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: 19.12.2022

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 zukünfitgen 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).

[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).

[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).

[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).

[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).

[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).

[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).

[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).

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.

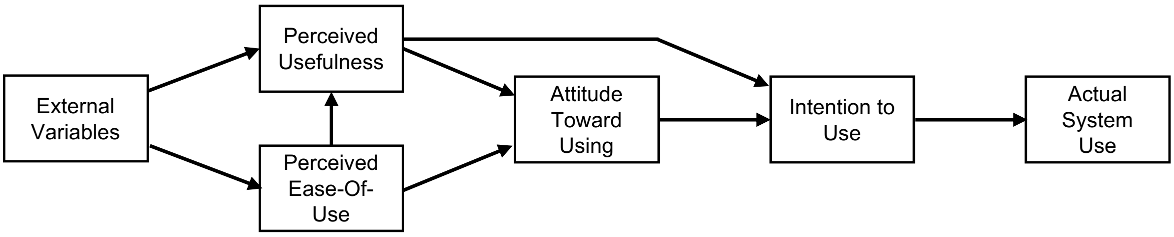


Figure 1.1: The original Technology Acceptance Model (TAM). (Figure adapted from [33], p. 4)

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.

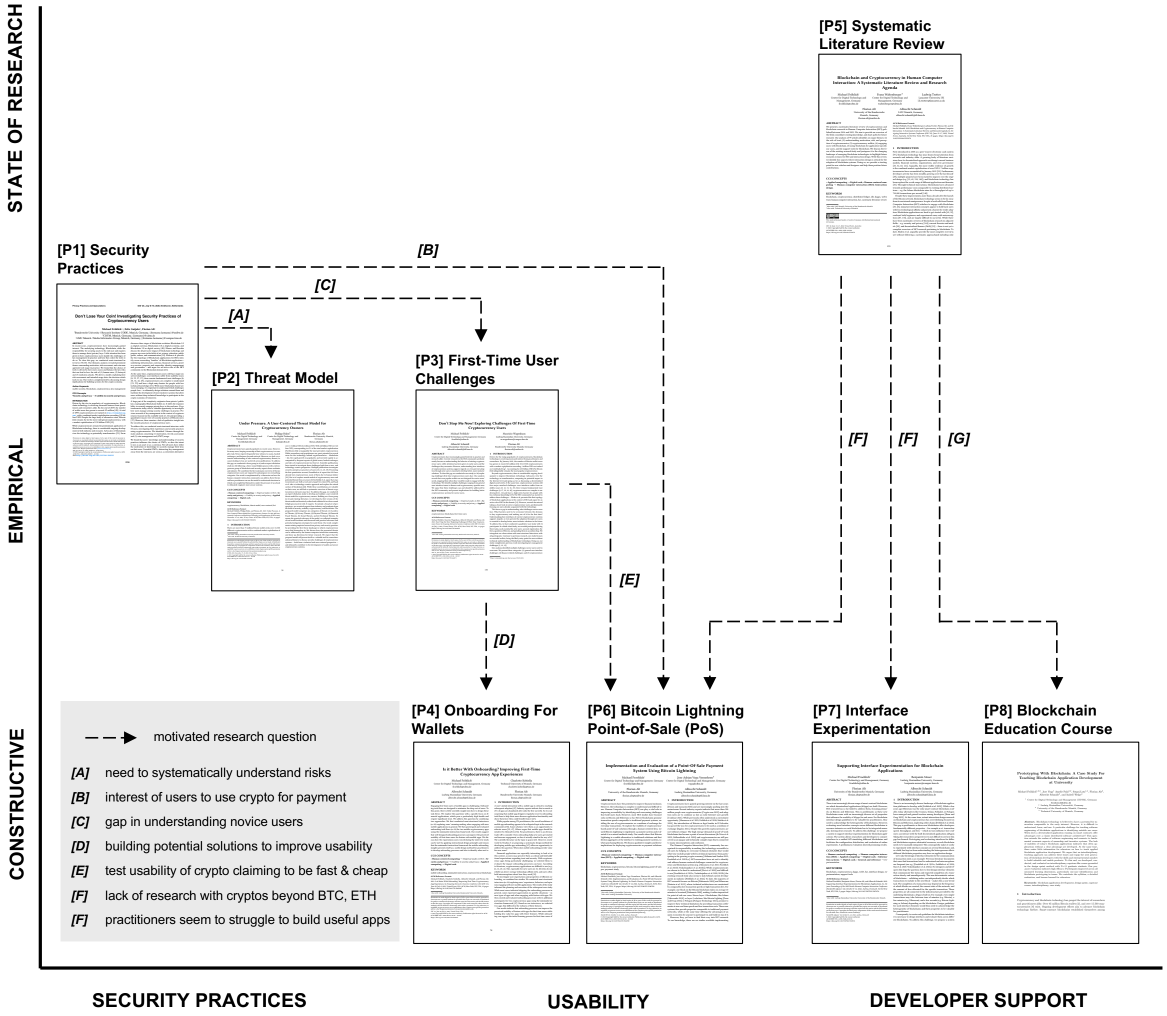

STATE OF RESEARCH
EMPIRICAL
CONSTRUCTIVE
[P5] Systematic Literature Review
[P1] Security Practices
[B]
[C]
[A]
[P2] Threat Model
[P3] First-Time User Challenges
[F]
[F]
[G]
[E]
[D]
motivated research question
[A] need to systematically understand risks
[B] interest of users to use crypto for payment
[C] gap in understanding novice users
[D] building potential solutions to improve usability
[E] test usability of crypto claiming to be fast & cheap
[F] lack of research with cryptos beyond BTC, ETH
[F] practitioners seem to struggle to build useful apps
[P4] Onboarding For Wallets
[P6] Bitcoin Lightning Point-of-Sale (PoS)
[P7] Interface Experimentation
[P8] Blockchain Education Course
SECURITY PRACTICES
USABILITY
DEVELOPER SUPPORT

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

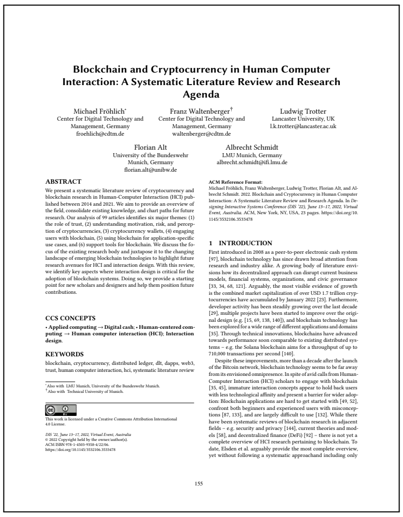
3.1 A Review of Cryptocurrency Research in Human-Computer Interaction

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

Summary: This paper contributes an overview of existing blockchain and cryptocurrency research in Human-Computer Interaction and discusses promising avenues for future research. The motivation for this paper emerged from reflections on a missing overview of design challenges for blockchain and cryptocurrency applications over the course of the dissertation. While this article was published towards the end of the dissertation the underlying research questions and the identified gaps in the body of existing literature influenced many of the publications published chronologically earlier. With this article our objective was to provide new scholars a starting point to understand the research field and help them position future contributions.



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
© 2022 Copyright held by the owner/author(s).
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

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.

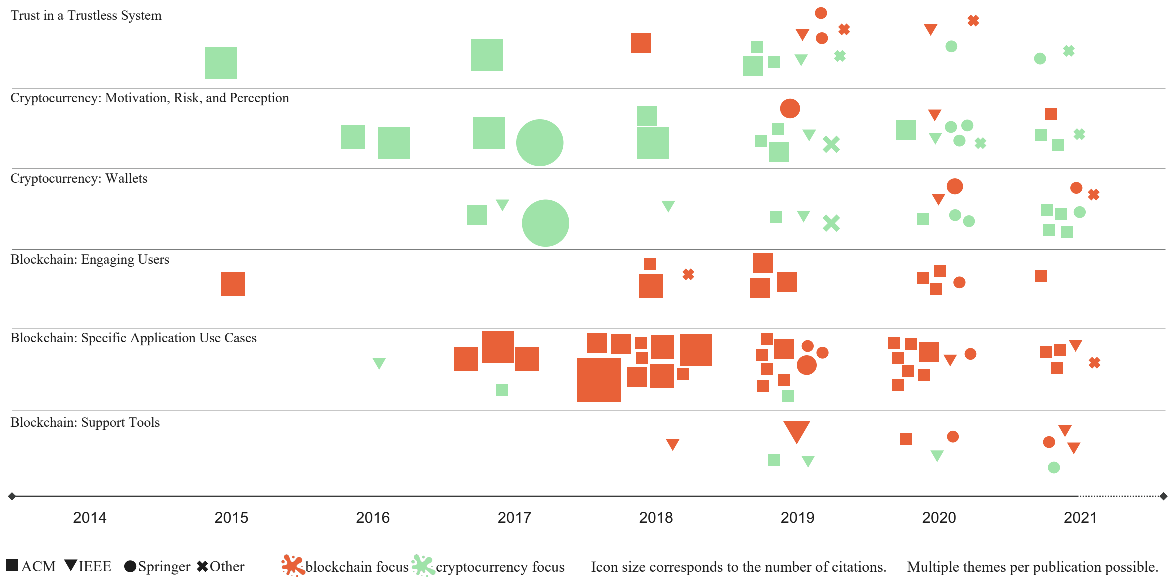


Figure 3.1: Overview of HCI research 2014 – 2021 by theme. (Originally published in [P5], p. 5)

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:

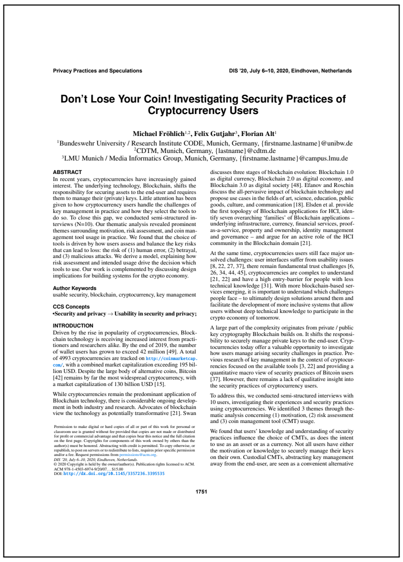
RQ2: "*How do users interact with cryptocurrency and blockchain systems and what implications arise from that?*"

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.

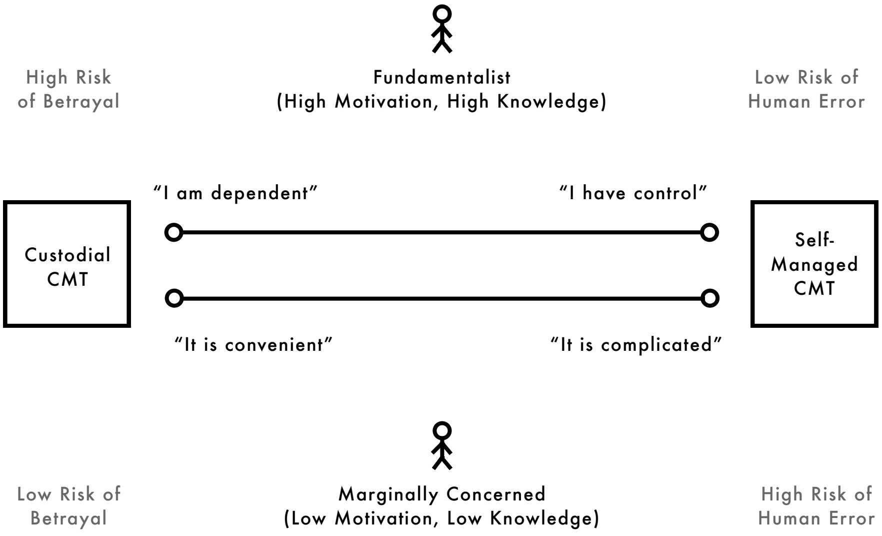


Figure 3.2: Conceptual model showing how security personas and individual risk assessment influence users' choice of Coin Management Tools (CMT). (Originally published in [P1], p. 8)

[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.

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.

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,.

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.
ICBTA 2021, December 17–19, 2021, Xi'an, China
© 2021 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-8746-0/21/12…$15.00
https://doi.org/10.1145/3510487.3510494

39

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.

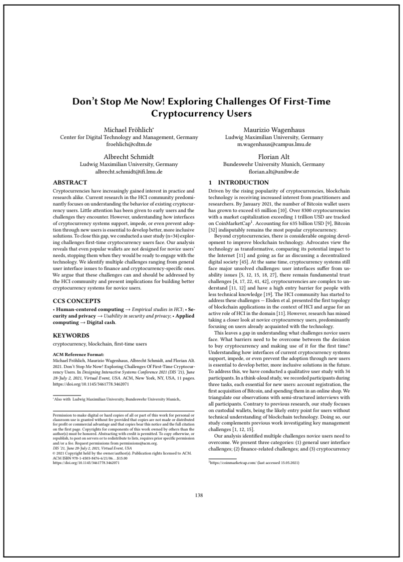
3.2.2 Challenges of New Users

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,.

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

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,.

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/10.1145/3461778.3462047

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.

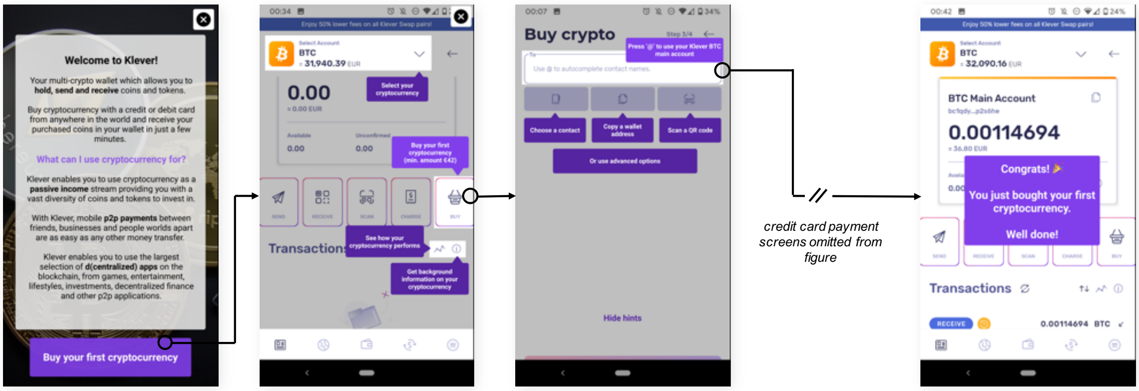
Our results indicate that onboarding processes can improve the perceived usability of feature-rich apps for first-time users while holding less value for apps with fewer features. While onboarding can support the initial learning process for first-time users of

78

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.



Welcome to Klever!

Your multi-crypto wallet which allows you to **hold, send and receive** coins and tokens.

Buy cryptocurrency with a credit or debit card from anywhere in the world and receive your purchased coins in your wallet in just a few minutes.

What can I use cryptocurrency for?

Klever enables you to use cryptocurrency as a **passive income** stream providing you with a vast diversity of coins and tokens to invest in.

With Klever, mobile **p2p payments** between friends, businesses and people worlds apart are as easy as any other money transfer.

Klever enables you to use the largest selection of **d(centralized) apps** on the blockchain, from games, entertainment, lifestyles, investments, decentralized finance and other p2p applications.

Congrats! You just bought your first cryptocurrency. Well done!

credit card payment screens omitted from figure

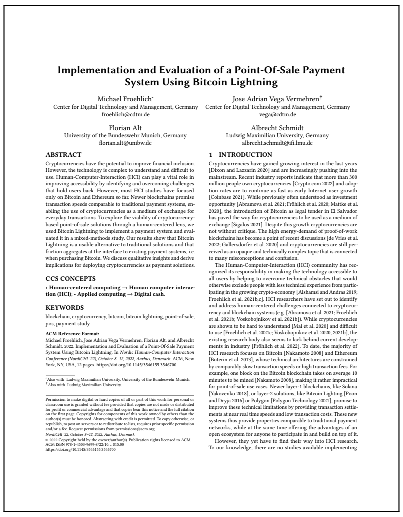
Figure 3.3: The interfaces of one prototyped onboarding process. (Originally published in [P4], p. 8)

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

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.



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.

1 INTRODUCTION

Cryptocurrencies have gained growing interest in the last years [Dixon and Lazzarin 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; Mattke 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 [Alshamsi and Andras 2019; Froehlich et al. 2021b,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; Voskobojnikov et al. 2021b]). While cryptocurrencies are shown to be hard to understand [Mai et al. 2020] and difficult to use [Froehlich et al. 2021c; Voskobojnikov et al. 2020, 2021b], the existing research body also seems to lack behind current developments 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 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 [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 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

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.

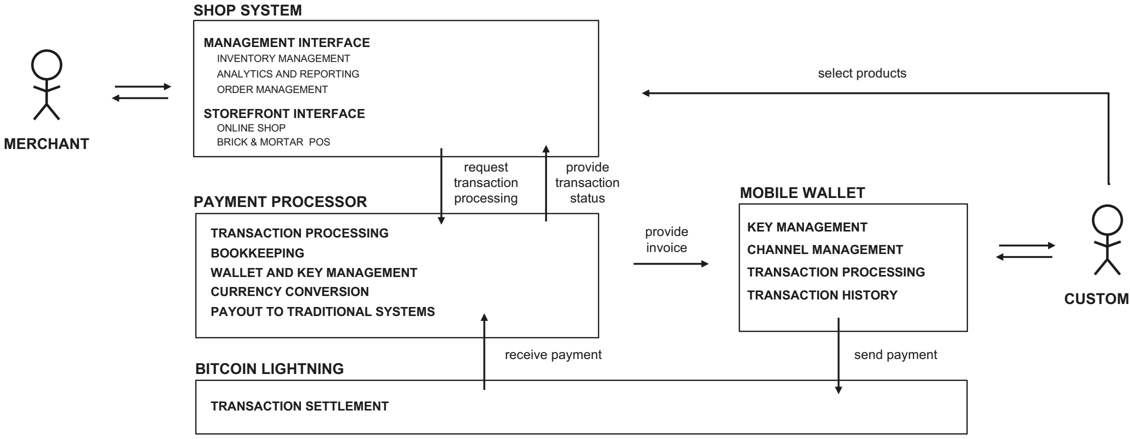


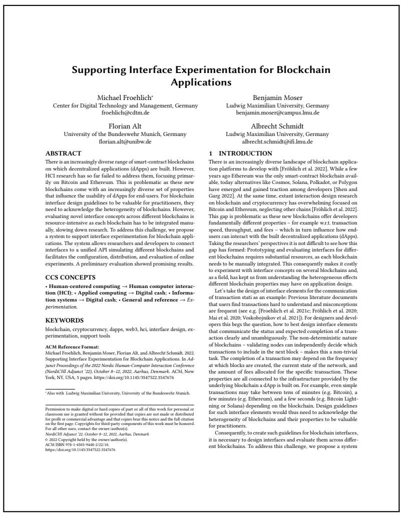
Figure 3.4: The subsystems of the proposed point-of-sale (PoS) system and their relationships to each other. (Originally published in [P6], p. 5)

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

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.

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

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.

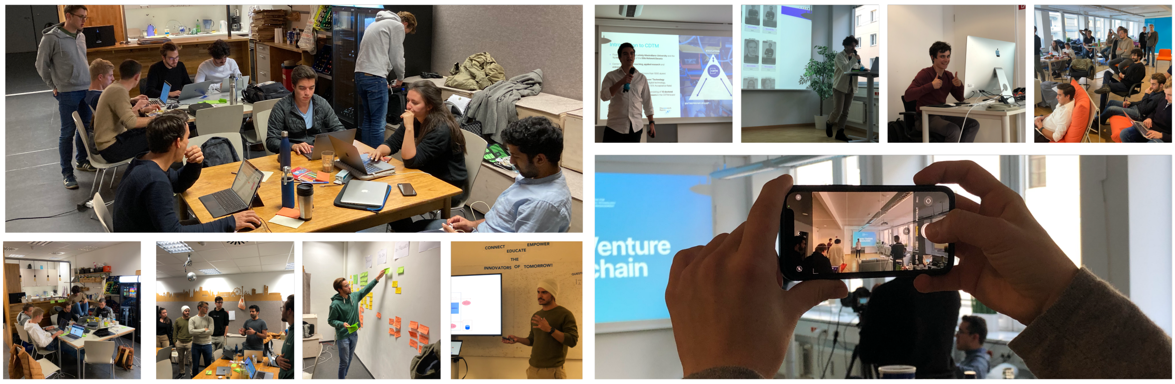


Figure 3.5: Impressions of the conducted course format. (Originally published in [P8], p. 4)

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.

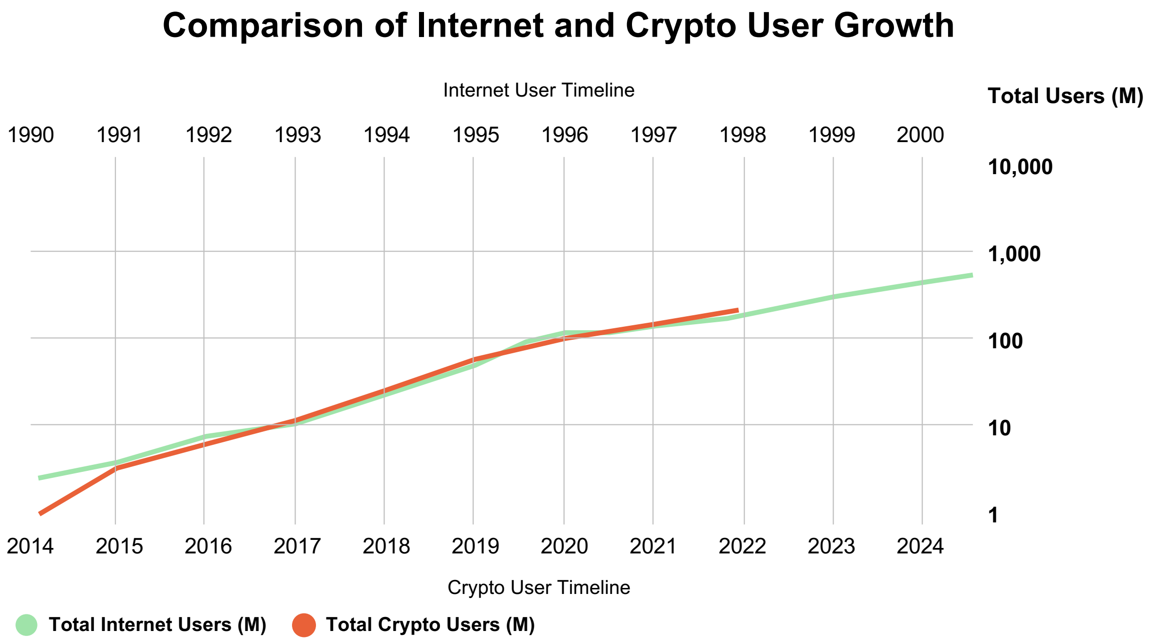


Figure adapted from: Third Quarter 2021 Shareholder Letter (Coinbase, 2021), page 3
Sources: Coinbase, World Bank, Crypto.com

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. 4, 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

Note: The original publications are provided digitally

[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).

[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).

[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).

[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).

[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).

[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).

[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).

[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 2

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