Examining User Perceptions of Stablecoins: Understandings and Risks

Yongqi Guan[1], Yaman Yu[2], Tanusree Sharma[2], Kaihua Qin[3], Yang Wang [2], Ye Wang [1]

[1]: *University of Macau, Macau, China;* [2]: *University of Illinois at Urbana-Champaign, Champaign, USA;* [3]: *Imperial College London, United Kingdom*

Abstract

Stablecoin, a type of cryptocurrency whose value is anchored to a specific asset to maintain price stability, has gained significant attention due to its rapid growth. However, research examining user perceptions of stablecoins is scarce. This study addresses this research gap by combining case analysis of various stablecoin projects and interviews with 16 participants to explore their experiences and practices. Our research uncovers user perceptions of stablecoins' roles within the blockchain ecosystem and identifies their misunderstandings about stablecoins. We also explore users' concerns regarding the security risks of stablecoins. Our findings underscore the necessity for improved user education and robust security protocols.

1 Introduction

Stablecoins, a type of cryptocurrency designed to maintain a fixed value, have grown increasingly popular in recent years and now play a crucial role in the cryptocurrency ecosystem [44]. They represent a significant part of the cryptocurrency market, with three of the top five most traded cryptocurrencies being stablecoins. This increase in popularity is underscored by the expansion of the stablecoin market, which had a market capitalization of 130 billion USD in 2023 [1].

As an important component of the blockchain ecosystem, stablecoins have attracted considerable academic attention. Studies have explored various aspects of stablecoins, such as their classifications [43,46], the mechanisms used to maintain price stability [41,42], and their effects on Bitcoin and the wider cryptocurrency markets [15,35]. However, the majority of these research studies are concentrated on investigating the technical and theoretical aspects of stablecoins, leaving a gap in our understanding from user perspectives. Given the large market capitalization and user base of stablecoins, it is critical to understand user perceptions, concerns, and experiences. Neglecting this aspect may limit our understanding of whether the current stablecoin effectively meets the needs and expectations of blockchain development. Consequently, our study sheds light on user-focused issues in the stablecoin realm, including user perceptions, their interactions with stablecoins, and the perceived security risks they associate with these digital assets. To guide our research, we pose the following research questions:

RQ1: How do users perceive and interact with stablecoins?

RQ2: What security risks do users perceive when using stablecoins?

We employed a two-stage method to understand the stablecoin ecosystem. Firstly, we analyzed nine mainstream stablecoins and conducted semi-structured interviews with 16 participants. Our investigation reveals that participants had varying levels of understanding and experience with stablecoins. They held misconceptions about stakeholder relationships and stability mechanisms. Participants identified stablecoins as risk management tools, mediums of exchange, investment assets, and payment methods. Concerns were raised about transparency and reserve insufficiency for fiat-backed stablecoins, collateral asset depreciation for crypto-backed stablecoins, and risks associated with algorithmic design for asset-less stablecoins. External risks were also highlighted, such as third-party issues and regulatory uncertainties.

Our study sheds light on the prevalent misunderstandings and risks associated with using stablecoin, providing the necessary groundwork for future research and aiding in bridging the gap between users and blockchain-related technology.

2 Background and Related Work

In this section, we first introduce the existing literature on stablecoin. Then, we review studies on the usability and security of cryptocurrency and blockchain.

2.1 Stablecoin in Blockchain

The existing literature mainly focuses on the classification of stablecoins [17, 19, 44, 46] as well as the design mechanism and the economic impact [33, 35, 42].

Most classifications are based on different collateralization mechanics. Some researchers suggest differentiating between collateralized and non-collateralized stablecoin [31, 44]. Collateral stablecoins can also be divided into legal currency collateral and cryptocurrency-backed stablecoins. Non-collateral stablecoins are algorithmically programmed on-chain to manage demand and supply autonomously [13, 19].

Apart from researching the categorization of stablecoins, another focus is how stablecoins achieve price stability. Researchers evaluate the effectiveness of stablecoin design in achieving price stability [33, 42], and often target algorithmic stablecoin [57]. Moreover, previous studies have examined the economic dynamic of stablecoin and its impact on cryptocurrency prices [16, 29]. Stablecoin issuances contribute to price discovery and market efficiency of cryptocurrencies [16].

While much research has been dedicated to the technicalities of stablecoins, there remains a conspicuous absence of studies that delve into users' perceptions of stablecoins and their functionality within the market. To bridge this knowledge gap, we center our research on the **RQ1**: *How do users perceive and interact with stablecoins?*

2.2 Usability and Security of Cryptocurrency and Blockchain

A growing body of research exists at the intersection of blockchain and human-computer interaction (HCI) [23, 27]. These studies focus on two main themes: the usability of cryptocurrency and the security challenges associated with blockchain applications.

Previous studies have conceived frameworks for understanding cryptocurrency's usability [12, 26]. These have delved into user motivations for engaging with cryptocurrencies, with a financial interest, personal liberty, curiosity about technology, and improved privacy and anonymity being key drivers [14, 18, 26, 36, 47, 50]. Cryptocurrencies and blockchain technology have found applications across diverse industries [11, 20, 24, 54], with most users managing their crypto assets using digital wallets [12].

The second theme focuses on security challenges in blockchain technology, which can be either systemically derived or human error-induced. Systemic risks can result from protocol-level disruptions, such as forking [56] and block reorganization [32, 58], causing transactional inconsistencies. Network-level threats, like Eclipse and Sybil attacks [22, 30], can fragment the network. Additionally, smart contracts are susceptible to security breaches leading to significant financial losses [28, 40, 45, 49, 52, 53]. Human-induced errors, such as lost passwords [12, 50] or mishandled key management [21, 25, 37], also present significant risks in blockchain technology usage.

Existing research on the usable security of blockchain applications remains sparse [55]. Stablecoins present distinct security challenges due to their intricate mechanisms and broad applications. Unfortunately, their usage security has not garnered much attention. To bridge this knowledge gap, we aim to understand how users perceive security challenges when using stablecoins. Consequently, we pose **RQ2**: *What security risks do users perceive when using stablecoins?*

3 Case Study on Stablecoin

Based on the market capitalization of different stablecoin types [1], we selected nine stablecoins for analysis. We classified into fiat-backed stablecoins (USDT [6], USDC [9], and BUSD [8]), crypto-backed stablecoins (DAI [5], VAI [7], and MIM [10]), and algorithmic stablecoins (AMPL [2], FEI [4], and FRAX [3]). Reviewing the whitepapers, we summarize the issuance process and ecological application scenarios for each type of stablecoin.

The most common variant of stablecoins, which has become popular among users, refers to **fiat-backed stablecoins**. They are pegged to a fiat currency such as USD. In order to maintain this peg, the fiat currency or asset is held in backup reserve to the token and is made available for direct exchange with the token at a fixed exchange rate [43]. Due to the involvement of off-chain centralized entities, it is often subject to regulatory oversight from relevant authorities. **Crypto-backed stablecoins** are backed by cryptocurrencies rather then fiat-currency [51]. Due to crypto's inherent volatility, assets are often over-collateralized. Finally, as a newer category, **algorithmic stablecoins** is not fully backed by collateral and relies upon an algorithm to maintain its 1:1 price peg. The laws of supply and demand are integral to the mechanics of this variety of stablecoin [34].

After the issuance of stablecoins, users can acquire them through exchanges and engage in various activities. Users tend to manage on-chain assets through **crypto wallets**, while for off-chain assets, they typically choose to store them on **centralized exchanges (CEXes)**. Users can also access various financial services on **decentralized exchanges (DEXes)** to earn interest, such as staking and providing liquidity.

Stablecoins have applications beyond the cryptocurrency market and are gradually used daily. For example, stablecoins can facilitate cross-border remittances, allowing people to send and receive money with lower fees and faster settlement. Online merchants also adopt stablecoins as a payment method for purchases made on their platforms.

Following a comprehensive exploration of the stablecoin ecosystem, we scrutinized the mechanisms underpinning diverse types of stablecoins alongside their expansive applications. This foundational understanding serves as the benchmark for further analyzing user perceptions and their practical

engagements with various categories of stablecoins.

4 Interview Study Method

We conducted an interview study to better understand users' knowledge and perception of stablecoin as well as users' perspectives on the security aspects associated with stablecoin usage. This study has been approved by the Institutional Review Board (IRB).

4.1 Participant Recruitment

We posted our recruitment message through online platforms, including Reddit and Discord. In addition, leveraging the research team's personal networks, we extended our recruitment efforts to individuals who personally use stablecoins. We informed users about our study procedure and data protection policy. We identified 16 eligible participants for the interview session. The interviewees' demographics are reported due to ethical considerations. The age of the participants ranged from 23 to 42 years, representing a broad spectrum of life experiences and occupational backgrounds.

4.2 Interview Protocol

From October 2022 to May 2023, we conducted semi-structured interviews with 16 participants online. Before each interview, the participants were presented with an oral consent form stating that the interviews would be recorded and that their words might be included in the final report anonymously. All interviewees agreed to this consent form before proceeding. The researchers used an interview guide to ensure consistency across all participants. The interview itself consisted of three parts.

In the first part, we gathered personal information from the interviewees, including age, occupation, and involvement with cryptocurrencies. We also discussed their cryptocurrency experiences, such as when they started buying and how they distributed their investments. The second part focused on the interviewees' experiences with stablecoins. We explored their knowledge of different types of stablecoins and how they acquired them. We also discussed situations where stablecoins proved useful. Lastly, we examined the interviewees' perceptions of risks associated with stablecoins and whether those risks affected their decision to continue using them. We also discussed their experiences and thoughts on significant crypto market events, such as the Futures Exchange (FTX) collapse [48] for users with assets deposited there.

5 Findings

Our results provide insights into users' knowledge, practices, and perceived risk on various stablecoins.

5.1 Users' Perceptions and Practices

We first compare the participants' perceptions of various types of stablecoins and examine how their practices have been influenced by these perceptions.

Diverse Perceptions of Fiat-backed Stablecoins The participants exhibited varying levels of understanding when it came to fiat-based stablecoins. Individuals with relatively limited and brief experience tend to harbor misunderstandings regarding the mechanisms of fiat-backed stablecoins. Many inexperienced users lack the knowledge to understand the importance of maintaining sufficient asset reserves for fiat-backed stablecoins to serve as reliable anchors. They often rely heavily on the operators and the large market capitalization of these stablecoins to make decisions. This reliance serves as a mental shortcut for them to mitigate risk and make choices. Some participants are aware of the credit endorsement provided by centralized institutions but lack complete knowledge of the specific details. They mistakenly believe in a cooperative association between a stablecoin operator and regulatory bodies like the SEC. Consequently, they tend to excessively trust the centralized entity and disregard operational intricacies, inadvertently exposing themselves to the risk of insufficient reserves without adopting necessary precautions.

Conversely, participants with diverse stablecoins demonstrate a more comprehensive understanding of their underlying mechanisms, yet they express negative sentiments towards centralized stablecoins. The root of their apprehensions can be traced back to the absence of transparency concerning the reserves that back fiat currencies. This lack of clarity engenders skepticism about the stability and reliability of centralized stablecoins. The opacity surrounding these reserves raises questions about the trustworthiness of such stablecoins, highlighting the need for greater transparency in their operations.

Conceptual Confusion about Decentralized Stablecoins In comparison to fiat-backed stablecoins, it is evident that participants possess significantly less understanding regarding crypto-based and algorithmic stablecoins. This knowledge gap is particularly pronounced in the case of decentralized stablecoins, with some participants not even aware of their existence and operating under the assumption that stablecoins can only be issued by centralized entities.

A subset of participants, while cognizant of the existence of crypto-based and algorithmic stablecoins, often conflate the two distinct concepts, erroneously interpreting algorithmic stablecoins as those being issued through smart contracts, such as DAI. This confusion may be attributed to the participants' limited exposure to decentralized mechanisms, which could explain their comparatively lower risk tolerance towards decentralized stablecoins. Participants commonly believe that the stability of algorithmic stablecoins depends on the confidence and support of the market. They share concerns about

the algorithms' ability to respond to significant deviations from the pegged value effectively.

Influence of Users' Knowledge on Stablecoin Practices The participants' usage of stablecoins varied based on their levels of understanding regarding how stablecoins function. Participants with higher levels of comprehension demonstrated different usage patterns compared to those with lower levels of understanding. Participants with higher levels of comprehension show a strong inclination towards utilizing stablecoins for cross-border payments and incorporating them into their daily financial transactions, such as salary payments and transactions between friends. They recognize the efficiency and potential cost savings associated with stablecoin usage. In contrast, participants with less awareness of stablecoin mechanisms tend to avoid actively using stablecoins as a means of payment in their daily lives, demonstrating a more cautious approach to adoption. While most of the participants engage in using stablecoins as investment and financial instruments, there is a notable distinction in their approach. Participants with a comprehensive understanding of stablecoin mechanisms exhibit a preference for high-yield farming applications within DeFi projects. They are more familiar with the associated risks and benefits, allowing them to navigate such platforms confidently. In contrast, participants with a lower level of understanding tend to avoid high-yield farming applications, exercising caution and potentially opting for less risky investment strategies. Hence, the lack of awareness among participants hinders their ability to make well-informed decisions and limits the applicability of stablecoins in their daily lives.

5.2 Perceived Risks & Mitigation

We provide insights into participants' perception of risks, their risk tolerance, and the countermeasures they took when dealing with stablecoins.

Perceived Risks in Stablecoin Adoption: Mechanisms & Misunderstandings Participants, predominantly holding fiat-backed stablecoins for an extended period of time demonstrate a high-risk tolerance, resulting from the belief that stablecoins would quickly return to pegged value, even in the event of a deviation. Participants hold a mix of fiat and crypto/algorithmic stablecoins but do not understand underlying mechanisms and operational differences, such as mistaking crypto-backed stablecoins, such as DAI, for algorithmic stablecoins. This can cause conceptual confusion, affecting their ability to manage risks when investing in stablecoins effectively. Another risk factor emerges from participants' inclination towards stablecoins' issuing entities with credit endorsement, favoring regulated and trusted audits, often stemming from a centralized mindset. However, relying solely on centralized audits may not address underlying risks, as the literature indicates potential exposure to mismanagement, fraud, and insufficient reserves [38]. Instances FTX and SVB bankruptcy demonstrate the impact of issuer fund storage on the stability and security of stablecoins [48]. Participants with a comprehensive understanding of stablecoin mechanisms and diverse investments report risks related to smart contract execution. They exhibit conservative risk tolerance and remain cautious about collateral assets, such as DAI's reliance on volatile assets like ETH, which increases risk exposure.

Risk Mitigation Strategies: Limitation & Challenges Participants commonly employ a strategy of converting their holdings directly into fiat currency, particularly those who hold fiat-backed stablecoin. during unfavorable market conditions. While this offers short-term protection, drawbacks include transaction costs and timing uncertainties when converting between assets [39]. Another strategy is continuously monitoring collateral asset prices and stablecoin collateralization ratios for timely withdrawals, mainly favored by participants with diverse stablecoin holdings and comprehensive market understanding. However, this strategy is challenging to obtain accurate and timely information in dynamic fast-paced markets. Furthermore, participants often consider code security as a determining factor when deciding whether to invest in on-chain stablecoins, even if they possess a technical background. These diverse attitudes towards risk and current mitigation practices highlight the importance of further exploring the motivators and deterrent factors that individuals consider when investing in stablecoins.

6 Conclusion

In this study, we utilized case studies and semi-structured interviews to delve into participants' perceptions, interactions, and apprehensions pertaining to stablecoins. Our findings underscored that participants harbor misunderstandings about the operational mechanisms of stablecoins and encounter security challenges in their usage. These challenges, which include issues related to operators and collaterals, raise considerable concern. Yet, intriguingly, a majority of participants expressed a willingness to continue their holdings, particularly in the case of fiat-backed stablecoins.

Acknowledgement

This work was supported by the grant from the Science and Technology Development Fund (FDCT) Macau SAR (File no. 0014/2022/AFJ and no. 0129/2022/A) and the University of Macau (File no. MYRG-CRG2022-00013-IOTSC-ICI and no. SRG2022-00032-FST).

References

[1] https://coinmarketcap.com/.

[2] https://docs.ampleforth.org/learn/about-the-ampleforth-protocol.

[3] https://docs.frax.finance/.

[4] https://docs.tribedao.xyz/docs/intro.

[5] https://makerdao.com/en/whitepaper.

[6] https://tether.to/en/how-it-works.

[7] https://vaiot.ai/en#token-allocation.

[8] https://www.binance.com/en/busd.

[9] https://www.circle.com/en/usdc.

[10] https://www.gemini.com/trust-center.

[11] Aydin Abadi, Jin Xiao, Roberto Metere, and Richard Shillcock. Valued: A blockchain-based trading platform to encouragestudent engagement in higher education. 2021.

[12] 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*, pages 1–19, 2021.

[13] Olakunle Alao and Paul Cuffe. A taxonomy of the risks and challenges of embracing blockchain smart contracts in facilitating renewable electricity transactions. In *2022 IEEE PES/IAS PowerAfrica*, pages 1–5. IEEE, 2022.

[14] Omar Alqaryouti, Nur Siyam, Zainab Alkashri, and Khaled Shaalan. Users' knowledge and motivation on using cryptocurrency. In *Information Systems: 16th European, Mediterranean, and Middle Eastern Conference, EMCIS 2019, Dubai, United Arab Emirates, December 9–10, 2019, Proceedings 16*, pages 113–122. Springer, 2020.

[15] Lennart Ante, Ingo Fiedler, and Elias Strehle. The impact of transparent money flows: Effects of stablecoin transfers on the returns and trading volume of bitcoin. *Technological Forecasting and Social Change*, 170:120851, 2021.

[16] Lennart Ante, Ingo Fiedler, and Elias Strehle. The influence of stablecoin issuances on cryptocurrency markets. *Finance Research Letters*, 41:101867, 2021.

[17] Aleksander Berentsen and Fabian Schär. Stablecoins: The quest for a low-volatility cryptocurrency. *The economics of Fintech and digital currencies*, pages 65–75, 2019.

[18] 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*, pages 94–101. IEEE, 2014.

[19] Dirk Bullmann, Jonas Klemm, and Andrea Pinna. In search for stability in crypto-assets: are stablecoins the solution? *Available at SSRN 3444847*, 2019.

[20] Chun-Wei Chiang, Eber Betanzos, and Saiph Savage. Exploring blockchain for trustful collaborations between immigrants and governments. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–6, 2018.

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

[22] John R Douceur. The sybil attack. In *Peer-to-Peer Systems: First InternationalWorkshop, IPTPS 2002 Cambridge, MA, USA, March 7–8, 2002 Revised Papers 1*, pages 251–260. Springer, 2002.

[23] 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*, pages 1–14, 2018.

[24] Chris Elsden, Ludwig Trotter, Mike Harding, Nigel Davies, Chris Speed, and John Vines. Programmable donations: exploring escrow-based conditional giving. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2019.

[25] Shayan Eskandari, Jeremy Clark, David Barrera, and Elizabeth Stobert. A first look at the usability of bitcoin key management. *arXiv preprint arXiv:1802.04351*, 2018.

[26] Michael Fröhlich, 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*, pages 1751–1763, 2020.

[27] Michael Fröhlich, Franz Waltenberger, Ludwig Trotter, Florian Alt, and Albrecht Schmidt. Blockchain and cryptocurrency in human computer interaction: A systematic literature review and research agenda. *arXiv preprint arXiv:2204.10857*, 2022.

[28] Liam Frost. Binance smart chain defi project burgerswap hacked for $7 million. https://cryptoslate.com/binance-smart-chain-defi-project-burgerswap-hacked-for-7-million/, 2021.

[29] John M Griffin and Amin Shams. Is bitcoin really untethered? *The Journal of Finance*, 75(4):1913–1964, 2020.

[30] Ethan Heilman, Alison Kendler, Aviv Zohar, and Sharon Goldberg. Eclipse attacks on bitcoin's peer-to-peer network. In *24th {USENIX} Security Symposium ({USENIX} Security 15)*, pages 129–144, 2015.

[31] Henri T Heinonen. On creation of a stablecoin based on the morini's scheme of inv&sav wallets and antimoney. In *2021 IEEE International Conference on Blockchain (Blockchain)*, pages 409–416. IEEE, 2021.

[32] Charlie Hou, Mingxun Zhou, Yan Ji, Phil Daian, Florian Tramer, Giulia Fanti, and Ari Juels. Squirrl: Automating attack analysis on blockchain incentive mechanisms with deep reinforcement learning. *arXiv preprint arXiv:1912.01798*, 2019.

[33] Klaudia Jarno and Hanna Kołodziejczyk. Does the design of stablecoins impact their volatility? *Journal of Risk and Financial Management*, 14(2):42, 2021.

[34] Clemens Jeger, Bruno Rodrigues, Eder Scheid, and Burkhard Stiller. Analysis of stablecoins during the global covid-19 pandemic. In *2020 Second International Conference on Blockchain Computing and Applications (BCCA)*, pages 30–37. IEEE, 2020.

[35] Feng Jin, Jingwei Li, and Yi Xue. Preferring stablecoin over dollar: Evidence from a survey of ethereum platform traders. *Journal of International Money and Finance*, 131:102796, 2023.

[36] 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*, pages 2872–2878, 2016.

[37] 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: 20th International Conference, FC 2016, Christ Church, Barbados, February 22–26, 2016, Revised Selected Papers 20*, pages 555–580. Springer, 2017.

[38] Yujin Kwon, Jihee Kim, Yongdae Kim, and Dawn Song. The trilemma of stablecoin. *Available at SSRN 3917430*, 2021.

[39] Cangshu Li and Yan Shen. The potential impacts and risks of global stablecoins. *China Economic Journal*, 14(1):39–51, 2021.

[40] David Lucid. Rari capital ethereum pool — post-mortem. https://medium.com/rari-capital/5-8-2021-rari-ethereum-pool-post-mortem-60aab6a6f8f9, 2021.

[41] Richard K Lyons and Ganesh Viswanath-Natraj. What keeps stablecoins stable? *Journal of International Money and Finance*, 131:102777, 2023.

[42] 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)*, pages 60–66. IEEE, 2019.

[43] Amani Moin, Kevin Sekniqi, and Emin Gun Sirer. Sok: A classification framework for stablecoin designs. In *Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24*, pages 174–197. Springer, 2020.

[44] Amani Moin, Emin Gün Sirer, and Kevin Sekniqi. A classification framework for stablecoin designs. *arXiv preprint arXiv:1910.10098*, 2019.

[45] Anton Permenev, Dimitar Dimitrov, Petar Tsankov, Dana Drachsler-Cohen, and Martin Vechev. Verx: Safety verification of smart contracts. In *2020 IEEE symposium on security and privacy (SP)*, pages 1661–1677. IEEE, 2020.

[46] Ingolf GA Pernice, Sebastian Henningsen, Roman Proskalovich, Martin Florian, Hermann Elendner, and Björn Scheuermann. Monetary stabilization in cryptocurrencies–design approaches and open questions. In *2019 crypto valley conference on blockchain technology (cvcbt)*, pages 47–59. IEEE, 2019.

[47] Wanda Presthus and Nicholas Owen O'Malley. Motivations and barriers for end-user adoption of bitcoin as digital currency. *Procedia Computer Science*, 121:89–97, 2017.

[48] Nathan Reiff. The collapse of ftx: What went wrong with the crypto exchange? https://www.investopedia.com/what-went-wrong-with-ftx-6828447, 2023.

[49] Michael Rodler, Wenting Li, Ghassan O Karame, and Lucas Davi. Evmpatch: Timely and automated patching of ethereum smart contracts. In *USENIX Security Symposium*, pages 1289–1306, 2021.

[50] 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*, pages 6499–6510, 2017.

[51] Fabian Schär. Decentralized finance: On blockchain- and smart contract-based financial markets. *FRB of St. Louis Review*, 2021.

[52] Clara Schneidewind, Ilya Grishchenko, Markus Scherer, and Matteo Maffei. ethor: Practical and provably sound static analysis of ethereum smart contracts. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pages 621–640, 2020.

[53] Liya Su, Xinyue Shen, Xiangyu Du, Xiaojing Liao, XiaoFeng Wang, Luyi Xing, and Baoxu Liu. Evil under the sun: Understanding and discovering attacks on ethereum decentralized applications. In *USENIX Security Symposium*, pages 1307–1324, 2021.

[54] 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 *Proceedings of the 32nd Australian Conference on Human-Computer Interaction*, pages 546–557, 2020.

[55] Ye Wang, Patrick Zuest, Yaxing Yao, Zhicong Lu, and Roger Wattenhofer. Impact and user perception of sandwich attacks in the defi ecosystem. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2022.

[56] Ren Zhang and Bart Preneel. Lay down the common metrics: Evaluating proof-of-work consensus protocols' security. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 175–192. IEEE, 2019.

[57] Wenqi Zhao, Hui Li, and Yuming Yuan. Understand volatility of algorithmic stablecoin: Modeling, verification and empirical analysis. In *Financial Cryptography and Data Security. FC 2021 International Workshops: CoDecFin, DeFi, VOTING, and WTSC, Virtual Event, March 5, 2021, Revised Selected Papers 25*, pages 97–108. Springer, 2021.

[58] Liyi Zhou, Kaihua Qin, Antoine Cully, Benjamin Livshits, and Arthur Gervais. On the just-in-time discovery of profit-generating transactions in defi protocols. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 919–936. IEEE, 2021.