 243–261.
[50] Daniel Wessel, Moreen Heine, Christiane Attig, and Thomas Franke. 2020. Affinity for Technology Interaction and Fields of Study: Implications for Human-Centered Design of Applications for Public Administration. In *Proceedings of the Conference on Mensch Und Computer*. Association for Computing Machinery, New York, NY, USA, 383–386. https://doi.org/10.1145/3404983.3410020

Blockchain and Cryptocurrency in Human Computer Interaction: A Systematic Literature Review and Research Agenda

Michael Fröhlich*
Center for Digital Technology and Management, Germany
froehlich@cdtm.de

Franz Waltenberger†
Center for Digital Technology and Management, Germany
waltenberger@cdtm.de

Ludwig Trotter
Lancaster University, UK
l.k.trotter@lancaster.ac.uk

Florian Alt
University of the Bundeswehr Munich, Germany
florian.alt@unibw.de

Albrecht Schmidt
LMU Munich, Germany
albrecht.schmidt@ifi.lmu.de

ABSTRACT

We present a systematic literature review of cryptocurrency and blockchain research in Human-Computer Interaction (HCI) published between 2014 and 2021. We aim to provide an overview of the field, consolidate existing knowledge, and chart paths for future research. Our analysis of 99 articles identifies six major themes: (1) the role of trust, (2) understanding motivation, risk, and perception of cryptocurrencies, (3) cryptocurrency wallets, (4) engaging users with blockchain, (5) using blockchain for application-specific use cases, and (6) support tools for blockchain. We discuss the focus of the existing research body and juxtapose it to the changing landscape of emerging blockchain technologies to highlight future research avenues for HCI and interaction design. With this review, we identify key aspects where interaction design is critical for the adoption of blockchain systems. Doing so, we provide a starting point for new scholars and designers and help them position future contributions.

CCS CONCEPTS

• **Applied computing** → **Digital cash**; • **Human-centered computing** → **Human computer interaction (HCI)**; **Interaction design**.

KEYWORDS

blockchain, cryptocurrency, distributed ledger, dlt, dapps, web3, trust, human computer interaction, hci, systematic literature review

*Also with LMU Munich, University of the Bundeswehr Munich.
†Also with Technical University of Munich.

DIS '22, June 13–17, 2022, Virtual Event, Australia

ACM ISBN 978-1-4503-9358-4/22/06.
https://doi.org/10.1145/3532106.3533478

ACM Reference Format:
Michael Fröhlich, Franz Waltenberger, Ludwig Trotter, Florian Alt, and Albrecht Schmidt. 2022. Blockchain and Cryptocurrency in Human Computer Interaction: A Systematic Literature Review and Research Agenda. In *Designing Interactive Systems Conference (DIS '22), June 13–17, 2022, Virtual Event, Australia.* ACM, New York, NY, USA, 23 pages. https://doi.org/10.1145/3532106.3533478

1 INTRODUCTION

First introduced in 2008 as a peer-to-peer electronic cash system [97], blockchain technology has since drawn broad attention from research and industry alike. A growing body of literature envisions how its decentralized approach can disrupt current business models, financial systems, organizations, and civic governance [33, 34, 68, 121]. Arguably, the most visible evidence of growth is the combined market capitalization of over USD 1.7 trillion cryptocurrencies have accumulated by January 2022 [23]. Furthermore, developer activity has been steadily growing over the last decade [29], multiple projects have been started to improve over the original design (e.g. [15, 69, 138, 140]), and blockchain technology has been explored for a wide range of different applications and domains [35]. Through technical innovations, blockchains have advanced towards performance soon comparable to existing distributed systems – e.g. the Solana blockchain aims for a throughput of up to 710,000 transactions per second [140].

Despite these improvements, more than a decade after the launch of the Bitcoin network, blockchain technology seems to be far away from its envisioned omnipresence. In spite of avid calls from Human-Computer Interaction (HCI) scholars to engage with blockchain [35, 45], immature interaction concepts appear to hold back users with less technological affinity and present a barrier for wider adoption: Blockchain applications are hard to get started with [49, 52], confront both beginners and experienced users with misconceptions [87, 133], and are largely difficult to use [132]. While there have been systematic reviews of blockchain research in adjacent fields – e.g. security and privacy [144], current theories and models [58], and decentralized finance (DeFi) [92] – there is not yet a complete overview of HCI research pertaining to blockchain. To date, Elsden et al. arguably provide the most complete overview, yet without following a systematic approachand including only

literature up to 2018 [35]. In a field characterized by rapid innovation, we thus see the need for a systematic review to understand the past, present, and future of HCI research on blockchain technology.

The objective of this paper is to develop an overview that can serve as a starting point when researching and designing with blockchain technology by showing how the field developed, mapping addressed questions and open challenges. To this end we ask the following research questions:

- How has HCI research on blockchain and cryptocurrency developed since the inception of Bitcoin?
- What themes, challenges, and design knowledge are discussed in the current research body?
- What are gaps that offer promising avenues for blockchain research in human computer interaction?

To address these questions, we conducted a systematic review of articles at the intersection of HCI and blockchain technology. We identified 99 relevant articles published between 2014 and 2021. While the majority has been published at SIGCHI conferences, there is a long tail of research published elsewhere. We organize the existing research body into six overarching themes and contrast them to the evolving blockchain ecosystem. Doing so, we highlight research opportunities for HCI and argue that interaction design research should boldly adopt modern blockchains as design materials to explore the creation of interactive decentralized applications.

Contribution Statement: With this systematic review, we make the following contributions: First, we present a descriptive overview of current blockchain and cryptocurrency research through an analysis of publication year, publishing databases, contribution types, and methodologies. Second, we analyze the existing research body and consolidate the produced knowledge into six major themes. Third, we conclude the paper by discussing salient gaps within the existing body of literature and draw up future research avenues for HCI and interaction design.

2 METHOD

The focus of this review is to summarize HCI related literature concerning cryptocurrency and blockchain. We structured the literature review in four overarching steps, following the PRISMA systematic review protocol [93]. An overview of our search results is depicted in Figure 1.

2.1 Step 1: Keyword Search

We selected the ACM Digital Library[1], IEEE Xplore[2], and Springer Link[3] as initial databases for this review. As a first step, we conducted a keyword search across all databases. We defined two sets of search terms: one related to the technology – i.e. blockchain – and one related to our research field – i.e. interaction design. The keywords were chosen by reviewing salient literature published at HCI venues (e.g. CHI, DIS, ToCHI) and iteratively refining them. Technology keywords[4] included for example "bitcoin", "cryptocurrency", and "blockchain". Qualifier keywords[5] included for example "user interface", "usability", and "design implication". We then computed query strings with pairwise combinations of technology and qualifier keywords and ran them against each of the databases. A publication would be included in our keyword search if either of the fields "title", "abstract", or "author keywords" matched against the pairwise combination. An abstract example of a query string would looks as follows: "*(title: keyword1 OR abstract: keyword1 OR author_keywords: keyword1) AND (title: keyword2 OR abstract:keyword2 OR author_keywords:keyword2)*". We conducted the search in July 2021 and did not restrict the search to a specific timeframe. We included all papers published before July 31, 2021 — the date of our search. The keyword search resulted in a total of 1,362 papers. Additionally, we iteratively conducted a forward search with Google Scholar[6] for all publications included in the review resulting in an additional 51 papers.

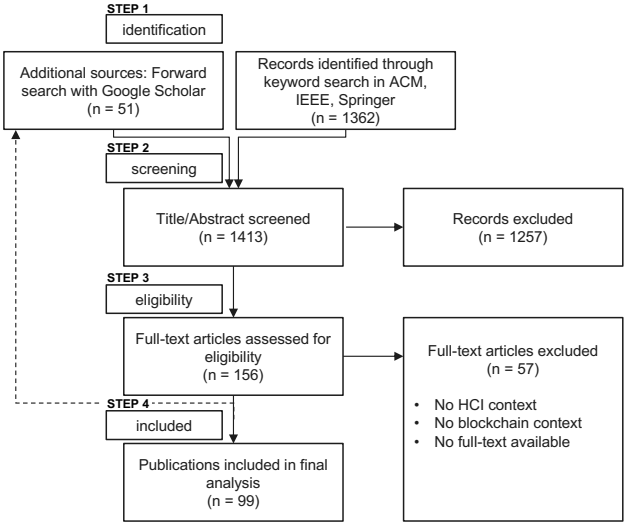


Figure 1: PRISMA flow diagram of the screening process.

2.2 Step 2: Screening Relevant Publications

In the second step, we screened the title and abstract of all 1,362 publications to identify those relevant for the review. We eliminated papers based on the following exclusion criteria:

- Publications with no blockchain or cryptocurrency focus
- Publications with no HCI focus (e.g. technical prototypes)
- Publications written in a language other than English
- Duplicates

A particularly high fraction of excluded publications can be attributed to keyword matches against "prototype" or "blockchain", resulting in technical prototypes without consideration of user interaction. In some situations, it was not apparent whether the

[1]https://dl.acm.org/ (last-accessed 2022-02-18)
[2]https://ieeexplore.ieee.org/ (last-accessed 2022-02-18)
[3]https://link.springer.com/ (last-accessed 2022-02-18)
[4]**Technology Keywords:** "bitcoin", "cryptocurrency", "crypto currency", "blockchain", "block chain", "distributed ledger", "dlt", "dapp", "crypto assets". (At the time of our search "web3" and "nft" did not return any relevant academic results and were therefore excluded. Given the recent rise of both concepts, future literature reviews may consider adding them.)
[5]**Qualifier Keywords:** "ui", "user interface", "interaction design", "ixd", "interaction", "user study", "usability", "ux", "user experience", "prototype", "interface" "interview study", "user-centered", "user-focused", "focus group", "HCI", "behavior", "end-user", "design implication", "design recommendation"
[6]https://scholar.google.com/ (last-accessed 2022-02-18)

Table 1: Overview of the retrieved publications by year.

		Library (Sum)				*Publication Type (Sum)*		*Metrics (Mean)*		
Year	**Total**	**ACM**	**IEEE**	**Springer**	**Other**	**Conference**	**Journal**	**Pages**	**Authors**	**Citations**
2014	1	0	1	0	0	1	0	5.0	4.0	37.0
2015	2	2	0	0	0	2	0	3.0	2.5	47.5
2016	3	2	1	0	0	3	0	7.7	3.7	33.7
2017	7	5	1	1	0	7	0	7.7	3.3	40.9
2018	14	11	2	0	1	12	2	10.2	4.0	25.9
2019	28	14	5	4	5	18	10	10.4	3.4	10.1
2020	26	10	6	8	2	22	4	9.6	4.5	4.1
2021	18	8	3	4	3	12	5	12.1	4.6	1.6
	99	52	19	17	11	77	21	8.2	3.7	25.1

Notes. Publications for 2021 are only included until July 31, 2021. Aggregated values are sums for the *Library* and *Publication Type* columns, and means for the *Metrics* columns. Citations numbers were retrieved from Google Scholar on December 20, 2021.

exclusion criteria were met solely by looking at the title and abstract. In these situations, we included the publication for a full-text review in the next step to not miss relevant literature. In total 156 publications were reviewed – initially 105 to which 51 were added throughout the forward search process. All selected publications were downloaded for analysis in the next step.

2.3 Step 3: Identifying Eligible Publications

In a final step, we reviewed the full text of the remaining publications. The eligible papers underwent more rigorous scrutiny based on the same exclusion criteria mentioned above, resulting in a final set of 99 papers.

2.4 Step 4: Qualitative Analysis

The 99 publications included in the review were read in full. In several iterations, the papers were analyzed and assigned codes. This information was entered into a database for further analysis. Throughout the process, publications were primarily coded by the main author and discussed for validation among the co-authors. Following a thematic analysis approach [12] the coded data was organized along initial emerging themes. In multiple rounds, these themes were revised, and the papers were re-coded until saturation was reached.

3 OVERVIEW

We included 99 publications in our review. Table 5 – located in the appendix – provides an overview of all included publications. For better accessibility, a spreadsheet of the table is included in the supplementary material. Table 1 provides an overview aggregated by *publication year*, *library*, *publication type*, and descriptive *metrics* of the papers. This review covers in total 8 years: The first included publication dates back to 2014, 6 years after the original Bitcoin whitepaper [97] was published. From then the number of publications increased year over year, peaking at 28 in 2019, slightly decreasing to 26 in 2020. These increases in scientific publications seem to be aligned with the crypto-hype-cycle peaks in 2013 and 2017, drawing in not only capital, startup activity, and developer activity [29], but as it appears also research interest.

The ACM Digital Library is the most relevant source with 52 (53%) publications, followed by IEEE and Springer. In total, eleven publications were identified from other databases (e.g. USENIX, Elsevier) using forward search. Only three venues have more than five publications attributed to them: CHI (21), DIS (7), and PACMHCI (5). A long-tail of 42 venues shows only one publication, indicating a fragmented field. Most work is published at conferences (78%), with journal publications only emerging over the past four years. The maturing of the field is also reflected by the steady increase of the average paper length (from 5.0 pages in 2014 to 12.1 pages in 2021) and the average number of authors contributing to a paper (from 4.0 authors in 2014 to 4.6 pages in 2021). The average paper has been cited 25.1 times. Not surprisingly, earlier publications show higher numbers of citations.

3.1 Two Perspectives: Blockchain or Cryptocurrency

We noticed that publications in our sample adopted one of two perspectives. Either they framed their research investigating *blockchain* technology (59, 60%) or *cryptocurrency* (40, 40%). Cryptocurrency publications mainly revolve around understanding users' motivation, perceived risks, and overall perception as well as users' interaction with wallets. Articles about blockchain focus on the design and development of blockchain-based systems for specific use-cases and their subsequent effects on users and society. The majority of empirical studies dealing with people evolve around cryptocurrency, whereas contributions about blockchain frequently contribute artifacts or system evaluations.

Among the 40 publications discussing cryptocurrencies in our corpus, 32 addressed Bitcoin, in eight cases the currency was not specified. This was, for example, the case when researchers explored the usability of different currency exchanges (e.g. [49, 64]). Among the 58 publications discussing blockchain, 13 addressed Bitcoin [97], 19 Ethereum [15], and six other blockchains such as IOTA [106]. 27 did not state a specific cryptocurrency. This was, for example, the case for publications surrounding interface prototypes (e.g. [11]) or design workshops (e.g. [32]).

3.2 Contribution Types

We coded all publications with regards to the contributions they were making, using the classification proposed by Wobbrock and Kientz [137] (see Figure 2). The majority of contributions are of empirical nature. In total 73 (74%) publications contribute either an *empirical study that tells us about how people use a system* (44

publications) or an *empirical study that tells us about people* (29 publications). 39 publications (38%) contribute an *artifact or system.* We included functional systems (e.g. [124, 129]) and interface or interaction prototypes (e.g. [9, 48]) under this category and excluded physical design kits (e.g. [72, 111]). Only few publications make *methodological* (2, 2%), *theoretical* (4, 4%), *dataset* (1, 1%), or systematic literature review (3, 3%) contributions. Eight publications (8%) contribute an *essay or argument.*

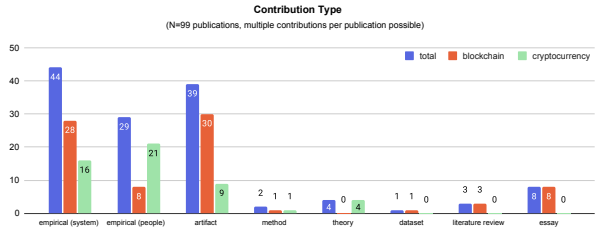


Figure 2: Contributions types of publications in our sample.

3.3 Used Methods

We analyzed the research methods used across the included papers (see Figure 3). We grouped the used data collection methods into six categories (several studies combined methods).

- **Quantitative data analysis** includes the analysis of secondary data such as log data (e.g. [41]), content analysis of forums and websites (e.g. [77]), or app reviews (e.g. [133]).
- **Interviews** include interview studies as primary source of data collection (e.g. [50, 51, 70, 115]) as well as interviews complementing evaluations of systems (e.g. [38, 79, 123]).
- **Questionnaires** include data collection through questionnaires as primary source of data collection (e.g. [2, 79]) as well as complementing other forms (e.g. [11, 143]).
- **Lab studies** include studies conducted in a lab environment in which rich data (e.g. screen-, video-, audio-recordings) could be collected. For example, usability studies (e.g. [8, 48, 104]) or heuristic evaluations through experts (e.g. [65]).
- **Field studies**, in contrast, include studies that are conducted in the natural environment of users. For example, ethnographic studies (e.g. [61, 62]) and deployed mobile applications (e.g. [11]) or systems (e.g. [40, 122]).
- **Workshops** include design research methods engaging groups of people in an effort to elicit design knowledge about people, specific systems, or speculative imaginaries (e.g. [37, 68, 111]).

The most used methods for data collection are interviews (25, 25%), lab studies (24, 24%), and questionnaires (18, 18%.) 51 publications report use of a single data collection method whereas 24 publications made use of method triangulation [105] by combining two or more types. For example, Tallyn et al. combined the analysis of log data and interviews during a field study deployment of an autonomous coffee machine [122]; Bidwell et al. used questionnaires and log data in a longitudinal field study to evaluate automated

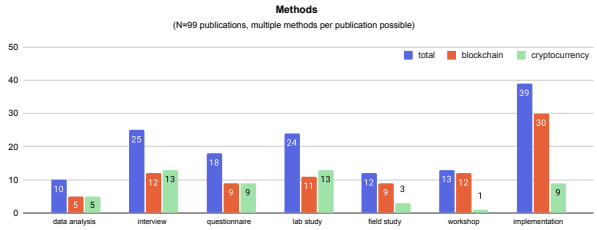


Figure 3: Method types used by publications in our sample.

conditional giving [11]; Jabbar et al. used interviews and ethnographic observation to understand blockchain assemblages [62]. Looking at generative methods, there are several efforts to elicit design knowledge about blockchain systems in workshops, many of which make use of novel design kits [72, 88, 90, 111]. Most publications contributing artifacts – either in the form of interface prototypes or functional systems – present systems using blockchain to implement application-specific use cases (22 publications, e.g. conditional giving [129], energy trading [116], or last mile delivery [123]) or support tools (nine publications, e.g. visual smart contract construction [125], or tools for transaction analysis [75]).

4 MAJOR THEMES

After providing an overview of blockchain research in the HCI community, we present and discuss salient themes that emerged as we reviewed the papers. We identified 6 major themes: (1) the role of trust, (2) understanding motivation, risk, and overall perception of cryptocurrencies, (3) explorations surrounding the usability of cryptocurrency wallets, (4) engaging users with blockchain, (5) using blockchain for the implementation of specific use-cases, and (6) designing support tools for blockchain systems. Figure 4 visualizes the included publications over time per theme.

4.1 Trust in a Trustless System

A central feature of blockchain systems are their *trustlessness* – i.e. the fact that decentralized actors can agree on a common valid state of the systems without the need to trust a central entity or each individual actor within the system. Several HCI publications address trust and the trustworthiness of blockchain and cryptocurrency systems. This strand of research particularly challenges the assumption that blockchains are *trustless* and argues to adopt a sociotechnical perspective [25, 26, 53, 76, 82, 84, 116] as trust in algorithms cannot entirely substitute trust in humans [85]. Investigating the role of trust and how to design trustworthy systems is viewed as particularly important to understand the adoption or non-adoption by users [26, 131]. Figure 5 provides a visual overview.

4.1.1 Factors Influencing Trust in Blockchain Systems. Sas and Khairuddin were the first to integrate trust and blockchain in the context of HCI [70, 114, 115]. Drawing from established models of trust, they discuss the roles of technological trust, social trust, and institutional trust and conclude that established models fail to adequately address decentralized systems. They propose a research framework for HCI to explore trust along three layers and highlight

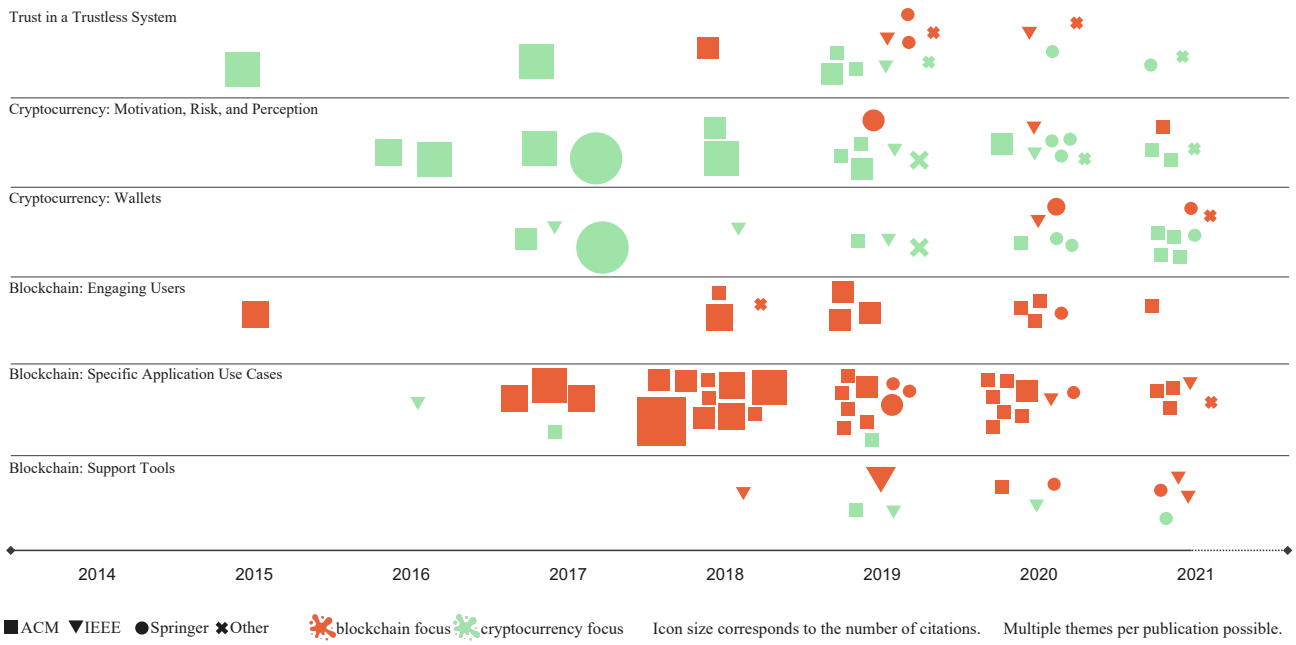


Figure 4: Overview of publications per major theme over time.

users, merchants, miners, exchanges, and governments as relevant stakeholder groups for Bitcoin [114]. In the context of Bitcoin they define technological trust *as people's trust in Bitcoin technology experienced before, during, and after engaging in online transactions*, social trust as *the trust that Bitcoin stakeholders develop between each other*, and institutional trust *as the trust of governmental institutions in Bitcoin technology* ([114], p. 340). In subsequent work they explore both users' [115] and miners' trust perceptions [70] through qualitative interviews. The remaining papers subsumed under this theme primarily address end-users as stakeholder group. An exemption is the work by Voskobojnikov et al. who surveyed 204 non-users to investigate factors influencing the adoption of cryptocurrencies. Their results show that trust is a critical factor affecting adoption intention [131].

While Sas and Khairuddin's framework has found limited adoption among the sampled papers, we use it in the following to organize the trust building factors identified by research. Looking at factors that can be attributed to technological trust, we find several publications. Using a quantitative research design, Wallenbach et al. find that *immutability* and the *traceability of information* positively influence the trust in the technology. In contrast, the *anonymity of a blockchain* has a negative influence [134]. These results confirm the tension arising from having an open and decentralized, yet anonymous system, reported by Sas and Khairuddin [114]. Ooi et al. identify *technical protections*, *transaction procedures*, and *security statements* as determinants of perceived trust for Bitcoin [102]. Looking at social trust, Heidt identify *trust in code, in data*, in a *project's vision*, and *systemic trust* in the interplay between these factors to be relevant for design [53]. Craggs et al. emphasize the role of interpersonal trust in cryptocurrency communities, particularly *interpersonal trust in other users* and *interpersonal trust in the maintainer of the network* [26]. Additionally, several papers report the negative effect of illicit activities [115, 131] on trust in cryptocurrency systems. We did not identify any publications focusing on the trust relationship governmental institutions have towards cryptocurrencies or other blockchains. However, we noticed that a lack of trust in established institutions is a common theme mentioned by cryptocurrency users when asked why they are drawn to the space (e.g. [50, 71, 76, 79, 115]). Also dubbed "the paradox of unregulation", there are qualitative accounts arguing both for and against regulation of cryptocurrenies as a means to foster trust in cryptocurrencies [51, 70, 115, 132].

4.1.2 Trust Challenges. Grounded in the multifaceted factors identified to influence trust, scholars highlight different challenges. Between merchants and buyers, users face the *risk of dishonest traders* [115] as only one side of the transaction is recorded on the blockchain. The pseudonymous nature of transaction poses a challenge to establish trust over time. To mitigate this challenge social strategies are suggested (trade with authorized exchanges, socially authorized traders, reputable traders, or de-anonymized traders) and researchers call for technical advancements (e.g. to support two-way transactions and reversible transactions) [115].

We found that across several publications a lack of knowledge and experience of blockchain technology by most users is mentioned as reason for missing trust [20, 76, 82, 142]. Users with limited understanding have difficulties establishing (technological) trust [82]. For the adoption of centralized payment systems the reputation of the provider plays an important role (see e.g. [44]

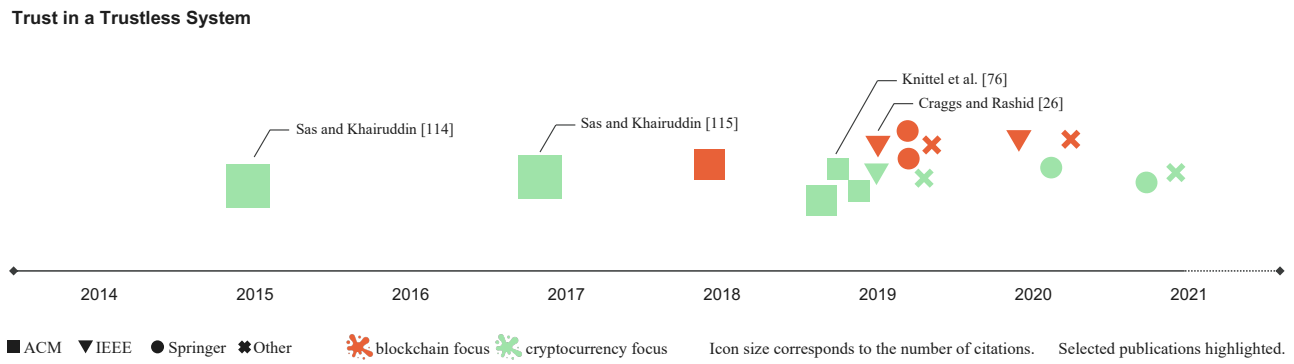


Figure 5: Overview of publications assigned to the *Trust in A Trustless System* theme.

for Apple Pay). In the case of cryptocurrencies there is no central authority to trust. Because of that social elements gain importance, elevating, for example, the role of communities [116]. Knittel et al. report at the example of the Reddit r/bitcoin forum that the ideology within the community reduces interpretive complexity and supports collective imaginaries of a positive Bitcoin future [76].

On the technological side of the spectrum, *trust in data* remains an unsolved challenge. While data on the blockchain is immutable, the correctness of the data written on the blockchain cannot be verified easily (also known as oracle problem) [20]. Trust in reputable intermediaries to connect the real-world with the blockchain is thus necessary [20].

Finally, Bitcoin miners face additional trust challenges, specifically related to the fair distribution of mining rewards when contributing their mining power to a mining pool [70]. Beyond this we did not find other research addressing miners or validators.

4.1.3 Designing Trustworthy Systems. Several publications implement interfaces or functional systems to facilitate trust in blockchain systems. Lee et al. explore how a chatbot is used both as an object and mediator of trust and highlight the arising sociotechnical trust gap. At the example of the chatbot they argue that trust in a known technology (i.e. a chatbot interface) can mediate trust in an unknown technology (i.e. cryptocurrency) [82].

Drawing on the results of their quantitative study, Voskobojnikov et al. recommend to focus designing for *situational normality* to establish trust: Crypto-assets providers should mimic established payment systems users are already familiar with and provide stablecoins (cryptocurrencies that track the value of existing fiat currency) to lower the entry barrier [131]. Some scholars recommend the use of trust-supporting design elements in interfaces, such as trust-labels issued by known institutions such as exchanges [131], governments [142], or blockchain consortia [142].

4.2 Cryptocurrency: Motivation, Risk, and Perception

The second salient theme surrounds the exploration of the experiences and perceptions of cryptocurrency users. It is noticeable that publications in this cluster overwhelmingly focused on cryptocurrency users, not blockchain users. The large majority of publications focuses on Bitcoin and generalizes to cryptocurrencies. Figure 6 provides a visual overview.

4.2.1 Motivation. Several studies investigate the underlying motivation of why people are interested to engage with cryptocurrencies. While there is no established taxonomy, similar themes have been reported across studies. Froehlich et al. group users' motivation into *financial interest*, *ideological interest* and *technical interest* [50]. Abramova et al. present quantitative results separated by user groups, with *financial gain* and *interest in the technology* being the most important self-reported motives across all groups [2]. Similar motives are reported by Sas and Khairuddin [71, 115]: the *oncoming monetary revolution*, *empowerment associated with the use of a decentralized cryptocurrency*, *perceived material value*, and an *economic rationale*. Krombholz et al. report *curiosity* and the *decentralized nature* as motivators [79]. Voskobojnikov et al. take a different approach and investigate motivations and reasons against cryptocurrency adoption [131]. Contrary to qualitative reports by Gao et al. [51], they only find an indirect negative effect of self-efficacy on adoption intention. Among non-users, association with illicit activities, a lack of regulation, and the belief that Bitcoin's value has peaked were also reported to hold them back [132].

4.2.2 Behavior and Perception. Several studies attempt to increase knowledge on how cryptocurrency users are behaving and how their perception in turn influences behavior. There are multiple qualitative and quantitative studies reported. Common methods include questionnaires (e.g. [2, 79]), interview studies (e.g. [50, 51, 115]), and content analysis of forums and other data sources (e.g. [41, 76]). Quantitative studies provide insight into the demographic composition of cryptocurrency user base. Table 2 provides and overview. There are samples from different continents available. While the specific ratio shifts between studies, there are substantially more male participants than female ones. This skew is acknowledged by most authors, but we were not able to find any attempt explaining why women are less prevalent. The reliability of these demographic variables should be taken with a grain of salt as all studies adopt a targeted sampling procedure.

Several studies report general usage behavior related to cryptocurrencies. Most do not distinguish between different cryptocurrencies or types of tokens; those that do limit their focus almost exclusively

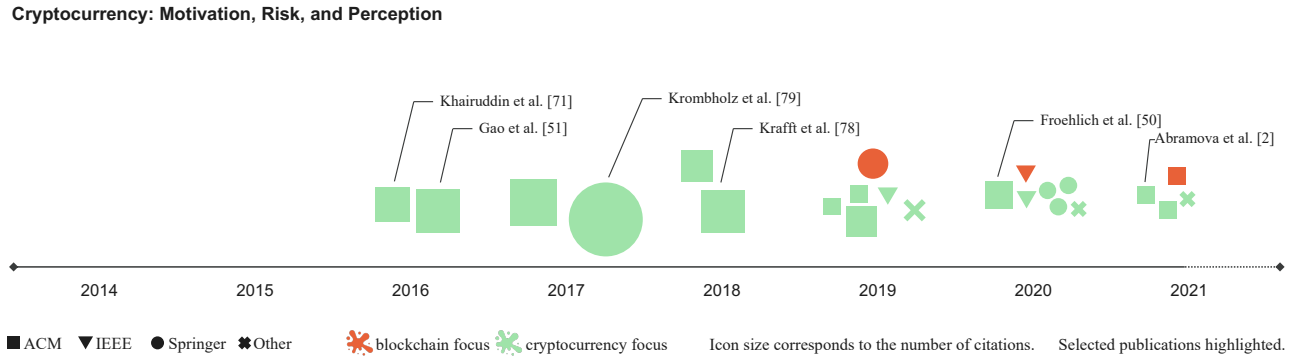


Figure 6: Overview of publications assigned to the *Cryptocurrency: Motivation, Risk, and Perception* theme.

Table 2: Sample demographics of cryptocurrency users across quantitative empirical studies.

Ref	Year	N	Geography	Age (μ)	Gender (m/ f)
[2]	2020	200	US	–	75% / 25%
[2]	2020	195	US, Canada, Europe	–	80% / 15%
[102]	2020	109	Asia	–	97% / 3%
[26]	2020	125	Europe, Americas	–	88% / 12%
[79]	2017	990	US, Europe	28.5	85% / 10%
[117]	2014	134	–	–	95% / 5%

Notes. All studies adopted a targeted sampling strategy.

on Bitcoin. Users typically own more than one cryptocurrency [2, 79] and use different types of wallets in parallel [50] – a recent analysis of Abramova et al. shows that 80% have more than one type of wallet to manage their cryptocurrency [2]. Krombholz et al. provide additional insight into backup behavior [79]. With a mixed methods approach Busse et al. examine payment cultures in four countries (US, Germany, Iran, China), finding higher penetration of cryptocurrencies in western countries [14].

While Bitcoin is titled a *currency*, researchers have raised the question whether it is actually being used like one [89]. While Sas and Khairrudin report that most participants use Bitcoin primarily as store of value [115], Gao et al. find support for both investment and currency [51]. Froehlich et al. distinguish between use as *money* (i.e. as medium of transaction) and use as *asset* (i.e. as store of value or investment) and argue for designers to focus on either one use case to build more usable applications [50] .

Knittel et al. provide a deep qualitative analysis of the r/bitcoin community on Reddit[7] [76, 77]. They find that forum users subscribe to a "True Bitcoiner" ideology, consisting of three core beliefs: (1) *viewing Bitcoin's technology as more trustworthy than its people*, (2) *rejecting 'corrupt' social hierarchies related to money*, and (3) *the importance of accumulating or "HODLing" quantities of Bitcoin as a strategy to create an ideal future* ([76], p. 1). With a similar approach Jahani et al. try to disentangle processes of collective sense making related to emerging cryptocurrencies in forums [63]. Most Bitcoin users are not mining Bitcoin themselves [51, 79]. Khairuddin and Sas provide qualitative insights into the practices of Bitcoin miners, considering individual and collective approaches (solo-miners, collaborative mining pools, data-centers) [70].

Krafft et al. investigate how peer-influences affect user behavior on cryptocurrency exchanges. With a novel experimental approach they find that already low-value transactions affect buying behavior. They hypothesize about the role of user interface design elements (e.g. price history, tickers charts, price direction indicators) on collective behavior [78]. Being one of the few studies focusing on Ethereum, Faqir et al. analyze the effect of gas price surges on user activity in decentralized autonomous organizations (DAOs). Despite major surges in transaction fee costs in the analyzed time frame, they find only a minor influence on user activity [41].

4.2.3 Risks, Security, and Privacy. Connected to the overall perception of cryptocurrencies are the questions which risks users are exposed to, how they perceive them, and how they ultimately deal with them. These questions are particularly interesting in the context of blockchain systems, as many security-related tasks are shifted to the end user.

The most recent and arguably the most rigorous work surrounding risk perceptions and security behaviors of cryptocurrency users is presented by Abramova, Voskobojnikov, Beznosov, and Böhme [2, 131, 132]. Particularly, their CHI 2021 publication [2] is worth mentioning for three reasons. First, they connect to and synthesize 15 prior empirical studies offering an excellent starting point for new scholars in this field. Second, they thoroughly ground their study in theoretic underpinnings (the Protection Motivation Theory [112], the Theory of Planned Behavior [4], and the Technology Acceptance Model [27, 83]). And third, they combine a broad and deep sampling strategy to collect their data. Based on their survey results, they identify three distinct clusters of crypto-asset users – *cypherpunks, hodlers, and rookies.*

Risks. Engaging with cryptocurrencies requires users to deal with different risks. Abramova et al. surveyed cryptocurrency users about their perceived risk of being extorted, theft of private keys, loss through own mistakes, vulnerabilities of wallets, and vulnerabilities of exchanges [2]. Sas and Khairuddin highlight users' risks

[7] https://reddit.com/r/bitcoin (last-accessed 2022-02-18)

surrounding lost passwords, malicious attacks, dishonest trading partners, and failure to recover from human error or malice [115]. Building on their work, Froehlich et al. synthesize three essential risk categories: (1) *the risk of human error*, (2) *the risk of betrayal*, and (3) *the risk of malicious attacks* [50]. Across studies self-induced human errors are frequently reported (e.g. [2, 47, 50, 79, 87, 132]). Examples include forgotten passwords [115], forgotten storage locations, lost private keys, wrongly sent transactions [50], or ill investment decisions [2]. Risks of betrayal result from users misplacing trust in a third party [50], such as exchanges that fail to adequately protect their customers cryptocurrency. Examples for malicious behavior are also well documented: dishonest traders [115], extortion [2], theft [2, 79], and vulnerable wallets or exchanges [2].

Interestingly, Voskobojnikov et al. find no significant effect of perceived risk on adoption intention. They reason that both users and non-users are most-likely aware of the most common risks [132]. Mai et al. find that while users are indeed able to explain a broad spectrum of risks, they often have incomplete or inaccurate mental models of how cryptocurrencies work [87]. Frequent misconceptions concern key management (who generates a key, how are transactions signed, that private keys should not be exposed) [87], what cryptocurrency addresses are [49, 87], transactions and fees (particularly how fees and transaction speed relate) [49, 50, 87, 133], and anonymity as well as security aspects [79, 87].

Security and Privacy Personas. Risk and security perceptions likely differ between individuals and it is reasonable to assume that cryptocurrency users are not a homogeneous group [2]. While studies try to distinguish between non-users [51, 131], beginners [48, 49], and cryptocurrency users [79, 102, 115], Abramova et al. are the first to define a typology of cryptocurrency users using an empirical approach [2]. They build on the concept of privacy personas [31, 80], a model distinguishing users based on their motivation and knowledge about security and privacy into five personas [31]. Froehlich et al. first connected privacy personas with user behavior in the cryptocurrency domain, suggesting that both knowledge and motivation about secure behavior would influence their risk perception. For example, *fundamentalists* (high knowledge, high motivation) would perceive a low risk of human error and value self-managed wallets over custodial ones. At the opposite side of the spectrum, the *marginally concerned* (low knowledge, low motivation) would prefer custodial wallets as they would perceive a higher risk of human error [50]. Abramova et al. applied hierarchical clustering on a sample of 395 participants and identified three robust clusters of users – *cypherpunks*, *hodlers*, and *rookies*. These personas differ in their security and privacy behavior. For example, cypherpunks rather opt for self-managed systems, whereas hodlers and rookies need to decide between custodial or self-managed wallets [2]. Their work may provide a valuable starting point for researchers who want to obtain a deeper understanding of user groups in cryptocurrency. Along with their analysis they also published the survey instrument they used to collect their data.

4.3 Cryptocurrency: Wallets

Wallets are the entrypoint to engage with blockchain applications and the cryptoeconomy at large.

We identified 16 publications which deal with the user experience or usability of wallets. Most publications present empirical results generated by evaluating one or several existing cryptocurrency wallets or exchanges [5, 8, 49, 64–67, 94, 109], or collected data through questionnaires [2, 79] and interview studies [50]. While most publications highlight challenges, usability issues, and provide recommendations to address them, hardly any implement and evaluate the proposed improvements. Surprisingly, only three publications contribute generative design artifacts: Froehlich et al. develop and evaluate onboarding flows to improve two wallets for beginners [48], Chen et al. present a prototype of an augmented reality cryptocurrency wallet [18], and Dlamini present a wallet for low cost mobile phones [30]. Beyond cryptocurrency wallets, we were surprised to find only one article focusing on decentralized applications (dApps) on the web [81]. Figure 7 provides a visual overview.

4.3.1 Wallet Usability. Several publications attempt to categorize wallets. Krombholz et al. initially present five categories related to key management and introduce the term "Coin Management Tool (CMT)" as synonym for wallet [79]. Froehlich et al. follow suit and distinguish between two categories: *Custodial wallets*, where a third party takes care of key management for users and *self-managed wallets* (also called non-custodial wallets [133]), where the user is in full control of and has full responsibility over key management [50]. Moniruzzaman et al. distinguish between mobile, hardware, paper, and web wallets [94]. In a similar fashion Voskobojnikov et al. distinguish software, mobile, hardware, paper, cloud, multisignature, and brain wallets as well as exchanges [133]. Empirical studies reveal that most users have several types of wallets [2, 50, 79]. Custodial wallets are generally believed to be less secure, but more convenient to use for beginners [50, 133]. Scholars recommend the use of software wallets which are connected to the internet for use cases with frequent interactions, and more secure self-managed wallets for the long term storage of larger amounts [39, 50, 79]. Studies in our sample address custodial wallets [48, 49, 67, 109], self-managed wallets [5, 50, 133], decentralized exchange [64–66], or do not explicitly distinguish between them [2].

Wallets on desktop devices [5, 67, 109] and on mobile phones [18, 30, 48, 64–66] are looked at. Two studies address both desktop and mobile devices [49, 94]. One study looks into the usability and security of a hardware wallet [5]. There are several studies which focus explicitly on beginners or new users [8, 48, 49, 67]. Additionally, some studies engage with participants without any prior experience [64–66]. Surprisingly, we have not found any studies that evaluate the usability of wallets longitudinally. Table 3 provides and overview of typical tasks used to evaluate cryptocurrency wallets in lab studies.

While cryptocurrency wallets at large have not been attested great usability [5, 8, 49, 59, 64, 67, 94, 133], there are also a few examples suggesting that it is not impossible to develop usable cryptocurrency wallets: The best performing wallet in the heuristic evaluation of Moniruzzaman et al. has a task success rate of 97.3% [94]. Froehlich et al. report a SUS score [13] of 70 for one evaluated custodial wallet [49] and are able to improve the perceived usability of another wallet by designing an onboarding process [48].

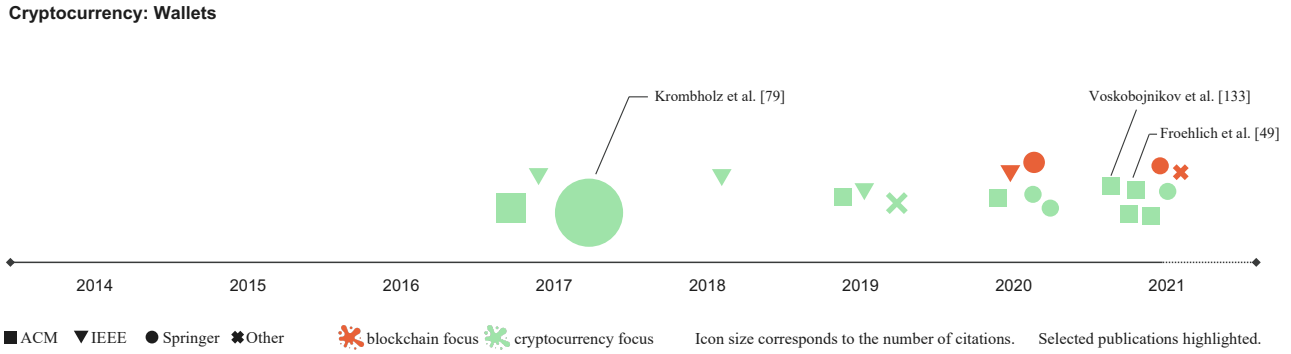


Figure 7: Overview of publications assigned to the *Cryptocurrency: Wallets* theme.

Table 3: Typical tasks during usability evaluations of wallets.

Task	Reference
Creating a new account (including verification)	[8, 49, 64, 65]
Creating a new wallet	[8, 49, 65–67, 94]
Depositing money and/or buying cryptocurrency	[49, 64–66, 94, 109]
Receiving or sending cryptocurrency	[8, 64–66, 109]
Purchasing goods with cryptocurrency	[8, 49]
Reviewing the portfolio value	[8, 48, 49, 65, 66]
Backing up and restoring the wallet	[8, 94]

4.3.2 Generalizable Design Insights. Most publications present usability evaluations specific to the wallets they analyze [5, 18, 30, 64–67, 94, 109]. Only few publications aim at producing generalizable design insights about cryptocurrency wallets [2, 8, 48–50, 133]. For scholars new to the field, the most complete overview of usability challenges of cryptocurrency wallets is probably found in the works of Froehlich et al. [49] and Voskobojnikov et al. [133].

Froehlich et al. present the results of a qualitative user study with 34 novice users who engaged with custodial wallets for the first time. Using three different wallets, they identify several challenges that new users face when first interacting with cryptocurrencies and group them into three categories: *user interface challenges*, *finance challenges*, and *cryptocurrency challenges* [49]. The work by Voskobojnikov et al. complements these findings. They analyze app store reviews of self-managed wallets, identifying 6,859 reviews relating to user experience issues. Their thematic analysis suggests that both new and experienced users struggle with a range of issues: Confirming results from a similar analysis of finance apps [59], mobile cryptocurrency apps at large still suffer many shortcomings related to user experience [133]. Voskobojnikov et al. distinguish in their analysis between *General UX Issues* and *Domain Specific UX Issues* that are closer related to cryptocurrencies. We adopt this perspective to collate the design challenges and recommendations across the reviewed papers in the following.

4.3.3 General User Experience Issues. Across the analyzed papers there are many issues and shortcomings that are not unique to cryptocurrency wallets. While not unique, they become more severe given the direct involvement of money and the irreversible nature of cryptocurrency transactions [49, 133]. For example, Voskobojnikov et al. report a case where poor interface design resulted in direct monetary loss when a user sent a transaction multiple times [133]. Performance issues, freezes, crashes, outdated protocol implementations, and blocking user interfaces are being reported by app reviewers [132]. Different issues related to the structure and functionality of user interfaces are being reported across publications: Poor layout and structure of the interface [5, 49], ambiguous system status or inaccurate information [49, 133], and a general lack of guidance [49, 87, 133]. Additionally, issues pertaining to technical jargon [87, 94], confusing iconography and naming [49, 64, 133], typos [133], color schemes [133], and ill-designed error messages [49] are common. Another issue reported by Froehlich et al. in the context of custodial wallets concerns the extended sign-up or verification process, often required by regulation [49, 133]. They report that anti-money-laundering (AML) and know-your-customer (KYC) procedures often feel invasive for users, are error prone, disrupt the user experience through context and device switches, and sometimes lead to confusion about the legitimacy of an app [49].

The prevalence of these issues suggests that the below average usability of cryptocurrency apps (e.g. reported by [49, 59]) might only partly related to technical aspects of cryptocurrencies. This consequently means that many of these issues can be addressed by following established design guidelines [49, 133].

Voskobojnikov et al. emphasize the importance of error recovery [98, 133] and advise practitioners to design for *situational normality* by mimicking existing online banking or payment systems users are already familiar with [133]. Other scholars draw similar examples to existing finance applications [49, 64]. Additional recommendations include designing for transparency and control [87, 116], focusing on the promotion of cryptocurrenies' benefits [67], supporting users' learning experience [49, 116] and designing for fun use [51].

4.3.4 Domain Specific User Experience Issues. The second category of issues directly relates to the cryptocurrency domain. Issues under this category result either from the user interface and application design or from misconceptions of users. While the former can be addressed through better design, misconceptions can only

be addressed by finding ways to educate users. Unfortunately, misconceptions about cryptocurrencies appear to be quite frequent [87, 133]. Studies with non-users and beginners have shown that cryptocurrencies are difficult to get started with [8, 49], also referred to as the *onboarding problem* [52]. Scholars attribute the steep learning curve, to the technology's embedded complexity [116] and complicated metaphors that often do not match users' expectations [49, 50, 132]. For example, several publications report confusion about the term "wallet" – drawing from their experience with physical wallets user expect different functionality [49, 50, 79] or they connect the term to other concepts such as the native iOS wallet app [49].

Addresses. Cryptocurrency addresses are another frequent cause for confusion among new users. Beginners regularly associate the term with e-mail addresses [49, 133]. Given that they are in essence long alphanumerical strings, it is not surprising that users find them difficult to handle [49] and hard to remember [64]. Almutari et al. show that this makes them vulnerable to man-in-the-middle attacks as they are difficult to compare [5].

Cryptocurrency Valuation. Several issues relate directly to cryptocurrencies' valuation. The high price volatility is reported to be problematic for everyday use [51, 115], particularly when making transaction and different platforms use different exchange rates [49, 133]. The often high exchange rates of cryptocurrencies (i.e. one Bitcoin being worth tens of thousands of US dollars) make them difficult to deal with. Users think in fiat currency when transacting [49], making it necessary to convert prices back and forth. When making purchases at everyday price points, the corresponding cryptocurrency value is a small sub-comma amount (i.e. 50 EUR would be 0.00089 BTC) that is hard to deal with [49]. Interestingly, all of these issues are being addressed on a technical level by so-called stable coins. To our knowledge, there is no published work that looks into the usability of stable coins.

Transactions. Being central to cryptocurrency wallets, many issues are reported relating to transactions. Interfaces that do not immediately show transactions after being sent, leave users in confusion about the state of the transaction [49, 64]. The status of pending transactions if often misunderstood [49, 133]. Resulting from an inaccurate mental model of how blockchains work [87], users often expect transactions to be reversible [115, 133]. With the majority of studies being conducted with Bitcoin, participants frequently report that they perceive transactions to be slow [49, 64, 115].

Fees. Fees emerged as another problematic and widely reported area: Many users have an incomplete or inaccurate understanding of fees [49, 87]. The relation between fees and transaction speed is unclear [87, 133], users often do not expect that they have to pay fees [49], and they are perceived as too high [133]. Wallet operators may charge additional platform fees making it even more complicated to understand fee structures [49, 64, 133]. Configuring transactions with too low fees can cause transactions to be stuck and not processed by miners and most interfaces do not offer the option to overwrite stuck transactions [133]. While some scholars recommend to simplify fee selection interfaces by providing expressive categories (i.e. "slow – low fees", "default", "fast – high fees" [87]), app reviews also show that some users take issue if they cannot configure fees themselves [133]. Fees calculated automatically based on heuristics were reported to be unexpectedly expensive if sent at unfortunate points of time [49].

Ecosystem Integration. Frequent tasks in the evaluation of cryptocurrency wallets involves the purchase of goods [8, 49]. While users would like to use them as a means of payment [50, 51], there is still a lack of mainstream adoption, making it difficult to find merchants [51]. Payment integrations that exist are perceived as problematic [49]. Froehlich et al. highlight the difficulties of using Bitcoin for online purchases when on a mobile device: While many wallets offer features to scan addresses displayed as QR code, this feature becomes useless when the QR code is displayed within the browser on the mobile device itself. Paired with missing shortcuts and broken links this makes it necessary to manually copy addresses and values back and forth [49]. They consequently argue for the necessity of better ecosystem integration to create a seamless checkout process [49], mimicking payment systems users are already familiar with [49, 133].

Key Management. Self-managed wallets largely expose the underlying technology and many users perceive dealing with key management as a burden and bad usability [50]. Some wallets generate key pairs without the knowledge of the user. While this can be perceived positively by users who do not want to deal with key management, it might be a restriction for others [94]. Given the often inaccurate understanding about key management [87], it might be negative in the long run to shield users of self-managed wallets from this. For example, many beginners do not know about the importance of their backup phrases [87] and users often struggle with recovery mechanisms of self-managed mobile wallets [133]. Given that irrecoverable keys are a frequent reason for cryptocurrency loss [79], scholars suggest different approaches. Mai et al. suggest to force users to input parts of their backup phrase to prove that they saved it [87]. Abramova et al. emphasize the importance of wallets to transparently communicate about key management, particularly about storage practices such as encryption [2].

User Groups. Across publications it is apparent that many wallets try to provide one-size-fits-all solutions [2, 50, 133]. However, both qualitative [49, 50, 133] and quantitative [2] studies provide evidence that cryptocurrency users are not a homogeneous group, but differ in their behavior and their needs. Scholars recommend to build wallets tailored to the needs of specific user groups [2, 49, 50, 133] and for different use cases [50]. Relevant dimensions for segmenting users have been identified in their security and privacy behavior and their affinity towards key management [2, 50]. To flatten the learning curve and enable beginners to get started, wallets should guide users through their cryptocurrency journey and create Aha! moments early on [48]. By allowing them to personalize their experience through user profiles [2], they can gradually progress from simple to more complex topics. The importance of educating users throughout this process is emphasized by many scholars [48, 49, 67, 116, 133], particularly to resolve misconceptions. This way, users might start with custodial wallets [50], learn about key management, and graduate to self-managed wallets [50, 133]

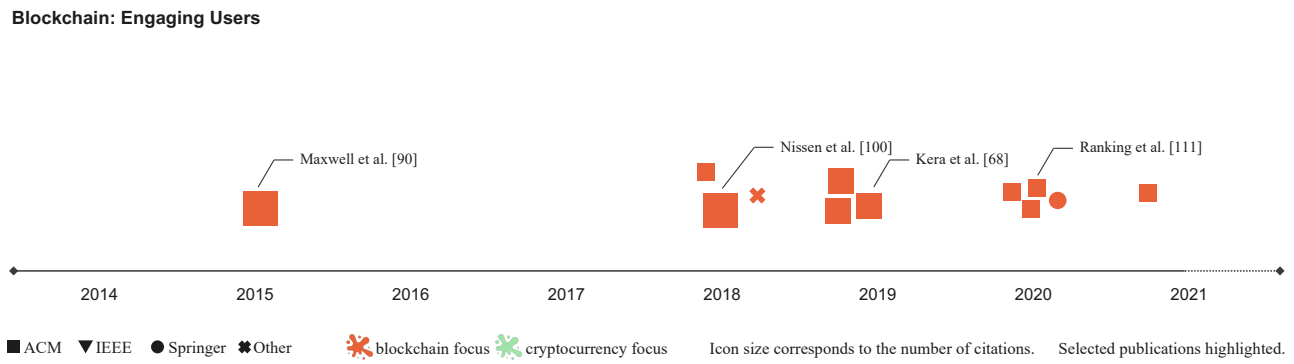


Figure 8: Overview of publications assigned to the *Blockchain: Engaging Users* theme.

4.4 Blockchain: Engaging Users

Several papers in our review focus on engaging participants in workshops and design activities surrounding blockchain applications. These speculative formats make use of physical design kits or participatory design activities to either facilitate understanding about blockchain or elicit user-centered requirements for the development of systems. Figure 8 provides a visual overview.

4.4.1 Engaging with Blockchain. With blockchain being perceived as "black box technology" [88], we found several publications reporting workshops and methods to engage a broader audience in the exploration of the technology. Khairuddin et al. presented BlocKit, a teaching kit based on materials such as clay, paper and padlocks in order to demonstrate usage and materialize virtual concepts via physical objects [72]. Other researchers have used LEGO blocks and role-playing games featuring pizza-shaped learning materials to educate about blockchain-based systems [90, 111]. Reporting results from three workshops, Manohar and Briggs demonstrate how creative methods are useful to enable critical reflection and knowledge exchange about blackbox technologies. They argue that design workshops offer a useful bridge between disciplines and are a valuable resource to inform future oriented design implications [88]. Nissen et al. present GeoCoin, a functional location-based application for learning and speculative ideation with smart contracts, through which users explore urban debit and credit zones. Building on this experience, they invited participants to engage in the exploration and design of further use cases in a subsequent workshop format [100]. Finally, Kera et al. present a design fiction: They use "anticipatory prototyping" to explore autonomous governance and combine a technical prototype with the artistic design fiction of *Lithopia*, a village governed by smart contracts. In this fictional village drones execute smart contracts based on the visual detection of certain actions among villagers by drones and satellites. The ultimately goal of the project was to explore and challenge promise of automated smart blockchain governance of participants and "onlookers" [68].

4.4.2 Participatory Design Activities. We also identified multiple publications reporting participatory design activities with users. In contrast to the research summarized above, these papers aim at ideating specific use cases or eliciting design requirements from participants and less at helping participants better understand blockchain technology. Elsden et al. asked participants about their experiences with donating money and collected ideas and opinions on conditional donations [38]. Together with Oxfam they addressed a similar question from the perspective of charitable organizations, and explored potential use-cases with employees [37]. Others have, together with rural and urban agricultural communities, explored blockchain use cases to level environmental and social inequalities in food supply chains [55, 107]. Beyond these examples, participatory design approaches were used for exploring local energy trading systems [32], location-based blockchain applications [100], and smart-contract governed delivery scenarios [124].

4.5 Blockchain: Specific Application Use Cases

We identified 39 articles in our systematic review that propose or evaluate specific blockchain applications or use cases. Figure 9 provides a visual overview. We categorize these articles according to the topology of blockchain applications by Elsden et al. [35]. Articles with overlaps across the categories were assigned based on the article's main focus. An overview of our results can be found in table 4.

Table 4: Proposed systems in the application-specific use cases theme according to the typology by Elsden et al.

Category	Count	Publications
Underlying Infrastructure	–	–
Currency	4	[40, 56, 60, 100]
Financial Services	7	[11, 20, 38, 107, 116, 128, 129]
Proof-as-a-service	7	[3, 37, 45, 61, 126, 136, 142]
Property and Ownership	5	[9, 19, 42, 54, 101]
Identity Management	–	–
Governance	15	[1, 16, 17, 22, 32, 34, 36, 55, 62] [84, 91, 113, 122–124]

Notes. Articles with overlaps across the categories proposed by Elsden et al. [35] were assigned based on the article's main contribution. Elsden et al.'s paper [35] proposing the typology is not assigned as it discusses all categories equally.

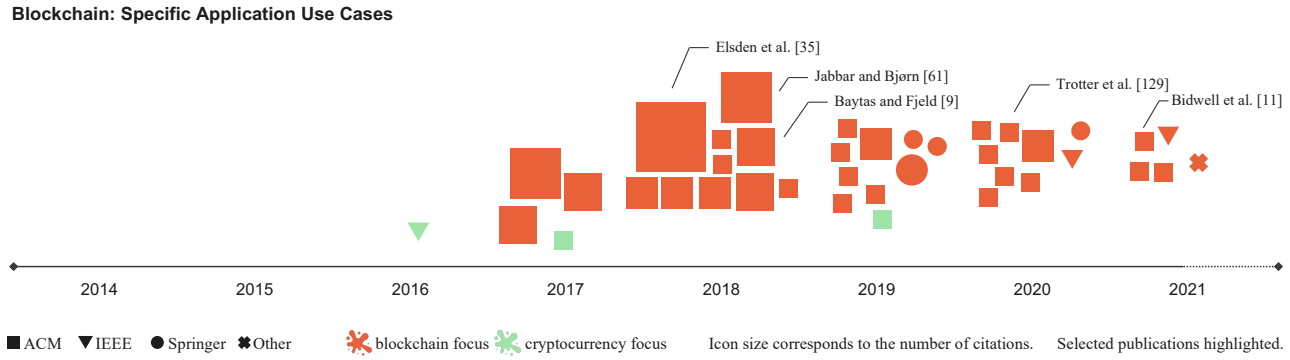


Figure 9: Overview of publications assigned to the *Blockchain: Specific Application Use Cases* theme.

4.5.1 Underlying Infrastructure. With blockchain protocols and decentralized ecosystems being the focus of more systems and cryptography oriented research, it is little surprise that this review found only a small number of articles focusing on underlying infrastructure technologies across research conducted in HCI. We identified work that uses blockchain technology as enabling, underlying software platform to create novel applications e.g. [1, 20, 38, 42, 129] and autonomous or semi-autonomous systems in the context of a networked internet of things [16, 17, 122]. While it may be argued that these examples fit into the taxonomy of underlying infrastructure, most of the work went beyond the mere technical implementation by exploring financial models, socio-economic phenomena and civic engagement and governance.

4.5.2 Currency. Originally invented as a "peer-to-peer electronic cash systems" [97], digital currencies are still the most prevalent use case for blocking technology. In addition, cryptocurrencies and custom utility tokens not only find widespread use to facilitate the exchange of value in the majority of use-cases we revived (e.g. [1, 16, 17, 20, 38, 42, 122, 129]), but form the underlying incentives for many to participate in the development and upkeep of the decentralized blockchain networks [97]. Sections 4.2 and 4.3 have covered work on motivations, risks and perceptions of digital cryptocurrencies and wallets, hence these are not taken into consideration in this section. Specific applications for currencies included an early point-of-sale (POS) system for a coffee shop to accept Bitcoin by Eskandari et al. [40], a browser plugin for tipping for educational resources [56], a prototype for mining cryptocurrency on mobile devices [60], and GeoCoin, an experimental platform enabling participants to interact with location-based smart contracts [100].

4.5.3 Financial services. A large body of HCI work focusing on financial services using on blockchain technologies developed around charitable donations. Research conducted by Elsden et al., Trotter et al., and Bidwell et al. [11, 128, 129] explored the use of blockchain technologies and smart contracts to increase trust and transparency through higher levels of agency and control. The "Smart Donations" system enables donors to attach rules to their charitable gift and triggers pre-specified pay-outs in response to real-world events that are validated through trusted third-party oracles [38, 128]. Trotter et al. outline domain considerations and challenges alongside a comprehensive reference implementation using smart contracts on the Ethereum blockchain. Notably, the authors decided to build a mobile application and custom user interface to abstract the underlying complexity of the Ethereum blockchain and highlighted challenges in the management and exchange of crypto-assets [129]. Their implementation was later evaluated by Bidwell et al. in an in-the-wild study with 93 donors over 8-weeks. The study provides insights into the temporal qualities that emerge from smart contracts that preserved and enforced financial intentions from donors. The authors suggest that sensitivity for time, when designing interactions with blockchains, could facilitate profound temporal orientations and meaningful user experiences [11]. Similarly, work by Chiang et al. demonstrate the potential of smart contracts as an automatic, impartial mediator to increase levels of trust among stakeholders in financial transactions. The authors find that for Mexican migrants living in the US, greater transparency and control around financial transactions and the flow of funds to their rural home communities facilitated by smart contracts can increase trust and cooperation between individuals and government institutions [20].

4.5.4 Proof-as-a-service. The use of blockchain technologies as a trusted digital data storage offers a plethora of possible use-cases and applications. While many applications make use of trusted digital storage on the ledger, often to facilitate higher degrees of trust [1, 20, 42, 107, 129], this section specific work developed around the theme of *proof-as-a-service*. Our review identified applications for provenance in supply and distribution chains, as a trustworthy, immutable digital notary for both, digital and physical artifacts and as immutable, trusted data registers.

We found many examples that investigated the application of blockchain technologies in supply and distribution chains. While some work has an emphasis on governance e.g. in agri-food [45, 107] and energy markets [32, 91, 116], Jabbar et al. provide detailed insight into the implementation of blockchain technology in the shipping industry [61]. Other work developed and evaluated a local courier service system based on smart contracts [123, 124]. Tharatipyakul and Pongnumkul [126] provide a comprehensive survey on user interfaces in blockchain-based agri-food provenance tracking applications. Their work categorizes means to collect (forms, scanning, and sensors) and visualize (text, tables, timelines,

graphs, and maps) provenance data. Their work reveals usability challenges and emphasizes the need to consider interface design to widen blockchain adoption in the future [126].

Examples for blockchain in digital notaries include a reference architecture for an academic certificates registry [3] while [113] highlighted conflicts deploying such a system within a higher education institution. Using the example of a system that collects and stores the history of cars over their life cycle, Zavolokina et al. discuss trust-enhancing design elements that interaction and user interface designers can use to increase trust in blockchain-based proof-as-a-service applications [142]. Wenceslao and Estuar propose a hybrid system using hashed links between off-chain and on-chain storage to support secure, tamper-proof storage and access control of (audio) recordings of medical consultations [136].

4.5.5 Property and Ownership. With immutable and trustless digital ledgers, combined with enforceable rules governed by smart contracts, blockchains support applications that aim to proof, manage and enforce rights related to author- and ownership of all types of digital and physical assets [9, 35, 42]. Despite its significant potential, so far, only little research has been conducted in this space[8]. Baytas and Fjeld provide a design provocation challenging the notions of permanence and disposability of digital and physical artifacts, exploring how the traditional concept of passed-along-generations heirlooms can be transferred into the digital realm using blockchain technologies [9]. Chen and Ko suggest to use augmented reality do materialize digital pets owned on the blockchain [18]. OLeary et al. address the problem of social loafing in the workplace through a secure, transparent, immutable and verifiable system that captures ownership of an employees individuals intellectual property [101]. Fedosov et al. explore distributed ledgers in digital sharing economy services through a blockchain-enabled peer-to-peer lending system. Their "Just Share It" system enables individuals to share equipment (e.g. tools, sports gear, toys), aiming to disintermediate interactions, increase trust among peers and mediate claim management if borrowed items were damaged [42].

4.5.6 Identity Management. Self-sovereign identity management (SSI) is a well-known and widely researched use case that gained significant attention across academia [43, 96, 119], industry[9] and governments[10]. The European Union Agency for Cybersecurity recently released a comprehensive review of SSI [99] and pilot test of SSI technologies are currently being carried out in Germany[11]. Amid this cross-sector interest in self-sovereign identity management, our review has not yielded relevant research conducted in HCI to address interaction design challenges for identity management. The roleplay game, PizzaBlock, by Rankin et al. [111] touches on decentralized identity management for charity volunteers, albeit with a focus on educating non-technical users. Our findings highlight a research gap that should be actively addressed by the HCI and interaction design community in the future.

4.5.7 Governance. Elsden et al. highlight smart contracts' ability to facilitate distributed decision making and governance [35]. This section builds on their definition and provides an overview of HCI research that explores disintermediated control mechanisms, including semi-autonomous and autonomous systems and decentralized autonomous organizations (DAOs). Themes that emerged in our qualitative analysis of prior work included socio-technical challenges around autonomous human-machine interactions, new forms of organizational governance and community engagement.

Lustig discusses visions of decentralized autonomous systems and identifies three possible frames through which to interpret imagineries about autonomous systems: (1) as physical objects, (2) as mathematical rules, or (3) as artificial mangers [84]. Tallyn et. al are the first to report the design of a blockchain-enabled system with the autonomously acting coffee machine BitBarista, which besides selling coffee was also capable of rewarding users for maintenance tasks such as replenishing beans or emptying coffee grinds [122] using Bitcoins. This idea was developed further by Cardenas and Kim which explored the design choices and social implications for financial robot-human agreements. Initial work presented roBU, a prototype robot that was able to provide financial incentives to humans helping the robot to archive targets (e.g. attending university classes and traveling around the world [16]. Later work included interactions with virtual robotic agents and more sophisticated configurations, e.g. an autonomous ride-sharing service [17].

Use-cases around organizational governance cover a broad scope. Several studies have discussed the use of decentralized smart contracts in the context of energy markets. Scuri et al. conducted human-centered research into self-governing, decentralized energy trading which provides insights into peoples perceptions, needs, motivations and proposes design guidelines for P2P energy trading platforms [116]. Doebelt and Kreußlein base their qualitative research on a similar use case exploring the needs and expectations of both consumers and considering gamification to facilitate engagement across the community. Notably, they conclude that energy supply through peer-to-peer communities should be considered as an additional rather than an alternative to the existing grid supply [32]. Early work by Meeuw et al. presents first results of user interface evaluations for autonomous peer-to-peer micro-grids [91].

Work by Rooksby and Dimitrov highlights the friction of deploying new forms of decentralized governance in established organizational structures by deploying a DAO within their university [113], while Abadi et al. aim to improve student engagement and participation through a decentralized student peer-trading platform with reputation system [1]. Other work explores the potential for socio-economic development and governance of rural communities through smart contracts. Pschetz et al. explore the use of decentralized governance in the context of smallholder farmers in the Caribbean. The authors highlight that the challenge is not in the actual money and commodity transactions but in the design of the terms and enforcement mechanisms implemented in smart contracts. [107]. This is developed further by Heitlinger et al., who discuss the possibilities of dehumanizing food systems through an algorithmic management on the blockchain.

[8]We are aware of recent research in the HCI community around the use of non-fungible tokens (NFTs) e.g. [46]. However, this research was conducted outside the time frame of this systematic review (see section 2) and has hence not been included in this review. We expect and encourage more work around the category of ownership and possession in the near future.

[9]https://www.typehuman.com/project/australian-red-cross (last-accessed 2022-02-18)

[10]https://idunion.org/ (last-accessed 2022-02-18)

[11]https://www.bundesregierung.de/resource/blob/998194/1898282/b5d50f1f53d99ee067edfcf43b2ecd31/digital-identity-neu-download-bundeskanzleramt-data.pdf (last-accessed 2022-02-18)

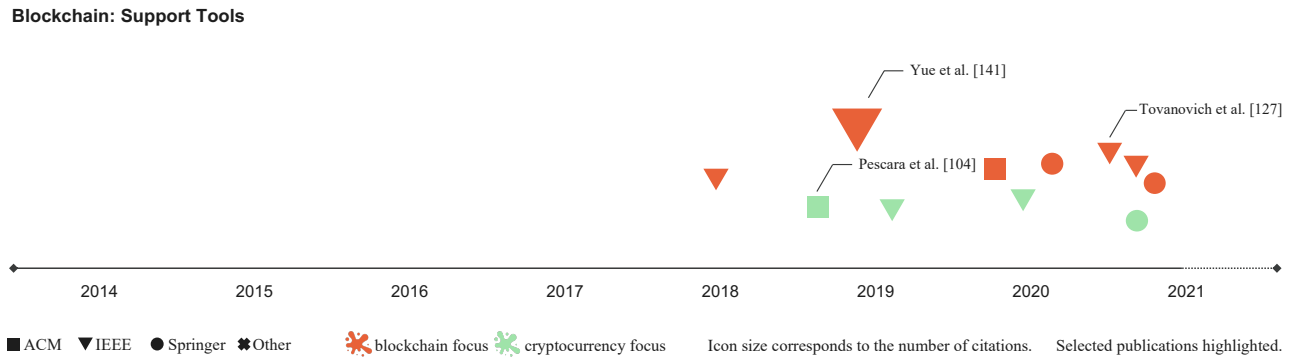


Figure 10: Overview of publications assigned to the *Blockchain: Support Tools* theme.

4.6 Blockchain: Support Tools

We identified multiple publications which present support tools. While publications in the previous section used blockchain as design material to build systems, the ones presented here are auxiliary tools for blockchain [35]. The majority of publications in this category is not published in ACM, but in IEEE and Springer. Salient subtopics concern interactive tools to analyze and make sense of blockchain transaction data, as well as development support tools for smart contracts. Other prototypes include StockSense, a wrist-worn vibrotactile display that signals its users cryptocurrency market movements [104] and Brokerbot, a multiplatform cryptocurrency chatbot [82]. Figure 10 provides a visual overview.

4.6.1 Transaction Analytics and Visualization. Transactions on most blockchain-based networks are public. However, due to the sheer number of transactions and their pseudonymous design it is hard for novices and experts alike to make sense of the data in front of them, which is usually only provided in the form of text [141]. Transaction analytics tools aim to transform this data into a more human-friendly format. Yue et al.'s BitExTract enables its users to gain a better understanding of transactions between large Bitcoin exchanges. Several researchers focus on systems to better visualize connections between Bitcoin addresses. By offering advanced filters and analytics they aim to support law enforcement or make interactions simpler for users [120, 141, 145]. Tovanovich et al. present an extensive review about visualization of blockchain data by surveying existing applications and academic literature [127], which offers an excellent overview of state-of-the-art approaches.

4.6.2 Development Support Tools. Another set of publications is dedicated to the improvement of smart contracts development – particularly, to lower the entry bar for developers with less technical expertise through low-code tools. Tan et al. present a prototype for a *visual smart contract construction system* that allows non-programmers to develop smart contracts [125].

Pursuing a similar objective, Weingärtner et al. aim to make smart contract development more accessible for non-computer experts. They present a graphical programming language for the development of legal smart contracts and, in a brief evaluation, collect indicative evidence that people without programming knowledge can use it [135]. Hossain et al. develop a graphical user interface for the Multichain, a cross-chain router protocol, to make it accessible for people from non-technical backgrounds. Their evaluation showed higher efficiency, better user satisfaction, and an increased overall usability when compared to the original command line interface [57].

5 DISCUSSION

Our systematic literature review provides an overview of HCI research on blockchain and cryptocurrencies. We aim to synthesize academic work that has evolved around the experiences, socio-technical challenges, and the design knowledge about blockchain applications. In the following, we draw on recent developments within the wider cryptocurrency and blockchain space to discuss overlaps and differences of the progress observed between research and practice.

5.1 Recent Developments in the Blockchain Ecosystem

The blockchain ecosystem has experienced fast-paced growth over the last decade [29]. While until recently, Ethereum was the only widely used permissionless blockchain platform supporting decentralized applications, today, several new blockchains for decentralized applications have reached maturity [118]. Ethereum and Bitcoin remain the largest ecosystems, yet newcomers like Solana, Polkadot, and Cosmos boast vibrant developer communities with more than 500 monthly active contributors. Many of these emerging blockchains (e.g. Solana, Polkadot, Terra) even exhibit faster ecosystem growth than Ethereum [118]. What distinguishes many of these new blockchains from Ethereum is a host of different technical innovations aimed at overcoming current limitations, particularly speed, transaction throughput, and expensive fees. Much of the challenge of improving the transaction throughput of a blockchain is related to the so-called *blockchain scalability trilemmma*. In essence, it is assumed that for any particular blockchain its *scalability*, *security*, and *decentralization* are dependent features. An improvement to either one of these properties will negatively affect at least one of the others [95]. While Ethereum, with its sizeable decentralized ecosystem, seems to struggle to deploy the required infrastructural changes

to overcome its current limitations, the upcoming challengers act more agile. The ongoing emergence of several blockchain systems in parallel can thus be traced back to an opportune moment to challenge the Ethereum ecosystem and to diverging approaches to balance the scalability trilemma in doing so.

Many believe that this new generation of blockchains, now providing transactions at instantaneous speed and low transaction costs, will herald the third stage of the web. Web 1.0 allowed users on the internet the possibility to *read* content. Web 2.0 introduced the option to *write*, and thus enabled rich interactive internet applications. Powered by blockchain, *web3* now adds the possibility to *own*, create, and distribute digital assets. Many practitioners believe this read-write-own paradigm will enable a new class of internet applications with a significant potential for innovation [10]. First indications of this paradigm shift are the emergence of decentralized finance (DeFi) and non-fungible tokens (NFTs), which by now account for over two-thirds of transactions on the Ethereum blockchain [130] and are a driver for user adoption of Ethereum [24].

Juxtaposing the development of the blockchain and cryptocurrency ecosystem with the available research analyzed in this review reveals several gaps. While many of the issues identified by past HCI research are now being addressed through emerging blockchain platforms and technological improvements, formal validation is outstanding. For example, stablecoins address price volatility, and new application blockchains, enabled by novel consensus algorithms, provide high transaction throughput with low-cost fees. The Ethereum Name Service[12] (ENS) maps alphanumerical wallet addresses to human-readable names, allowing users to easily share their wallets. Emerging gateway services like Infura[13] bridge the gap between blockchains and the web for developers. However, until now, HCI research has overwhelmingly focused on only two large blockchain platforms, Bitcoin and Ethereum. This leaves a gap in understanding the full potential of these new technologies, particularly how we can build interactive, usable, secure, and user-centered blockchain applications.

While some work designed and discussed dedicated mobile applications (e.g. [9, 100, 107, 129]), the majority of decentralized applications (dApps) runs in the web browser. Being the de-facto gateway to web3, browser-based wallets such as Metamask[14] facilitate the interaction with dApps. However, we have not found a single study looking into browser-based wallets, leaving a critical gap in understanding their role for interaction with decentralized applications. This is particularly relevant as the emergence of web3 is accompanied by phenomena challenging human interaction and collaboration on the internet. DeFi, NFTs, and decentralized autonomous organizations (DAOs) are the most widespread examples that have driven recent user adoption. To date, only little research has been conducted around DeFi and NFTs. While research started exploring specific use cases for DAOs from a technical perspective, we have only identified a single paper that examined the specific impact of infrastructural limitations (i.e. fees) on user participation in DAOs. We know little about how people within these decentralized organizations manage the socio-technical challenges arising from the tension between pseudonymity and the need to collaborate and trust each other.

Arguably, it is time for HCI to move beyond Bitcoin, chart into new waters, and explore the increasingly diverse ecosystem of cryptocurrencies and distributed ledger technologies[15] as a whole. The technical advances in the field offer a plethora of opportunities to use blockchain as a design material to experiment with novel forms of interaction design and craft rich and interactive experiences.

5.2 Future Research Agenda

This discussion and its preceding literature review highlight the importance of HCI in the ongoing development of blockchain applications. Over the past 8 years, a diverse research body has been established through the works of many scholars. To conclude this paper, we present five research avenues the HCI and interaction design community may address in the future.

5.2.1 A better understanding of Blockchain Users. Existing research shows that blockchain and cryptocurrency users are an increasingly heterogeneous group with different motivations, needs, skills, and experiences. With first works untangling the user base of cryptocurrency existing [2], there remains more work to better understand and segment users. Particularly, the recent emergence of web3, most prominently through DeFi and NFTs, has likely drawn in new users with different motivations and expectations than the early Bitcoin adopters. For example, "Twitter NFT" has emerged as a subculture with its own language (e.g. "gm", "probably nothing", "WAGMI") [108]. Likely the ideology connecting people within this group is quite different from the "True Bitcoiner" ideology reported by Knittel et al. [76, 77] and HCI should continue to aim for a better understanding of the economic context under which people become involved with web3. Contesting borders between the digital and physical world, we have seen examples of virtual groups of people organizing themselves into DAOs to achieve common goals. For example, Constitution DAOs attracted more than 19,000 members in an effort to buy a rare copy of the US constitution [110]. Building on the existing research body about trust, future scholars may explore how these decentralized pseudonymous groups organize themselves, build trust, and maintain it over time.

With diversity and inclusion being longstanding values within the HCI community, another topic to address is the question of why there is such a gender imbalance in the blockchain space. Multiple authors recognize this imbalance in the demographics of their papers, yet none of them attempted to find an explanation. With organizations like Global Women in Blockchain[16] aiming to empower women to engage with the technology, change is happening, and numbers are slowly growing [86]. Being champions of diversity, we urge the HCI community to take an active role in identifying the reasons that hold women back from engaging with the technology and make an effort to change that.

[12] https://ens.domains/ (last-accessed 2022-2-18)
[13] https://infura.io/ (last-accessed 2022-02-18)
[14] https://metamask.io/ (last-accessed 2022-2-18)

[15] For practitioners and researchers with interest in designing and building with blockchain, we can recommend the following article providing an overview of the unique capabilities of recent blockchain protocols and platforms: https://medium.com/coinmonks/unhyped-comparison-of-blockchain-platforms-679e122947c1 (last-accessed 2022-04-19)
[16] https://globalwomeninblockchain.org/ (last-accessed 2022-2-18)

5.2.2 Generative Interaction Design for Wallets. Our review shows that existing research has investigated the perception and usability of various cryptocurrency wallets in both qualitative and quantitative studies. Many scholars highlight challenges and propose implications for design – however, these remain largely untested. We identified only three publications [18, 30, 48] implementing wallets or prototyping interfaces. Given that wallets are essential to interact with cryptocurrencies and dApps, future interaction design research is challenged to fill this gap. The ultimate outcome of this strand of research could be a set of validated design heuristics and guidelines specific to cryptocurrencies, as suggested by Voskobojnikov et al. [133]. Against the backdrop of an increasingly diverse blockchain ecosystem, it is likely necessary to explore wallets for different use cases and on different devices to develop these heuristics: Hardware wallets for secure long term storage, exchanges and online wallets for quick access and trading, mobile wallets for payments, and browser-based wallets for interaction with dApps on both desktop and mobile devices.

Assuming a growing integration of blockchain into the web, more and more information will be tied to a specific address. It will be important to design and evaluate educational concepts helping users to update their mental models and overcome misconceptions that otherwise could lead to costly mistakes. To make use of the full benefits promised by blockchain technology, users need to manage their keys on their own. While certainly not desired by all users, exploring ways to safely transition from custodial to self-managed wallets will be important to reduce losses for users who want to. Even though some papers mentioned the positive innovation cryptocurrency has brought to key management (e.g. mnemonics, private keys encoded in 12-word phrases) there was no study in our sample that actively explored this design space. Interaction design can take an active role in developing concepts for key management that nudge users towards secure behavior and provide usable security.

5.2.3 Moving beyond Bitcoin. Bitcoin has laid the foundation for cryptocurrency and blockchain adoption, so it is not surprising that the majority of existing research focuses on the use of Bitcoin. However, the cryptocurrency and blockchain space is diversifying with new generations of blockchain platforms, which are being increasingly adopted by users, developers, and the market [118]. This can also be seen in the gradual decline of Bitcoin's dominance [28]. We argue that future research should be confident to move beyond Bitcoin and adopt state-of-the-art blockchains both as a research subject and platform for new designs and innovation. Doing so two directions will be particularly interesting.

First, we suggest to evaluate whether emerging technologies are able to fulfill their promise to overcome the performance and scalability issues identified by literature across the domain. Due to the current focus on technology that was introduced some 6-10 years ago, some of the issues pertaining to cryptocurrencies might be less prevalent or even solved through advancements in the technology today. In particular, the challenges around scalability and fees could be revisited to update the sector's understanding.

The second direction is to explore and prototype with the increasingly specialized set of blockchains as design material: Decentralized application platforms – e.g. layer-1 platforms such as Polkadot, Solana and Cosmos and layer-2 blockchains like Polygon, Avalanche, Terra, or Bitcoin Lightning – offer novel opportunities for interaction design. Development tools for smart contract development have matured over the past years, making it easier to design and build smart contracts and decentralized applications. With their promise for faster transaction speeds at lower costs researchers and designers can chart the design space for truly interactive blockchain applications.

5.2.4 Engaging with Web3 and Decentralized Applications (dApps). An increasing number of decentralized applications is being adopted by users [24]. This large variety of new applications offers vast opportunities for HCI to research fundamental socio-technical mechanisms connected to blockchain technology. With new technical and mental models being developed, it is a promising space for service and interaction designers.

Measured by the gas fee burn rates, today around two-thirds of transactions on the Ethereum blockchain can be attributed to either NFTs or DeFi, having superseded the mere monetary transfers [130]. While these application areas have been exhibiting increased adoption by users in recent years, this trend has not been reflected in the amount of research being carried out within HCI. In the case of DeFi, the design of interfaces and support tools could have a substantial influence on user behavior (c.f. [78]). More dynamic, intelligent interfaces could, for example, guide users to make better decisions on complex transactions within decentralized exchanges to avoid transactions being delayed or even intercepted. Elsden et al. [35] envisaged the opportunities of digital ownership on blockchain. With the emergence of NFTs this became a reality. NFTs offer an opportunity to further explore the meaning of digital ownership and could revolutionize how digital content creators design, create, trade, and own digital assets. At the same time, NFTs sparked discussion about the value and uniqueness of digital items that can be easily copied. Nevertheless, more and more people are willing to pay for them and thus derive some benefit from owning them.

With the majority of decentralized applications being consumed through the web browser, there is a need to better understand the role of gateway services. Decentralized applications on web3 frequently do not connect to the blockchain directly but through centralized services like Infura. The role of reintermediation of a disintermediated system raises questions about how to maintain power balances, privacy, and the integrity of data visualized in the actual user interfaces that have so far not been addressed by research.

5.2.5 Identity on the ledger. Despite the large public interest, our findings highlighted a significant research gap in HCI around self-sovereign identity management (SSI). SSI has the potential to manage identities in a simple, uncomplicated, trustworthy, and self-reliant way. We would like to encourage the HCI and interaction design community to explore research avenues in this direction. Comparable to an identity document like a passport, web3 opens up opportunities to create virtual identities and reputation that counter-balance the trust challenges [114, 115] in an otherwise pseudonymous system. Aimed at overcoming the need for isolated

accounts on every web platform, Sign-In-With-Ethereum[17] allows developers to use the wallet address of a user to authenticate them. While beneficial from the standpoint of privacy and security from a user's standpoint – gone is the need to share e-mail addresses or enter passwords – this arguably raises questions for website operators on how to deal with the loss of information that today is often at the core of internet business models.

Blockchain-based identity extends beyond technical aspects and opens up fundamental questions about how human identity can be expressed in an increasingly digital world. The Ethereum Name Service is the most widely used tool that allows users to connect their wallet address to a human-readable name, comparable to how domain name services (DNS) map names and IP addresses. This seemingly superficial abstraction allows users to establish a shareable and permanent identity to which they can link their online personas. By doing so, they can build a reputation through transactions connected to their addresses that is public to see and easy to verify by others. This phenomenon can already be seen in the context of web3: People are starting to use NFTs as a form of human expression and self-identity on social media. They present themselves through online personas disconnected from their real identities, set NFTs as profile pictures, use them as avatars in video calls (see e.g. huddle01.com[18]), or use the transaction history connected to their wallets as source of reputation (see e.g. POAPs[19]). It remains to be seen in how far self-sovereign identity can prevail against the centralized services that govern the internet today. For HCI, there is an opportunity to chart the designed space of digital identity, connecting the underlying technological constraints with the fundamental human need for the expression of one's identity.

6 CONCLUSION

This paper presents a systematic literature review of blockchain and cryptocurrency research in HCI. Our analysis includes 99 relevant papers published between 2014 and 2021. We identify six salient themes: 1) the role of trust, (2) understanding motivation, risk, and perception of cryptocurrencies, (3) the usability of cryptocurrency wallets, (4) engaging users with blockchain, (5) using blockchain for application-specific use-cases, and (6) designing support tools for blockchain. We summarize the generated design knowledge, discuss open challenges, and juxtapose the current research body with the changing landscape of emerging blockchain technologies to chart the space for future HCI research. We encourage HCI researcher to better understand blockchain users, take an active approach to designing wallets, adopt new blockchains as design material, engage with web3 and decentralized applications, and explore digital identity. We hope that this paper provides a valuable overview of the current state of blockchain and cryptocurrency research in HCI and that it can act as road map for researchers and practitioners moving forward.

ACKNOWLEDGMENTS

This work was supported by the EU Horizon 2020 (grant agreement No 761758), dtec.bw – Digitalization and Technology Research Center of the Bundeswehr [LIONS], the UK EPSRC project "OxChain: Towards secure and trustworthy circular economies through distributed ledger technologies" (EP/N028198/1), and UK EPSRC project "PETRAS IoT Research Hub – Cybersecurity of the Internet of Things" (EP/N023234/1).

[17] https://login.xyz/ (last-accessed 2022-2-18)
[18] https://huddle01.com/ (last-accessed 2022-2-18)
[19] https://poap.xyz/ (last-accessed 2022-2-18)

REFERENCES

[1] Aydin Abadi, Jin Xiao, Roberto Metere, and Richard Shillcock. 2021. ValuED: A Blockchain-based Trading Platform to Encourage Student Engagement in Higher Education. https://doi.org/10.31234/osf.io/na2qu
[2] Svetlana Abramova, Artemij Voskobojnikov, Konstantin Beznosov, and Rainer Böhme. 2021. Bits Under the Mattress: Understanding Different Risk Perceptions and Security Behaviors of Crypto-Asset Users. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 692, 19 pages. https://doi.org/10.1145/3411764.3445679
[3] Antonio Welligton S. Abreu, Emanuel F. Coutinho, and Carla I. M. Bezerra. 2020. A Blockchain-Based Architecture for Query and Registration of Student Degree Certificates. In *Proceedings of the 14th Brazilian Symposium on Software Components, Architectures, and Reuse* (Natal, Brazil) *(SBCARS '20)*. Association for Computing Machinery, New York, NY, USA, 151–160. https://doi.org/10.1145/3425269.3425285
[4] Icek Ajzen. 1991. The theory of planned behavior. *Organizational behavior and human decision processes* 50, 2 (1991), 179–211.
[5] Emad Almutairi and Shiroq Al-Megren. 2019. Usability and Security Analysis of the KeepKey Wallet. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. 149–153. https://doi.org/10.1109/BLOC.2019.8751451
[6] Omar Alqaryouti, Nur Siyam, Zainab Alkashri, and Khaled Shaalan. 2020. Cryptocurrency Usage Impact on Perceived Benefits and Users' Behaviour. In *Information Systems (Lecture Notes in Business Information Processing)*, Marinos Themistocleous and Maria Papadaki (Eds.). Springer International Publishing, 123–136. https://doi.org/10.1007/978-3-030-44322-1_10
[7] Omar Alqaryouti, Nur Siyam, Zainab Alkashri, and Khaled Shaalan. 2020. Users' Knowledge and Motivation on Using Cryptocurrency. In *Information Systems (Lecture Notes in Business Information Processing)*, Marinos Themistocleous and Maria Papadaki (Eds.). Springer International Publishing, 113–122. https://doi.org/10.1007/978-3-030-44322-1_9
[8] Abdulla Alshamsi and Prof. Peter Andras. 2019. User perception of Bitcoin usability and security across novice users. *International Journal of Human-Computer Studies* 126 (2019), 94–110. https://doi.org/10.1016/j.ijhcs.2019.02.004
[9] Mehmet Aydin Baytaş, Aykut Coşkun, Asim Evren Yantaç, and Morten Fjeld. 2018. Towards Materials for Computational Heirlooms: Blockchains and Wristwatches. In *Proceedings of the 2018 Designing Interactive Systems Conference* (Hong Kong, China) *(DIS '18)*. Association for Computing Machinery, New York, NY, USA, 703–717. https://doi.org/10.1145/3196709.3196778
[10] Juan Benet. 2018. What Exactly is Web3? by Juan Benet at Web3 Summit 2018 (Video). Retrieved 2021-12-13 from https://youtu.be/l44z35vabvA (Video).
[11] Nicola J. Bidwell, Chris Elsden, Ludwig Trotter, Josh Hallwright, Sadie Moore, Kate Jeite-Delbridge, Mike Harding, Peter Shaw, Nigel Davies, Chris Speed, and John Vines. 2021. A Right Time to Give: Beyond Saving Time in Automated Conditional Donations. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 49, 20 pages. https://doi.org/10.1145/3411764.3445371
[12] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. https://doi.org/10.1191/1478088706qp063oa arXiv:https://www.tandfonline.com/doi/pdf/10.1191/1478088706qp063oa
[13] John Brooke. 1996. SUS: a 'quick and dirty' usability scale. *Usability evaluation in industry* (1996), 189.
[14] Karoline Busse, Mohammad Tahaei, Katharina Krombholz, Emanuel von Zezschwitz, Matthew Smith, Jing Tian, and Wenyuan Xu. 2020. Cash, Cards or Cryptocurrencies? A Study of Payment Culture in Four Countries. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. 200–209. https://doi.org/10.1109/EuroSPW51379.2020.00035
[15] Vitalik Buterin et al. 2013. Ethereum white paper. *GitHub repository* 1 (2013), 22–23.
[16] Irvin Steve Cardenas and Jong Hoon Kim. 2018. Robot-Human Agreements and Financial Transactions Enabled by a Blockchain and Smart Contracts. In *Companion of the 2018 ACM/IEEE International Conference on Human-Robot Interaction* (Chicago, IL, USA) *(HRI '18)*. Association for Computing Machinery, New York, NY, USA, 337–338. https://doi.org/10.1145/3173386.3177818
[17] Irvin Steve Cardenas and Jong-Hoon Kim. 2020. Robonomics: The Study of Robot-Human Peer-to-Peer Financial Transactions and Agreements. In *Companion of the 2020 ACM/IEEE International Conference on Human-Robot Interaction*

(Cambridge, United Kingdom) *(HRI '20)*. Association for Computing Machinery, New York, NY, USA, 8–15. https://doi.org/10.1145/3371382.3380735

[18] You-Ping Chen and Ju-Chun Ko. 2019. CryptoAR Wallet: A Blockchain Cryptocurrency Wallet Application That Uses Augmented Reality for On-Chain User Data Display. In *Proceedings of the 21st International Conference on Human-Computer Interaction with Mobile Devices and Services* (Taipei, Taiwan) *(MobileHCI '19)*. Association for Computing Machinery, New York, NY, USA, Article 39, 5 pages. https://doi.org/10.1145/3338286.3344386

[19] You-Ping Chen and Ju-Chun Ko. 2020. The Impact of AR Filter Combines Blockchain Virtual Online Pets and brings Blockchain into our lives. In *2020 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-Taiwan)*. 1–2. https://doi.org/10.1109/ICCE-Taiwan49838.2020.9258040

[20] Chun-Wei Chiang, Eber Betanzos, and Saiph Savage. 2018. Exploring Blockchain for Trustful Collaborations between Immigrants and Governments. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI EA '18)*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3170427.3188660

[21] Chun-Wei Chiang, Eber Betanzos, and Saiph Savage. 2019. The Challenges and Trends of Deploying Blockchain in the Real World for the Users' Need. *Journal of Cyberspace Studies* 3, 2 (2019), 119–128. https://doi.org/10.22059/jcss.2019.72454

[22] Nazli Cila, Gabriele Ferri, Martijn de Waal, Inte Gloerich, and Tara Karpinski. 2020. *The Blockchain and the Commons: Dilemmas in the Design of Local Platforms*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376660

[23] Coinmarketcap. 2022. *Top 100 Cryptocurrencies by Market Capitalization*. Retrieved Feb 7, 2022 from https://coinmarketcap.com/

[24] ConsenSys. 2021. *Web 3 Report Q3 2021*. ConsenSys. Retrieved 2022-02-11 from https://consensys.net/reports/web3-report-q3-2021/

[25] Karlene Cousins, Hemang Subramanian, and Pouyan Esmaeilzadeh. 2019. A Value-sensitive Design Perspective of Cryptocurrencies: A Research Agenda. *Communications of the Association for Information Systems* 45, 1 (Dec 2019). https://doi.org/10.17705/1CAIS.04527

[26] Barnaby Craggs and Awais Rashid. 2019. Trust Beyond Computation Alone: Human Aspects of Trust in Blockchain Technologies. In *2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Society (ICSE-SEIS)*. 21–30. https://doi.org/10.1109/ICSE-SEIS.2019.00011

[27] Fred D Davis. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly* (1989), 319–340.

[28] Raynor de Best. 2022. *Bitcoin Market Dominance*. Statista. Retrieved 2022-02-11 from https://www.statista.com/statistics/1269669/bitcoin-dominance-historical-development/

[29] Chris Dixon and Eddy Lazzarin. 2020. *The Crypto Price-Innovation Cycle*. Andreessen Horowitz. Retrieved 2021-12-13 from https://a16z.com/2020/05/15/the-crypto-price-innovation-cycle/

[30] Nelisiwe Peaceness Dlamini, Mfundo Shakes Scott, and Kishor Krishnan Nair. 2017. Development of an SMS system used to access Bitcoin wallets. In *2017 IST-Africa Week Conference (IST-Africa)*. 1–10. https://doi.org/10.23919/ISTAFRICA.2017.8102316

[31] Janna Lynn Dupree, Richard Devries, Daniel M. Berry, and Edward Lank. 2016. Privacy Personas: Clustering Users via Attitudes and Behaviors toward Security Practices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 5228–5239. https://doi.org/10.1145/2858036.2858214

[32] Susen Döbelt and Maria Kreußlein. 2020. Peer-to-Peer Traded Energy: Prosumer and Consumer Focus Groups about a Self-consumption Community Scenario. In *HCI International 2020 - Posters (Communications in Computer and Information Science)*, Constantine Stephanidis and Margherita Antona (Eds.). Springer International Publishing, 130–140. https://doi.org/10.1007/978-3-030-50726-8_17

[33] Dmitry Efanov and Pavel Roschin. 2018. The all-pervasiveness of the blockchain technology. *Procedia Computer Science* 123 (2018), 116–121. https://doi.org/10.1016/j.procs.2018.01.019

[34] Chris Elsden, Inte Gloerich, Anne Spaa, John Vines, and Martijn de Waal. 2019. Making the Blockchain Civic. *Interactions* 26, 2 (Feb 2019), 60–65. https://doi.org/10.1145/3305364

[35] Chris Elsden, Arthi Manohar, Jo Briggs, Mike Harding, Chris Speed, and John Vines. 2018. *Making Sense of Blockchain Applications: A Typology for HCI*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3173574.3174032

[36] Chris Elsden, Kate Symons, Raluca Bunduchi, Chris Speed, and John Vines. 2019. Sorting Out Valuation in the Charity Shop: Designing for Data-Driven Innovation through Value Translation. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 109 (nov 2019), 25 pages. https://doi.org/10.1145/3359211

[37] Chris Elsden, Kate Symons, Chris Speed, John Vines, and Anne Spaa. 2019. Searching for an OxChain: Co-designing blockchain applications for charitable giving. *Ubiquity: The Journal of Pervasive Media* 6, 1 (Nov 2019), 5–16. https://doi.org/10.1386/ubiq_00002_1

[38] Chris Elsden, Ludwig Trotter, Mike Harding, Nigel Davies, Chris Speed, and John Vines. 2019. *Programmable Donations: Exploring Escrow-Based Conditional Giving*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300609

[39] Shayan Eskandari, David Barrera, Elizabeth Stobert, and Jeremy Clark. 2015. A First Look at the Usability of Bitcoin Key Management. *Proceedings 2015 Workshop on Usable Security* (2015). https://doi.org/10.14722/usec.2015.23015

[40] Shayan Eskandari, Jeremy Clark, and Abdelwahab Hamou-Lhadj. 2016. Buy Your Coffee with Bitcoin: Real-World Deployment of a Bitcoin Point of Sale Terminal. In *2016 Intl IEEE Conferences on Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*. 382–389. https://doi.org/10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0073

[41] Youssef Faqir-Rhazoui, Miller-Janny Ariza-Garzón, Javier Arroyo, and Samer Hassan. 2021. *Effect of the Gas Price Surges on User Activity in the DAOs of the Ethereum Blockchain*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411763.3451755

[42] Anton Fedosov, Agon Bexheti, Egor Ermolaev, and Marc Langheinrich. 2018. Sharing Physical Objects Using Smart Contracts. In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct* (Barcelona, Spain) *(MobileHCI '18)*. Association for Computing Machinery, New York, NY, USA, 346–352. https://doi.org/10.1145/3236112.3236162

[43] Md Sadek Ferdous, Farida Chowdhury, and Madini O. Alassafi. 2019. In Search of Self-Sovereign Identity Leveraging Blockchain Technology. *IEEE Access* 7 (2019), 103059–103079. https://doi.org/10.1109/ACCESS.2019.2931173

[44] Silke Finken and Louisa Heiduk. 2021. Factors influencing the acceptance of proximity mobile payment in Germany: The example of Apple Pay. *Journal of Payments Strategy & Systems* 15, 1 (2021), 92–108.

[45] Marcus Foth. 2017. The Promise of Blockchain Technology for Interaction Design. In *Proceedings of the 29th Australian Conference on Computer-Human Interaction* (Brisbane, Queensland, Australia) *(OZCHI '17)*. Association for Computing Machinery, New York, NY, USA, 513–517. https://doi.org/10.1145/3152771.3156168

[46] Allan Fowler and Johanna Pirker. 2021. *Tokenfication - The Potential of Non-Fungible Tokens (NFT) for Game Development*. Association for Computing Machinery, New York, NY, USA, 152–157. https://doi.org/10.1145/3450337.3483501

[47] Michael Froehlich, Philipp Hulm, and Florian Alt. 2021. Under Pressure. A User-Centered Threat Model for Cryptocurrency Owners. In *2021 the 4th International Conference on Blockchain Technology and Applications* (Xi'an, China) *(ICBTA 2021)*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3510487.3510494

[48] Michael Froehlich, Charlotte Kobiella, Albrecht Schmidt, and Florian Alt. 2021. *Is It Better With Onboarding? Improving First-Time Cryptocurrency App Experiences*. Association for Computing Machinery, New York, NY, USA, 78–89. https://doi.org/10.1145/3461778.3462047

[49] Michael Froehlich, Maurizio Raphael Wagenhaus, Albrecht Schmidt, and Florian Alt. 2021. *Don't Stop Me Now! Exploring Challenges Of First-Time Cryptocurrency Users*. Association for Computing Machinery, New York, NY, USA, 138–148. https://doi.org/10.1145/3461778.3462071

[50] Michael Fröhlich, Felix Gutjahr, and Florian Alt. 2020. *Don't Lose Your Coin! Investigating Security Practices of Cryptocurrency Users*. Association for Computing Machinery, New York, NY, USA, 1751–1763. https://doi.org/10.1145/3357236.3395535

[51] Xianyi Gao, Gradeigh D. Clark, and Janne Lindqvist. 2016. Of Two Minds, Multiple Addresses, and One Ledger: Characterizing Opinions, Knowledge, and Perceptions of Bitcoin Across Users and Non-Users. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 1656–1668. https://doi.org/10.1145/2858036.2858049

[52] Leonhard Glomann, Maximilian Schmid, and Nika Kitajewa. 2020. Improving the Blockchain User Experience - An Approach to Address Blockchain Mass Adoption Issues from a Human-Centred Perspective. In *Advances in Artificial Intelligence, Software and Systems Engineering (Advances in Intelligent Systems and Computing)*, Tareq Ahram (Ed.). Springer International Publishing, 608–616. https://doi.org/10.1007/978-3-030-20454-9_60

[53] Michael Heidt, Arne Berger, and Andreas Bischof. 2019. Blockchain and Trust: A Practice-Based Inquiry. In *HCI in Business, Government and Organizations. eCommerce and Consumer Behavior (Lecture Notes in Computer Science)*, Fiona Fui-Hoon Nah and Keng Siau (Eds.). Springer International Publishing, 148–158. https://doi.org/10.1007/978-3-030-22335-9_10

[54] Michael Heidt, Andreas Bischof, and Arne Berger. 2019. Interactional Aesthetics of Blockchain Technology. In *HCI in Business, Government and Organizations. eCommerce and Consumer Behavior (Lecture Notes in Computer Science)*, Fiona Fui-Hoon Nah and Keng Siau (Eds.). Springer International Publishing, 137–147. https://doi.org/10.1007/978-3-030-22335-9_9

[55] Sara Heitlinger, Lara Houston, Alex Taylor, and Ruth Catlow. 2021. Algorithmic Food Justice: Co-Designing More-than-Human Blockchain Futures

for the Food Commons. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 305, 17 pages. https://doi.org/10.1145/3411764.3445655

[56] Mitchell Hentges, Sheldon Roddick, and Haytham Elmiligi. 2017. Fambit: A Promising Solution to Support Open Educational Resources Initiatives. In *Proceedings of the 22nd Western Canadian Conference on Computing Education* (Abbotsford, BC, Canada) *(WCCCE '17)*. Association for Computing Machinery, New York, NY, USA, Article 4, 4 pages. https://doi.org/10.1145/3085585.3085589

[57] Tani Hossain, Tasniah Mohiuddin, A. M. Shahed Hasan, Muhammad Nazrul Islam, and Syed Akhter Hossain. 2021. Designing and Developing Graphical User Interface for the MultiChain Blockchain: Towards Incorporating HCI in Blockchain. In *Intelligent Systems Design and Applications (Advances in Intelligent Systems and Computing)*, Ajith Abraham, Vincenzo Piuri, Niketa Gandhi, Patrick Siarry, Arturas Kaklauskas, and Ana Madureira (Eds.). Springer International Publishing, 446–456. https://doi.org/10.1007/978-3-030-71187-0_41

[58] Huawei Huang, Wei Kong, Sicong Zhou, Zibin Zheng, and Song Guo. 2021. A Survey of State-of-the-Art on Blockchains: Theories, Modelings, and Tools. *ACM Comput. Surv.* 54, 2, Article 44 (mar 2021), 42 pages. https://doi.org/10.1145/3441692

[59] Johannes Huebner, Remo Manuel Frey, Christian Ammendola, Elgar Fleisch, and Alexander Ilic. 2018. What People Like in Mobile Finance Apps: An Analysis of User Reviews. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia* (Cairo, Egypt) *(MUM 2018)*. Association for Computing Machinery, New York, NY, USA, 293–304. https://doi.org/10.1145/3282894.3282895

[60] Sinh Huynh, Kenny Tsu Wei Choo, Rajesh Krishna Balan, and Youngki Lee. 2019. CryptoCurrency Mining on Mobile as an Alternative Monetization Approach. In *Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications* (Santa Cruz, CA, USA) *(HotMobile '19)*. Association for Computing Machinery, New York, NY, USA, 51–56. https://doi.org/10.1145/3301293.3302372

[61] Karim Jabbar and Pernille Bjørn. 2018. Infrastructural Grind: Introducing Blockchain Technology in the Shipping Domain. In *Proceedings of the 2018 ACM Conference on Supporting Groupwork* (Sanibel Island, Florida, USA) *(GROUP '18)*. Association for Computing Machinery, New York, NY, USA, 297–308. https://doi.org/10.1145/3148330.3148345

[62] Karim Jabbar and Pernille Bjørn. 2019. *Blockchain Assemblages: Whiteboxing Technology and Transforming Infrastructural Imaginaries*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300496

[63] Eaman Jahani, Peter M. Krafft, Yoshihiko Suhara, Esteban Moro, and Alex Sandy Pentland. 2018. ScamCoins, S*** Posters, and the Search for the Next BitcoinTM: Collective Sensemaking in Cryptocurrency Discussions. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 79 (nov 2018), 28 pages. https://doi.org/10.1145/3274348

[64] Hyeji Jang, Sung H. Han, and Ju Hwan Kim. 2020. User Perspectives on Blockchain Technology: User-Centered Evaluation and Design Strategies for DApps. *IEEE Access* 8 (2020), 226213–226223. https://doi.org/10.1109/ACCESS.2020.3042822

[65] Hyeji Jang, Sung H. Han, Ju Hwan Kim, and Kimin Kown. 2020. Identifying and Improving Usability Problems of Cryptocurrency Exchange Mobile Applications Through Heuristic Evaluation. In *Advances in Usability, User Experience, Wearable and Assistive Technology (Advances in Intelligent Systems and Computing)*, Tareq Ahram and Christianne Falcão (Eds.). Springer International Publishing, 15–21. https://doi.org/10.1007/978-3-030-51828-8_3

[66] Hyeji Jang, Sung H. Han, Ju Hwan Kim, and Kimin Kwon. 2021. Usability Evaluation for Cryptocurrency Exchange. In *Convergence of Ergonomics and Design (Advances in Intelligent Systems and Computing)*, Alma Maria Jennifer Gutierrez, Ravindra S. Goonetilleke, and Rex Aurellius C. Robielos (Eds.). Springer International Publishing, 192–196. https://doi.org/10.1007/978-3-030-63335-6_20

[67] Ali Kazerani, Domenic Rosati, and Brian Lesser. 2017. Determining the Usability of Bitcoin for Beginners Using Change Tip and Coinbase. In *Proceedings of the 35th ACM International Conference on the Design of Communication* (Halifax, Nova Scotia, Canada) *(SIGDOC '17)*. Association for Computing Machinery, New York, NY, USA, Article 5, 5 pages. https://doi.org/10.1145/3121113.3121125

[68] Denisa Reshef Kera, Petr Šourek, Mateusz Kraiński, Yair Reshef, Juan Manuel Corchado Rodríguez, and Iva Magdalena Knobloch. 2019. Lithopia: Prototyping Blockchain Futures. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI EA '19)*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3290607.3312896

[69] Evan Kereiakes, Marco Di Maggio Do Kwon, and Nicholas Platias. 2019. Terra money: Stability and adoption.

[70] Irni Eliana Khairuddin and Corina Sas. 2019. *An Exploration of Bitcoin Mining Practices: Miners' Trust Challenges and Motivations*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300859

[71] Irni Eliana Khairuddin, Corina Sas, Sarah Clinch, and Nigel Davies. 2016. Exploring Motivations for Bitcoin Technology Usage. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI EA '16)*. Association for Computing Machinery, New York, NY, USA, 2872–2878. https://doi.org/10.1145/2851581.2892500

[72] Irni Eliana Khairuddin, Corina Sas, and Chris Speed. 2019. BlocKit: A Physical Kit for Materializing and Designing for Blockchain Infrastructure. In *Proceedings of the 2019 on Designing Interactive Systems Conference* (San Diego, CA, USA) *(DIS '19)*. Association for Computing Machinery, New York, NY, USA, 1449–1462. https://doi.org/10.1145/3322276.3322370

[73] Duoaa Khalifa, Nadya Abdel Madjid, and Davor Svetinovic. 2019. Trust Requirements in Blockchain Systems: A Preliminary Study. In *2019 Sixth International Conference on Software Defined Systems (SDS)*. 310–313. https://doi.org/10.1109/SDS.2019.8768490

[74] Hafiz M Mudassar Khan, Waqas Saeed, M Waseem Iqbal, Akbar Ali, Maria Zuraiz, M Naveed Shahzad, and M Ahmed. 2021. The Promises of Blockchain and Cryptocurrencies Technology for Architecture and Interaction Design. *International Journal of Advanced Trends in Computer Science and Engineering* 10, 3 (2021), 2651–2657.

[75] Christoph Kinkeldey, Jean-Daniel Fekete, Tanja Blascheck, and Petra Isenberg. 2022. BitConduite: Exploratory Visual Analysis of Entity Activity on the Bitcoin Network. *IEEE Computer Graphics and Applications* 42, 1 (2022), 84–94. https://doi.org/10.1109/MCG.2021.3070303

[76] Megan Knittel, Shelby Pitts, and Rick Wash. 2019. "The Most Trustworthy Coin": How Ideological Tensions Drive Trust in Bitcoin. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 36 (nov 2019), 23 pages. https://doi.org/10.1145/3359138

[77] Megan L. Knittel and Rick Wash. 2019. How "True Bitcoiners" Work on Reddit to Maintain Bitcoin. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI EA '19)*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3290607.3312969

[78] Peter M. Krafft, Nicolas Della Penna, and Alex Sandy Pentland. 2018. *An Experimental Study of Cryptocurrency Market Dynamics*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3173574.3174179

[79] Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer, and Edgar Weippl. 2017. The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy. In *Financial Cryptography and Data Security (Lecture Notes in Computer Science)*, Jens Grossklags and Bart Preneel (Eds.). Springer, 555–580. https://doi.org/10.1007/978-3-662-54970-4_33

[80] Ponnurangam Kumaraguru and Lf Cranor. 2005. Privacy indexes: A survey of westin's studies. *School of Computer Science, Carnegie Mellon University* Tech. rep., December (2005), 1–22. http://repository.cmu.edu/isr%5Cnhttp://www.casos.cs.cmu.edu/publications/papers/CMU-ISRI-05-138.pdf%5Cnhttp://repository.cmu.edu/isr/856/

[81] Kimin Kwon, Sung H. Han, Hyeji Jang, and Ju Hwan Kim. 2021. Usability in a Token-Based Ecosystem. In *Advances in Usability, User Experience, Wearable and Assistive Technology (Lecture Notes in Networks and Systems)*, Tareq Z. Ahram and Christianne S. Falcão (Eds.). Springer International Publishing, 880–885. https://doi.org/10.1007/978-3-030-80091-8_104

[82] Minha Lee, Lily Frank, and Wijnand IJsselsteijn. 2021. Brokerbot: A Cryptocurrency Chatbot in the Social-technical Gap of Trust. *Computer Supported Cooperative Work (CSCW)* 30, 1 (2021), 79–117.

[83] Younghwa Lee, Kenneth A Kozar, and Kai RT Larsen. 2003. The technology acceptance model: Past, present, and future. *Communications of the Association for information systems* 12, 1 (2003), 50.

[84] Caitlin Lustig. 2019. Intersecting Imaginaries: Visions of Decentralized Autonomous Systems. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 210 (Nov 2019), 27 pages. https://doi.org/10.1145/3359312

[85] Caitlin Lustig and Bonnie Nardi. 2015. Algorithmic authority: The case of Bitcoin. In *2015 48th Hawaii International Conference on System Sciences*. IEEE, 743–752.

[86] Julia Magas. 2020. *Women in Blockchain: Has Gender Distribution Come to the Crypto Market?* Retrieved 2022-02-11 from https://cointelegraph.com/news/women-in-crypto-has-gender-consensus-come-to-the-market

[87] Alexandra Mai, Katharina Pfeffer, Matthias Gusenbauer, Edgar Weippl, and Katharina Krombholz. 2020. User Mental Models of Cryptocurrency Systems - A Grounded Theory Approach. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, 341–358. https://www.usenix.org/conference/soups2020/presentation/mai

[88] Arthi Manohar and Jo Briggs. 2018. Designing InWith Black Box Technologies and PD. *DRS Biennial Conference Series* (Jun 2018). https://dl.designresearchsociety.org/drs-conference-papers/drs2018/researchpapers/170

[89] Jens Mattke, Christian Maier, and Lea Reis. 2020. Is Cryptocurrency Money? Three Empirical Studies Analyzing Medium of Exchange, Store of Value and Unit of Account. In *Proceedings of the 2020 on Computers and People Research Conference* (Nuremberg, Germany) *(SIGMIS-CPR'20)*. Association for Computing Machinery, New York, NY, USA, 26–35. https://doi.org/10.1145/3378539.3393859

[90] Deborah Maxwell, Chris Speed, and Dug Campbell. 2015. 'Effing' the Ineffable: Opening up Understandings of the Blockchain. In *Proceedings of the*

2015 British HCI Conference (Lincoln, Lincolnshire, United Kingdom) *(British HCI '15)*. Association for Computing Machinery, New York, NY, USA, 208–209. https://doi.org/10.1145/2783446.2783593

[91] Arne Meeuw, Sandro Schopfer, Benjamin Ryder, and Felix Wortmann. 2018. LokalPower: Enabling Local Energy Markets with User-Driven Engagement. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI EA '18)*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3170427.3188610

[92] Eva Meyer, Isabell M Welpe, and Philipp G Sandner. 2021. Decentralized Finance—A systematic literature review and research directions. *Available at SSRN 4016497* (2021). https://doi.org/10.2139/ssrn.4016497

[93] David Moher, Larissa Shamseer, Mike Clarke, Davina Ghersi, Alessandro Liberati, Mark Petticrew, Paul Shekelle, and Lesley A Stewart. 2015. Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. *Systematic reviews* 4, 1 (2015), 1–9.

[94] Md Moniruzzaman, Farida Chowdhury, and Md Sadek Ferdous. 2020. Examining Usability Issues in Blockchain-Based Cryptocurrency Wallets. In *Cyber Security and Computer Science (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering)*, Touhid Bhuiyan, Md. Mostafijur Rahman, and Md. Asraf Ali (Eds.). Springer International Publishing, 631–643. https://doi.org/10.1007/978-3-030-52856-0_50

[95] Gianmaria Del Monte, Diego Pennino, and Maurizio Pizzonia. 2020. Scaling Blockchains without Giving up Decentralization and Security: A Solution to the Blockchain Scalability Trilemma. In *Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems* (London, United Kingdom) *(CryBlock '20)*. Association for Computing Machinery, New York, NY, USA, 71–76. https://doi.org/10.1145/3410699.3413800

[96] Nitin Naik and Paul Jenkins. 2020. uPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain. In *2020 IEEE International Symposium on Systems Engineering (ISSE)*. 1–7. https://doi.org/10.1109/ISSE49799.2020.9272223

[97] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review* (2008), 21260.

[98] Jakob Nielsen and Rolf Molich. 1990. Heuristic Evaluation of User Interfaces. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Seattle, Washington, USA) *(CHI '90)*. Association for Computing Machinery, New York, NY, USA, 249–256. https://doi.org/10.1145/97243.97281

[99] Viktor Nikolouzou Evgenia, Paggio and Dekker Marnix. 2021. *Digital Identity: Leveraging the SSI Concept to Build Trust*. Technical Report. European Union Agency for Cybersecurity,.

[100] Bettina Nissen, Larissa Pschetz, Dave Murray-Rust, Hadi Mehrpouya, Shaune Oosthuizen, and Chris Speed. 2018. *GeoCoin: Supporting Ideation and Collaborative Design with Smart Contracts*. Association for Computing Machinery, New York, NY, USA, 1–10. https://doi.org/10.1145/3173574.3173737

[101] Kevin O'Leary, Philip O'Reilly, Joseph Feller, Rob Gleasure, Shanping Li, and Jerry Cristoforo. 2017. Exploring the Application of Blockchain Technology to Combat the Effects of Social Loafing in Cross Functional Group Projects. In *Proceedings of the 13th International Symposium on Open Collaboration* (Galway, Ireland) *(OpenSym '17)*. Association for Computing Machinery, New York, NY, USA, Article 13, 8 pages. https://doi.org/10.1145/3125433.3125464

[102] Say Keat Ooi, Chai Aun Ooi, Jasmine A. L. Yeap, and Tok Hao Goh. 2021. Embracing Bitcoin: users' perceived security and trust. *Quality & Quantity* 55, 4 (Aug 2021), 1219–1237. https://doi.org/10.1007/s11135-020-01055-w

[103] Andreea-Elena Panait. 2020. Is the user identity perception influenced by the blockchain technology?. In *2020 IEEE International Conference on Intelligence and Security Informatics (ISI)*. 1–3. https://doi.org/10.1109/ISI49825.2020.9280530

[104] Erik Pescara, Ilya Fillipov, and Michael Beigl. 2019. StockSense: A Wrist-Worn Vibrotactile Display for Tracking Volatile Markets. In *Proceedings of the 10th Augmented Human International Conference 2019* (Reims, France) *(AH2019)*. Association for Computing Machinery, New York, NY, USA, Article 4, 4 pages. https://doi.org/10.1145/3311823.3311834

[105] Ingrid Pettersson, Florian Lachner, Anna-Katharina Frison, Andreas Riener, and Andreas Butz. 2018. *A Bermuda Triangle? A Review of Method Application and Triangulation in User Experience Evaluation*. Association for Computing Machinery, New York, NY, USA, 1–16. https://doi.org/10.1145/3173574.3174035

[106] Serguei Popov. 2018. The tangle. *White paper* 1, 3 (2018).

[107] Larissa Pschetz, Billy Dixon, Kruakae Pothong, Arlene Bailey, Allister Glean, Luis Lourenço Soares, and Jessica A. Enright. 2020. *Designing Distributed Ledger Technologies for Social Change: The Case of CariCrop*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376364

[108] punk6529. 2021. *A Guide to NFT Twitter Terminology*. Retrieved 2022-02-11 from https://www.one37pm.com/nft/art/nft-twitter-meanings-definitions

[109] Bagus Anugrah Ramadhan and Billy Muhamad Iqbal. 2018. User Experience Evaluation on the Cryptocurrency Website by Trust Aspect. In *2018 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS)*, Vol. 3. 274–279. https://doi.org/10.1109/ICIIBMS.2018.8550019

[110] Anita Ramaswamy and Natasha Mascarenhas. 2021. *ConstitutionDAO's bold crypto bid for US Constitution falls short*. Retrieved 2022-02-11 from https://techcrunch.com/2021/11/18/constitutiondaos-bold-crypto-bid-for-us-constitution-falls-short/

[111] Jonathan Rankin, Chris Elsden, Ian Sibbald, Alan Stevenson, John Vines, and Chris Speed. 2020. *PizzaBlock: Designing Artefacts and Roleplay to Understand Decentralised Identity Management Systems*. Association for Computing Machinery, New York, NY, USA, 1593–1606. https://doi.org/10.1145/3357236.3395568

[112] Ronald W Rogers. 1975. A protection motivation theory of fear appeals and attitude change1. *The journal of psychology* 91, 1 (1975), 93–114.

[113] John Rooksby and Kristiyan Dimitrov. 2019. Trustless education? A blockchain system for university grades1. *Ubiquity: The Journal of Pervasive Media* 6, 1 (Nov 2019), 83–88. https://doi.org/10.1386/ubiq_00010_1

[114] Corina Sas and Irni Eliana Khairuddin. 2015. Exploring Trust in Bitcoin Technology: A Framework for HCI Research. In *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction* (Parkville, VIC, Australia) *(OzCHI '15)*. Association for Computing Machinery, New York, NY, USA, 338–342. https://doi.org/10.1145/2838739.2838821

[115] Corina Sas and Irni Eliana Khairuddin. 2017. Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 6499–6510. https://doi.org/10.1145/3025453.3025886

[116] Sabrina Scuri, Gergana Tasheva, Luísa Barros, and Nuno Jardim Nunes. 2019. An HCI Perspective on Distributed Ledger Technologies for Peer-to-Peer Energy Trading. In *Human-Computer Interaction – INTERACT 2019 (Lecture Notes in Computer Science)*, David Lamas, Fernando Loizides, Lennart Nacke, Helen Petrie, Marco Winckler, and Panayiotis Zaphiris (Eds.). Springer International Publishing, 91–111. https://doi.org/10.1007/978-3-030-29387-1_6

[117] Aamna Al Shehhi, Mayada Oudah, and Zeyar Aung. 2014. Investigating factors behind choosing a cryptocurrency. In *2014 IEEE International Conference on Industrial Engineering and Engineering Management*. 1443–1447. https://doi.org/10.1109/IEEM.2014.7058877

[118] Maria Shen and Avichal Garg. 2022. *Developer Report 2021*. Electric Capital. Retrieved 2022-02-11 from https://github.com/electric-capital/developer-reports/blob/master/dev_report_2021_updated_012622.pdf

[119] Quinten Stokkink and Johan Pouwelse. 2018. Deployment of a Blockchain-Based Self-Sovereign Identity. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. 1336–1342. https://doi.org/10.1109/Cybermatics_2018.2018.00230

[120] Yujing Sun, Hao Xiong, Siu Ming Yiu, and Kwok Yan Lam. 2019. BitVis: An Interactive Visualization System for Bitcoin Accounts Analysis. In *2019 Crypto Valley Conference on Blockchain Technology (CVCBT)*. 21–25. https://doi.org/10.1109/CVCBT.2019.000-3

[121] Melanie Swan. 2015. *Blockchain: Blueprint for a New Economy* (1st ed.). O'Reilly Media, Inc.

[122] Ella Tallyn, Larissa Pschetz, Rory Gianni, Chris Speed, and Chris Elsden. 2018. Exploring Machine Autonomy and Provenance Data in Coffee Consumption: A Field Study of Bitbarista. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 170 (nov 2018), 25 pages. https://doi.org/10.1145/3274439

[123] Ella Tallyn, Joe Revans, Evan Morgan, Keith Fisken, and Dave Murray-Rust. 2021. Enacting the Last Mile: Experiences of Smart Contracts in Courier Deliveries. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 639, 14 pages. https://doi.org/10.1145/3411764.3445525

[124] Ella Tallyn, Joe Revans, Evan Morgan, and Dave Murray-Rust. 2020. *GeoPact: Engaging Publics in Location-Aware Smart Contracts through Technological Assemblies*. Association for Computing Machinery, New York, NY, USA, 799–811. https://doi.org/10.1145/3357236.3395583

[125] Sean Tan, Sourav S Bhowmick, Huey Eng Chua, and Xiaokui Xiao. 2020. LATTE: Visual Construction of Smart Contracts. In *Proceedings of the 2020 ACM SIGMOD International Conference on Management of Data* (Portland, OR, USA) *(SIGMOD '20)*. Association for Computing Machinery, New York, NY, USA, 2713–2716. https://doi.org/10.1145/3318464.3384687

[126] Atima Tharatipyakul and Suporn Pongnumkul. 2021. User Interface of Blockchain-Based Agri-Food Traceability Applications: A Review. *IEEE Access* 9 (2021), 82909–82929. https://doi.org/10.1109/ACCESS.2021.3085982

[127] Natkamon Tovanich, Nicolas Heulot, Jean-Daniel Fekete, and Petra Isenberg. 2021. Visualization of Blockchain Data: A Systematic Review. *IEEE Transactions on Visualization and Computer Graphics* 27, 7 (2021), 3135–3152. https://doi.org/10.1109/TVCG.2019.2963018

[128] Ludwig Trotter, Mike Harding, Chris Elsden, Nigel Davies, and Chris Speed. 2020. A Mobile Platform for Event-Driven Donations Using Smart Contracts. In *Proceedings of the 21st International Workshop on Mobile Computing Systems and Applications* (Austin, TX, USA) *(HotMobile '20)*. Association for Computing Machinery, New York, NY, USA, 108. https://doi.org/10.1145/3376897.3379161

[129] Ludwig Trotter, Mike Harding, Peter Shaw, Nigel Davies, Chris Elsden, Chris Speed, John Vines, Aydin Abadi, and Josh Hallwright. 2020. Smart Donations: Event-Driven Conditional Donations Using Smart Contracts On The Blockchain.

In *32nd Australian Conference on Human-Computer Interaction* (Sydney, NSW, Australia) *(OzCHI '20)*. Association for Computing Machinery, New York, NY, USA, 546–557. https://doi.org/10.1145/3441000.3441014

[130] Ultrasound.money. 2022. Ultra Sound Awakening – track ETH become ultra sound. Retrieved 2022-02-11 from https://ultrasound.money/

[131] Artemij Voskobojnikov, Svetlana Abramova, Konstantin Beznosov, and Rainer Boehme. 2021. Non-Adoption of Crypto-Assets: Exploring the Role of Trust, Self-Efficacy, and Risk. *ECIS 2021 Research Papers* 9 (2021). https://aisel.aisnet.org/ecis2021_rp/9

[132] Artemij Voskobojnikov, Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. 2020. Surviving the Cryptojungle: Perception and Management of Risk Among North American Cryptocurrency (Non)Users. In *Financial Cryptography and Data Security*, Joseph Bonneau and Nadia Heninger (Eds.). Springer International Publishing, Cham, 595–614.

[133] Artemij Voskobojnikov, Oliver Wiese, Masoud Mehrabi Koushki, Volker Roth, and Konstantin (Kosta) Beznosov. 2021. The U in Crypto Stands for Usable: An Empirical Study of User Experience with Mobile Cryptocurrency Wallets. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 642, 14 pages. https://doi.org/10.1145/3411764.3445407

[134] Sören Wallbach, Roland Lehner, Konstantin Roethke, Ralf Elbert, and Alexander Benlian. 2020. Trust-Building Effects of Blockchain Features – An Empirical Analysis of Immutability, Traceability and Anonymity. *ECIS 2020 Research Papers* (Jun 2020). https://aisel.aisnet.org/ecis2020_rp/182

[135] Tim Weingaertner, Rahul Rao, Jasmin Ettlin, Patrick Suter, and Philipp Dublanc. 2018. Smart Contracts Using Blockly: Representing a Purchase Agreement Using a Graphical Programming Language. In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. 55–64. https://doi.org/10.1109/CVCBT.2018.00012

[136] Stephen John Matthew C. Wenceslao and Maria Regina Justina E. Estuar. 2019. Using CTAKES to Build a Simple Speech Transcriber Plugin for an EMR. In *Proceedings of the Third International Conference on Medical and Health Informatics 2019* (Xiamen, China) *(ICMHI 2019)*. Association for Computing Machinery, New York, NY, USA, 78–86. https://doi.org/10.1145/3340037.3340044

[137] Jacob O. Wobbrock and Julie A. Kientz. 2016. Research Contributions in Human-Computer Interaction. *Interactions* 23, 3 (apr 2016), 38–44. https://doi.org/10.1145/2907069

[138] Gavin Wood. 2016. Polkadot: Vision for a heterogeneous multi-chain framework. *White Paper* 21 (2016), 2327–4662.

[139] Jia-zhi Xia, Yu-hong Zhang, Hui Ye, Ying Wang, Guang Jiang, Ying Zhao, Cong Xie, Xiao-yan Kui, Sheng-hui Liao, and Wei-ping Wang. 2020. SuPoolVisor: a visual analytics system for mining pool surveillance. *Frontiers of Information Technology & Electronic Engineering* 21, 4 (Apr 2020), 507–523. https://doi.org/10.1631/FITEE.1900532

[140] Anatoly Yakovenko. 2018. Solana: A new architecture for a high performance blockchain v0. 8.13. *Whitepaper* (2018).

[141] Xuanwu Yue, Xinhuan Shu, Xinyu Zhu, Xinnan Du, Zheqing Yu, Dimitrios Papadopoulos, and Siyuan Liu. 2019. BitExTract: Interactive Visualization for Extracting Bitcoin Exchange Intelligence. *IEEE Transactions on Visualization and Computer Graphics* 25, 1 (2019), 162–171. https://doi.org/10.1109/TVCG.2018.2864814

[142] Liudmila Zavolokina, Noah Zani, and Gerhard Schwabe. 2019. Why Should I Trust a Blockchain Platform? Designing for Trust in the Digital Car Dossier. In *Extending the Boundaries of Design Science Theory and Practice (Lecture Notes in Computer Science)*, Bengisu Tulu, Soussan Djamasbi, and Gondy Leroy (Eds.). Springer International Publishing, 269–283. https://doi.org/10.1007/978-3-030-19504-5_18

[143] Liudmila Zavolokina, Noah Zani, and Gerhard Schwabe. 2020. Designing for Trust in Blockchain Platforms. *IEEE Transactions on Engineering Management* (2020), 1–15. https://doi.org/10.1109/TEM.2020.3015359

[144] Rui Zhang, Rui Xue, and Ling Liu. 2019. Security and Privacy on Blockchain. *ACM Comput. Surv.* 52, 3, Article 51 (jul 2019), 34 pages. https://doi.org/10.1145/3316481

[145] Zengsheng Zhong, Shuirun Wei, Yeting Xu, Ying Zhao, Fangfang Zhou, Feng Luo, and Ronghua Shi. 2020. SilkViser: A Visual Explorer of Blockchain-based Cryptocurrency Transaction Data. In *2020 IEEE Conference on Visual Analytics Science and Technology (VAST)*. 95–106. https://doi.org/10.1109/VAST50239.2020.00014

Table 5: Overview of all publications included in the review.

Reference		Focus		Blockchain				Contribution Type								Major Themes					
	year	blockchain	cryptocurrency	bitcoin	ethereum	Other	not specified	empirical (system)	empirical (people)	artifact	method	theory	dataset	literature review	essay	trust	motivation,risk,perc.	wallets	engaging users	specific use cases	support tools
[117]	2014	-	●	●	-	●	-	-	●	-	-	-	-	-	-	-	●	-	-	-	-
[90]	2015	●	-	●	-	-	-	●	-	-	-	-	-	-	-	-	-	-	●	-	-
[114]	2015	-	●	●	-	-	-	-	-	-	-	●	-	-	-	●	-	-	-	-	-
[40]	2016	-	●	●	-	-	-	●	-	●	-	-	-	-	-	-	-	-	-	●	-
[71]	2016	-	●	●	-	-	-	-	●	-	-	-	-	-	-	-	●	-	-	-	-
[51]	2016	-	●	●	-	-	-	-	●	-	-	-	-	-	-	-	●	-	-	-	-
[45]	2017	●	-	●	-	-	-	-	-	-	-	-	-	-	●	-	-	-	-	●	-
[113]	2017	●	-	-	●	-	-	●	-	●	-	-	-	-	-	-	-	-	-	●	-
[101]	2017	●	-	-	●	-	-	-	-	●	-	-	-	-	-	-	-	-	-	●	-
[67]	2017	-	●	●	-	-	-	●	-	-	-	-	-	-	-	-	-	●	-	-	-
[115]	2017	-	●	●	-	-	-	-	●	-	-	●	-	-	-	●	●	-	-	-	-
[79]	2017	-	●	●	-	-	-	-	●	-	-	-	-	-	-	-	●	●	-	-	-
[56]	2017	-	●	●	-	-	-	-	-	●	-	-	-	-	-	-	-	-	-	●	-
[30]	2017	-	●	●	-	-	-	-	-	●	-	-	-	-	-	-	-	●	-	-	-
[35]	2018	●	-	●	●	●	-	-	-	-	-	-	●	●	-	-	-	-	-	●	-
[100]	2018	●	-	●	-	-	-	●	-	●	-	-	-	-	-	-	-	-	●	●	-
[122]	2018	●	-	●	-	-	-	●	-	●	-	-	-	-	-	-	-	-	-	●	-
[135]	2018	●	-	-	●	-	-	●	-	●	-	-	-	-	-	-	-	-	-	-	●
[16]	2018	●	-	-	●	-	-	-	-	●	-	-	-	-	-	-	-	-	-	●	-
[42]	2018	●	-	-	●	-	-	-	-	●	-	-	-	-	-	-	-	-	-	●	-
[91]	2018	●	-	-	-	-	●	●	-	●	-	-	-	-	-	-	-	-	-	●	-
[88]	2018	●	-	-	-	-	●	●	-	-	-	-	-	-	-	-	-	-	●	-	-
[37]	2018	●	-	-	-	-	●	●	-	-	-	-	-	-	-	-	-	-	●	●	-
[20]	2018	●	-	-	-	-	●	-	●	-	-	-	-	-	-	●	-	-	-	●	-
[61]	2018	●	-	-	-	-	●	-	●	-	-	-	-	-	-	-	-	-	-	●	-
[9]	2018	●	-	-	-	-	●	-	-	●	-	-	-	-	-	-	-	-	-	●	-
[63]	2018	-	●	●	●	●	-	-	●	-	-	-	-	-	-	-	●	-	-	-	-
[78]	2018	-	●	●	●	●	-	-	●	-	-	-	-	-	-	-	●	-	-	-	-
[109]	2018	-	●	●	-	-	-	●	-	-	-	-	-	-	-	-	-	●	-	-	-
[72]	2019	●	-	●	-	-	-	●	-	●	-	-	-	-	-	-	-	-	●	-	-
[141]	2019	●	-	●	-	-	-	-	-	●	-	-	-	-	-	-	-	-	-	-	●
[53]	2019	●	-	●	-	-	-	-	-	-	●	-	-	-	-	●	-	-	-	-	-
[136]	2019	●	-	-	-	●	-	●	-	●	-	-	-	-	-	-	-	-	-	●	-
[116]	2019	●	-	-	-	●	-	●	-	●	-	-	-	-	-	-	●	-	-	●	-
[68]	2019	●	-	-	-	●	-	-	-	●	-	-	-	-	-	-	-	-	●	-	-
[142]	2019	●	-	-	-	-	●	●	-	-	-	-	-	-	-	●	-	-	-	●	-
[38]	2019	●	-	-	-	-	●	-	●	-	-	-	-	-	-	-	-	-	●	●	-
[36]	2019	●	-	-	-	-	●	-	●	-	-	-	-	-	-	-	-	-	-	●	-
[62]	2019	●	-	-	-	-	●	-	●	-	-	-	-	-	-	-	-	-	-	●	-
[73]	2019	●	-	-	-	-	●	-	-	-	-	-	-	-	●	●	-	-	-	-	-
[54]	2019	●	-	-	-	-	●	-	-	-	-	-	-	-	●	-	-	-	-	●	-
[21]	2019	●	-	-	-	-	●	-	-	-	-	-	-	-	●	●	-	-	-	-	-
[84]	2019	●	-	-	-	-	●	-	-	-	-	-	-	-	●	-	-	-	-	●	-
[34]	2019	●	-	-	-	-	●	-	-	-	-	-	-	-	●	-	-	-	-	●	-
[5]	2019	-	●	●	-	-	-	●	-	-	-	-	-	-	-	-	●	●	-	-	-
[8]	2019	-	●	●	-	-	-	●	-	-	-	-	-	-	-	-	●	●	-	-	-
[76]	2019	-	●	●	-	-	-	-	●	-	-	-	-	-	-	●	●	-	-	-	-
[70]	2019	-	●	●	-	-	-	-	●	-	-	●	-	-	-	●	●	-	-	-	-
[77]	2019	-	●	●	-	-	-	-	●	-	-	-	-	-	-	●	●	-	-	-	-

Table 5 (continued): Overview of all publications included in the review.

Reference		Focus		Blockchain				Contribution Type								Major Themes					
	year	blockchain	cryptocurrency	bitcoin	ethereum	Other	not specified	empirical (system)	empirical (people)	artifact	method	theory	dataset	literature review	essay	trust	motivation,risk,perc.	wallets	engaging with users	specific use cases	support tools
[26]	2019	-	●	●	-	-	-	-	●	-	-	-	-	-	-	●	-	-	-	-	-
[25]	2019	-	●	●	-	-	-	-	●	-	-	-	-	-	-	●	●	-	-	-	-
[120]	2019	-	●	●	-	-	-	-	-	●	-	-	-	-	-	-	-	-	-	-	●
[18]	2019	-	●	-	●	-	-	●	-	●	-	-	-	-	-	-	-	●	-	-	-
[60]	2019	-	●	-	-	-	●	●	-	●	-	-	-	-	-	-	-	-	-	●	-
[104]	2019	-	●	-	-	-	●	●	-	●	-	-	-	-	-	-	-	-	-	-	●
[64]	2020	●	-	●	●	●	-	●	-	●	-	-	-	-	-	-	-	●	-	-	-
[139]	2020	●	-	●	-	-	-	-	-	●	-	-	-	-	-	-	-	-	-	-	●
[17]	2020	●	-	-	●	-	-	●	-	●	-	-	-	-	-	-	-	-	-	●	-
[124]	2020	●	-	-	●	-	-	●	-	●	-	-	-	-	-	-	-	-	●	●	-
[129]	2020	●	-	-	●	-	-	-	-	●	-	-	-	-	-	-	-	-	-	●	-
[125]	2020	●	-	-	●	-	-	-	-	●	-	-	-	-	-	-	-	-	-	-	●
[3]	2020	●	-	-	●	-	-	-	-	●	-	-	-	-	-	-	-	-	-	●	-
[19]	2020	●	-	-	●	-	-	-	-	●	-	-	-	-	-	-	-	-	-	●	-
[107]	2020	●	-	-	-	-	●	●	-	●	-	-	-	-	-	-	-	-	●	●	-
[143]	2020	●	-	-	-	-	●	●	-	-	-	-	-	-	-	●	-	-	-	-	-
[52]	2020	●	-	-	-	-	●	●	-	-	-	-	-	-	-	-	-	●	-	-	-
[111]	2020	●	-	-	-	-	●	●	-	-	-	-	-	-	-	-	-	-	●	-	-
[103]	2020	●	-	-	-	-	●	-	●	-	-	-	-	-	-	-	●	-	-	-	-
[32]	2020	●	-	-	-	-	●	-	●	-	-	-	-	-	-	-	-	-	●	●	-
[134]	2020	●	-	-	-	-	●	-	●	-	-	-	-	-	-	●	-	-	-	-	-
[128]	2020	●	-	-	-	-	●	-	-	●	-	-	-	-	-	-	-	-	-	●	-
[22]	2020	●	-	-	-	-	●	-	-	-	-	-	-	-	●	-	–	-	-	●	-
[94]	2020	-	●	●	●	●	-	●	-	-	-	-	-	-	-	-	-	●	-	-	-
[14]	2020	-	●	●	●	●	-	-	●	-	-	-	-	-	-	-	●	-	-	-	-
[145]	2020	-	●	●	-	-	-	●	-	●	-	-	-	-	-	-	-	-	-	-	●
[50]	2020	-	●	●	-	-	-	-	●	-	-	●	-	-	-	-	●	●	-	-	-
[87]	2020	-	●	●	-	-	-	-	●	-	-	-	-	-	-	-	●	-	-	-	-
[102]	2020	-	●	●	-	-	-	-	●	-	-	-	-	-	-	●	●	-	-	-	-
[7]	2020	-	●	●	-	-	-	-	●	-	-	-	-	-	-	-	●	-	-	-	-
[65]	2020	-	●	-	-	-	●	●	-	-	-	-	-	-	-	-	-	●	-	-	-
[6]	2020	-	●	-	-	-	●	-	●	-	-	-	-	-	-	-	●	-	-	-	-
[55]	2021	●	-	●	●	-	-	●	-	-	-	-	-	-	-	-	-	-	●	●	-
[127]	2021	●	-	●	●	-	-	-	-	-	-	-	-	●	-	-	-	-	-	-	●
[75]	2021	●	-	●	-	-	-	●	-	●	-	-	-	-	-	-	-	-	-	-	●
[123]	2021	●	-	-	●	-	-	●	-	●	-	-	-	-	-	-	-	-	-	●	-
[81]	2021	●	-	-	●	-	-	●	-	-	-	-	-	-	-	-	-	●	-	-	-
[41]	2021	●	-	-	●	-	-	●	-	-	-	-	-	-	-	-	●	-	-	-	-
[1]	2021	●	-	-	●	-	-	-	-	●	-	-	-	-	-	-	-	-	-	●	-
[57]	2021	●	-	-	-	●	-	●	-	●	-	-	-	-	-	-	-	-	-	-	●
[11]	2021	●	-	-	-	-	●	●	-	●	-	-	-	-	-	-	-	-	-	●	-
[126]	2021	●	-	-	-	-	●	-	-	-	-	-	-	●	-	-	-	-	-	●	-
[74]	2021	●	-	-	-	-	●	-	-	-	-	-	-	-	●	-	-	●	-	-	-
[133]	2021	-	●	●	●	●	-	●	-	-	-	-	-	-	-	-	●	●	-	-	-
[2]	2021	-	●	●	●	●	-	-	●	-	-	-	-	-	-	-	●	●	-	-	-
[48]	2021	-	●	●	-	-	-	●	-	●	●	-	-	-	-	-	-	●	-	-	-
[49]	2021	-	●	●	-	-	-	●	-	-	-	-	-	-	-	-	-	●	-	-	-
[82]	2021	-	●	-	-	-	●	●	●	-	-	-	-	-	-	●	-	-	-	-	●
[66]	2021	-	●	-	-	-	●	●	-	-	-	-	-	-	-	-	-	●	-	-	-
[131]	2021	-	●	-	-	-	●	-	●	-	-	-	-	-	-	●	●	-	-	-	-

Implementation and Evaluation of a Point-Of-Sale Payment System Using Bitcoin Lightning

Michael Froehlich*
Center for Digital Technology and Management, Germany
froehlich@cdtm.de

Jose Adrian Vega Vermehren†
Center for Digital Technology and Management, Germany
vega@cdtm.de

Florian Alt
University of the Bundeswehr Munich, Germany
florian.alt@unibw.de

Albrecht Schmidt
Ludwig Maximilian University, Germany
albrecht.schmidt@ifi.lmu.de

ABSTRACT

Cryptocurrencies have the potential to improve financial inclusion. However, the technology is complex to understand and difficult to use. Human-Computer-Interaction (HCI) can play a vital role in improving accessibility by identifying and overcoming challenges that hold users back. However, most HCI studies have focused only on Bitcoin and Ethereum so far. Newer blockchains promise transaction speeds comparable to traditional payment systems, enabling the use of cryptocurrencies as a medium of exchange for everyday transactions. To explore the viability of cryptocurrency-based point-of-sale solutions through a human-centered lens, we used Bitcoin Lightning to implement a payment system and evaluated it in a mixed-methods study. Our results show that Bitcoin Lightning is a usable alternative to traditional solutions and that friction aggregates at the interface to existing payment systems, i.e. when purchasing Bitcoin. We discuss qualitative insights and derive implications for deploying cryptocurrencies as payment solutions.

CCS CONCEPTS

• **Human-centered computing** → **Human computer interaction (HCI)**; • **Applied computing** → **Digital cash**.

KEYWORDS

blockchain, cryptocurrency, bitcoin, bitcoin lightning, point-of-sale, pos, payment study

ACM Reference Format:
Michael Froehlich, Jose Adrian Vega Vermehren, Florian Alt, and Albrecht Schmidt. 2022. Implementation and Evaluation of a Point-Of-Sale Payment System Using Bitcoin Lightning. In *Nordic Human-Computer Interaction Conference (NordiCHI '22), October 8–12, 2022, Aarhus, Denmark*. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3546155.3546700

*Also with Ludwig Maximilian University, University of the Bundeswehr Munich.
†Also with Ludwig Maximilian University.

NordiCHI '22, October 8–12, 2022, Aarhus, Denmark

ACM ISBN 978-1-4503-9699-8/22/10…$15.00
https://doi.org/10.1145/3546155.3546700

1 INTRODUCTION

Cryptocurrencies have gained growing interest in the last years [11] and are increasingly pushing into the mainstream. Recent industry reports indicate that more than 300 million people own cryptocurrencies [9] and adoption rates are to continue as fast as early Internet user growth [8]. While previously often understood as investment opportunity [1, 16, 29], the introduction of Bitcoin as legal tender in El Salvador has paved the way for cryptocurrencies to be used as a medium of exchange [41]. Despite this growth cryptocurrencies are not without critique. The high energy-demand of proof-of-work blockchains has become a point of recent discussions [10, 18] and cryptocurrencies are still perceived as an opaque and technically complex topic that is connected to many misconceptions and confusion.

The Human-Computer-Interaction (HCI) community has recognized its responsibility in making the technology accessible to all users by helping to overcome technical obstacles that would otherwise exclude people with less technical experience from participating in the growing crypto-economy [3, 14, 15]. HCI researchers have set out to identify and address human-centered challenges connected to cryptocurrency and blockchain systems (e.g. [1, 14, 46]). While cryptocurrencies are shown to be hard to understand [28] and difficult to use [15, 45, 46], the existing research body also seems to lack behind current developments in industry [17]. To date, the majority of HCI research focuses on Bitcoin [31] and Ethereum [5], whose technical architectures are constrained by comparably slow transaction speeds or high transaction fees. For example, one block on the Bitcoin blockchain takes on average 10 minutes to be mined [31], making it rather impractical for point-of-sale use cases. Newer layer-1 blockchains, like Solana [48], or layer-2 solutions, like Bitcoin Lighting [34] or Polygon [33], promise to improve these technical limitations by providing transaction settlements at near real time speeds and low transaction costs. These new systems thus provide properties comparable to traditional payment networks, while at the same time offering the advantages of an open ecosystem for anyone to participate in and build on top of it.

However, they yet have to find their way into HCI research. To our knowledge, there are no studies available implementing these state-of-the-art cryptocurrency payment systems to evaluate them for point-of-sale use cases. This leaves a gap in understanding whether these systems deliver on their promises and are a viable alternative to established payment systems. With this work we close the gap: We implemented a point-of-sale system on top of the Bitcoin Lightning network and evaluated it in a mixed method

study during which N=31 participants conducted 202 payments using the system.

Our analysis shows that Bitcoin Lightning worked well as a payment settlement layer, and users perceived the usability of the system as satisfactory during use. We identified a stark contrast in the perceived ease-of-use between the setup and initial configuration of wallets and the continued use during the study. Using the system was perceived as relatively easy. However, during setup procedure, in particular purchasing Bitcoin and charging the Lightning wallet were points of struggle for many new users. These results hint at the importance of improving the initial user experience at the interface between existing payment systems and cryptocurrencies. We conclude with a discussion of adoption consideration for using and Bitcoin Lightning as settlement layer for point-of-sale cryptocurrency systems.

Contribution Statement: This paper makes two main contributions: We present (1) a reference implementation for a point-of-sale system integrating Bitcoin Lightning as settlement layer, and (2) contribute an empirical evaluation of the system through a user-centered lens. Based on these results we discuss current limitations and implications for cryptocurrency-based payment systems.

2 BACKGROUND & RELATED WORK

Bitcoin was introduced in 2008 as "*peer-to-peer electronic cash*" [31]. While it has exhibited remarkable growth over the past decade, its adoption was driven primarily by its use as an investment and store of value, not as a means of transaction. While users would like to use it as a form of payment [15], merchants accepting cryptocurrency have remained scarce.

2.1 Cryptocurrency in HCI

In recent years, the Human-Computer-Interaction community has taken interest in understanding how users perceive and use cryptocurrencies. Scholars explored the motivation and perceptions of users [15, 26] and non-users [19, 44] alike to understand how cryptocurrencies are being used. Froehlich et al. report that while users are motivated by financial interests, they would also like to use it for purchases but lack opportunities to do so [16]. Additionally, usability issues [1, 15, 45, 46] seem to hold back the adoption of cryptocurrencies: Across studies they are described to be complicated to understand and get started with [3, 15], subject to misconceptions [28], slow in transaction speed [15, 22, 38], and expensive in fees [46]. Many of the issues highlighted by existing research – particularly slow transactions and high transaction fees – have been addressed by more recent projects, such as Solana [48], Polygon [33], or Bitcoin Lightning [34] at a technical level. These improvements offer an opportunity to revisit the question of whether cryptocurrencies can become a viable alternative to existing payment systems. Especially, the recent introduction of Bitcoin as legal tender in El Salvador [41] shows the relevance of the subject and draws open questions for the adoption of cryptocurrencies for everyday payments. While HCI literature indicates the usability of Bitcoin is worse than those of credit cards [3], adoption in El Salvador appears to progress nonetheless. Unfortunately, verified reports from El Salvador are sparse and little is known about the real usability of systems built on Bitcoin Lightning.

While an emerging body of research reports on the usability of cryptocurrencies and cryptocurrency wallets brings forward valuable insights [1–3, 14–16, 20, 22–25, 30, 36, 46], these studies are not without limitations. Existing studies investigating the usability of purchasing goods with Bitcoin [3, 15] are limited to a laboratory context. For example, Alshamsi and Andras compare the usability of Bitcoin with the usability of credit cards in an between-subject setup with 22 cryptocurrency beginners and 33 credit card users [3]. Froehlich et al. explore the challenges of first-time cryptocurrencies users in-depth while making a purchase in an online shop with Bitcoin [15]. In either case, the short observation period provides little insight in whether cryptocurrencies would be viable for everyday payments as repeated interaction with any system may get easier as users become familiar with it over time.

We identified two projects concerning the use of cryptocurrency for point-of-sale use cases – interestingly enough, both pertaining to coffee. Eskandari et al. deployed an early version of a Bitcoin sales terminal in a coffee shop in 2014 [12] and Tallyn et al. explored notions of machine autonomy with a Bitcoin-enabled coffee machine in an office context [35, 42]. While Eskandari et al.'s work takes a software engineering perspective and presents the requirement engineering process as well as lessons learned, they do not report on users' perceptions of the systems. They define usability (user-friendly, time-efficient, fair exchange rates, availability), deployability (low cost to run, enabling branching), and privacy (no information leakage, maintaining payee's privacy, maintaining payer's privacy, confidential payment lists) as core requirements. To avoid the average block time of 10 minutes, their system accepts 0-confirmation transactions instead of waiting until the transaction is included in the blockchain. While this allows to facilitate point-of-sale transactions with Bitcoin without waiting, it effectively makes the system susceptible to attacks through double-spending [13]. Tallyn et al.'s work, on the other hand, is interesting as it goes into depth, exploring machine autonomy during a 1-month field study in office environments. The focus of their work, however, lies less on using Bitcoin as payment infrastructure, but on the influence of machine autonomy on everyday activities in shared community spaces. From a technical view, they do not specify how they address the slow transaction times of the Bitcoin blockchain [35, 42].

2.2 Bitcoin Lightning

Bitcoin Lightning [34] is a payment protocol built on top of the Bitcoin network that settles transactions through a network of bi-directional payment channels. This offers several advantages over Bitcoin without compromising security the same way accepting 0-confirmation transaction would: near instant transaction speed, low transaction costs, and a significantly higher throughput [34]. It is particularly interesting in the context of point-of-sale payment systems as it provides an infrastructure layer that fulfills the core requirements. To our knowledge, there is no research in the HCI field exploring the use of Bitcoin Lightning.

From a technical perspective[1] Bitcoin Lightning can be described as a payment channel network built on top Bitcoin [47]. This architecture, in essence, allows participating nodes to carry out any number of transaction off-chain. Only the initial transaction to create a payment channel and the final transaction to close it are written to the blockchain [34].

The simplest element of the Lightning network is a payment channel between two Lightning nodes. Any two nodes can open a channel by committing an initial amount of Bitcoin to the channel. The initial creation of the channel is stored on the Bitcoin blockchain in the form of a special multi-signature transaction. By doing so, both parties can now send each other transactions by updating their balances and committing new transactions. Newer transactions invalidate previous ones. If the channel is closed – either bilaterally or unilaterally – the latest transaction is written back to the blockchain and reimburses the final balances to the respective owners [34, 47]. To make a payment between any two nodes in the network, it must be routed through a series of payment channels. For this, the Lightning network broadcasts all known channels between nodes. In contrast to Bitcoin, transactions cannot be sent directly to the receiving node. Instead, the receiver first needs to generate an invoice, which is valid for only a limited amount of time. The sender then determines a valid route through the network and a chain of payments is created. The sent transaction is secured by a cryptographic secret contained in the invoice. Only once the transaction reaches its final destination, can the participating channels finalize their channel transactions and redeem their funds [34, 47].

Bitcoin Lightning's design goals emphasize fast transactions at low cost. In practice, however, the network's typology plays a significant role on whether these promises can be met. With the Lightning network launching into Beta in 2018 and growing increasingly fast since then [21], first empirical research is emerging: Based on a longitudinal measurement study, Zabka et al. find that channel endpoints rarely cheat and behave fair. At the same time, the majority of channels in the Lightning network appears to be inactive [49]. Waugh et al. attempted to investigate the network's availability and reliability to route transactions in practice. In late 2019 they conducted a series of payments to different nodes within the network using amounts equivalent to USD 0.01 to USD 100. They report that while routes to almost all nodes can be constructed, routing payments in practice "*fail much too often, in particular when sending larger payments in excess of USD 50*" [47].

2.3 Summary

In the context of this paper, we build on several learnings from previous work. There is an emerging body of HCI research surrounding cryptocurrencies. However, there are only few studies exploring its use as a payment system. Those studies have focused only on Bitcoin so far. Over the past years cryptocurrency projects improving over the original design of Bitcoin have started to reach maturity, promising to solve many of the challenges described in literature (i.e. high fees, slow transactions). Bitcoin Lightning is one such protocol aimed at enabling low-cost and near instant transactions through an off-chain payment channel network. On paper, this makes Bitcoin Lightning an ideal payment layer for everyday point-of-sale transactions. However, we lack empirical evidence in how far these promises can be met in practice. The goal of this paper is to fill this gap by building a functional point-of-sale system with Bitcoin Lightning and evaluating it in a real-world context.

3 IMPLEMENTATION: PAYMENT SYSTEM

In this section we present design considerations, the architectural approach, and the implemented point-of-sale system.

3.1 Design Rationale

Our overarching rationale for building the system was to understand in how far Bitcoin Lighting is a viable option to be used as underlying payment layer for everyday point-of-sale transactions. The system described in the following could be equally realized by integrating existing proprietary payment providers such as PayPal[2] or Stripe[3]. The unique advantage cryptocurrency-based systems may offer in the future is their open ecosystem: Open systems that allow equal participation of people without restriction are beneficial to closed proprietary systems as they enable competition and innovation. Therefore, our goal in implementing a payment system with Bitcoin Lightning is not to directly compare it with existing more mature alternatives. Instead, we want to explore whether core properties of Bitcoin Lightning offer an acceptable experience to users when deployed as a functional point-of-sale system. With this objective in mind, we prioritized the use of state-of-the-art services and libraries during the implementation. The developed system should thus reflect a realistic deployment merchants can hope to achieve with service providers available at the moment.

3.2 Actors & Use Cases

Payment systems are typically used by two actors facilitating a transaction to exchange goods. Our system includes two actors: The CUSTOMER is interested in making a purchase. The MERCHANT interested in selling goods. We distinguish three use cases for how Bitcoin Lightning may be used during a checkout process: (1) in an online environment, (2) during a checkout process in a traditional brick-and-mortar store, and (3) during a self-service checkout process, such as vending machines. Table 1 details the different use cases and their flow of events.

3.3 Requirements

From the described use cases, we derive several functional and non-functional requirements. These requirements describe the envisioned behavior of the system, independent of its actual implementation [4].

3.3.1 Functional Requirements. We identify several functional requirements describing the system regarding the interactions with its surrounding environment, including the user [4].

[1] For an in-depth description of the technical architecture and the cryptographic mechanisms of the Lightning network, please refer to the original whitepaper by Poon and Dryja [34] and consult the resources on https://lightning.network/ (last-accessed: 2022-04-21).

[2] https://paypal.com/ (last-accessed: 2022-04-05)

[3] https://stripe.com/ (last-accessed: 2022-04-21)

Table 1: Use cases for Bitcoin Lightning for different types of checkout experiences.

Online Checkout	Offline Checkout	Offline Self-Service Checkout
Customer	Customer, Merchant	Customer
1. The customer opens the website of an online shop and adds one or several products to the basket.	1. The customer selects one or several products in the shop and brings them to the checkout counter.	1. The customer scans a QR code with their smartphone to open the website and adds one or several products to the basket.
2. The customer starts the checkout procedure, enters their shipping address, and selects Bitcoin Lightning as method of payment.	2. The merchant registers each product and, once completed, uses the wallet that is integrated in the shop system to generate a Lightning invoice.	2. The customer reviews the products in the basket, confirms the selection, and is presented with a Bitcoin Lightning invoice encoded in a URL.
3. The customer is presented with a Bitcoin Lightning invoice on the website and uses their mobile wallet to scan the QR code of the invoice.	3. The customer reviews whether the products were accounted for correctly, opens their wallet, scans the QR code of the invoice, and confirms the transaction.	3. The customer clicks on the URL to open their wallet or copies the invoice manually and then opens the wallet. After reviewing the transaction, they confirm it.
4. The customer confirms the transaction in the wallet. After a few seconds, the wallet and website show a confirmation.	4. After a few seconds, the customer and the merchant receive a confirmation of the transaction in their respective wallets.	4. After waiting a few seconds, the customer is presented a confirmation of the success of the transaction in their wallet.
5. The website redirects to a new page showing an order confirmation.	5. The customer takes their purchase and leaves.	5. The customer takes their purchase and leaves.

Notes. The entry condition for all three use cases is that both customer and merchant have a configured Bitcoin Lightning wallet with sufficient funds.

- **FR1: Inventory Management**. The system should provide a way for the merchant to add, remove, and keep track of their inventory of products.
- **FR2: Order Management**. The system should provide a way for the merchant to keep track of the orders made by customers and which status the orders are in.
- **FR3: Analytics and Reporting**. The system should provide the merchant with a way to analyze past sales.
- **FR4: Storefront Interface**. The system should provide an interface for customers to interact with / select products.
- **FR5: Transaction Processing**. The system should provide a way for merchants to issue Bitcoin Lightning invoices, to process incoming transactions, and associate them with orders.
- **FR6: Bookkeeping**. The system should provide a way to keep track of transactions for bookkeeping.
- **FR7: Wallet and Key Management**. The system should provide a way for the merchant to manage their wallet and their private keys.
- **FR8: Currency Conversion**. The system should provide the merchant with a way to convert cryptocurrency into fiat currency.
- **FR9: Payout**. The system should provide the merchant with a way to pay out their revenue to the traditional finance system, such as bank accounts.
- **FR10: Mobile Wallet**. The system should provide the customer with a way to pay with Bitcoin Lightning.

3.3.2 Non-Functional Requirements. We additionally identify non-functional requirements that further "*describe aspects of the system that are not directly related to the functional behavior of the system*" [4] and contribute to the quality perceived by the user [7].

- **NFR 1: Security**. The systems should provide adequate security measures to both the merchant and the customer. Private keys should be stored encrypted. The system should provide ways to back up or recover keys.
- **NFR 2: Privacy**. The system should maintain the privacy of both the merchant and the customer. Transactions should not be visible to anyone who is not involved in them.
- **NFR 3: Usability**. The system should provide a usability comparable to existing point-of-sale system. Two aspects crucial to achieve this are affordable fees and near-instant transaction speeds. Additionally, the interaction flow during payment should be simple and quick to complete.
- **NFR 4: Availability**. The system should be able to process transactions without any major interruptions.

3.4 System Overview

Based on the functional requirements and the overall use cases, we decompose the system into four major subsystems with clearly defined responsibilities and interfaces: the shop system, the payment processor, the customer's mobile cryptocurrency wallet, and Bitcoin Lightning as settlement layer. Figure 1 provides a high-level overview of the subsystems and their interaction.

Shop System: The shop system bundles all functionality related to the management of products and the interaction between merchant and customer (FR1 - FR4). Merchants keep track of their inventory, manage outstanding orders, and review their order history. To customers, it provides a storefront to select products and initiate the checkout process.

Payment Processor: The payment processor bundles all functionality related to the processing and management of transactions (NFR5 - NFR9). It provides an interface to the shop system to initiate the payment process for an order, return the status of the respective transaction, and keeps a ledger of past transactions. Specific to Bitcoin Lightning, it provides an abstraction layer to deal with key management (NFR1) and the interaction with the Bitcoin Lightning network, such as the generation of invoices for specific orders. Additionally, it provides services for conversion of cryptocurrency to fiat currency and to transfer available funds to traditional bank accounts.

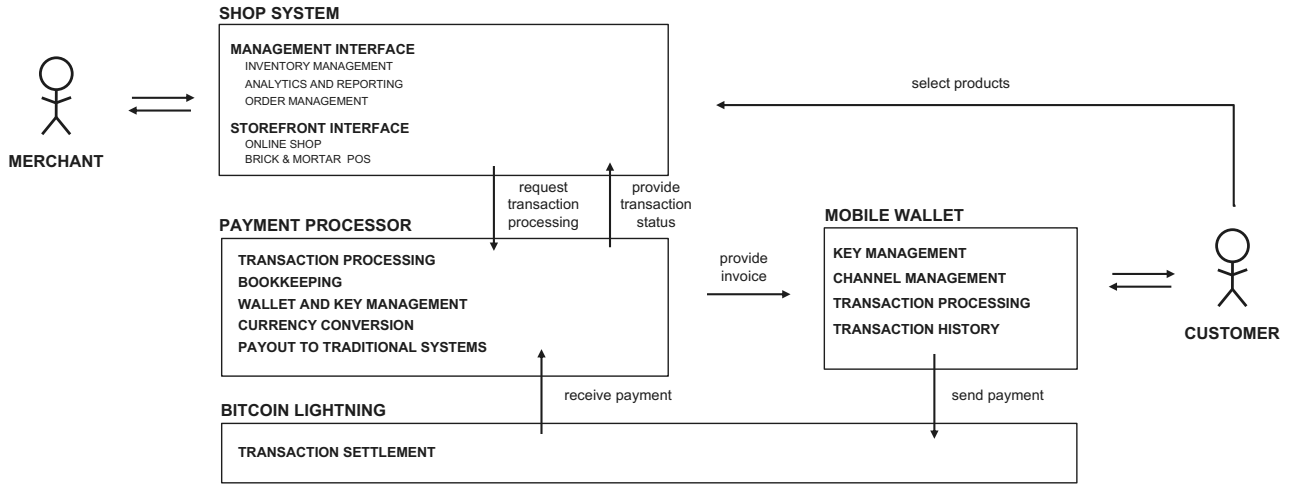


Figure 1: An overview of the subsystems.

Mobile Wallet: The mobile wallet (FR10) provides the customer with the necessary functionality to manage their Bitcoin Lightning funds and make payments with them. This includes the creation of the Bitcoin Lightning wallet as well as tasks concerning key management (NFR1), channel management, transaction processing, and a history of past transactions. The customer uses their wallet to open Bitcoin Lightning invoices – i.e. by clicking on a URL or scanning a QR code – and confirming and settling them via the Bitcoin Lightning network.

Bitcoin Lightning: The Bitcoin Lightning network provides the agnostic payment layer through which transactions are routed and settled (see section 2.2). By design it provides privacy (NFR2) for the involved parties as payments are settled off-chain.

An advantage of the described architecture is that the decomposition into separate subsystems leads to high cohesion within the subsystems and low coupling between them. For example, the PAYMENT PROCESSOR provides an abstraction over the actual type of payment used to settle a transaction. This means that alternative payments beyond Bitcoin Lightning could be integrated without affecting the SHOP SYSTEM. Merchants could also decide to switch their SHOP SYSTEM while keeping their PAYMENT PROCESSOR, not affecting the transaction history and bookkeeping. The interface between the PAYMENT PROCESSOR and the customer's WALLET is provided as a standardized Bitcoin Lightning invoice. This gives customers free choice which actual wallet to use instead of being locked in to the proprietary solutions of centralized payment processors. Thus, users have the option to choose the right wallet for them, with differing degrees of self-managed to custodial options available on the market[4].

3.5 Implementation: Self-Service Checkout

We realized the described system with an **Offline Self-Service Checkout** use case (see Table 1) in mind while keeping our implementation open for future extensions. As described in our design rational, we wanted to keep the implementation close to a real-world deployment merchants can achieve with service providers available today.

Shop System: Targeting a self-service checkout use case in an offline environment, we simplified the shop system to its minimum. We printed QR codes encoding URLs redirecting to check out websites of the respective products. This approach is comparable to using QR codes to PayPal accounts to collect payments. While simple, this system fulfills the needed requirements to evaluate the overall system.

Payment Processor: We integrated Opennode[5] as Bitcoin Lightning payment processor. Opennode is one of the leading services for processing payments with Bitcoin and Bitcoin Lightning. It met the requirements we needed for the payment processing subsystem, allowed for quick integration, and future extensibility of the system as it offers a rich set of API endpoints as well as integrations to established shop systems such as Shopify[6]. Our design choice to select a payment processing service instead of running our own Bitcoin Lightning node has several reasons: First, considering our design rationale it is not realistic to assume that most merchants have the required technical knowledge or resources to deploy, manage, and integrate a full Bitcoin Lightning node on their own. The more likely scenario is that they would look for services that provide the needed functionality and plug into their shop system without much extra effort. Second, using a professional payment processing service has advantages considering the network architecture of Bitcoin Lightning. Their nodes are likely to be better connected within the

[4]The following blog article provides an overview of different architectures of contemporary Bitcoin Lightning wallets for the interested reader: https://www.veriphi.io/en/blog/lightning-wallet-architecture (last-accessed: 2022-04-21)

[5]https://www.opennode.com/ (last-accessed: 2022-04-21)
[6]https://www.shopify.com/ (last-accessed: 2022-04-21)

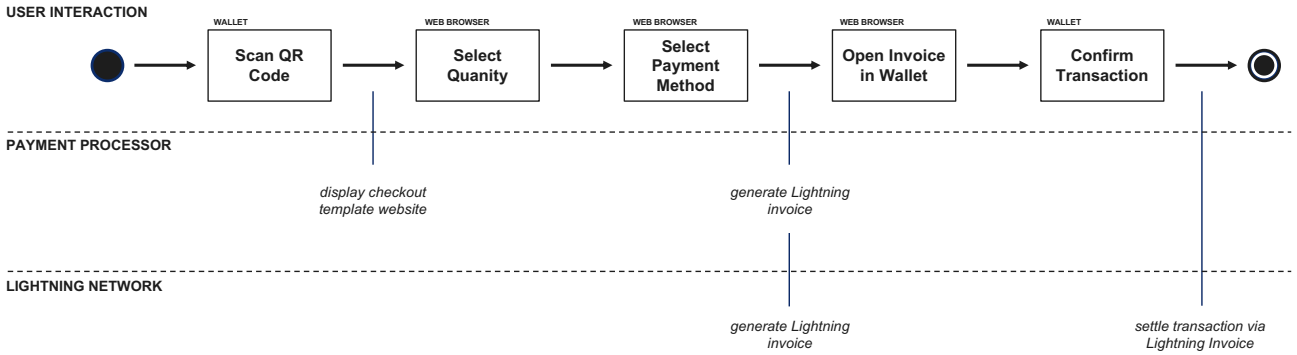


Figure 2: Interaction flow for making a purchase using the implemented payment system for the self-service checkout flow.

payment channel network and thus, we expect that transactions can be routed more reliably and more quickly.

Figure 3: Interface of the mobile Bitcoin Lightning wallet (based on bluewallet.io).

Mobile Wallet: To be able to holistically explore how users would interact with the system, we also deployed a mobile wallet. After evaluation of different open source projects, we created a fork of the popular Bitcoin Lightning wallet BlueWallet[7], and modified it to be able to collect usage logs. We were careful not to change the app interface to provide a realistic baseline of the experience users can expect today when using Bitcoin Lightning. Figure 3 provides an annotated overview of the mobile wallet interface. The modified app provided users with a non-custodial Bitcoin wallet and a custodial Bitcoin Lightning wallet. Following a similar reasoning as for choosing to use a payment processor, a custodial wallet provider is likely better connected within the Bitcoin Lightning network. Thus, it provides less risk of transactions not being able to be routed to their destination.

[7]https://bluewallet.io/ (last-accessed: 2022-04-21)

3.6 Interaction Flow

Following the defined non-functional requirements, our aim was to create a simple and quick checkout process. Figure 2 provides an overview of the interaction flow between a CUSTOMER and the system during the checkout process. Figure 4 provides screenshots of the implemented user interfaces during the checkout process. The entire process takes five steps: The entry-point to the self-service payment is provided as a QR code linking directly to the checkout website, presenting the product. After (1) scanning the QR code, the customer (2) selects the desired quantity of the product, (3) selects the desired payment method (Bitcoin or Bitcoin Lightning), and then (4) opens the invoice in their wallet where they (5) confirm the transaction. As a consequence of the decoupled subsystem design, step 2 to 4 are completed in a web browser and only the final step is completed in the wallet of the customer. As the user walks through this checkout process, the Bitcoin Lightning invoice is generated dynamically through the PAYMENT PROCESSOR and the Bitcoin Lightning Network. The process is completed, once the transaction is settled through the Bitcoin Lightning network. One caveat, evident from the process is the need to generate the invoice dynamically. It can be generated only after the customer selected the required quantity of the product. It is not possible to provide a permanent invoice that can be reused.

4 EVALUATION

To evaluate the system, we conducted a two week-long mixed-method study in March 2022. Prior to the start, we obtained approval from the ethics board of our university (ID: EK-MIS-2020-018). 31 people participated in the study. Participants first completed a setup study comprising the initial setup of their wallets and first usage of the system, comparable to laboratory studies used in previous studies (e.g. [3, 15]). Once the system was set up, they used it over the course of two weeks to purchase drinks and coffee in an office environment. The overall goal of the evaluation was to understand whether the developed system met the requirements to be used as point-of-sales systems.

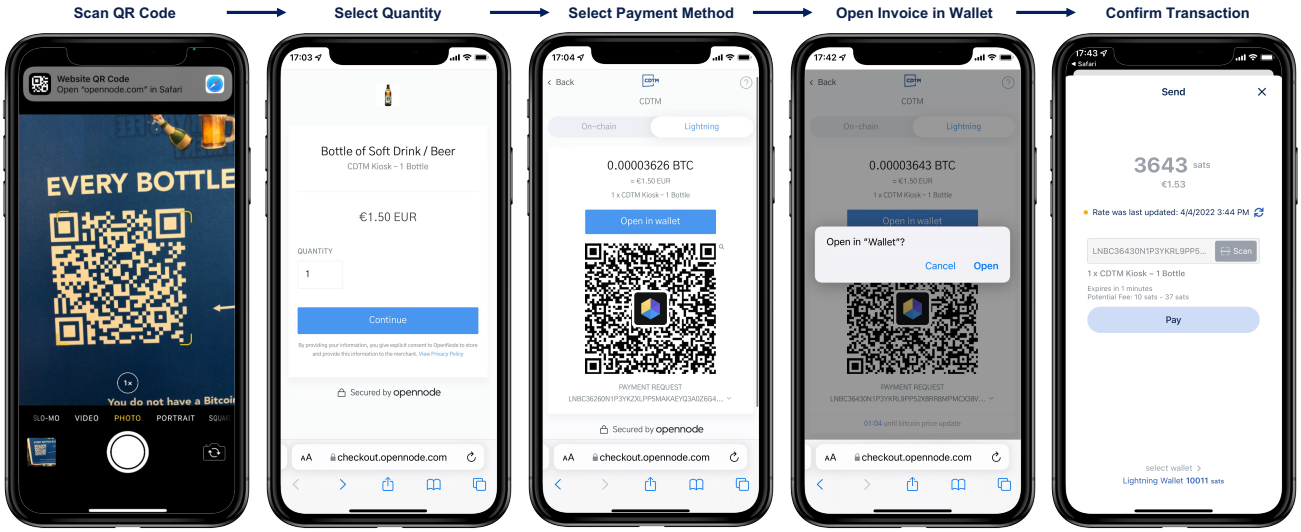


Figure 4: User interfaces for the realized interaction flow for purchasing one product for the self-service checkout.

4.1 Participants & Context

We conducted the study at a research and educational institute associated with a German university. We recruited participants from the staff and a cohort of students in the associated program. Unlike in a traditional university setting, all participants worked full time (Monday - Friday) and in presence at the institute, resembling the context one would find in typical offices spaces. We recruited in total 31 participants. The participants' educational background varied from undergraduate to postgraduate degrees in computer science and engineering (15), business administration (11) and other study backgrounds (5). Participants were between 20 and 34 (mean of 24.55) years old. 61.3% were male and 38.7% female.

4.2 Data Collection

We combined several methods to obtain a rich understanding during the evaluation. Figure 5 provides an overview of the study procedure and the collected data.

4.2.1 Methods. Throughout the study, we collected data from various sources and combined several methods to do so. During the setup study, we used an adopted think-aloud protocol. Participants were assigned in groups and recorded one another while completing the tasks and sharing their thoughts aloud. After each task we collected data with questionnaires including open and closed questions. At the end of each week, we collected additional data with questionnaires including open and closed questions. We complemented the structured data collection with ethnographic methods. We occasionally observed participants as they were using the system and inquired about their experiences. Finally, we collected usage logs from the mobile wallet and the payment processor.

4.2.2 Apparatus. Our apparatus comprised the implemented system described in section 3.5, an instruction guide for the tasks during the setup study, and several questionnaires. Table 2 provides an overview of the different measures collected with questionnaires. We collected demographic data (age, gender, educational background). We used the Single-Ease-Questionnaire (SEQ) [40] as a quantifiable measure to proxy the perceived usability of the system. Users were asked to rate on a scale from 1 (very easy) to 7 (very difficult) how they perceived the respective task (during the setup study) or using the system over the past week (in the weekly questionnaire) – i.e., "*How difficult or easy did you find using Bitcoin Lightning as payment system?*". As recommended [39], we followed with an open question asking participants "*What made you choose this number?*" to elicit qualitative insight. Similarly, we used one item out of the User Experience Questionnaire (UEQ) [27] to measure the perceived speed of the system by asking users to rate it on a scale from 1 (fast) to 7 (slow). Additionally, we collected task completion rates, the number of times participants used the

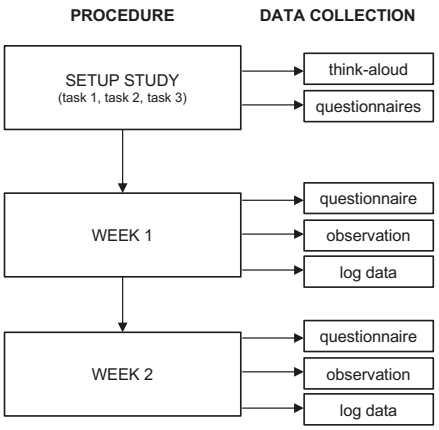


Figure 5: Overview of the study procedure and the collected data.

system over the past week, and queried for encountered problems, positive moments, and suggestions for improvement with open questions.

Table 2: Overview of the data collected with questionnaires.

		T1	T2	T3	W
demographics	multiple			•	
task completion	y/n	•	•	•	
SEQ	scale (1-7), text	•	•	•	•
fast vs slow	scale (1-7)			•	•
no. times used	number			•	•
open questions	text			•	•

4.2.3 Procedure. Our evaluation is comprised out of two phases: The initial setup study and the subsequent usage of the system over the course of two weeks. During the setup study, participants had to complete three tasks: (T1) create a bitcoin wallet and buy bitcoin, (T2) create a bitcoin lightning wallet and transfer bitcoin onto it, and (T3) make a first purchase with the wallet. Participants formed groups of two, recording each other with smartphone cameras while following a think-aloud protocol. After completion of each task, participants individually filled the respective task questionnaire. We chose these tasks because they represent the first steps users would need to take to use Bitcoin Lightning as a means of payment. After completion of all three tasks, we distributed EUR 40 in Bitcoin to the participants as compensation for participating in the study.

Over the course of the next two weeks, participants were free to purchase coffee (EUR 0.5) and an assortment of beverages (EUR 1.5) with the deployed system. At the end of each week, a questionnaire was distributed to participants to inquire about their experience.

5 RESULTS

We collected in total 116 qualitative statements, including 236 relevant coded statements. Complemented by quantitative measurements, we present the results of the evaluation of the system. Table 3 provides an overview of the quantitative metrics describing the usage behavior and the perception of the system.

Our point-of-sale system offered participants the opportunity to purchase beverages and coffee using Bitcoin Lightning as a payment method. In total 896 app sessions and 202 payments were conducted by participants over the course of the study. The majority of app session happened within the first week, whereas the majority of transactions happened in the second week. The difference in app sessions can be explained by the additional interaction needed during the setup procedure. On average, each participant made 3.0 purchases during the first week and 4.21 purchases in the second week (min=0, max=10 for both weeks).

5.1 Ease of Use

We observed a stark contrast in the perceived ease-of-use during the setup study and the subsequent use. In particular, the purchase of Bitcoin (T1) and transfer to their Bitcoin Lightning wallet (T2) was perceived as cumbersome and frustrating by many participants. In part, this is reflected in the task completion rates (c.f. T1, T2, T3) and the difference in SEQ scores (c.f. T1, T2 vs T3, W1, W2).

Table 3: Overview of the collected quantitative metrics during the evaluation.

		T1	T2	T3	W1	W2
task completion	quest.	57%	91%	95%	–	–
SEQ	quest.	3.00	3.10	2.30	2.35	2.42
fast vs slow	quest.	–	–	3.95	3.74	3.88
mean times used	quest.	–	–	–	3.00	4.21
total transactions	logs	–	–	–	86	116
total app sessions	logs	–	–	–	706	190
mean session time	logs	–	–	–	59s	34s

Notes. The high number of app sessions in W1 can be attributed to the initial setup procedure. Testing with ANOVA, the difference in SEQ scores between T1, T2, T3, W1, W2 are not statistically significant ($F(4, 110) = 1.495$, $p = 0.209$). Likewise, the difference in fast-slow scores between T3, W1, W2 are not statistically significant ($F(2, 64) = 0.082$, $p = 0.921$).

43% of participants could not complete the first task, purchasing the equivalent of EUR 40 in Bitcoin [8]. In the majority of cases, the cause was related to payments for the purchase of Bitcoin being declined by the banks or credit card issuers of the participants or issues during the Know-Your-Customer (KYC) id verification. One participant described their experience, "*The onboarding went well and was easy, until the transaction got blocked by the bank. After unblocking the credit card, we retried the transaction and the card got blocked again*". It was surprising to see that this was not an isolated issue, but affected multiple participants across several German banks. Another participant stated, "*For me, it did not work with BANK1 and BANK2 credit cards. Although the id verification process was successful, the transaction did not work. I tried it several times with no success.*" (bank names redacted). For other participants, purchasing Bitcoin was halted by the KYC process. For example, "*when trying to purchase Bitcoin, I was supposed to receive an email to confirm my identity within 60 seconds. Even several hours later, it has not arrived.*". While many participants had issues during the process and found it tedious, there were also some for whom it worked well, e.g. "*The money transfer was easily done by Apple Pay.*" or "*I have transferred coins from another wallet, so the process was very easy.*".

Looking at the ease-of-use after the setup, there was a notable decrease in perceived difficulty once participants had a set-up Bitcoin Lightning wallet. SEQ scores decreased from 3.00 and 3.10 (T1, T2) to 2.30, 2.35, and 2.42 (T3, W1, W2). The collected qualitative data and our observations back up the SEQ measures: Participants found it overall easier to use the system for payments than to initially configure and fill their wallets. For example, participants stated, "*Having the transaction go through for the first time was quite fun, especially after the boring and time-intensive setup.*", or "*After the first successful payment, it is pretty straightforward.*", or "*Once everything is set up, the payment itself is very simple and fast.*".

In addition, the collected data contained comments related to different aspects of the user experience that are not directly related

[8] If participants were not able to finish task 1 (e.g., because their credit cards were declined) we sent them the compensation for participating in Bitcoin after task 1, so they could continue the study.

to Bitcoin Lightning. Examples include the load performance of the app, the structure of the user interface, or the interaction flow during the checkout process. For example, we received comments complementing the user interface and others criticizing it to be "*not very intuitive*". While most of the reported issues in this category can be addressed by iteratively improving the system in line with design guidelines and software engineering best practices, one criticized aspect cannot without implementing an entirely different payment layer: Several participants argued that the checkout process is too complicated, involving too many redirects, and they would rather "*scan the QR code directly in the wallet and pay*". The underlying architecture of the Bitcoin Lightning network requires invoices to have an expiry date. Thus, they can only be generated dynamically once the final payment amount in known, making a static invoice for now infeasible.

5.2 Perceived Transaction Speed

We measured the perceived speed of the system by surveying participants in the questionnaires after the setup study, after week one, and after week two (1=fast, 7=slow). The mean ratings provided by participants revolved around the center of the scale, slightly tipping to the 'fast' side (T3=3.95, W1=3.74, W2=3.88). Based on the recorded usage logs, we can further see that app sessions on average took 53.86 seconds. The average session length decreased from 59.29 seconds in week one to 33.67 seconds in week two. Looking at the second week in particular, we can see that the app was used in 61% of cases to make payments: 190 app sessions resulted in 116 transactions. Our observations as well as participants comments in the weekly survey are in line with these measurements, indicating that the overall checkout process takes around 30 to 60 seconds beginning to end. With regards to whether this speed was acceptable to participants, we received both supportive and opposing comments. On the positive side, participants stated, "*It is quick and easy.*", "*It only took like 30s!*", and "*The transaction went through really quick!*". Others perceived this as too slow: "*It should be faster!*", "*It is a bit annoying that it always takes around 10 seconds for the payment to go through.*", or "*Sometimes there's a lag in the transaction, and it takes a little longer than I'd like for the payment to complete*".

One additional aspect captured during our contextual observations was a notable increase in transaction speed during the second half of week two. One participant reported, "*The app seems to work quicker, or maybe this is only a feeling after getting used to it.*". We observed that during the first week, transactions would take between 10-20 seconds to complete after an invoice was scanned and confirmed in the wallet of a user. This suddenly changed during the second week, at which point transactions across all users would take only around 4-6 seconds. This change was particularly noticeable as the user interface of the deployed mobile wallet would previously time out after about 20 seconds and ask users to check back later. After that point, the wallet provided a confirmation of the transaction's success and automatically closed the screen. This change did not go unnoticed: One participant remarked, "*Lightning transactions are now completed within seconds and a confirmation of the transaction is shown.*", and another one, "*Transactions worked smoothly, the payment process got faster.*".

5.3 Transaction Fees

Another relevant aspect for deploying point-of-sales systems affecting users' adoption are transaction fees. Overall, two types of fees were charged during the study in the current implementation: First, the payment channels involved in forwarding a transaction in the Bitcoin Lightning network can announce fees. Every channel can announce fees with a fixed component and a variable component. Consequently, the calculation of the exact network fee for a specific transaction depends on the amount transferred and the channels through which it is routed. In addition, the implemented payment processor, Opennode, charged a 1% fee for every incoming transaction. This 1% fee, however, is not visible on the customer's side, as it is deducted from the incoming payment the merchant receives. Thus, as with other cryptocurrencies, only transaction fees relating to the network have to be paid by the sender, i.e. the customer.

In line with these expectations, we observed that the full cost for transactions were slightly higher than the charged price (in EUR) due to the network fees. Typically, the price would be 1-2 cents over the purchase price, meaning 1.51 or 1.52 EUR for a drink sold at 1.5 EUR, and 0.51 or 0.52 for a drink sold at 0.5 EUR at the time of sale. Participants did not specifically complain about the size of the fee charged for transactions. However, they identified the need to pay fees as a clear disadvantage over alternative solutions. For example, one person described the fees as simply "*unpleasant*" and another one stated, "*One thing I don't like is the transaction fee, which wouldn't occur if we would simply use Paypal.*".

Bitcoin price volatility was another aspect that surfaced in our dataset. Depending on the Bitcoin-EUR exchange rate at a specific time, a different amount of Bitcoin would be charged to equal the fixed product prices in EUR. Looking at the recorded transaction data, there was a 15 point difference between the lowest (90.6%) and highest price paid for a transaction (105.6%) when compared to the mean (100%). Some participants expressed that they experienced this volatility negatively. For example, one participant said when asked whether they could imagine using Bitcoin Lightning in the future, "*The Bitcoin price would have to be more stable, I want my coffee to be the same price every day.*".

The user interface in the wallet allowed participants to view their available funds and past transactions in either Bitcoin, Satoshi[9], or Euro. If set to Euro, past transaction values were shown based on the current exchange rate, e.g. at EUR 1.52, 1.58, or 1.36, not the exchange rate at the time of purchase. From a users' perspective, it was thus not really possible to distinguish easily between the paid price and the associated transactions fees. This further irritated participants. One explained, "*It is irritating that the value of the payment in the past is changing as well. I would rather like to have a fixed amount of money, as this reduces risk for me as a user and additional stress of not knowing how much I can buy in the future.*".

5.4 Reliability

Over the entire course of the study, we observed that transactions could be successfully routed most of the time. We asked all participants to report any error messages they would receive throughout using the app when making payments. We received only one report

[9]One satoshi refers to the smallest denomination of bitcoin, equivalent to 100 millionth of a bitcoin

of a transaction failing connected to issues with the Bitcoin Lightning network, due to an (apparent) "*lack of inbound capacity of the receiver along the payment channel route*". However, by scanning the invoice again, the participant could almost immediately send their payment at the second try. However, throughout the setup study, we observed that for many participants the mobile wallet would return API Errors. These errors were not caused by the Bitcoin Lightning network, but the API of the custodial Bitcoin Lightning wallet on the user's side. If that happened for a user, their wallet would not be able to send Bitcoin Lightning transactions for around 15 minutes. One participant explained, "*I was confused by an API error that didn't allow me to transfer from bitcoin to lightning. But after some time it worked fine.*". These errors were in effect due to exceeded rate limits against the custodial wallet API, and largely subsided within the first week.

6 DISCUSSION

In this paper, we present the implementation of a point-of-sales system built on Bitcoin Lightning and its evaluation in a mixed-methods field study. Our evaluation shows that it worked reliably throughout the study, and users had no major problems using the system for payments once they had a configured wallet. However, it also showed that the initial process of setting up the wallet and getting started is difficult for many users. This discussion aims to reflect on these results and highlight implications for future research and practice.

6.1 System Performance

Considering the overall results collected during our evaluation, we find that the system provided an acceptable experience. Throughout the observed period, transactions were reliably settled over the Lightning network. While the transaction speed was slow-moving at the beginning of the study, its increase in the second half of week two points to the advantage of utilizing central nodes within the network to improve performance. Most users deemed the transaction fees of 1-2 cents acceptable, as only few participants complained about them. This said, all of these aspects – perceived usability, transaction fees, and transaction speed – leave room for improvement. Especially during the setup study, several problems and challenges surfaced that underline the conclusions made by previous work (e.g. [14, 15, 20]): There is a need to improve the onboarding experience of new users – an aspect where the HCI community is uniquely positioned to contribute to. Additionally, we observed that the interface to established systems like banks or identity verification providers remain a major cause of friction [15]. Upcoming regulations surrounding cryptocurrencies could both be a catalyst for addressing these issues, or lead to more restrictive measures. While the achieved transaction speed of 4-6 seconds is in itself comparable to existing systems, the interaction flow it is embedded in was perceived as complicated by users. While permanent invoices are not technically feasible for now, a recent proposal aims to change this by extending the Bitcoin Lightning protocol [37].

6.2 Adoption Considerations

Reflecting on our experience developing the system, we found that the decision of using a payment processing services made it relatively easy to integrate and accept Bitcoin Lightning payments. We argue, that merchants without much technical expertise would be able to implement such solutions, i.e. through plugins to popular shop system such as Shopify. One downside of using a service provider instead of running a dedicated Bitcoin Lightning node is that a merchant would arguably not exploit the full benefit of decentralization and would have to pay fees to the service provider. Dealing with these tradeoffs between the independence of decentralization and scale effects of using centralized services connects to the emerging phenomenon of reintermediation [17, 43] seen in many blockchain related applications. Taking a business perspective, the question for merchants remains whether accepting Bitcoin Lightning or other cryptocurrencies is economically beneficial and sustainable in the long run. As new payment solutions generally face a cold start problem [6], it remains questionable whether users are motivated to change from established solutions to Bitcoin Lightning if both choices are offered. From the customer's perspective, except for edge cases, there is little to no advantage using Bitcoin Lightning at the user experience level compared to centralized solutions. Today systems like PayPal appear to offer a better value proposition: free transactions for individuals, wide acceptance, fiat currencies without price volatility, and a buyer protection. While many of these features are not yet available, we believe that the current state of the technology allows for them to be built on top of the open ecosystem that Bitcoin Lightning (or other cryptocurrencies) offers.

6.3 Limitations and Future Work

This paper provides a first evaluation of Bitcoin Lightning for an offline point-of-sale use case. Our study is not without limitations and leaves room for future research. Our study ran for only a short time and was tested with a small basket size (typically EUR 0.5 to EUR 1.5). A benchmark study of the Lightning network [47] showed grave differences in network reliability depending on the size of a transaction. Exploring scenarios with higher item values would be interesting not only to understand the technical limitations of Bitcoin Lightning, but also whether users would expect features such as cash-backs common with many credit card providers today.

Additionally, our evaluation focused primarily on the system performance and did not explore participants' experience using Bitcoin Lightning in depth. Particularly during the adoption of new technologies, users may be motivated to engage due to more than pure functional benefits. Building on recent ethnographic research on centralized alternative currencies [32], future work may disassemble the social experiences of everyday cryptocurrency use (e.g. around trust, anonymity, decentralization, volatility and perceived environmental impact) in more detail.

Thus, there are exciting opportunities for HCI scholars to explore lived user experience during the adoption of cryptocurrency based payment systems over longer periods of time and in different contexts. Particularly the recent real-world deployment of

Bitcoin-Lightning in some regions around the world offers interesting opportunities to study the use of cryptocurrencies in the field.

7 CONCLUSION

This paper presents design considerations and a reference implementation for a point-of-sale (PoS) system using Bitcoin Lightning as underlying payment layer. The evaluation of the system in a mixed methods study shows that low-value transactions can be reliably routed via the Lightning network, and users found making payments reasonably easy once they had a configured wallet. Setting up the wallet and initially acquiring Bitcoin was, however, prone to different challenges, highlighting the need to research on how to decrease entry barriers to cryptocurrencies. We examine the performance of the system with regards to ease-of-use, speed, transaction fees, and reliability and discuss implications for adoption of cryptocurrency based payment systems.

ACKNOWLEDGMENTS

This work was supported by the Deutsche Forschungsgemeinschaft (DFG) (grant no. 316457582 and 425869382). We thank the team from https://condens.io/ for supporting us with their qualitative research analysis tool — it helped us analyze and understand the interview data we collected.

REFERENCES

[1] Svetlana Abramova, Artemij Voskobojnikov, Konstantin Beznosov, and Rainer Böhme. 2021. Bits Under the Mattress: Understanding Different Risk Perceptions and Security Behaviors of Crypto-Asset Users. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 692, 19 pages. https://doi.org/10.1145/3411764.3445679

[2] Emad Almutairi and Shiroq Al-Megren. 2019. Usability and Security Analysis of the KeepKey Wallet. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. 149–153. https://doi.org/10.1109/BLOC.2019.8751451

[3] Abdulla Alshamsi and Prof. Peter Andras. 2019. User perception of Bitcoin usability and security across novice users. *International Journal of Human-Computer Studies* 126 (2019), 94–110. https://doi.org/10.1016/j.ijhcs.2019.02.004

[4] Bernd Bruegge and Allen H Dutoit. 2009. Object–oriented software engineering. using uml, patterns, and java. *Learning* 5, 6 (2009), 7.

[5] Vitalik Buterin et al. 2013. Ethereum white paper. *GitHub repository* 1 (2013), 22–23.

[6] Andrew Chen. 2014. How to solve the cold-start problem for social products. https://andrewchen.com/how-to-solve-the-cold-start-problem-for-social-products/ (last accessed: 2021-04-21).

[7] Lawrence Chung and Julio Cesar Sampaio do Prado Leite. 2009. On non-functional requirements in software engineering. In *Conceptual modeling: Foundations and applications*. Springer, 363–379.

[8] Coinbase. 2021. Coinbase Third Quarter 2021 Shareholder Letter. https://s27.q4cdn.com/397450999/files/doc_financials/2021/q3/Coinbase-Q321-Shareholder-Letter.pdf (last accessed: 2021-12-13).

[9] Crypto.com. 2022. Global Crypto Owners Near 300 Million, Predicted to Hit 1 Billion by the End of 2022. https://blog.crypto.com/global-crypto-owners-near-300-million-predicted-to-hit-1-billion-by-the-end-of-2022/ (last accessed: 2021-04-03).

[10] Alex de Vries, Ulrich Gallersdörfer, Lena Klaaßen, and Christian Stoll. 2022. Revisiting Bitcoin's carbon footprint. *Joule* 6, 3 (2022), 498–502. https://doi.org/10.1016/j.joule.2022.02.005

[11] Chris Dixon and Eddy Lazzarin. 2020. *The Crypto Price-Innovation Cycle.* Andreessen Horowitz. Retrieved 2021-12-13 from https://a16z.com/2020/05/15/the-crypto-price-innovation-cycle/

[12] Shayan Eskandari, Jeremy Clark, and Abdelwahab Hamou-Lhadj. 2016. Buy Your Coffee with Bitcoin: Real-World Deployment of a Bitcoin Point of Sale Terminal. In *2016 Intl IEEE Conferences on Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*. 382–389. https://doi.org/10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0073

[13] Michael Froehlich, Philipp Hulm, and Florian Alt. 2021. Under Pressure. A User-Centered Threat Model for Cryptocurrency Owners. In *2021 the 4th International Conference on Blockchain Technology and Applications* (Xi'an, China) *(ICBTA 2021)*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3510487.3510494

[14] Michael Froehlich, Charlotte Kobiella, Albrecht Schmidt, and Florian Alt. 2021. *Is It Better With Onboarding? Improving First-Time Cryptocurrency App Experiences.* Association for Computing Machinery, New York, NY, USA, 78–89. https://doi.org/10.1145/3461778.3462047

[15] Michael Froehlich, Maurizio Raphael Wagenhaus, Albrecht Schmidt, and Florian Alt. 2021. *Don't Stop Me Now! Exploring Challenges Of First-Time Cryptocurrency Users.* Association for Computing Machinery, New York, NY, USA, 138–148. https://doi.org/10.1145/3461778.3462071

[16] Michael Fröhlich, Felix Gutjahr, and Florian Alt. 2020. *Don't Lose Your Coin! Investigating Security Practices of Cryptocurrency Users.* Association for Computing Machinery, New York, NY, USA, 1751–1763. https://doi.org/10.1145/3357236.3395535

[17] Michael Fröhlich, Franz Waltenberger, Ludwig Trotter, Florian Alt, and Albrecht Schmidt. 2022. Blockchain and Cryptocurrency in Human Computer Interaction: A Systematic Literature Review and Research Agenda. https://doi.org/10.48550/ARXIV.2204.10857

[18] Ulrich Gallersdörfer, Lena Klaaßen, and Christian Stoll. 2020. Energy Consumption of Cryptocurrencies Beyond Bitcoin. *Joule* 4, 9 (2020), 1843–1846. https://doi.org/10.1016/j.joule.2020.07.013

[19] Xianyi Gao, Gradeigh D. Clark, and Janne Lindqvist. 2016. Of Two Minds, Multiple Addresses, and One Ledger: Characterizing Opinions, Knowledge, and Perceptions of Bitcoin Across Users and Non-Users. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 1656–1668. https://doi.org/10.1145/2858036.2858049

[20] Leonhard Glomann, Maximilian Schmid, and Nika Kitajewa. 2020. Improving the Blockchain User Experience - An Approach to Address Blockchain Mass Adoption Issues from a Human-Centred Perspective. In *Advances in Artificial Intelligence, Software and Systems Engineering (Advances in Intelligent Systems and Computing)*, Tareq Ahram (Ed.). Springer International Publishing, 608–616. https://doi.org/10.1007/978-3-030-20454-9_60

[21] Mark Hunter. 2022. Bitcoin's Lightning Network Already Breaking Records in 2022. https://fullycrypto.com/bitcoins-lightning-network-already-breaking-records-in-2022 (last accessed: 2021-04-03).

[22] Hyeji Jang, Sung H. Han, and Ju Hwan Kim. 2020. User Perspectives on Blockchain Technology: User-Centered Evaluation and Design Strategies for DApps. *IEEE Access* 8 (2020), 226213–226223. https://doi.org/10.1109/ACCESS.2020.3042822

[23] Hyeji Jang, Sung H. Han, Ju Hwan Kim, and Kimin Kown. 2020. Identifying and Improving Usability Problems of Cryptocurrency Exchange Mobile Applications Through Heuristic Evaluation. In *Advances in Usability, User Experience, Wearable and Assistive Technology (Advances in Intelligent Systems and Computing)*, Tareq Ahram and Christianne Falcão (Eds.). Springer International Publishing, 15–21. https://doi.org/10.1007/978-3-030-51828-8_3

[24] Hyeji Jang, Sung H. Han, Ju Hwan Kim, and Kimin Kwon. 2021. Usability Evaluation for Cryptocurrency Exchange. In *Convergence of Ergonomics and Design (Advances in Intelligent Systems and Computing)*, Alma Maria Jennifer Gutierrez, Ravindra S. Goonetilleke, and Rex Aurellius C. Robielos (Eds.). Springer International Publishing, 192–196. https://doi.org/10.1007/978-3-030-63335-6_20

[25] Ali Kazerani, Domenic Rosati, and Brian Lesser. 2017. Determining the Usability of Bitcoin for Beginners Using Change Tip and Coinbase. In *Proceedings of the 35th ACM International Conference on the Design of Communication* (Halifax, Nova Scotia, Canada) *(SIGDOC '17)*. Association for Computing Machinery, New York, NY, USA, Article 5, 5 pages. https://doi.org/10.1145/3121113.3121125

[26] Irni Eliana Khairuddin, Corina Sas, Sarah Clinch, and Nigel Davies. 2016. Exploring Motivations for Bitcoin Technology Usage. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI EA '16)*. Association for Computing Machinery, New York, NY, USA, 2872–2878. https://doi.org/10.1145/2851581.2892500

[27] Bettina Laugwitz, Theo Held, and Martin Schrepp. 2008. Construction and evaluation of a user experience questionnaire. In *Symposium of the Austrian HCI and usability engineering group*. Springer, 63–76.

[28] Alexandra Mai, Katharina Pfeffer, Matthias Gusenbauer, Edgar Weippl, and Katharina Krombholz. 2020. User Mental Models of Cryptocurrency Systems - A Grounded Theory Approach. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, 341–358. https://www.usenix.org/conference/soups2020/presentation/mai

[29] Jens Mattke, Christian Maier, and Lea Reis. 2020. Is Cryptocurrency Money? Three Empirical Studies Analyzing Medium of Exchange, Store of Value and Unit of Account. In *Proceedings of the 2020 on Computers and People Research Conference* (Nuremberg, Germany) *(SIGMIS-CPR'20)*. Association for Computing

Machinery, New York, NY, USA, 26–35. https://doi.org/10.1145/3378539.3393859
[30] Md Moniruzzaman, Farida Chowdhury, and Md Sadek Ferdous. 2020. Examining Usability Issues in Blockchain-Based Cryptocurrency Wallets. In *Cyber Security and Computer Science (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering)*, Touhid Bhuiyan, Md. Mostafijur Rahman, and Md. Asraf Ali (Eds.). Springer International Publishing, 631–643. https://doi.org/10.1007/978-3-030-52856-0_50
[31] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review* (2008), 21260.
[32] Mark Perry and Jennifer Ferreira. 2018. Moneywork: Practices of Use and Social Interaction around Digital and Analog Money. *ACM Trans. Comput.-Hum. Interact.* 24, 6, Article 41 (jan 2018), 32 pages. https://doi.org/10.1145/3162082
[33] Polygon Technology. 2021. Polygon: Ethereum's Internet of Blockchains. *Whitepaper* (Feb 2021). https://polygon.technology/lightpaper-polygon.pdf
[34] Joseph Poon and Thaddeus Dryja. 2016. The bitcoin lightning network: Scalable off-chain instant payments.
[35] Larissa Pschetz, Ella Tallyn, Rory Gianni, and Chris Speed. 2017. Bitbarista: Exploring Perceptions of Data Transactions in the Internet of Things. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 2964–2975. https://doi.org/10.1145/3025453.3025878
[36] Bagus Anugrah Ramadhan and Billy Muhamad Iqbal. 2018. User Experience Evaluation on the Cryptocurrency Website by Trust Aspect. In *2018 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS)*, Vol. 3. 274–279. https://doi.org/10.1109/ICIIBMS.2018.8550019
[37] Rusty Russel. 2020. Offers: Lightning's Native Experience, Everywhere. https://bolt12.org/ (last accessed: 2021-04-21).
[38] Corina Sas and Irni Eliana Khairuddin. 2017. Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 6499–6510. https://doi.org/10.1145/3025453.3025886
[39] Jeff Sauro. 2021. 10 Things To Know About The Single Ease Question (SEQ). https://measuringu.com/seq10/ (last accessed: 2021-04-21).
[40] Jeff Sauro and Joseph S. Dumas. 2009. Comparison of Three One-Question, Post-Task Usability Questionnaires. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Boston, MA, USA) *(CHI '09)*. Association for Computing Machinery, New York, NY, USA, 1599–1608. https://doi.org/10.1145/1518701.1518946
[41] MacKenzie Sigalos. 2021. El Salvador looks to become the world's first country to adopt bitcoin as legal tender. https://www.cnbc.com/2021/06/05/el-salvador-becomes-the-first-country-to-adopt-bitcoin-as-legal-tender-.html (last accessed: 2021-04-03).
[42] Ella Tallyn, Larissa Pschetz, Rory Gianni, Chris Speed, and Chris Elsden. 2018. Exploring Machine Autonomy and Provenance Data in Coffee Consumption: A Field Study of Bitbarista. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 170 (nov 2018), 25 pages. https://doi.org/10.1145/3274439
[43] Ludwig Trotter, Mike Harding, Peter Shaw, Nigel Davies, Chris Elsden, Chris Speed, John Vines, Aydin Abadi, and Josh Hallwright. 2020. Smart Donations: Event-Driven Conditional Donations Using Smart Contracts On The Blockchain. In *32nd Australian Conference on Human-Computer Interaction* (Sydney, NSW, Australia) *(OzCHI '20)*. Association for Computing Machinery, New York, NY, USA, 546–557. https://doi.org/10.1145/3441000.3441014
[44] Artemij Voskobojnikov, Svetlana Abramova, Konstantin Beznosov, and Rainer Boehme. 2021. Non-Adoption of Crypto-Assets: Exploring the Role of Trust, Self-Efficacy, and Risk. *ECIS 2021 Research Papers* 9 (2021). https://aisel.aisnet.org/ecis2021_rp/9
[45] Artemij Voskobojnikov, Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. 2020. Surviving the Cryptojungle: Perception and Management of Risk Among North American Cryptocurrency (Non)Users. In *Financial Cryptography and Data Security*, Joseph Bonneau and Nadia Heninger (Eds.). Springer International Publishing, Cham, 595–614.
[46] Artemij Voskobojnikov, Oliver Wiese, Masoud Mehrabi Koushki, Volker Roth, and Konstantin (Kosta) Beznosov. 2021. The U in Crypto Stands for Usable: An Empirical Study of User Experience with Mobile Cryptocurrency Wallets. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 642, 14 pages. https://doi.org/10.1145/3411764.3445407
[47] Finnegan Waugh and Ralph Holz. 2020. An empirical study of availability and reliability properties of the Bitcoin Lightning Network. *CoRR* abs/2006.14358 (2020). arXiv:2006.14358 https://arxiv.org/abs/2006.14358
[48] Anatoly Yakovenko. 2018. Solana: A new architecture for a high performance blockchain v0. 8.13. *Whitepaper* (2018).
[49] Philipp Zabka, Klaus-T. Foerster, Stefan Schmid, and Christian Decker. 2022. Empirical evaluation of nodes and channels of the lightning network. *Pervasive and Mobile Computing* (2022), 101584. https://doi.org/10.1016/j.pmcj.2022.101584

Supporting Interface Experimentation for Blockchain Applications

Michael Froehlich*
Center for Digital Technology and Management, Germany
froehlich@cdtm.de

Benjamin Moser
Ludwig Maximilian University, Germany
benjamin.moser@campus.lmu.de

Florian Alt
University of the Bundeswehr Munich, Germany
florian.alt@unibw.de

Albrecht Schmidt
Ludwig Maximilian University, Germany
albrecht.schmidt@ifi.lmu.de

ABSTRACT

There is an increasingly diverse range of smart-contract blockchains on which decentralized applications (dApps) are built. However, HCI research has so far failed to address them, focusing primarily on Bitcoin and Ethereum. This is problematic as these new blockchains come with an increasingly diverse set of properties that influence the usability of dApps for end-users. For blockchain interface design guidelines to be valuable for practitioners, they need to acknowledge the heterogeneity of blockchains. However, evaluating novel interface concepts across different blockchains is resource-intensive as each blockchain has to be integrated manually, slowing down research. To address this challenge, we propose a system to support interface experimentation for blockchain applications. The system allows researchers and developers to connect interfaces to a unified API simulating different blockchains and facilitates the configuration, distribution, and evaluation of online experiments. A preliminary evaluation showed promising results.

CCS CONCEPTS

• **Human-centered computing** → **Human computer interaction (HCI)**; • **Applied computing** → **Digital cash**; • **Information systems** → **Digital cash**; • **General and reference** → *Experimentation.*

KEYWORDS

blockchain, cryptocurrency, dapps, web3, hci, interface design, experimentation, support tools

ACM Reference Format:
Michael Froehlich, Benjamin Moser, Florian Alt, and Albrecht Schmidt. 2022. Supporting Interface Experimentation for Blockchain Applications. In *Adjunct Proceedings of the 2022 Nordic Human-Computer Interaction Conference (NordiCHI Adjunct '22), October 8–12, 2022, Aarhus, Denmark.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3547522.3547676

*Also with Ludwig Maximilian University, University of the Bundeswehr Munich.

NordiCHI Adjunct '22, October 8–12, 2022, Aarhus, Denmark

ACM ISBN 978-1-4503-9448-2/22/10.
https://doi.org/10.1145/3547522.3547676

1 INTRODUCTION

There is an increasingly diverse landscape of blockchain application platforms to develop with [10]. While a few years ago Ethereum was the only smart-contract blockchain available, today alternatives like Cosmos, Solana, Polkadot, or Polygon have emerged and gained traction among developers [15]. At the same time, extant interaction design research on blockchain and cryptocurrency has overwhelming focused on Bitcoin and Ethereum, neglecting other chains [10]. This gap is problematic as these new blockchains offer developers fundamentally different properties – for example w.r.t. transaction speed, throughput, and fees – which in turn influence how end-users can interact with the built decentralized applications (dApps). Taking the researchers' perspectives it is not difficult to see how this gap has formed: Prototyping and evaluating interfaces for different blockchains requires substantial resources, as each blockchain needs to be manually integrated. This consequently makes it costly to experiment with interface concepts on several blockchains and, as a field, has kept us from understanding the heterogeneous effects different blockchain properties may have on application design.

Let's take the design of interface elements for the communication of transaction stati as an example: Previous literature documents that users find transactions hard to understand and misconceptions are frequent (see e.g. [9, 11, 14, 16]). For designers and developers this begs the question, how to best design interface elements that communicate the status and expected completion of a transaction clearly and unambiguously. The non-deterministic nature of blockchains – validating nodes can independently decide which transactions to include in the next block – makes this a non-trivial task. The completion of a transaction may depend on the frequency at which blocks are created, the current state of the network, and the amount of fees allocated for the specific transaction. These properties are all connected to the infrastructure provided by the underlying blockchain a dApp is built on. For example, even simple transactions may take between tens of minutes (e.g. Bitcoin), a few minutes (e.g. Ethereum), and a few seconds (e.g. Bitcoin Lightning or Solana) depending on the blockchain. Design guidelines for such interface elements would thus need to acknowledge the heterogeneity of blockchains and their properties to be valuable for practitioners.

Consequently, to create such guidelines for blockchain interfaces, it is necessary to design interfaces and evaluate them across different blockchains. To address this challenge, we propose a system to support interface experimentation for blockchain applications.

The proposed system allows researchers and developers to connect their interfaces to a unified API that simulates different blockchains and provides a management interface to configure, distribute, and evaluate online experiments. We present an early implementation of the system and report the results of a preliminary study with N=160 participants on Amazon Mechanical Turk (mTurk).

2 PROTOTYPE

We developed a system to support rapid interface experimentation for blockchain applications. In the following we lay out the requirements, its architecture, and implementation.

2.1 Use Case and Requirements

We illustrate the envisioned use case by contrasting an *as-is-scenario* with a *visionary-scenario* [4]. The system has two actors: the interface DEVELOPER and the study PARTICIPANT.

Table 1: Use-Case: As-Is-Scenario and Visionary-Scenario

Situation
Dora is an interface developer for a mobile social payment app that supports multiple cyrptocurrencies. By analyzing comments on the app store she notices that some users complain that transactions are sometimes taking too long to complete or even get stuck. After conducting desk research and some user interviews she realizes that new users often do not understand the connection between fee-amount and transaction speed and thus face difficulties to select the right fee. She decides to prototype different input elements and test them with users before suggesting changes to the production app. She wants to understand which input elements help users select the appropriate fees and is interested in understanding whether different cryptocurrencies require different input elements.
As-Is-Scenario: Dora implements the different input elements on different branches of the Github repository. After collecting qualitative input from a small sample, she wants to test the different interfaces in an online experiment. Due to cost constraints she cannot distribute real cryptocurrency to participants. Instead, she decides to mock the sending of transactions and fees. For each cryptocurrency she starts implementing realistic behavior mocking the fees and transaction speed for the specific experiment she has in mind. After completing the implemention, she deploys the app and creates a document outlining the task instruction for the participants. In another tool she creates a questionnaire. Finally, creates four tasks on Amazon mTurk, each linking to a different version of the app and distributes her experiment.
Visionary-Scenario: Dora prototypes four input elements on a new branch of the Github project. She integrates the API of the blockchain experimentation system. Based of the programatic assignment through the API the respective input element is rendered. To mock sending transactions, she uses the unified interface of the API. She sends the respective cryptocurrency, the amount, and selected transaction, and additional transaction details and the API returns the status of the transaction. After completing the implementation she switches to the web-interface of the experimentation system. She configures the study procedure, adds a questionnaire step and an experimentation step with an appropriate task description. She configures the simulated cryptocurrencies and tested input elements. With the generated link she distributes the experiment via Amazon mTurk.

From the described use case we derived several functional requirements [4] for the system:

- **R1 Blockchain Simulation:** The system should allow the simulation of different blockchains and their core properties. It should provide an common interface to simulate transactions on the supported blockchains to decouple interface implementation and evaluation from the specific blockchain implementation.
- **R2 Experiment Management:** The system should support the configuration and management of experiments. It should be configurable with respect to which cryptocurrencies and which interface variations are part of an experiment and manage subsequent randomized assignment of participants.
- **R3 Rapid Dissemination:** The system should enable a fast dissemination of experiments. Task descriptions for participants and questionnaires should be integrated into the experimentation system to allow for fast distribution.

2.2 Conceptual Architecture

We decomposed the proposed system into several components with specific responsibilities. Figure 1 provides an overview of the conceptual architecture. The experimentation system comprises three subsystems: The BLOCKCHAIN SIMULATOR bundles blockchain simulation functionality and exposes an REST API that integrates with the interface prototypes of the DEVELOPER. The EXPERIMENT CONFIGURATOR provides a management interface for the DEVELOPER to configure and monitor their experiments. The STUDY DISSEMINATION subsystem manages the distribution of the experiment to PARTICIPANTS in accordance to the configuration of the experiment.

The decompostion in subsystem has several advantages. First, decoupling functionality allows composability and re-use. For example, experiments could be easily repeated with different interfaces by duplicating experiment configurations. Second, it allows for maintainability and extensibility. By exposing only a limited interface to other components, the underlying implementation can be changed or improved in the future. For example, new blockchain simulations could be added without affecting existing experiments or the simulation of a specific blockchain could be implemented in a more advanced way.

2.3 Implementation

We implemented the proposed system in a first prototype. We realized the experimentation system using NodeJS[1], ExpressJS[2] and MongoDB[3]. The implemented system supports an abstraction layer to simulate the Bitcoin and Ethereum blockchain and allows for the integration of additional blockchains in the future. Figure 2 shows a low-fidelity interface prototype and the actual realized interface of the experimentation system.

The interface of the EXPERIMENT CONFIGURATOR shows three main pages (see navigation bar on the left). The Blockchain page shows the blockchains that can be simulated. The Questionnaires page shows an overview of existing questionnaires and allows to created new ones. Finally, the Experiments pages shows an overview of the created experiment, allows to create new ones, and configure existing ones. The configuration of an experiment comprises chaining different tasks together, i.e. questionnaire tasks or experiment

[1] https://nodejs.org/ (last-accessed: 2022-05-21)
[2] http://expressjs.com/ (last-accessed: 2022-05-21)
[3] https://www.mongodb.com/ (last-accessed: 2022-05-21)

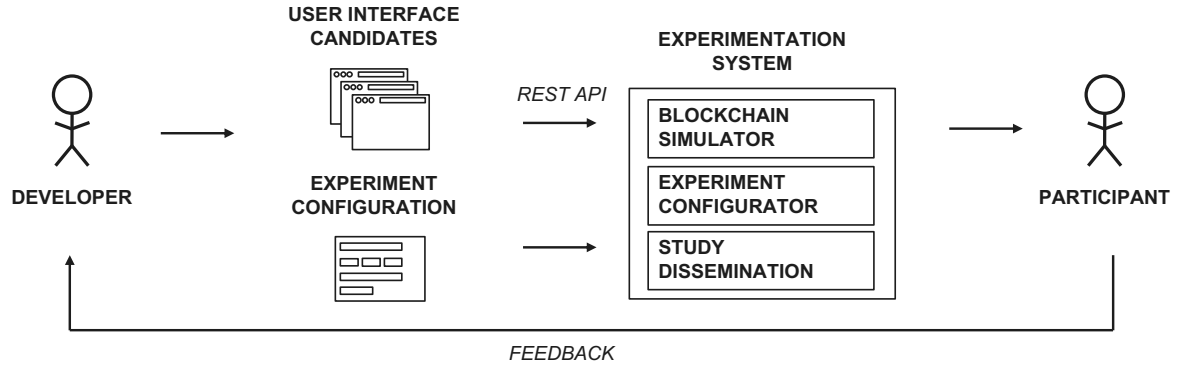


Figure 1: Conceptual overview of the prototyped system.

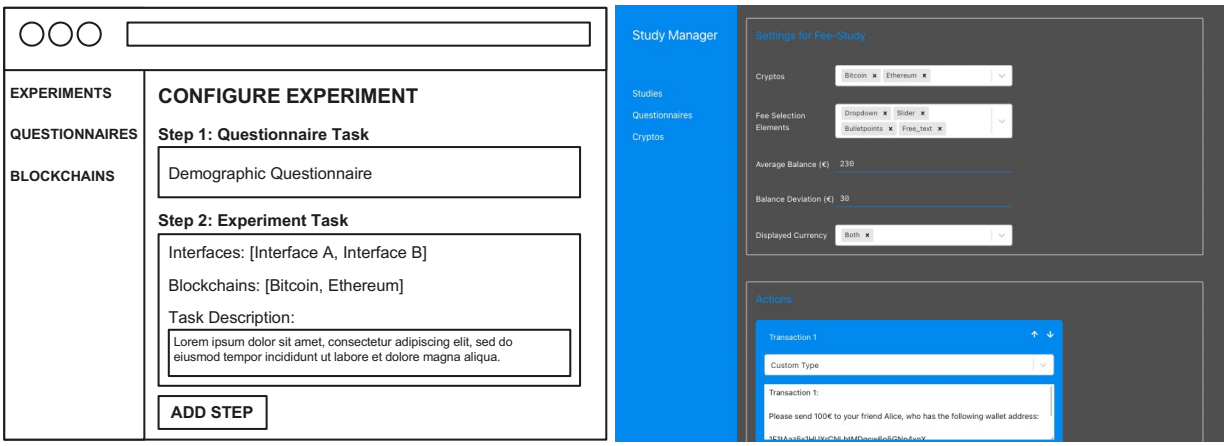


Figure 2: The interface of the Experimentation System: A low fidelity prototype (left) and the realized implementation (right).

tasks. Experiment tasks require specific configuration: identifier for the respective interfaces, which blockchain simulations to use, and the task descriptions that are shown to participants.

3 EVALUATION AND RESULTS

To evaluate the system we designed and ran an initial experiment with it. The experiment evaluated four types of input elements (free input, select, dropdown, slider) for sending transactions with two cryptocurrencies (Bitcoin, Ethereum) in a between-subject online experiment. The main purpose of running the experiment was to test designed system under realistic conditions.

3.1 Experimental Setup

We used a between-subject design to compare different interface elements for selecting fees when sending a transaction in an online experiment with n=160 participants who we recruited from Amazon mTurk. There were 8 experimental conditions (4 input elements times 2 cryptocurrencies). We recruited in total 160 participants who were randomly assigned to one condition by our system. The instructions for the experiment were provided within our system and could be accessed by participants using a dedicated button at all times. Additionally, participants had to fill a questionnaire after completing the user study.

Procedure: During the study participants were provided with three task descriptions asking them to consider a specific scenario under which they should send a cryptocurrency transactions. The task description contained cues about the expected speed at which the user would like the transaction to complete to induce interaction during the fee selection process. For example, "*Please send 10€ to your colleague Tim [...] He made it clear that he needs the money within 30 minutes.*". Participants conducted these transactions with a mobile wallet interface presented in the browser. At the start of the study they were randomly assigned to one of the conditions, which remained the same during the study. The wallet interface integrated the developed system and displayed the respective interface elements.

Collected Data and Hypotheses: We collected several metrics and variables to understand system performance and users' perception. We were specifically interested in the **perceived usability**, **time needed for the fee selection**, and **the selected fee value**. Our hypotheses for all collected output variables were that there would be a difference between cryptocurrencies and input elements.

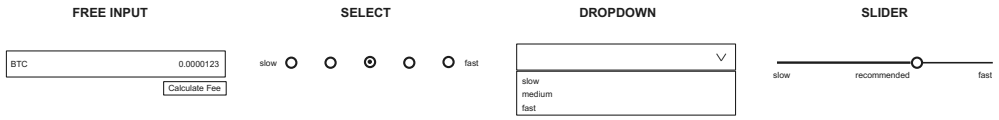


Figure 3: Illustrations of the different input elements used to select the transaction fee during the experiment.

3.2 Results

In total 160 people participated in the experiment. The median age was 32 years. 57 (35.6%) were female, the other 103 (64.4%) were male. 76.9% reported being from the USA. Two thirds of participants had previously made a cryptocurrency transaction. Overall, the analysis showed that the system could successfully be used to collect experimental data, did not suffer performance issues, and supported the intended use cases. We observed that in 15.6% of tasks were not completed correctly. Common mistakes included incorrectly entered receiver addresses or transaction amounts, also reported in literature (see e.g. [7, 14]).

Table 2: Overview of the collected metrics (arithmetic mean).

	Usability	Time	Values
free input	64.55	39.9 sec	0,0668 ETH
select	56.59	15.0 sec	0,0178 ETH
dropdown	60.43	9.7 sec	0,0247 ETH
slider	69.79	11.9 sec	0,0178 ETH
BTC	60.33	18.9 sec	67,13 sat/byte
ETH	64.81	19.1 sec	0,0283 ETH
Total	62.48	19.0 sec	–

Usability: Overall, the mean SUS score [3] was 62.48, which is below average usability compared to general consumer apps [13] and comparable to existing cryptocurrency apps [8, 9]. Regarding input elements, usability was highest (69.79) for the slider. A Kruskal-Wallis test showed significant difference between input elements. The respective Dunn-Bonferroni post-hoc analysis showed differences are only significant between *slider-select* (p=0.006). A Mann-Whitney-U-Test did not find statistical significant differences between cryptocurrencies.

Time: The average time to select a fee was between 9.7 and 39.9 seconds depending on the input element. The *free input* element required the most time. A Welch's Anova showed difference between groups. A post-hoc pairwise Games-Howell test showed statistically significant differences between *free input-dropdown* (=0.024) and *free input-slider* (p=0.028).

Fee Value: A Kruskal-Wallis test showed statistically significant differences in selected transaction fee value by input element for Ethereum (p<0.001) but not for Bitcoin. For Ethereum, pairwise post-hoc comparisons show statistically significant differences for *slider-free input* (p=0.006), *select-free input* (p=0.001), *dropdown-free-input* (p=0.002).

4 DISCUSSION

Overall, the preliminary evaluation of the developed system showed promising results. The implemented system could fulfill the initial requirements and facilitate a blockchain interface experiment including configuration, simulation, and distribution. We did not encounter any technical problems or load issues during the experiment. While mTurk has established itself as popular platform for microtasks and research [12], we observed that some participants attempted to cheat the system – i.e. they they just tried to enter bogus data and click through the prototype as fast a possible. This behavior is in line with previous findings (see e.g. [1]) discussing data quality of mTurk.

4.1 Limitations & Future Work

The results presented in this paper are not without limitations. The implementation of the proposed system is an early version with room for future development. The evaluation presented primarily serves to demonstrate the feasibility of the approach. Future evaluations of the system should aim to understand whether using the system enables researchers and developers to improve their workflow in a more holistic ways. The experimental comparison of input element was conducted with a small sample and tentative findings presented here should be complemented by qualitative research in the future to support interface designers.

Future System Development: The described system is early technical work. To unlock its full value for researchers and developers it will require a larger set of blockchains to be available for simulation. While there new generations of blockchain have become available for developers to build on, a recent literature review shows that there is a research gap in HCI concerning studies that go beyond Bitcoin and Ethereum [10]. A second point for future development concerns the level of sophistication at which blockchain transactions can be simulated. While simulation of simple transactions enables interface experimentation with regards to sending and receiving cryptocurrency, a larger design space can arguable found in the area of smart contracts and dApps [5, 10]. Thus, a way to realistically simulate transactions calling smart contracts on various blockchains may be beneficial for more complex blockchain experiments. From a technical point-of-view, this could be achieved by integrating more sophisticated systems to simulated the underlying blockchain (see e.g. [2, 6]). Another opportunity would be the possibility to not just simulate blockchains, but replay specific states of the blockchain. This would allow testing hypotheses related to cryptocurrency valuations and network congestion.

Future System Evaluation: With researchers and developers being the primary users of the system, future evaluation should test whether the system delivers value to them. This includes questions related to their user experience integrating the API and running

the experiments with the system as well as more objective measure like the time and resource savings generated through use of the system. Additionally, future evaluations should analyze whether data gathered via mTurk fulfills the required standards for scientific research in this context and, if not, implement additional services.

5 CONCLUSION

This paper presents a system to support interface experimentation for blockchain applications. In a preliminary evaluation it shows promising results for reducing the time and effort needed to conduct experiments with novel users interfaces. We would like to engage with the HCI community at NordiCHI to discuss how the system could be extended to support researchers, designers, and users beyond experiment driven evaluation of novel interfaces. In line with the conference's themes we would like to explore how users could be empowered to participate not just in the evaluation but the design process itself.

REFERENCES

[1] Douglas J Ahler, Carolyn E Roush, and Gaurav Sood. 2019. The micro-task market for lemons: Data quality on Amazon's Mechanical Turk. *Political Science Research and Methods* (2019), 1–20.

[2] Maher Alharby and Aad van Moorsel. 2019. BlockSim: A Simulation Framework for Blockchain Systems. *SIGMETRICS Perform. Eval. Rev.* 46, 3 (jan 2019), 135–138. https://doi.org/10.1145/3308897.3308956

[3] John Brooke. 1996. SUS: a 'quick and dirty' usability scale. *Usability evaluation in industry* (1996), 189.

[4] Bernd Bruegge and Allen H. Dutoit. 2009. *Object-Oriented Software Engineering Using UML, Patterns, and Java* (3rd ed.). Prentice Hall Press, USA.

[5] Chris Elsden, Arthi Manohar, Jo Briggs, Mike Harding, Chris Speed, and John Vines. 2018. *Making Sense of Blockchain Applications: A Typology for HCI.* Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3173574.3174032

[6] Carlos Faria and Miguel Correia. 2019. BlockSim: Blockchain Simulator. In *2019 IEEE International Conference on Blockchain (Blockchain).* 439–446. https://doi.org/10.1109/Blockchain.2019.00067

[7] Michael Froehlich, Philipp Hulm, and Florian Alt. 2021. Under Pressure. A User-Centered Threat Model for Cryptocurrency Owners. In *2021 the 4th International Conference on Blockchain Technology and Applications* (Xi'an, China) *(ICBTA 2021).* Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3510487.3510494

[8] Michael Froehlich, Charlotte Kobiella, Albrecht Schmidt, and Florian Alt. 2021. *Is It Better With Onboarding? Improving First-Time Cryptocurrency App Experiences.* Association for Computing Machinery, New York, NY, USA, 78–89. https://doi.org/10.1145/3461778.3462047

[9] Michael Froehlich, Maurizio Raphael Wagenhaus, Albrecht Schmidt, and Florian Alt. 2021. *Don't Stop Me Now! Exploring Challenges Of First-Time Cryptocurrency Users.* Association for Computing Machinery, New York, NY, USA, 138–148. https://doi.org/10.1145/3461778.3462071

[10] Michael Froehlich, Franz Waltenberger, Ludwig Trotter, Florian Alt, and Albrecht Schmidt. 2022. Blockchain and Cryptocurrency in Human Computer Interaction: A Systematic Literature Review and Research Agenda. In *Designing Interactive Systems Conference* (Virtual Event, Australia) *(DIS '22).* Association for Computing Machinery, New York, NY, USA, 155–177. https://doi.org/10.1145/3532106.3533478

[11] Michael Fröhlich, Felix Gutjahr, and Florian Alt. 2020. *Don't Lose Your Coin! Investigating Security Practices of Cryptocurrency Users.* Association for Computing Machinery, New York, NY, USA, 1751–1763. https://doi.org/10.1145/3357236.3395535

[12] Aniket Kittur, Ed H. Chi, and Bongwon Suh. 2008. Crowdsourcing User Studies with Mechanical Turk. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Florence, Italy) *(CHI '08).* Association for Computing Machinery, New York, NY, USA, 453–456. https://doi.org/10.1145/1357054.1357127

[13] James R Lewis. 2018. The system usability scale: past, present, and future. *International Journal of Human–Computer Interaction* 34, 7 (2018), 577–590.

[14] Alexandra Mai, Katharina Pfeffer, Matthias Gusenbauer, Edgar Weippl, and Katharina Krombholz. 2020. User Mental Models of Cryptocurrency Systems - A Grounded Theory Approach. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020).* USENIX Association, 341–358. https://www.usenix.org/conference/soups2020/presentation/mai

[15] Maria Shen and Avichal Garg. 2022. *Developer Report 2021.* Electric Capital. Retrieved 2022-02-11 from https://github.com/electric-capital/developer-reports/blob/master/dev_report_2021_updated_012622.pdf

[16] Artemij Voskobojnikov, Oliver Wiese, Masoud Mehrabi Koushki, Volker Roth, and Konstantin (Kosta) Beznosov. 2021. The U in Crypto Stands for Usable: An Empirical Study of User Experience with Mobile Cryptocurrency Wallets. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21).* Association for Computing Machinery, New York, NY, USA, Article 642, 14 pages. https://doi.org/10.1145/3411764.3445407

Prototyping With Blockchain: A Case Study For Teaching Blockchain Application Development at University

Michael Fröhlich[1,2,3], Jose Vega[1] Amelie Pahl[1,2], Sergej Lotz[1,4], Florian Alt[3], Albrecht Schmidt[2], and Isabell Welpe[4]

[1] Center for Digital Technology and Management (CDTM), Germany
froehlich@cdtm.de
[2] Ludwig Maximilian Universität, Germany
[3] University of the Bundeswehr Munich, Germany
[4] Technical University of Munich, Germany

Abstract. Blockchain technology is believed to have a potential for innovation comparable to the early internet. However, it is difficult to understand, learn, and use. A particular challenge for teaching software engineering of blockchain applications is identifying suitable use cases: When does a decentralized application running on smart contracts offer advantages over a classic distributed software architecture? This question extends the realms of software engineering and connects to fundamental economic aspects of ownership and incentive systems. The lack of usability of today's blockchain applications indicates that often applications without a clear advantage are developed. At the same time, there exists little information for educators on how to teach applied blockchain application development. We argue that an interdisciplinary teaching approach can address these issues and equip the next generation of blockchain developers with the skills and entrepreneurial mindset to build valuable and usable products. To this end, we developed, conducted, and evaluated an interdisciplinary capstone-like course grounded in the design sprint method with N=11 graduate students. Our pre-/post evaluation indicates high efficacy: Participants improved across all measured learning dimensions, particularly use-case identification and blockchain prototyping in teams. We contribute the syllabus, a detailed evaluation, and lessons learned for educators.

Keywords: blockchain application development, design sprint, capstone course, interdisciplinary, case study

1 Introduction

Cryptocurrency and blockchain technology has gauged the interest of researchers and practitioners alike. Over 65 million Bitcoin wallets [2], and over 15.500 cryptocurrencies [6] exist. Ongoing development efforts aim to advance blockchain technology further. Smart-contract blockchains established themselves among

the most active projects – e.g. Ethereum, Solana, Cardano, and Polkadot list among the ten highest-valued projects [6]. Supporters view the technology as transformative [8] and data from Coinbase's shareholder letter indicates growth rates comparable to internet user adoption in 1998 [5]. Particularly the ability to *read, write and own* is perceived as a paradigm shift enabling a new generation of internet applications, and with it, the so-called *Web3* [1].

However, research from the field of Human-Computer-Interaction (HCI) reveals that existing blockchain applications suffer from usability issues (e.g [11–13, 17, 34]), are difficult to understand [12], and home to frequent misconceptions [23]. One cause for this is that many blockchain applications address use-cases that do not derive clear advantages for the user from using blockchain technology. While scholars in software engineering have started exploring concepts for education (see e.g. Xu et al. [35] and Labouseur et al. [21]), we argue that an interdisciplinary approach is necessary to address these issues. For the next generation of blockchain developers to be able to truly build valuable and usable products, they need to be able to evaluate blockchain use-cases w.r.t technical feasibility (engineering), value-creation (entrepreneurship), and user experience (human-computer-interaction).

To address this gap, we developed, conducted, and evaluated an interdisciplinary capstone-like course with N=11 graduate students. During a 5-day period, the participants ideated, developed, implemented, and deployed a smart-contract trading-card game, allowing users to collect and trade researchers as non-fungible tokens (NFT). The course curricula builds on the design sprint framework [19]. It is, to our knowledge, the first course combining blockchain application development in an interdisciplinary setting. Our evaluation shows that the course is well-perceived by participants and enables participants to distinguish use cases (not) suited for the technology. We distill lessons learned for educators and discuss the benefits and advantages of an interdisciplinary approach to teaching.

2 Background & Related Work

Our work draws from several strands of research, most notably from design sprint methodology as framework for designing our course.

2.1 The Potential of Blockchain and Web3

Together with Bitcoin [25] the world was introduced to the technology powering it – the blockchain – in 2008. Since then developer activity has been steadily growing [7] and many projects were started to improve the original design. Ethereum, started in 2013 was the first blockchain that enabled the development of decentralized smart contracts [3]. Newer projects – e.g. Cosmos, Solana, Polkadot – have come forward to overcome Ethereum's limitations, particularly speed and transaction throughput. This new generation of blockchains, providing transactions at instant speed and low transaction costs, is believed to bring

along the third stage of the web: Web 1.0 offered internet users the possibility to *read* content. Web 2.0 added the possibility to *write*, enabling rich interactive internet applications. Web3 now adds the possibility to *own* digital assets on the internet. Practitioners believe this read-write-own paradigm will enable a new class of internet applications with a sizable potential for innovation [1, 13].

2.2 Blockchain Applications and Their Usability

Cryptocurrencies and blockchain started to become a topic of increasing interest in the research community [13]. A recent literature review, reveals that the usability of blockchain and cryptocurrency applications was shown to be problematic [13]. Users face many threats [10], cryptocurrencies are hard to understand, and misconceptions (e.g. keys, fees, and anonymity) are common [14, 23]. Even though onboarding can support users' meaning-making process [11], first-time users struggle with the complexity of the technology [12]. Particular the identification of use-cases in which blockchain can truly provide value seems to be difficult [15]. Trying to address this, there are some approaches outside the university context trying to engage laymen in participatory design activities [18,29,31]. While other technology domains have been exploring novel teaching concepts spanning across disciplines (e.g. Kopeć et al. presented insights from a VR hackathon [20]) we did not find any for blockchain.

2.3 The Design Sprint Framework

To develop our course we used the design sprint framework as a theoretical basis [19]. Related to design thinking [30], it formalizes a user-centered product development process. While design thinking does not define clear boundaries with regards to resources and time [32], the design sprint framework integrates the different aspects of design thinking into a five day program. One sprint is composed of five phases – map, sketch, decide, prototype and test – each completed in one day [19]. We identified a few research publications using the framework at university, however, non related to blockchain. Sarooghi et al. propose the design sprint as process model to integrate design thinking into entrepreneurship education [33]. Larusdottir et al. present the a two-week long user-centered design course [22] and highlight the importance of balancing "talking and doing". Sari and Zulaikha adopted the framework to include more prototype development time in UX design courses and evaluated the approach in a longitudinal study [32].

2.4 Summary

Blockchain technology, particularly smart contract development in the context of Web3, offers the potential to build new types of applications surrounding the notion of ownership. While research has started to explore blockchain teaching, no teaching concepts integrating software engineering, entrepreneurial thinking,

and user-centric methods have been reported so far. This is problematic as use-case identification for blockchain applications is a core challenge that requires a multidisciplinary perspective. The design sprint framework offers a starting point to integrate these aspects and design a blockchain application development course at university-level that equips students with the skills to create both useful and usable blockchain applications in the future.

3 Course Description

Our goal was to integrate technical, entrepreneurial, and human-centered elements into an applied blockchain application development course in an effort to enable students to identify problems and find valuable solutions. The resulting course heavily relies on collaboration and interaction between students of different disciplines, with the objective to empower participating students to:

- identify and evaluate use cases for blockchain applications
- apply user-centered methods to define product requirements
- prototype and develop a functional decentralized application

The course differs from typical software engineering courses in its focus on interaction and collaboration between disciplines. It differs from typical hackathon formats by providing a structured syllabus providing guidance throughout the course.

Fig. 1. We present a case study of an interdisciplinary course on blockchain and smart contract application development at a German university. The image shows impressions of the course (left) and of final presentation (right).

We used the design sprint [19] as theoretical starting point to design the course. We added a kickoff session two weeks prior to its start, in which participants were introduced to the blockchain, were assigned into teams, and received homework assignments. The second phase was a 5-day-long hackathon-like course adapting the design sprint method which finished with the public launch of the prototype. Figure 1 provides impression of the course (printed with permission of the participants).

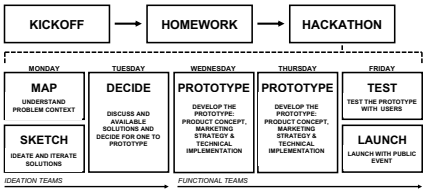


Fig. 2. The procedure of the overall course and the hackathon-week based on the design sprint framework.

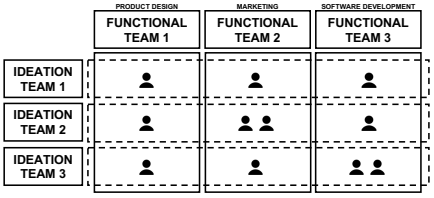


Fig. 3. The team assignment: At the kick-off each participant is assigned to one functional and one ideation team.

3.1 Participants & Team Assignment

We recruited N=11 graduate students at our university. The syllabus was shared in advance for interested students to sign up and receive 2 ECTS for successful participation. We did not require participants to have prior knowledge about blockchain. The final sample consisted of four students enrolled in computer science or data science majors and four business administration majors. The average age was 24 years. One participant identified as female, ten as male.

At the kickoff, participants were assigned to *functional teams* (product design, marketing, software development) based on educational background and personal preference. The most experienced student in each functional team was selected as team-lead to organize communication between teams. To evaluate use cases, participants were additionally assigned to cross-functional *ideation teams*, each responsible to cover a different problem space (c.f. Fig. 3).

3.2 Course Structure & Procedure

The structure of the course is inspired by the design sprint framework [19], which defines a 5-day process for user-centered prototype development. We adapted the original method to fit our educational goals: We introduced a kickoff event and an up-front homework assignment, combined the *map* and *sketch* stages into one day to accommodate an additional *prototyping* day, and launched a functional prototype at the end of the week (c.f. Fig 2).

1. **Kickoff Workshop:** Participants were introduced to the course structure and received an introductory lecture about blockchain. In a moderated session they ideated for broad problem spaces addressable with blockchain in the "university" context. The final clusters were each assigned to one ideation team for further evaluation as homework assignments.
2. **Homework Assignment:** Each ideation team had to evaluate and prepare three cluster-specific problems addressable with blockchain. Additionally, each functional team had to prepare a presentation on state-of-the-art product design, marketing, or software development approaches for blockchain. Hence, the homework integrated the *map* phase of the design sprint.
3. **Design Sprint Hackathon:** The hackathon took place between October 11th and 15th 2021. During the first two days, participants worked primarily

in their ideation teams. Once prototyping started on day three, teams organized primarily around their functions, albeit collaborated flexibly when necessary. Each day stand-up meetings were held before lunch and dinner. A backlog of tasks was tracked with sticky notes. As support five experts from industry and academia were accessible throughout the week.

(a) **Monday – Map and Sketch:** The functional teams generated a task backlog for the week. The ideation teams presented their ideas and used the day to evaluate and decide on three candidate ideas by the evening.
(b) **Tuesday – Decide:** The ideation teams further detailed the ideas. In functional team meetings ideas were evaluated w.r.t. feasibility and impact. After feedback from industry experts, the final idea was selected.
(c) **Wednesday – Prototype:** Organized by functional teams, participants started product design, partner acquisition, and prototype development.
(d) **Thursday – Prototype:** In addition to the ongoing development user testing of the early prototype and preparation of the launch event started.
(e) **Friday – Test and Launch:** The prototype was tested, finalized, deployed, and launched. The hackathon concluded with a demonstration of the functional prototype in front of an in-person and livestream audience.

4 Results & Evaluation

In total 11 graduate students participated in the course. 55% participated in a blockchain related course at university before, two in a blockchain hackathon. 73% participants owned one or several cryptocurrencies. Participants rated their interest in blockchain technology with ideological aspects (mean 4.455), followed by technological curiosity (mean 4.364), and financial opportunities (mean 3.636). For example, P6 stated: "*I am interested in blockchain because I'm always curious about new technologies and trying to see what benefits they can bring*".

4.1 Developed Blockchain Application

Over the course of the week, the students narrowed their idea pool from initially nine down to one final idea and implemented it. Figure 4 shows two screenshots of the final prototype: *Profini*, "The Professors' Panini", is a card trading platform inspired by the children trading game. It features university professors and researchers as tradable NFT cards. The idea arose from the increasing distance participants felt between professors and students as university education became virtual during the COVID-19 pandemic. The cards are meant to humanize the academic faculty, increase their visibility, and foster interaction with students. The prototype implemented the trading card logic in a smart contract, deployed on the Polygon blockchain [27]. The frontend uses ReactJS [9] and integrates with web3.js [4] to access the smart contract. The prototype was launched with a public event at the final day with in-person attendance and via livestream. In total 25 researchers could be collected at launch. By connecting a Metamask [24] wallet on the website users could purchase booster packs, each containing three random cards. Owned cards can be sent directly to other wallets or traded on marketplaces such as OpenSea [26].

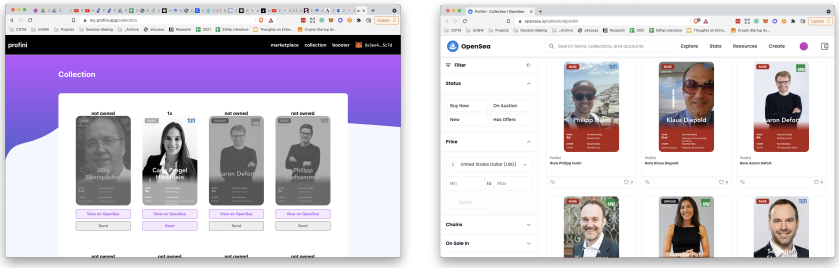


Fig. 4. Screenshots of the final prototype – *Profini*. The web application (left) showing available and owned NFT trading cards after connecting the Metamask wallet. Owned trading cards can be traded on Opensea (right).

4.2 Learning Outcomes

To evaluate the educational impact we conducted a pre-/post assessment. Numerical values were collected on Likert-Scales from 1 (Totally Disagree) to 5 (Totally Agree). We introduced the questionnaires before the start of the week and the day after its completion. The first questionnaire also collected demographics, previous experience, interest in the blockchain space, and motivation to participate in the course. The second questionnaire also evaluated participants' overall perception of the course. Both evaluated the following dimensions:

1. perceived potential of blockchain technology
2. perceived difficulty to engage with blockchain technology
3. perceived skills and abilities related to blockchain application development
4. perceived intention to engage with blockchain technology in the future

Perception of Blockchain The course had a measurable effect on the students' perception of blockchain technology. Table 1 and 2 provide an overview. After the course participants were on average more convinced that blockchain will have a positive societal impact (+0.273), less doubtful of its technological potential (-0.364), and more confident about its future adoption (+0.818). The course also had the desired effect on the perceived difficulty to use (-0.364), learn (-0.091), and prototype with (-0.455) blockchain technology.

Table 1. The perceived perceived potential of blockchain technology before and after the course.

measure	Pre	Post	Change
positive_impact_on_society	3.909	4.182	+0.273
limited_technological_potential	2.818	2.455	−0.364
future_use_by_everyone	3.727	4.545	+0.818

Table 2. The perceived difficulty to use, learn, and interact with blockchain technology before and after the course.

measure	Pre	Post	Change
difficult_to_use	3.636	3.273	−0.364
difficult_to_learn	3.273	3.182	−0.091
difficult_to_prototype_with	3.273	2.818	−0.455

Skills and Abilities We evaluated nine skills and abilities around blockchain use and development. Along all of them the course had a positive impact, though some improved more than others. Table 3 provides an overview. While general tasks (create and use wallet, send and receive cryptocurrency, interact with dapps, find learning resources) were rated rather high to begin with, they showed improvement driven by learnings from the less experienced participants. While participants' confidence to identify suitable use cases for blockchain technology increased by 0.455 points, they felt even more confident (+0.909) to spot those use cases where blockchain would not bring benefits. Students' confidence to prototype with blockchain on their own remained the lowest score before and after the course (2.818 and 2.909) while their confidence to prototype with a team increased by 0.455 points to 4.273.

Future Engagement After the course students felt motivated to continue interacting with the technology. Table 4 provides an overview. There is a notable increase (+0.455) in the intention of students to engage with online blockchain communities. The intention to buy cryptocurrencies (+0.273), interact with smart contracts and Web3 applications (+0.273), and enroll in further blockchain education (+0.182) increased less pronounced.

Table 3. The self-rated skills & abilities related to blockchain application development before and after the course.

measure	Pre	Post	Change
explain_blockchain	4.000	4.364	+0.364
create_wallet_and_buy	4.636	5.000	+0.364
send_and_receive_crypto	4.636	5.000	+0.364
interact_with_dapps	4.182	4.818	+0.636
eval_suitable_use_cases	3.818	4.273	+0.455
eval_nonsuitable_use_cases	3.636	4.545	+0.909
find_learning_resources	4.364	4.455	+0.091
prototype_alone	2.818	2.909	+0.091
prototype_with_team	3.818	4.273	+0.455

Table 4. Questions about planned future interaction with different blockchain related aspects before and after the course.

measure	Pre	Post	Change
engage_blockchain_com	3.636	4.091	+0.455
enroll_in_blockchain_edu	4.182	4.364	+0.182
buy_cryptocurrency	4.545	4.818	+0.273
interact_with_web3	4.545	4.818	+0.273

4.3 Overall Course Evaluation & Student Perception

To understand participants' experiences we asked several questions about the overall course perception in the post-course questionnaire. To quantify their overall perception of the course, we asked them to indicate on a scale from 1 to 10, "*If we offered this course again, how likely would it be that you recommended it to your friends?*". The Net Promotor Score (NPS) [16] calculated from their answers is 81.818, which can be considered "world-class" [28]. To elicit qualitative feedback we asked two open questions, "*What are the main learnings for yourself?*", and "*If there was one thing you could change, what would it be?*". The reported learnings turned out to be quite unique to each participant. They included technical aspect (i.e. how to develop a smart contract), use-case specific

aspects (i.e. when it makes sense to decentralize), method related (how to use user story maps), or process related (how important communication between teams is). There was, however, a clear indication what participants would like to change. Seven participants (63%) suggested to re-allocate one day from the earlier ideation phases to prototyping and implementation.

5 Discussion

Our study set out to shed light on whether an interdisciplinary course would be an appropriate format to teach university students about blockchain application development. We found that the design sprint framework offers a sound theoretical underpinning for creating such a course. Our assessment further indicates a high efficacy of the approach: Across all measured learning dimensions participants' perception improved.

5.1 Educational Impact

Our evaluation shows a positive educational impact of the course across all measured dimensions. Particularly, teaching goals that benefit from interdisciplinary exchanges – e.g. prototyping with a team (+0.455), identifying suitable (+0.455), and identifying not suitable (+0.909) use cases – improved substantially. We attribute much of the learning effects to the applied and interdisciplinary environment created by the course structure. Provided with autonomy, equipped with diverse skills and abilities, and different degrees of knowledge on blockchain technology, students were encouraged to quickly learn from and teach one another. As such, they were required to collaborate closely to solve problems together and compromise with one another to overcome conflicting viewpoints. These results are naturally limited by the small sample and the study design. Future research should evaluate the impact at larger samples, over longer time, and with appropriate control groups. Nonetheless, we believe that the syllabus and evaluation are valuable for educators to design applied blockchain education in the future. Beyond blockchain, our case study shows that the design sprint method is a useful framework for creating applied teaching concepts bridging gaps between disciplines.

5.2 Lessons learned

We share four key lessons learned from the field study:

1. **Diverging from the traditional design sprint timeline can increase sense of achievement.** While the design sprint provided a good theoretical basis to design the course, in future we would allocate more time to the development of the prototype to give students the opportunity to engage with the technology in more depth. To enable a sense of achievement we recommend to aim at creating a functional prototype by the end of the week

and have participants organize a launch event around it. To allow for more time for the actual development, we suggest to conduct the *map* step entirely before the start of the week and begin implementation one day earlier.

2. **Interdisciplinary team compositions can promote a more holistic understanding.** We observed a beneficial effect of students being from different study programs, as their diverse experiences fostered discussion, collaboration, and facilitated a more holistic understanding. The course empowered students in their skills and abilities to explain blockchain (+0.364), create a wallet and buy crypto (+0.362) or interact with dapps (+0.636). We believe that the exchange within an interdisciplinary peer group was a significant factor for the positive development, as the wide range of knowledge fostered a broader understanding of blockchain through peer-learning.
3. **Domain constraints can provide necessary focus for use-case ideation.** Restricting the initial brainstorming to the university context was an important frame to guide students' ideas. This constraint allowed students to focus their ideation and allowed practicing to differentiate useful use cases (+0.455) from not useful use cases (+0.909) in a specific domain rather than on a theoretical level. Ideally, contextual constraints are set beforehand by the organizers, for which some experience with both the domain and the technology is beneficial.
4. **Decision autonomy can enable joint problem solving.** As organizers, we took on a moderating role – managing the process and refraining from engaging in decisions. The respective teams entirely owned goal setting, project management, and direction of their product. This autonomy enabled active discussions and empowered students to learn from and teach one another to overcome challenges. As a result, students felt more comfortable prototyping with blockchain. Yet, the effect was greater for prototyping with team (+0.455) as opposed to prototyping alone (+0.091), which supports our idea of joint problem solving being valuable.

6 Conclusion

This work contributes (1) the syllabus of an interdisciplinary blockchain application development course integrating engineering, entrepreneurial, and user-centered elements, (2) a detailed evaluation of its learning outcomes, (3) and lessons-learned for educators. We found that the design sprint framework offers a sound theoretical underpinning for creating such a course. Our assessment further indicates a high efficacy of the approach: Across all measured learning dimensions participants' perceptions improved. We report the syllabus of the course for other educators to benefit from it and discuss lessons learned for future iterations. We believe that the course design can serve as a blueprint to run engaging practice-oriented courses on blockchain application development. For the wider community of engineering educators, the course can be adapted to different engineering contexts (e.g. artificial intelligence) integrating technology education with entrepreneurial thinking.

References

1. Benet, J.: What exactly is web3? by juan benet at web3 summit 2018 (video) (oct 2018), https://youtu.be/l44z35vabvA
2. de Best, R.: Number of Blockchain wallet users worldwide from November 2011 to January 24, 2021 (Jan 2021), https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/
3. Buterin, V., et al.: Ethereum white paper. GitHub repository 1, 22–23 (2013)
4. ChainSafe: ChainSafe/web3.js (Dec 2021), https://github.com/ChainSafe/web3.js
5. Coinbase: Coinbase Third Quarter 2021 Shareholder Letter (09 2021), https://s27.q4cdn.com/397450999/files/doc_financials/2021/q3/Coinbase-Q321-Shareholder-Letter.pdf, (last accessed: 2021-12-13)
6. Coinmarketcap: Top 100 Cryptocurrencies by Market Capitalization (Dec 2021), https://coinmarketcap.com/
7. Dixon, C., Lazzarin, E.: The Crypto Price-Innovation Cycle (May 2020), https://a16z.com/2020/05/15/the-crypto-price-innovation-cycle/
8. Elsden, C., Manohar, A., Briggs, J., Harding, M., Speed, C., Vines, J.: Making sense of blockchain applications: A typology for hci. CHI '18, ACM (2018), https://doi.org/10.1145/3173574.3174032
9. Facebook Inc.: React (Dec 2021), https://reactjs.org/
10. Froehlich, M., Hulm, P., Alt, F.: Under pressure. a user-centered threat model for cryptocurrency owners. ICBTA 2021, ACM (2021), https://doi.org/10.1145/3510487.3510494
11. Froehlich, M., Kobiella, C., Schmidt, A., Alt, F.: Is it better with onboarding? improving first-time cryptocurrency app experiences. DIS '21, ACM (2021), https://doi.org/10.1145/3461778.3462047
12. Froehlich, M., Wagenhaus, M.R., Schmidt, A., Alt, F.: Don't stop me now! exploring challenges of first-time cryptocurrency users. DIS '21, ACM (2021), https://doi.org/10.1145/3461778.3462071
13. Froehlich, M., Waltenberger, F., Trotter, L., Alt, F., Schmidt, A.: Blockchain and cryptocurrency in human computer interaction: A systematic literature review and research agenda. DIS '22, ACM (2022), https://doi.org/10.1145/3532106.3533478
14. Fröhlich, M., Gutjahr, F., Alt, F.: Don't lose your coin! investigating security practices of cryptocurrency users. DIS '20, ACM (2020), https://doi.org/10.1145/3357236.3395535
15. Graham, W.: Building it better: A simple guide to blockchain use cases (feb 2018), https://medium.com/blockchain-at-berkeley/building-it-better-a-simple-guide-to-blockchain-use-cases-de494a8f5b60
16. Grisaffe, D.B.: Questions about the ultimate question: conceptual considerations in evaluating reichheld's net promoter score (nps). Journal of Consumer Satisfaction, Dissatisfaction and Complaining Behavior 20, 36 (2007)
17. Huebner, J., Frey, R.M., Ammendola, C., Fleisch, E., Ilic, A.: What people like in mobile finance apps: An analysis of user reviews. MUM 2018, ACM (2018), https://doi.org/10.1145/3282894.3282895
18. Khairuddin, I.E., Sas, C., Speed, C.: Blockit: A physical kit for materializing and designing for blockchain infrastructure. DIS '19, ACM (2019), https://doi.org/10.1145/3322276.3322370
19. Knapp, J., Zeratsky, J., Kowitz, B.: Sprint: How to solve big problems and test new ideas in just five days. Simon and Schuster (2016)

20. Kopeć, W., Kalinowski, K., Kornacka, M., Skorupska, K.H., Paluch, J., Jaskulska, A., Pochwatko, G., Możaryn, J.F., Kobyliński, P., Gago, P.: VR Hackathon with Goethe Institute: Lessons Learned from Organizing a Transdisciplinary VR Hackathon. CHI EA '21, ACM (2021), https://doi.org/10.1145/3411763.3443432
21. Labouseur, A.G., Johnson, M., Magnusson, T.: Demystifying blockchain by teaching it in computer science: Adventures in essence, accidents, and data structures. J. Comput. Sci. Coll. 34(6), 43–56 (apr 2019)
22. Larusdottir, M., Roto, V., Stage, J., Lucero, A., Šmorgun, I.: Balance talking and doing! using google design sprint to enhance an intensive ucd course. pp. 95–113. Springer International Publishing (2019)
23. Mai, A., Pfeffer, K., Gusenbauer, M., Weippl, E., Krombholz, K.: User mental models of cryptocurrency systems-a grounded theory approach (2020)
24. MetaMask – A ConsenSys Formation: MetaMask - A crypto wallet & gateway to blockchain apps (Dec 2021), https://metamask.io/
25. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. bitcoin.org (2008)
26. Ozone Networks, Inc: OpenSea, the largest NFT marketplace (Dec 2021), https://opensea.io/
27. Polygon Technology: Polygon (Dec 2021), https://polygon.technology/
28. Qualtrics: What is a good Net Promoter Score? (Dec 2021), https://www.qualtrics.com/uk/experience-management/customer/good-net-promoter-score/
29. Rankin, J., Elsden, C., Sibbald, I., Stevenson, A., Vines, J., Speed, C.: Pizzablock: Designing artefacts and roleplay to understand decentralised identity management systems. DIS '20, ACM (2020), https://doi.org/10.1145/3357236.3395568
30. Razzouk, R., Shute, V.: What is design thinking and why is it important? Review of Educational Research 82(3), 330–348 (2012), https://doi.org/10.3102/0034654312457429
31. Sanders, S.P., Sanders, G.L.: The blockchain art simulation (barts) and experiential exercises. ITiCSE '21, ACM (2021), https://doi.org/10.1145/3456565.3460038
32. Sari, E., Zulaikha, E.: Disrupting Tertiary User-Centered Design Course with Design Thinking 2.0. ACM (2021), https://doi.org/10.1145/3429360.3468178
33. Sarooghi, H., Sunny, S., Hornsby, J., Fernhaber, S.: Design thinking and entrepreneurship education: Where are we, and what are the possibilities? Journal of Small Business Management 57, 78–93 (2019)
34. Voskobojnikov, A., Wiese, O., Mehrabi Koushki, M., Roth, V., Beznosov, K.K.: The U in Crypto Stands for Usable: An Empirical Study of User Experience with Mobile Cryptocurrency Wallets. CHI '21, ACM (2021), https://doi.org/10.1145/3411764.3445407
35. Xu, K., Wang, Z., Guo, F.: The "four-level guidance" blockchain practice teaching model for undergraduate. ICIEI 2021, ACM (2021), https://doi.org/10.1145/3470716.3470722

APPENDIX: EIDESSTATTLICHE VERSICHERUNG

Eidesstattliche Versicherung

(Siehe Promotionsordnung vom 12.07.11, § 8, Abs. 2 Pkt. 5)

Hiermit erkläre ich an Eidesstatt, dass die Dissertation von mir selbstständig und ohne unerlaubte Beihilfe angefertigt wurde.

München, den 18.10.2022

Michael Fröhlich