Security Perceptions of Users in Stablecoins: Advantages and Risks within the Cryptocurrency Ecosystem

***Abstract*—Stablecoins, a type of cryptocurrency pegged to another asset to maintain a stable price, have rapidly become an important part of the cryptocurrency ecosystem. Prior studies have primarily focused on examining the security of stablecoins from technical and theoretical perspectives, with limited investigation into users' risk perceptions and security behaviors in stablecoin practices. To address this research gap, we conducted a mixed-method study that included constructing a stablecoin interaction framework based on literature, which inspired the interview protocol design, semi-structured interviews (n=21), and Reddit data analysis (9,326 posts). We found that participants see stable value and regulatory compliance as key security advantages of stablecoins over other cryptocurrencies. Participants raised concerns about centralization risks in fiat-backed stablecoins, perceived challenges in crypto-backed stablecoins due to limited reliance on fully automated execution, and felt confused by the complex mechanisms of algorithmic stablecoins. We also proposed improving user education and optimizing mechanisms to address these concerns and promote the safer use of stablecoins.**

1. Introduction

A stablecoin is a cryptocurrency that attempts to maintain price stability either by being backed by specific assets or by using algorithms to adjust their supply based on demand [6]. Notably, three of the five most traded cryptocurrencies are stablecoins, with a collective market capitalization surpassing 130 billion USD by 2023 [16]. Tether USD (USDT), a prominent stablecoin, is utilized by over four million accounts on the Ethereum blockchain [17].

The widespread adoption of stablecoins has increasingly made them targets for malicious attacks, with losses amounting to 27 million dollars [1]. This underscores the critical importance of researching security within the stablecoin sector. Stablecoins uniquely combine the stability of fiat currencies with the cryptographic security and transparency offered by blockchain technology. This dual nature means that interactions with stablecoins span both traditional financial systems and the cryptocurrency ecosystem, raising security concerns from both domains [9].

Existing research predominantly examines the security of stablecoins from technical and theoretical perspectives, exploring aspects such as the stability of stablecoin value [41], [45], the impact of stablecoins on financial robustness [5], [33], [36], and attacks on protocol designs [27], [35], [53], leaving a gap in our understanding of users' risk perceptions and security behaviors in stablecoin practices. Given the substantial market capitalization and widespread usage of stablecoins, it is crucial to investigate why users prefer stablecoins and the security risks they perceive during cryptocurrency transactions. This study aims to bridge this gap by focusing on user-centered issues related to stablecoins. We explore users' perceptions and interactions within traditional and crypto financial systems, and the security risks they face while using stablecoins. The research questions guiding our investigation are as follows:

RQ1: *What security advantages do users perceive in using stablecoins compared to other cryptocurrencies?*

RQ2: *How do users perceive unique security risks when using stablecoins?*

Our study aims to deepen our understanding of stablecoins through a mixed-methods approach that addresses our research questions. Initially, we collected online resources and conducted an open coding analysis to understand the interaction of stablecoins within the crypto market. This foundation allowed us to conduct a qualitative study through semi-structured interviews with 21 participants. Additionally, we analyzed online discussions on Reddit to understand community attitudes and interactions, enriching our findings with perspectives from a broader demographic.

Our study reveals that users perceive stablecoins to offer significant security advantages over other cryptocurrencies, notably in terms of value stability and regulatory compliance. The consistent value of stablecoins is a critical factor that influences users to adopt stablecoins for the secure storage of crypto assets and diversification of investment risks. In terms of regulatory compliance, most users believe that stablecoins provide a secure entry to engage in the crypto market. Some users, however, exploit regulatory loopholes to use stablecoins for tax evasion, viewing this as an "unethical" security advantage. Security risks vary depending on the type of stablecoin. For fiat-backed stablecoins, major concerns include transparency, reserve adequacy, third-party risks, and regulatory ambiguities. Crypto-backed stablecoins elicit worries about the potential devaluation of the collateral and limited reliance on fully automated execution. Algorithmic stablecoins, which lack collateral, raise concerns regarding the stability of their underlying algorithms and the robustness of their ecosystems. We further discuss confusions among users regarding the mechanisms of stablecoins, as well as the technical characteristics of cryptocurrencies and their implications for user risk profiles.

Our research makes three key contributions that aim to inform both the practical development and usability design of stablecoins and the broader cryptocurrency ecosystem:

- Firstly, we present the unique perceived risks associated with stablecoins compared to other cryptocurrencies, analyzing the specific concerns users have regarding stablecoin risks.
- Secondly, we uncover common confusions and identify perceived security risks of stablecoins, offering design implications aimed at addressing these challenges. This is pivotal for bridging the gap between user perceptions and stablecoin designs, establishing a foundation for future research to enhance stablecoin usability and security, and guiding stakeholders toward developing stablecoins that are both user-friendly and secure.
- Lastly, by focusing on users' perspectives, our research highlights the relationship between the technical features of cryptocurrencies and users' perceived security risks. This offers valuable insights into the broader design of cryptocurrencies, suggesting ways to improve user engagement and security.

2. Background and Related Work

In this section, we first provide a brief introduction to stablecoins and summarize existing research on the topic. We then review prior studies on the perception of security risks associated with cryptocurrencies.

2.1. An Introduction to Stablecoins

Stablecoins are a rapidly evolving subcategory of cryptocurrency designed to minimize price volatility [45], [59]. The stability is achieved by pegging the price to a stable asset, typically a fiat currency (e.g., the US dollar). To keep the price stable, operators either maintain physical reserves of the underlying asset or employ algorithms that adjust to fluctuations in demand and supply [45], [47]. There are three main types of stablecoins: *fiat-backed stablecoins*, *crypto-backed stablecoins*, and *algorithmic stablecoins* [47].

Fiat-backed stablecoins are supported by funds held by an issuer for safekeeping. They are issued by an entity that accepts a corresponding amount of fiat money at a predetermined ratio (e.g., 1:1) [45], [47]. For every unit of the stablecoin in circulation, an equivalent amount of fiat currency is held in reserve by the financial institution [46]. Examples include USDT [57] and USD Coin (USDC) [14].

Crypto-backed stablecoins are backed by cryptocurrencies held as collateral [45]. Due to the volatile nature of cryptocurrencies, crypto-backed stablecoins generally need to be over-collateralized at a certain ratio to maintain the stability. For example, a collateralization ratio requirement of 150% means a user needs to deposit $150 worth of cryptocurrencies to mint $100 of a stablecoin. A well-known example of a crypto-backed stablecoin is DAI [44].

Algorithmic stablecoins leverage algorithmic and incentive mechanisms to maintain their price stability. They often operate under-collateralized, meaning they don't rely on a reserve of assets to maintain a stable value. The laws of supply and demand are integral to the mechanics of algorithmic stablecoins [32]. For instance, when demand rises, the algorithm can mint new tokens to maintain stability, and when demand decreases, it can burn tokens to reduce supply. A well-known example is TerraUSD (UST) [56], which unfortunately experienced a severe crash.

2.2. Studies on Stablecoins

Prior research has primarily examined the stability of stablecoins [31], [32], [64] and identified the interrelations between stablecoins and other cryptocurrencies [31], [45]. There are few papers that have studied users' perceptions of stablecoins [33], [34] and a special type of stablecoin named Central Bank Digital Currency (CBDC) [2], [3].

Researchers find that the stability of stablecoins differs based on the underlying design choices. A study analyzing high-frequency data of six major stablecoins found them excessively volatile [28]. Another study models how the prices of fully collateralized stablecoins change due to traders' behaviors, focusing on the interplay of trend following and peg deviations, i.e., the role of arbitrage in keeping stablecoins "stable" [50]. Some identify that volatility varies across different stablecoins; for instance, the instabilities of major stablecoins such as USDT and USDC drive comparatively smaller stablecoins, while algorithmic stablecoins are easily de-pegged [31], [45], [64].

Moreover, previous studies examine the relationship between stablecoins and cryptocurrency [26], [38]. Some studies focus on the impact of stablecoins on the returns and trading volumes of other cryptocurrencies, especially Bitcoin (BTC, a cryptocurrency) [26], [62]. It has been observed that there is a significant increase in BTC prices during the crypto boom following purchases with USDT, which tends to occur after market downturns. However, other research argues that there is no evidence that stablecoins positively influence the price of other crypto assets; rather, an increase in stablecoin issuance follows other crypto asset price increases [38].

Two studies discuss the user perceptions of stablecoins. One study summarizes that an affinity for new technologies and a penchant for political autonomy have emerged as motivations for the preference towards stablecoins [33]. The other study takes Libra, a stablecoin proposed in 2019 by Facebook, as an example to discuss the adoption of stablecoins [34]. Concurrently, scholarly attention has shifted towards the exploration of CBDCs in recent years [2], [3]. CBDCs are digital currencies issued by a country's central bank to function as the digital equivalent of that nation's official fiat currency [65]. Prior research encompasses analyses of various attributes and potential risks associated with CBDCs, including concerns over privacy [3], [7]. It is important to emphasize that CBDCs are different from stablecoins. Since CBDCs are centrally issued and

managed, they contrast with stablecoins, which are typically praised for their decentralized nature and the anonymity they provide in the cryptocurrency market. Consequently, the public's perception and the security challenges associated with stablecoins may significantly differ from those related to CBDCs.

2.3. Perceived Security Risks of Cryptocurrency

Since the inception of BTC [48], cryptocurrencies have garnered significant interest in the field of user studies. Their decentralized nature places greater responsibility on end users for managing their assets, thereby exposing them to security risks when using cryptocurrencies [24].

Sas and Khairuddin pinpointed various risks encountered by users, ranging from lost passwords and malicious attacks to engaging with dishonest trading partners, and failure to recover from human error or malice [54]. Additionally, Abramova et al. conducted a survey among cryptocurrency users, exploring their perceptions of risks such as extortion, theft of private keys, mistakes leading to loss, and vulnerabilities associated with wallets and exchanges [4]. Based on previous work, Froehlich et al. categorized these risks into three areas: human error, betrayal, and malicious attacks [23]. Human errors are frequently reported across studies, including forgotten passwords, forgotten storage locations, lost private keys, wrongly sent transactions, or poor investment decisions [4], [54], [60]. Risks of betrayal result from users misplacing trust in a third party, such as exchanges that fail to adequately protect their customers' cryptocurrency [60]. Instances of malicious activities are widely recorded, including dishonest traders, extortion, and vulnerable wallets or exchanges [4], [39], [60].

2.4. Summary of Gaps in the Literature

Although stablecoins are widely adopted within crypto ecosystem, our understanding of stablecoins in user studies is still limited. Existing studies have predominantly focused on crypto users' perception on interaction and security concerns with cryptocurrencies, the macroeconomic implications of stablecoins and the stability mechanisms. Yet, there is a significant gap in qualitative research exploring the reasons users choose to use stablecoins compared with other cryptocurrencies and how they perceive and mitigate security risks during crypto practices. The security issues associated with stablecoins exceed the risks faced by traditional cryptocurrencies, as stablecoins employ more complex stabilization mechanisms and also exhibit significant differences in market performance. Given the importance of stablecoins in the blockchain ecosystem, there is a critical need for further research focusing on the security implications from a user-centered perspective. To bridge this knowledge gap, we propose two research questions to understand users' perceptions of the security advantages of stablecoins and security concerns.

3. Methods

We adopted a mixed methods approach to explore users' perception on stablecoins. Initially, we collected online resources to establish a foundational understanding of the stablecoin market and users' interactions. This preparatory study informed the design of our subsequent in-depth interviews and enabled us to design the interview protocol. Then we conducted a semi-structured interview with 21 participants to explore users' perceptions. We also examined online discussions within cryptocurrency communities on Reddit to capture a broader spectrum of perspectives, reaching a broader user base and thereby complementing and enriching our interview findings.

3.1. Study1: Construction of a Stablecoin Interaction Framework Based on Online Resources

We collected resources to understand how users interact with stablecoins. Three primary sources were chosen for a broad overview: (1) stablecoin introductions by the Ethereum Foundation [20], which hosts many stablecoin projects; (2) whitepapers and websites of notable stablecoin projects highlighted by the Ethereum Foundation; and (3) information from stablecoin projects listed on CoinMarketCap [16], a leading crypto market data provider.

We then applied an inductive thematic analysis approach [29] to process the resources. We provide a summary of the stabilization mechanisms, the methods for acquiring stablecoins, and their various application scenarios. This foundational understanding serves as the benchmark for further analyzing user perceptions and their practical engagements with various types of stablecoins. For detailed information, please refer to Figure 2 and online appendix, which illustrates the interaction scenarios of stablecoins within the crypto ecosystem.

3.2. Study2: Interview Study

3.2.1. Participant Recruitment. Web3 users frequently engage in discussions on platforms such as Discord and Telegram [25], so we posted our recruitment message through these platforms. Prospective participants first completed a screening survey that captured details such as age, gender, and years of experience using stablecoins. We first recruited 9 participants from Discord and 2 participants from Telegram. During the interviews, we asked the directly recruited participants if they could share our recruitment message within their networks, which led to an additional 10 participants across three snowball sampling chains.

3.2.2. Participant Background. We had 21 participants, with their demographics detailed in Table 3 in Appendix A.2. Eight participants were aged 18-24, eleven were 25-34, and two were 35-44; eighteen identified as men and three as women. All participants had prior experience using stablecoins, though the length of their experience varied. Specifically, thirteen participants reported over three years of expertise, five had 2-3 years, and three had 1-2 years.

3.2.3. Semi-structure Interview. The interview was structured into two specific sections, each corresponding to one of our research questions. (1) *Experience with Stablecoin*: In the first part of our study, we explored the participants' experience with stablecoins, including their preferences. The discussions focused on the reasons behind their preference for using stablecoins and their perceptions of the security advantages these offer compared to traditional cryptocurrencies like BTC and Ether (ETH). Sample questions included "How do you think stablecoins differ from other cryptocurrencies like BTC?", "Can you give some examples of stablecoins you are familiar with?", and "What made you choose to use [specific stablecoins mentioned by the participant]?".

(2) *Risk Perception and Mitigation*: The second part of our study aims to delve deeply into participants' perceptions of the security risks associated with stablecoins. Initially, we encouraged open dialogues, prompting participants to articulate their personal views on the vulnerabilities of stablecoins. For example, we posed questions such as "Have you ever been concerned about the price instability of stablecoins?" As the discussion progressed, we explored further into the reasons behind their concerns to better understand the depth and nuances of their views. Additionally, we inquired about how they managed these various risks.

3.2.4. Interview Data Analysis. We transcribed interview recordings and analyzed the qualitative data using thematic analysis [11]. During the initial phase, two researchers independently analyzed a subset comprising 20% of the full set of interview transcripts. Two researchers engaged in a comparative discussion of the emergent themes. Points of divergence were thoroughly debated, and themes were subsequently refined and synthesized into a preliminary codebook. After coding all transcripts, the same researchers checked an additional 10% to further verify the codebook's reliability. Both researchers independently conducted a deductive thematic analysis using the preliminary codebook. The analysis yielded a Cohen's Kappa score of 0.81, signifying a high degree of interrater reliability. We identified emergent themes across two core dimensions: users' perception of the security advantages of stablecoins and security risks of using stablecoins. To assess the robustness and completeness of our data, we conducted a data saturation analysis. All emergent themes were listed in the order of their appearance from participant P1 to P21. The absence of new themes in the latter stages of the interview sequence substantiated our claim of achieving data saturation.

3.3. Study3: Online Discussion Data Analysis

We selected Reddit as the data source to gather online interaction data. Reddit boasts a diverse user base representing various geographic locations and cultural backgrounds [37], enabling us to gather more insights for our research. Detailed information is provided in Appendix B.

3.3.1. Data Collection. We selected the top 7 subreddits labeled in the "crypto" category in the ranking of the top 500 subreddits provided by Reddit. For our dataset, we extracted posts from these subreddits utilizing keywords associated with stablecoins. Details can be found in the online appendix. This extraction process was facilitated by the Python Pushshift.io API Wrapper (PSAW) [10].

3.3.2. Data Processing. We removed sensitive information, such as personally identifiable details, from the data locally before uploading it to GPT-4 [49]. This was achieved with the assistance of the open-source toolkit Microsoft Presidio [51], which can anonymize sensitive data with an accuracy rate of up to 99% [21]. To uphold privacy and ethical research standards, we paraphrased all Reddit user quotations in our main text to prevent identification via search functionalities. Totally, we collected $9,326$ posts from Reddit.

3.3.3. Data Analysis and Categorization. In this phase of our research, we focused on categorizing the content of posts about stablecoins to investigate the topics discussed by online users. Details can be found in the online appendix.

We conducted three rounds of post classification. Each round of classification followed a specific procedure: Initially, we randomly selected 100 posts from each category. Two researchers independently analyzed 20% of the selected posts, developed an initial coding framework, and refined it through iterative comparison until a consistent codebook was established. This finalized codebook was then applied to the remaining posts by the two researchers, followed by a final consistency check after all posts were coded. Subsequently, the codebook was organized into classification criteria through thematic analysis, which served as prompts for GPT-4 to analyze the posts. In this process, GPT-4 first categorized the same 100 posts that had been manually classified by the researchers. The results were compared, and if the accuracy rate reached 85%, the same standard was used to allow GPT-4 to continue classifying the remaining posts. For posts that could not be automatically classified, the researchers conducted manual reviews.

3.4. Ethics and Data Protection

Our study and data protection measures were thoroughly reviewed and approved by our Institutional Review Board (IRB) to safeguard against undue participant risk. For interview study, participants were asked for explicit consent to participate in the study and to use their anonymized data for research purposes. After the interview, participants received 20 dollars or equivalent as compensation. All data were securely stored in university server, accessible only to our team. Identifying details were removed or altered during analysis to prevent participant identification. Regarding the use of Reddit data, we implemented several measures to protect user anonymity and privacy. These measures included: (1) unlinking usernames from the data set before conducting any analysis, (2) refraining from using usernames to search

for additional information about users during or after the study, and (3) paraphrasing quotes in our published work to further protect user identities.

3.5. Limitation

Our study has identified three principal limitations: the constrained sample size, the regional homogeneity of our participants and the unbalanced gender representation.

Firstly, the sample size of our interviews limits the generalizability of our findings to the broader stablecoin user population. Although we attempted to augment this by integrating data from Reddit discussions, which included a more varied participant demographic. Therefore, the themes and patterns identified in this research serve as preliminary insights and a foundational base for more extensive future studies. Secondly, most of our participants are from Asian nations. Although the decentralized and worldwide nature of blockchain technology diminishes the potential for location-based biases to impact our findings, this geographic concentration might bring in specific regional viewpoints or issues. While we attempted to mitigate this by including Reddit data for a more global perspective, future research should explicitly aim to include participants from a wider range of geographical locations to ensure the findings are universally applicable. Thirdly, there was a notable gender imbalance among our interviewees, with a majority being male. This imbalance reflects the broader trend in cryptocurrency and digital asset engagement [15] but points to the need for future research to include a more diverse gender representation to capture a wider array of perspectives.

In conclusion, the insights we provide should be seen as preliminary, laying the groundwork for further research that is more expansive, inclusive, and representative of the global stablecoin user base.

4. User Perceptions of Security Advantages of Stablecoins (RQ1)

In this section, we present the perceived security advantages of stablecoins as compared to other cryptocurrencies by our participants, which are primarily evident in two key aspects: value stability and regulatory compliance.

4.1. Value Stability

In our study, nearly all participants agreed that stablecoins address the high price fluctuations associated with traditional cryptocurrencies such as BTC and ETH. Due to the advantage of value stability, participants chose stablecoins as tools for risk hedging and investment to help maintain asset stability in the uncertain crypto market.

Hedge for Crypto Portfolios. The consensus among the majority of our participants was that stablecoins acted as an essential instrument for hedging against risk. Instead of exiting the crypto market altogether, our participants shared that they could temporarily convert their cryptocurrencies into stablecoins. This strategy enhanced the resilience of their investments against sudden market downturns. For example, P13, who held ETH for participating in various decentralized finance (DeFi) activities on the Ethereum blockchain, explained that she converted ETH to USDT to protect their investment from unpredictable market fluctuations. *"I used USDT to mitigate the volatility of the crypto market. By converting ETH into stablecoins, I could avoid sudden price fluctuations and preserve the value of my investments"*(P13). In online posts, we found that 11% of the posts in the topic "Concerns and Discussions About Using Stablecoins" were focused on the use of stablecoins for risk hedging. A post expressed a similar view: *"People who had significant amounts of stablecoins staked barely felt a thing and didn't panic as much as others... it was reassuring to ensure a portion of my wealth remained secure through each dip"*(Post 63).

Stable Investment Profit. Eleven participants (P2-6, P8, P12-13, P18-20) actively integrated stablecoins into their investment strategies as a method to diversify their crypto asset holdings. Numerous use cases for stablecoins have emerged in the crypto market (see Figure 2), with many participants turning to these assets for investment purposes, such as staking in DeFi platforms or participating in yield farming. The advantage of using stablecoins in these scenarios lies in their ability to provide steady returns while minimizing the risk associated with the extreme volatility of other cryptocurrencies. As P5 mentioned, by doing so, he could enjoy the dual benefits of participating in the cryptocurrency market while safeguarding a portion of their portfolio against sudden market corrections. *"The market offered a variety of stablecoin investment services, providing investors with new opportunities for returns ... I personally held a certain amount of USDT ... to earn income. The stable income generated from such stablecoins offered more peace of mind compared to holding BTC alone"*(P5). Similar sentiments were also observed on Reddit, where 231 posts discussed how using stablecoins could earn stable returns, highlighting the community's perception of stablecoins as a strategic asset for reinvestment.

4.2. Regulatory Compliance

Regulatory compliance was a consideration for half of the participants when selecting stablecoins over other cryptocurrencies. They perceived stablecoins as providing a secure entry into the crypto market. And five participants viewed the absence of taxation on stablecoin transactions as a safety advantage compared to other cryptocurrencies.

Secure Entry for the Crypto Market. Fifteen participants (P1-6, P8, P12-14, P16-20) perceived stablecoins as a crucial and secure entry point to the cryptocurrency market, facilitating the safe conversion of fiat currency into cryptocurrencies. The fact that many centralized exchanges evaluate stablecoin operators before listing their stablecoins ensures adherence to operational standards, which provides users with a sense of security. P3 highlighted that stablecoins acted as a reliable base currency for trading pairs: *"USDC operated under a licensed framework and could*

be directly purchased from exchanges ... supported multiple trading pairs ... convert USDC to other cryptocurrencies, thereby reducing exchange costs ... since the difference of the exchange rate"(P3). In our analysis, we found that a considerable number of posts discussed stablecoins as a medium of exchange within the crypto market. These discussions particularly emphasized the safety and convenience of using stablecoins for converting into other cryptocurrencies. Many users noted how stablecoins facilitate smoother and more secure transactions (see Table 4 in Appendix B).

Avoidance of Tax Obligations. Stablecoins were seen by five participants (P5, P7-8, P18, P21) as having a security advantage over other cryptocurrencies because they were not currently subject to taxation on payments. P21 explained that *"my employer paid me in USDT as my salary, which I then converted into fiat currency for use. For the company, this behavior helped to reduce tax liabilities"*(P21). P8 supported this view and highlighted an additional privacy benefit: by using stablecoins for salary payments and not triggering taxable events, the number of transactions reportable to tax authorities was minimized. *"Paying with stablecoins meant no taxes were incurred, which kept my financial status unclear and enhanced privacy protection"*(P8). A few posts on Reddit also discussed the tax implications of stablecoins, including their treatment under various tax jurisdictions. For instance, one post mentioned the possibility of avoiding taxes by using stablecoins. *"Avoiding Taxes: Sometimes, if you sold your valuable stuff, you had to pay taxes. But if you used it to get DAI, it was like getting a loan, and you might not trigger those taxes"*(Post 142).

5. User Perception of Security Risks and Corresponding Mitigations (RQ2)

In this section, we present the common risks associated with several stablecoins and the unique risks associated with each stablecoin. To emphasize, we discovered that the risks perceived by users, such as human error and cyber attacks, are consistent with those reported in previous studies on the use of cryptocurrencies [4], [23], [54]. Therefore, we will not reiterate these previously reported risks. Instead, we will focus on the unique risks that are pertinent to stablecoins. Furthermore, we will outline specific strategies for mitigating these risks.

5.1. Common Risks Faced by Stablecoins

In this section, we discuss the common risks faced by several stablecoins. Participants reported concerns about the smart contracts used to issue and operate the stablecoin projects, as well as regulatory issues.

5.1.1. Risks Shared by Three Types of Stablecoins. Participants identified vulnerabilities in smart contracts and potential regulatory issues as major risks associated with the use of the three types of stablecoins.

Code Vulnerability Impact on Operations. Eleven participants (P1, P4-6, P8, P11-15, P18) expressed concerns about vulnerabilities in the smart contracts that were used for issuing and managing stablecoins, a concern particularly evident among software engineers. Given that stablecoins relied heavily on these contracts to maintain their value and execute critical functions such as minting, burning, and transferring assets, any vulnerabilities in the smart contract code could pose significant risks. P6 noted that although smart contracts were usually reviewed before being launched on the market, they did not fully trust the reliability of such reviews. *"Even though the code was reviewed, it could not guarantee 100% security, and many reviews were merely formalities"*(P6). If coding errors existed, malicious attackers could have exploited these vulnerabilities to manipulate the price of stablecoins or steal assets. *"Once this occurred, it would trigger market panic, leading to users selling off the coins, causing a chain reaction"*(P18).

Regulatory Oversight. Concerns about the imposition of regulatory measures by government on operators were raised by twelve participants. Users in the cryptocurrency industry, such as P5, P6, and P11, pointed out that the impact remained unknown due to the uncertain nature of government policies and regulations concerning these digital currencies. *"Do not assume that stablecoins were more stable than cryptocurrencies like BTC and thus not subject to government regulation. After all, they still involved fiat currency and could not escape regulation"*(P5). P11 concurred, suggesting that as the usage of stablecoins increased, so too would the attention from relevant authorities. Recent developments, such as the Securities and Exchange Commission (SEC)'s regulatory actions against Paxos [58], further amplified these concerns. The possibility of impending regulatory actions could influence user behavior. P6 expressed apprehension about the SEC's recent moves. *"Due to the SEC's use of securities laws to sanction BUSD, I was worried that the SEC might employ the same rationale to target other stablecoins and cryptocurrencies, causing concerns about the safety of my assets"* (P6). Our analysis of online conversations revealed that 1449 Reddit posts focused on the repercussions of rigorous regulations on stablecoins, demonstrating that regulatory risk was one of the most significant concerns for users.

5.1.2. Risks Shared by Fiat-Backed and Crypto-Backed Stablecoins. Our participants perceived that both fiat-backed stablecoins and crypto-backed stablecoins faced collateral risks. Additionally, 638 online posts discussed concerns related to collateral risks.

Inadequate Reserves for Full Redemption. Nineteen participants (P1-16, P18-19, P21) voiced concerns regarding the inadequacy of collateral reserves backing fiat-based stablecoins. They understood that a 1:1 backing by a reference asset should allow a stablecoin's value to track the peg. However, they were concerned that in practice, issuers might not have sufficiently liquid assets to ensure full and on-demand redemption for holders. P12 emphasized the importance of sufficient reserves, urging issuers to maintain enough collateral to fulfill redemption promises. *"USDC's reserves were ample ... the assets were relatively stable*

and reliable ... capable of satisfying user redemption demands. Such reserves offered some protection against bank runs"(P12). Online discussions exhibited palpable skepticism regarding the sufficiency of reserves, particularly for USDT. One user cautioned, *"The company had to have reserves that matched the current supply of USDT circulating ... Tether, if they didn't always hold their reserves accordingly, it only took something happening for USDT to spiral down and crash the entire market"*(Post 252).

A few participants admitted their limited understanding of reserve sufficiency. Their awareness often coincided with media reports criticizing stablecoin issuers like USDT for lacking adequate reserves. Participants such as P1 and P13 initially chose USDT based on its high market cap, without knowing the risks associated with insufficient reserves. *"Initially, I opted for the most widely used stablecoin, USDT, without delving into its mechanisms or realizing the potential risks. It was not until recently, when USDT faced frequent scrutiny over its purportedly inadequate reserves, that I became aware of the risks"*(P1).

Sharp Fluctuations of Collateral Assets. Our participants noted that significant fluctuations in cryptocurrency prices could lead to scenarios where the collateral's value was insufficient to cover the stablecoin's value. For instance, P4 expressed a lack of optimism regarding DAI, with no guarantee that ETH would not experience significant price drops again. *"I was not very optimistic about DAI because its collateral mainly came from ETH, and the price of ETH fluctuated a lot. Nobody could guarantee that the value of ETH wouldn't be significantly reduced again. In my opinion, it could happen at any time"*(P4). P2 shared the same concern and believed that collateral volatility made the stablecoin less stable. *"When pledging ETH to generate DAI, the collateral itself was highly volatile, which implied that the stablecoin was relatively less stable. Moreover, there was a risk of under-collateralization, where the value of the collateral fell short, potentially triggering the liquidation mechanism"*(P2).

5.2. Risks of Fiat-Backed Stablecoins

Participants cited threats when using fiat-backed stablecoins, risks stem from factors related to centralization, including the stablecoin operator and reserve institution.

5.2.1. Operator Risks. From Figure 2, we learned that fiat-backed stablecoins were issued and managed by centralized operators. The characteristic of centralization posed a perceived risk for our participants, who were particularly concerned about the operators' lack of transparency and significant control over the system.

Operator's Lack of Transparency. 17 out of the 21 participants (P1-8, P10, P12-P15, P18-21) expressed concerns regarding the lack of transparency by operators who issued and managed fiat-backed stablecoins. They feared that if operators did not disclose their reserves during management processes, it could have led to over-issuance and a lack of sufficient fiat currency for exchange when decoupling issues arose. P14 emphasized the importance of operational transparency to enhance user confidence. *"I believed the operator should have disclosed reserve assets regularly to let us know whether there had been any over-issuance ... if I attempted to convert USDT into fiat currency and discovered that the actual reserves were insufficient ... I might not have received the full amount of fiat currency"*(P14). This sentiment resonated with the broader community, as evidenced by Reddit discussions. One post pointed out the uncertainty surrounding custodial stablecoin issuers, stating, *"This meant that investors could not easily verify whether everything was going as promised. Instead, everyone was asked to have faith in the company behind the coin ... which was quite ironic"*(Post 67). Moreover, P5 highlighted that concerns about transparency with stablecoin operators reflected similar issues that plagued traditional banking operations prior to the advent of cryptocurrencies. *"Initially, cryptocurrencies were introduced to eliminate various problems associated with centralized institutions; however, the collateral-based model reignited concerns over transparency"*(P5).

Centralized Control in Management. The role of stablecoin operators extended beyond management; it included the significant power to enforce compliance measures, which sometimes undermined user interests. 8 out of 21 participants (P2-5, P9, P11, P15-16) voiced concerns over the substantial power held by operators, especially their ability to freeze user accounts. News that USDC operator Circle had frozen assets related to Tornado Cash sparked public scrutiny and debate [8]. P5 and P9 both cited the criticism faced by Circle for its actions, noting the inherent risks in operating fiat-backed stablecoins under centralized control. *"Most fiat-backed stablecoins were at risk of censorship, especially after the Tornado Cash debacle, and these US dollar stablecoins remained subject to US regulatory policies. When the US Treasury imposed sanctions on a project, these stablecoin projects might also be required to take corresponding measures. I feared that my account would be frozen one day for no reason"*(P5). However, a few participants had not been concerned about this risk until the accounts related to Tornado Cash were frozen by Circle, raising fears about potential freezes of their own stablecoin usage. For instance, P17 expressed fear that his account could be frozen one day. *"I had never considered the possibility of an account being frozen before the Tornado Cash incident. Now I realize how extensive an operator's power could be, and I am now worried that my account could be arbitrarily blocked"*(P17). This apprehension was not confined to our participant pool but was also echoed in broader online discussions. For instance, Post 1489 explicitly warned, *"Reminder: Tether (and some other stablecoins) can freeze your tokens"*(Post 1489).

5.2.2. Reserve Institution Risk. The reserve institution was responsible for managing the collateral, and mismanagement could lead to significant risks. Poor management practices could result in insufficient collateral, which undermined the stability and trust in the stablecoin.

Mismanagement of Reserves. Fourteen participants

(P1-4, P6-10, P12-14, P16, P18) and 5% of online posts expressed concerns that reserve institutions might have faced risks leading to de-pegging events. Participants initially trusted these institutions to manage reserves as reliably as traditional banks. However, the crypto market experienced instances that undermined this confidence. USDC deviated from its dollar peg following the disclosure of a $3.3 billion exposure to Silicon Valley Bank [52]. Our participants, including P9, P13, and P16, who held USDC, were caught off guard by this event. P9 emphasized the risks associated with custodial institutions in the stablecoin sector, highlighted by the SVB incident, stating, *"The SVB event was a wake-up call, revealing the extent of the impact that custodial institutions could have on the stability of the stablecoin ecosystem, which I had not fully appreciated before"*(P9). P16 further noted that problems with reserve institutions could have led to contagion risks within the cryptocurrency ecosystem, similar to past financial crises. A few participants pointed out that choosing reliable partners remained a challenge for stablecoin operators. Although some operators, like Tether, transparently disclosed where reserves were held, the safety of these banks was questionable. *"These funds, when deposited in banks, were likely to be utilized for other trading and investment activities"*(P5). Such reinvestment of funds might have increased risk exposure, especially during unstable market conditions. Operators should have had a clear understanding of the financial health of partner banks to assess the security of the funds deposited.

5.3. Risks of Crypto-backed Stablecoin

In our interviews, participants were cautious about crypto-backed stablecoins, considering them highly risky due to their heavy reliance on automated smart contract management and governance concentration.

Limited Reliance on Fully Automated Execution. All operations of crypto-backed stablecoins were executed by smart contracts, which raised some resilience concerns. Our participants who used DAI generally believed that stablecoins relying solely on code execution might not be able to respond promptly in extreme situations. They expressed concerns about this purely code-based automated execution process. For example, when the market experienced significant volatility, the value of the collateral decreased, or the system faced attacks, participants were concerned that smart contracts might not have been able to take appropriate measures to maintain the stability of the stablecoin's value. P8 took liquidation as an example and perceived that if the liquidation was not reasonable and timely, it might have led to the system becoming insolvent and users facing losses. *"The liquidation involves auctioning off collateral to repay the debt. However, the liquidation may take a while to complete due to market volatility and the time required for auctions. During this time, if the value of the collateral continued to decline, the system might have been unable to fully protect users' interests, exposing them to greater risks"*(P8).

Concentration of Decision-Making Powers. Five participants (P3-5, P13, P21) highlighted that governance weaknesses arose from the concentration of decision-making power. P4 used DAI as an example to state that although the protocol was ostensibly managed by a decentralized autonomous organization (DAO) and was theoretically decentralized, this was not the case in practice. *"The DAO was decentralized in name only; in reality, it was controlled by a small group of individuals, particularly crypto whales. They held a majority of the voting power, enabling them to enact protocol changes that served their interests"*(P4). Since the parameters of the DAI protocol were often determined by MakerDAO governance, this centralization of decision-making authority could result in protocol changes that disproportionately benefited a few large stakeholders. *"The major stakeholders held a significant amount of tokens, allowing them to make decisions that benefited their own profits, such as adjusting the stability fee. We small investors had little to no say in the matter"*(P3).

5.4. Risks of Algorithmic Stablecoin

Our participants evaluated algorithmic stablecoins unfavorably, citing security risks from their reliance on complex algorithms and lack of physical collateral. The immature application ecosystem was also a concern.

Complex Algorithms. Participants who held algorithmic stablecoins(P4-5, P16-18), there was a belief that stabilizing prices through complex algorithmic mechanisms made these stablecoins less accessible due to their high entry barrier. P4, an investor in the cryptocurrency industry, thought that the mechanism behind algorithmic stablecoins was complex. *"Algorithmic stablecoins operated on an economic model . . . the principle was to adjust supply and demand . . . involving many parameters. Hence, ordinary people who did not thoroughly review the white paper or understand the code logic could hardly grasp how the price was pegged to the US dollar"*(P4). If users did not fully understand how these algorithms functioned to maintain value, they might have felt uneasy about continuing to invest in such uncollateralized assets. P16 shared his opinion: *"I vaguely understood that the price of UST was related to Luna, but in reality, I didn't know what this dual-token model was about, which left me confused when the death spiral occurred, prompting me to quickly sell off as the UST price plummeted"*(P16).

Additionally, we found that a minority of participants displayed misconceptions regarding the stabilization mechanisms of crypto-backed and algorithmic stablecoins. For instance, P10 erroneously classified DAI as an algorithmic stablecoin. He asserted, *"Decentralized stablecoins like DAI are algorithmic stablecoins. They possess virtual assets in the background and utilize algorithms to stabilize their prices"*(P10). In reality, DAI did not use an algorithm specifically for price stabilization but rather employed an algorithmic liquidation mechanism designed to maintain sufficient collateral levels to protect user assets. Online discussions similarly revealed such confusions. For example,

in Post 990, one user expressed the belief that both types of stablecoins relied on a single asset, stating, *"I'm not familiar with the technical details and the code, but on the surface, these two seemed identical—they both lost their peg significantly when the single asset they were linked to experienced a major downturn in the market ... UST was still mostly or entirely backed by LUNA and still had the issues of a single collateral-backed coin"*(Post 990).

Poor Ecosystem Integration. The risk of algorithmic stablecoins was influenced by their degree of integration within the broader crypto ecosystem. As stated by five participants (P4-5, P15, P17-18), the ecosystem for algorithmic stablecoins was currently immature. They believed that if an algorithmic stablecoin was well-integrated across multiple application scenarios, it could offer users greater flexibility and utility. Conversely, if such stablecoins lacked broad support within the crypto ecosystem, users faced heightened risks. P15 noted the challenges posed by the lack of ecosystem support for algorithmic stablecoins, especially when users needed to liquidate or transact their holdings. *"I had looked into Luna and UST before and noticed that while they had certain applications within their own protocol ecosystem, they were not as widely used as USDT and USDC. This limited their liquidity, which was not favorable for me when I wanted to sell during market fluctuations"*(P15). Online discussions also highlighted the issue of a poor ecosystem, indicating that insufficient liquidity could lead to significant problems. *"In practice, this space was still nascent and hadn't reached peak potential or actually acquired the critical mass of users and liquidity to keep their pegs and offer a viable incentive to users to stabilize ... the goal was to find ... how they interacted with the user and the broader ecosystem"*(Post 4125).

5.5. Corresponding Mitigation Strategies

Our study also uncovers the various mitigation strategies that users employ to address their security risks. Organized into four categories—*risk acceptance*, *risk diversification*, *risk avoidance* and *risk prevention*. Figure 1 presents risk profiles and corresponding mitigation. Compared with the study by [55], which identifies user-perceived security risks and their adopted mitigation strategies in the Web3 ecosystem, we found some consistent mitigation strategies, such as being forced to accept the occurrence of risks and adopting risk diversification. However, a notable difference is that users tended to continue holding stablecoins, specifically diversifying their holdings among different types of stablecoins when risks arose, as they perceived stablecoins as having many use cases within the crypto ecosystem and being a preferable asset to hold.

5.5.1. Risk Acceptance. Risk acceptance is the decision to acknowledge the presence of a risk and consciously decide to tolerate it without taking action to mitigate it. It becomes reasonable to accept those risks when participants believe that the risks cannot be reasonably mitigated and feel optimistic about certain stablecoins.

Accept Reluctantly. Participants recognized certain risks, such as centralized issues like the management of collateral by custodial institutions and exchange bankruptcies, as well as decentralized issues like governance flaws, which were beyond their personal control. They felt helpless in the face of these risks. *"Even though I chose multiple stablecoins to avoid the risk of relying on a single one, I was still vulnerable to the centralization issues of fiat-backed stablecoins. If there were problems with the institutions, I could only accept the losses"*(P2). Additionally, nearly half of the participants believed that vulnerabilities in smart contracts were unavoidable. Despite audits conducted by projects, code attacks still occurred. This concern was particularly raised by participants with a technical background. Moreover, a large portion of participants felt powerless regarding regulatory risks, as the pressure from authorities forced them to accept these risks. *"Any decision made by the government or relevant authorities was something I had to accept, even if all I could do was complain"*(P9).

Keep Holdings Optimistically. A number of participants who had held fiat-backed stablecoins exhibited a high tolerance for collateral risks. This type of stablecoin had already captured a significant market share, leading some participants to believe that they would quickly regain their pegged price even in the event of a deviation. For instance, P3 and P15 firmly believed they could tolerate risks and accept temporary deviations during stablecoin de-pegging events. P3 mentioned that users should have confidence that stablecoins would quickly recover to a stable price level and choose to continue holding them despite the de-pegging. *"Stablecoins backed by fiat collateral increased my confidence because of the assurance of having a tangible asset as the underlying collateral. I believed that they would quickly regain their regular prices as their market share was large, and they were less likely to encounter issues easily"*(P3).

5.5.2. Risk Diversification. Risk diversification, which involves selecting a varied portfolio of cryptocurrency assets, serves as a mitigation strategy to reduce the impact of security breaches or financial losses associated with single stablecoin.

Choose Various Stablecoins. This strategy targeted risks associated with fiat-backed stablecoins, including those related to operators, collateral, and reserve institutions. Users tended to choose multiple stablecoins to engage in the cryptocurrency market, as P3 mentioned, *"Don't put all your eggs in one basket"*(P3). This strategy allowed users to diversify risk and mitigate potential losses from relying on a single stablecoin. Additionally, a few participants mentioned selecting different types of stablecoins based on specific trading needs. However, from a long-term holding perspective, they tended to prefer fiat-backed stablecoins, *"as these were generally perceived as more reliable and trustworthy, offering higher security and stability"*(P18). Choosing various stablecoins not only effectively diversified risk but also enabled users to respond more flexibly to different market conditions.

M01: Accept Reluctantly	M02: Keep Holdings Optimistically	M03: Choose Various Stablecoins	M04: Use Different Management Tools	M05: Exit the Crypto Market	M06: Refuse Certain Stablecoin Usage	M07: Review Project Information	Security Risk Perceptions
11		10	6		6		Code Vulnerability Impact on Operations
6		3	9				Regulatory Oversight
	18	11		8		10	Inadequate Reserves for Full Redemption
	12			7			Sharp Fluctuations of Collateral Assets
	8	8		5		11	Operator's Lack of Transparency
	8	5					Centralized Control in Management
	13	14	10	6		10	Mismanagement of Reserves
		7			5		Limited Reliance on Fully Automated Execution
2		2				5	Concentration of Decision-Making Powers
					5	3	Complex Algorithms
		2			4	5	Poor Ecosystem Integration

Figure 1: Mitigation Strategies for Different Security Risk Perceptions. This matrix presents the relationship between users' security concerns and specific mitigation strategies. The initial row enumerates seven strategies (M01-M07), and the last column outlines the security concerns that each strategy is equipped to mitigate. The number represents the number of our respondents who chose this option.

Use Different Management Tools. This strategy allowed users to utilize a variety of management tools to handle their stablecoin assets, mitigating risks associated with exchange failures and wallet theft. By selecting different management tools, such as hardware wallets, software wallets, and decentralized exchanges, users effectively diversified their risk and avoided concentrating all assets on a single platform or tool. P6 shared his experience, *"I used to store my USDT on exchanges, but after hearing news about exchange hacks, I decided not to keep it there anymore. Now I store some in wallets, and I even have several different wallets"*(P6). Participants agreed that the efficacy of this strategy lay in its capacity to distribute risk, thereby insulating assets from the adverse effects of a single tool's failure. However, while portfolio diversification could reduce risk, it did not eradicate it entirely.

5.5.3. Risk Avoidance. Risk avoidance is a mitigation strategy in which individuals cease using a particular stablecoin after encountering a risk or choose not to use a stablecoin upon becoming aware of certain risks.

Exit the Crypto Market. Participants who used stablecoins for savings mentioned that when issues arose with the collateral or operators of stablecoins, leading to price depegging, they chose to temporarily exit the cryptocurrency market to mitigate potential losses. *"I chose to use stablecoins because they offered higher returns compared to storing fiat currency directly in a bank, but now the operating team has problems and there's insufficient collateral, so I'm afraid of losses and will exit the market immediately"*(P12). Once the market stabilized, they re-entered the market. P9 added that the emergence of stablecoins enabled users to freely convert between crypto assets and fiat currency. *"It is convenient for users to enter and exit the crypto market"*(P9). This functionality significantly lowered the entry barrier, allowing users to more flexibly manage and adjust their investment portfolios.

Refuse Certain Stablecoin Usage. This strategy referred to users choosing not to use a particular stablecoin, typically due to concerns about its stability. Notably, users, based on news reports or their own research, decided not to use algorithmic stablecoins to avoid potential risks. As discussed in Section 5.4, algorithmic stablecoins relied on complex algorithms to maintain price stability, and the immature ecosystem undermined users' confidence in these types of stablecoins. *"Stablecoins like UST are too complex; I don't even understand how it maintains its $1 value, so how can I use it"*(P21). Algorithmic stablecoins lacked actual collateral support, and if problems arose, they could only rely on pre-set rules or mechanisms for adjustments. This further exacerbated users' concerns. Therefore, they chose not to try algorithmic stablecoins to protect their assets from potential risks.

5.5.4. Risk Prevention. Risk prevention is a proactive mitigation strategy that involves identifying potential risks and implementing measures to reduce negative impact before stablecoins encounter risks.

Review Project Information. Reviewing project information was a crucial way for users to understand the overall state of stablecoins. It helped them identify risks related to operators and collateral, such as assessing the possibility of over-issuance by understanding the current amount of collateral. *"Whitepapers and official websites are excellent sources of information for understanding a stablecoin. We should not merely trade but constantly stay informed about the project's latest developments"*(P14). This practice also served as a measure to address governance risks by providing insights into the project's governance structure. *"I regularly followed MakerDAO updates because many de-*

cisions in the DAI project were made through voting, so I needed to keep an eye on the latest governance models and holdings"(P5). Participants considered reviewing project information to be a more technical approach to risk prevention, predominantly conducted by users with technical backgrounds. They would examine the project's code and analyze its logic to identify potential code vulnerabilities or logical flaws in the mechanism. *"I reviewed the code and focused on the technical details of stablecoins that relied on smart contracts"*(P18).

6. Discussion

In this section, we discuss users' understanding and confusions of stablecoins, examine how the technical characteristics of cryptocurrencies influence user risk profiles, and explore design implications for stablecoins to mitigate potential risks and enhance user education.

6.1. User Understanding of Stablecoin

By exploring participants' experiences with various stablecoins, we discovered varying levels of understanding and confusions. Such perceptions significantly influence their views on the security risks of stablecoins.

Varying Understanding of Fiat-backed Stablecoins. We observed varying levels of participant understanding regarding the risks of fiat-backed stablecoins. In Section 5.2, most participants recognized collateral-related risks but often overlooked the dangers of central control by operators. Awareness of this issue typically emerged only after hearing about incidents like the freezing of user accounts in the news. While some participants acknowledged the authority of central institutions, their lack of knowledge about specific operations led to misplaced trust, increasing the risk to their assets. Many users relied on market value and reputation when choosing stablecoins, often selecting those with high market capitalization without fully understanding the issuing mechanism. Collapse events in the crypto market, such as the SVB incident, underscored users' limited understanding of stablecoin risks and highlighted a knowledge gap that could lead to significant financial losses. Interestingly, despite these risks, users displayed a high tolerance for fiat-backed stablecoins. As shown in Figure 1, even when faced with risks related to operators or collateral, users remained optimistic and continued to hold this type of stablecoin.

Confusion Between Crypto-Backed and Algorithmic Stablecoins. Participants demonstrated significant gaps in understanding regarding crypto-backed stablecoins and algorithmic stablecoins. For instance, some conflated crypto-backed stablecoins with algorithmic stablecoins, mistakenly identifying DAI as an algorithmic stablecoin. This conceptual ambiguity likely stems from their limited understanding of the stabilization mechanisms, thereby affecting their relatively low risk tolerance for these types of stablecoins. Interestingly, despite these confusions, it's worth noting that getting the classification wrong may not have substantial practical implications. While clarity and precision are useful, such misclassifications may not significantly affect how users interact with or use these assets in real-world applications. However, it's crucial to recognize that such misclassifications could lead to conceptual issues. For example, when discussions arise about the security vulnerabilities inherent in algorithmic stablecoins, erroneous categorization could result in users forming incorrect perceptions and beliefs about specific coins.

6.2. Risks Perceptions in Cryptocurrencies

Cryptocurrencies, encompassing a wide array of digital assets, are distinguished by technical foundations and design principles. Native tokens, like BTC, are native to their blockchain platforms and generated through specific consensus mechanisms [40]. Non native tokens, such as Ethereum's ERC-20 tokens, are generated via smart contracts and serve varied purposes across applications [40]. Among these, stablecoins represent a unique subset of tokens, anchored in blockchain technology through smart contracts and backed by diverse collateral types [45]. Despite the extensive body of research on the risks associated with cryptocurrency participation, users' risk perceptions vary significantly among different cryptocurrency categories. Table 1 presents the comparison of risk profiles across different cryptocurrency types.

Native Tokens Carry Systemic Risks Inherent to the Blockchain Technology. Primary concerns include vulnerabilities within the blockchain system, such as protocol-level disruptions caused by forking [63] and block reorganization [66], which can lead to transactional inconsistencies. The dependency of native tokens on network infrastructure introduces additional layers of risk [6], [43], which can experience security vulnerabilities, or network congestion, leading to potential losses. We observe that users manage on-chain assets through wallets and store off-chain assets in CEXes in Figure 2, yet both approaches introduce third-party risks [4], [23]. The incidents of exchange bankruptcies and attacks on wallets [30] serve as direct manifestations of this risk. In addition, crypto users frequently report asset loss due to human error [23], [42], [61]. The decentralized nature of native tokens shifts the responsibility of asset protection to the users themselves [23]. However, due to a general lack of familiarity with the operation, users often make errors in key management and transaction processes, such as forgetting passwords, losing track of storage locations, misplacing private keys, and mistakenly sending transactions [4], [54], [60].

Non Native Tokens Present Smart Contract Risks Due to Their Technical Characteristics. Tokens are created by project teams through the deployment of smart contracts on a blockchain, and this process introduces the risk of smart contract vulnerabilities. Even a minor error in the smart contract can lead to vulnerabilities that malicious actors might exploit, resulting in a loss of partial or total value of tokens [67]. This vulnerability also raises concerns about the risks associated with project teams and their operations. Some unscrupulous project teams might

TABLE 1: Comparison of Risk Profiles Across Different Cryptocurrency Types. The checkmarks indicate the presence of a particular risk for each type of cryptocurrency. As shown, stablecoins face risks that include fundamental risks applicable to all cryptocurrencies, token-specific risks, and stablecoin-specific risks.

	Native Token	Non-Native Token	Stablecoin
Blockchain System Risk	✓	✓	✓
Human Error Risk	✓	✓	✓
Third-Party Risk	✓	✓	✓
Smart Contract Risk		✓	✓
Operator Risk		✓	✓
Operation Risk		✓	✓
Collateral Risk			✓
Regulation Risk			✓

TABLE 2: Summary of Security Concerns Associated with Different Security Issue Sources in Cryptocurrencies. The table outlines specific security concerns linked to various risk sources.

Security Issue Sources	Security Concerns
Smart Contract Risk	Code Vulnerability Impact on Operations
Operator Risk	Operator's Lack of Transparency Centralized Control in Management
Operational Risk	Concentration of Decision-Making Powers Complex Algorithms Poor Ecosystem Integration
Third-Party Risk	Limited Reliance on Fully Automated Execution
Collateral Risk	Inadequate Reserves for Full Redemption
Regulatory Risk	Regulatory Oversight Sharp Fluctuations of Collateral Assets

deliberately exploit these vulnerabilities in smart contracts to commit fraud and scam, such as by writing flawed code to misappropriate user funds or engage in other fraudulent activities [22]. For instance, there have been cases of "rug pulls" where project teams suddenly withdraw all invested capital, leaving investors with worthless tokens [18].

Stablecoins Introduce Distinct Risks Related to Stability Mechanisms. Although we identify the security advantages of stablecoins in Section 4, we also find that stablecoins still have numerous security risks. Nowadays, the most widespread stablecoins are fiat-backed stabelcoins and their stability largely relies on real-world assets held as collateral [13], necessitating the involvement of bank accounts that are compatible with these fiat currencies and inherently linked to a centralized financial system. As we mentioned in Section 5, our participants recognize the risks inherent in fiat-backed stablecoins, particularly those tied to centralized entities, including mismanagement, fraud, and insufficient reserves. Financial difficulties or a loss of public trust in stablecoin operators and third parties (i,e., reserve custodians) could lead to a loss of confidence, potentially undermining the stablecoin's value. Historically, there has been a palpable concern among consumers regarding the potential for financial institutions to mismanage or misappropriate deposits [19]. Cryptocurrencies present a novel opportunity to alleviate some of the inherent risks tied to traditional financial systems [12], however, stablecoins have paradoxically reestablished the dependency on centralized institutions. Additionally, for stablecoins backed by cryptocurrency collateral, apprehensions arise regarding the volatility of the underlying crypto assets. As stablecoins are anchored to the real world and gain widespread adoption, they may be subject to financial regulations aimed at ensuring they do not disrupt the traditional financial system and protect consumers from fraudulent activities. We categorized the risks associated with stablecoins and integrated them with cryptocurrencies' risk dimensions, as detailed in Table 2.

6.3. Design Implications

In response to users' confusions and perceived risks associated with stablecoins, we have proposed several design implications for different stakeholders to help mitigate participants' confusions and reduce potential risks. Through these design implications, we aim to enhance the transparency and trustworthiness of stablecoins, thereby facilitating their broader adoption in the financial markets.

6.3.1. Reduce Confusion Through User Education. Participants' confusions about stablecoins are mainly from the lack of transparency and information availability. We discuss design implications for educating users through multiple channels to reduce confusion.

CEXes Presenting Various Metrics Information. Our findings indicate that participants encounter challenges in comprehending crypto-backed and algorithmic stablecoins. Their primary preference leans towards fiat-backed stablecoins due to their market capitalization. As emphasized in Section 4, CEXes serve as one of the most frequently utilized financial applications among participants, playing a critical role in the stablecoin ecosystem. We recommend that CEXes enhance the user experience by integrating detailed stablecoin information directly into the purchase interface. This information should specifically include key metrics such as trading volume, liquidity, market depth, and recent price movements, which should be readily available at the point of transaction. Additionally, we suggest that CEXes introduce distinct informational segments for different types of stablecoins. Each segment should offer comprehensive details about the stablecoin's backing assets, issuance and redemption processes, and regulatory compliance. Moreover, clearly presenting typical use cases for each stablecoin type will help users understand how they can best utilize these assets in their own financial activities.

Enhancing User Awareness through Digital Wallets. A digital wallet is not only a secure storage solution for stablecoins but also a tool to improve participants' awareness. In Figure 2, we can see that part of the stablecoin is stored in the wallet. We intend to utilize the wallet as a tool to provide participants with multiple channels for enhancing their awareness. Wallet providers can offer educational resources within their platforms that explain the concept of stablecoins. These resources can cover topics such as the different types of stablecoins and their underlying mechanisms, such as fiat collateralization or algorithmic algorithms. It

empowers participants to make informed decisions when using stablecoins and fosters a greater understanding of the intricacies of the stablecoin ecosystem.

Centralized Institution Disclosing Information in Real Time. Due to the significant market presence of fiat-backed stablecoins, their reliance on legal tender as collateral has raised widespread concern and attention. For participants, having detailed information about the collateral is crucial for accurately assessing associated risks. Currently, the collateral information provided by stablecoin issuers is often limited, making it difficult for investors to access essential data such as the amount and location of the collateral assets. Furthermore, we have observed that participants often place excessive trust in centralized issuing authorities, believing that these institutions will adhere to declared mechanisms, such as regularly updating information in white papers and on platforms. However, the reality may differ from these expectations. To enhance transparency and trust, we recommend that these central institutions adopt more transparent measures, such as publishing key on-chain data like issuance volumes, as well as off-chain data, including the exact quantities of reserve assets, in real-time.

6.3.2. Optimizing Mechanisms to Mitigate Risks. Our findings reveal that participants primarily perceive stablecoin risks related to the operator and the collateral, so we focus on designing and optimizing solutions in these two areas.

Distributing Roles and Tasks to Form the Decentralization Organization. In seeking to enhance the operational mechanisms of stablecoins, we recognize the pivotal role of transparency. Section 5.2.1 highlighted user concerns regarding the operator's transparency. Without robust transparency, users are left in the dark about key aspects such as collateral management and the extent to which the stablecoin's supply is backed by reserves. This information opacity hampers users' ability to proactively identify and evaluate potential risks. The current model, where a single entity controls all stablecoin operations, accentuates the risk of a single point of failure. One proposed design choice is decentralization, distributing tasks and responsibilities among multiple participants. For instance, the issuer could handle token minting and burning, while collateral management might fall to a dedicated institution or community, with independent data validators managing on-chain data. This model promotes mutual supervision and verification, potentially enhancing transparency and system stability, and addressing user concerns about centralized operations. However, this strategy has drawbacks. Decision-making processes could become more complex and time-consuming due to the need for consensus among stakeholders. Additionally, the risk of conflicting interests among participants may increase, potentially leading to inefficiencies. Thus, while decentralization offers benefits like enhanced transparency and reduced systemic risk, it is crucial to evaluate its implementation carefully and consider potential drawbacks.

Promoting Decentralization and Diversification of Collateral. Addressing the collateral-associated risks warrants attention to three crucial aspects of collateral design: (1) selection of collateral, (2) storage location of collateral, and (3) management of the collateral. Our findings from Section 5.1.2 highlight that participants have significant concerns regarding risks intrinsic to collateral, such as insufficiency and price volatility. Insufficient collateral could stem from operator mismanagement or economic struggles faced by third-party reserve institutions, as discussed in Section 5.2.2. To mitigate these risks, we propose two key strategies: collateral diversification and storage decentralization. To attenuate the risk attributed to extreme price volatility, we can incorporate assets with inherent value stability, such as physical assets. On the storage front, adopting a distributed approach can drastically curtail the risk of reserve asset reduction caused by either operational errors by a solitary third party or systemic failures in a single system. In this regard, collateral can be securely stored across both on-chain and off-chain platforms, effectively hedging operational risks inherent in the ecosystem. Furthermore, decentralization of management responsibility, orchestrated through smart contracts or decentralized governance protocols, can significantly enhance transparency in collateral management, thus instilling greater trust among stablecoin holders. This blend of strategies, we argue, forms a robust framework for addressing the prevalent collateral-associated risks in the current stablecoin market. However, diversifying collateral introduces challenges like price volatility, liquidity, and market demand, increasing operational complexity. Nonetheless, innovative solutions are crucial for building a resilient stablecoin ecosystem.

6.4. Future Work

Future research could address the demographic and geographical limitations by conducting large-scale survey studies or cross-cultural user studies. Given the diverse regulations and policies in different countries, crypto users in regions with stricter restrictions might exhibit distinct behaviors and perceptions. Additionally, we have highlighted design recommendations related to enhancing users' education and optimizing mechanisms for stablecoin organizations. Future studies could delve deeper into this design space, examining the usability and effectiveness of these mechanisms across different user groups and contexts.

7. Conclusion

In this study, we combined observational research, semi-structured interviews, and online discussions to examine participants' perceptions and interactions with stablecoins. Our findings revealed that users perceive stablecoins as more secure than volatile cryptocurrencies. However, there are significant security concerns associated with different types of stablecoins. To address these issues, we proposed specific design recommendations aimed at overcoming these challenges and fostering the development of a more user-friendly stablecoin ecosystem.

References

[1] $27 million stablecoin (usdt) hack attack. https://cryptonews.net/news/security/27830117/, 2023.

[2] Svetlana Abramova, Rainer Böhme, Helmut Elsinger, Helmut Stix, and Martin Summer. What can cbdc designers learn from asking potential users? results from a survey of austrian residents. Technical report, Working Paper, 2022.

[3] Svetlana Abramova, Rainer Böhme, Helmut Elsinger, Helmut Stix, and Martin Summer. What can central bank digital currency designers learn from asking potential users? In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, pages 151–170, 2023.

[4] 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.

[5] 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.

[6] Douglas W Arner, Raphael Auer, and Jon Frost. Stablecoins: risks, potential and regulation. 2020.

[7] Raphael Auer, Rainer Böhme, Jeremy Clark, and Didem Demirag. Mapping the privacy landscape for central bank digital currencies. *Communications of the ACM*, 66(3):46–53, 2023.

[8] Osato Avan-Nomayo and Aislinn Keely. Circle freezes usdc funds in tornado cash's us treasury-sanctioned wallets. https://www.theblock.co/post/162172/circle-freezes-usdc-funds-in-tornado-cashs-us-treasury-sanctioned-wallets, 2022.

[9] Parma Bains, Arif Ismail, Fabiana Melo, and Nobuyasu Sugimoto. *Regulating the crypto ecosystem: the case of stablecoins and arrangements*. International Monetary Fund, 2022.

[10] Jason Baumgartner, Savvas Zannettou, Brian Keegan, Megan Squire, and Jeremy Blackburn. The pushshift reddit dataset. In *Proceedings of the international AAAI conference on web and social media*, volume 14, pages 830–839, 2020.

[11] Richard E Boyatzis. *Transforming qualitative information: Thematic analysis and code development*. sage, 1998.

[12] Yan Chen and Cristiano Bellavitis. Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*, 13:e00151, 2020.

[13] Jonathan Chiu, Emre Ozdenoren, Kathy Yuan, and Shengxing Zhang. On the fragility of defi lending. *Available at SSRN 4328481*, 2022.

[14] Circle. Usd coin (usdc). https://www.circle.com/en/usdc. Accessed 2023.

[15] CNBC. Cryptocurrency has a big gender problem. https://www.cnbc.com/2021/08/30/cryptocurrency-has-a-big-gender-problem.html. Accessed 2023.

[16] CoinMarketCap. Cryptocurrency market capitalizations. https://coinmarketcap.com/. Accessed 2023.

[17] CoinMarketCap. Tether analytics on coinmarketcap. https://coinmarketcap.com/currencies/tether/#Analytics. Accessed 2023.

[18] Lin William Cong, Kimberly Grauer, Daniel Rabetti, and Henry Updegrave. The dark side of crypto and web3: Crypto-related scams. *Available at SSRN 4358572*, 2023.

[19] Daniel Folkinshteyn and Mark Lennon. Braving bitcoin: A technology acceptance model (tam) analysis. *Journal of Information Technology Case and Application Research*, 18(4):220–249, 2016.

[20] Ethereum Foundation. Stablecoins. https://ethereum.org/stablecoins. Accessed 2023.

[21] Alexander Friebely. *Analyzing the Efficacy of Microsoft Presidio in Identifying Social Security Numbers in Unstructured Text*. PhD thesis, Utica University, 2022.

[22] Michael Froehlich, Philipp Hulm, and Florian Alt. Under pressure. a user-centered threat model for cryptocurrency owners. In *Proceedings of the 2021 4th International Conference on Blockchain Technology and Applications*, pages 39–50, 2021.

[23] 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.

[24] 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.

[25] Sam Gilbert. Crypto, web3, and the metaverse. *Bennett Institute for Public Policy, Cambridge, Policy Brief*, 2022.

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

[27] Lewis Gudgeon, Daniel Perez, Dominik Harz, Benjamin Livshits, and Arthur Gervais. The decentralized financial crisis. In *2020 crypto valley conference on blockchain technology (CVCBT)*, pages 1–15. IEEE, 2020.

[28] Lai T Hoang and Dirk G Baur. How stable are stablecoins?(january 31, 2020). *Available at SSRN 3519225*.

[29] Judith A Holton. The coding process and its challenges. *The Sage handbook of grounded theory*, 3:265–289, 2007.

[30] Sabine Houy, Philipp Schmid, and Alexandre Bartel. Security aspects of cryptocurrency wallets—a systematic literature review. *ACM Computing Surveys*, 56(1):1–31, 2023.

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

[32] 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.

[33] 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.

[34] Johana Kimmerl. Understanding users' perception on the adoption of stablecoins-the libra case. 2020. Publisher and location not available.

[35] Ariah Klages-Mundt, Dominik Harz, Lewis Gudgeon, Jun-You Liu, and Andreea Minca. Stablecoins 2.0: Economic foundations and risk-based models. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, pages 59–79, 2020.

[36] Ariah Klages-Mundt and Andreea Minca. While stability lasts: A stochastic model of noncustodial stablecoins. *Mathematical Finance*, 32(4):943–981, 2022.

[37] 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, page 1–6, New York, NY, USA, 2019. Association for Computing Machinery.

[38] Ladislav Kristoufek. Tethered, or untethered? on the interplay between stablecoins and major cryptoassets. *Finance Research Letters*, 43:101991, 2021.

[39] 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.

[40] Bartosz Kusmierz and Roman Overko. How centralized is decentralized? comparison of wealth distribution in coins and tokens. In *2022 IEEE International Conference on Omni-layer Intelligent Systems (COINS)*, pages 1–6. IEEE, 2022.

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

[42] Alexandra Mai, Katharina Pfeffer, Matthias Gusenbauer, Edgar Weippl, and Katharina Krombholz. User mental models of cryptocurrency systems—-a grounded theory approach. 2020.

[43] Igor Makarov and Antoinette Schoar. Cryptocurrencies and decentralized finance (defi). Technical report, National Bureau of Economic Research, 2022.

[44] MakerDAO. Makerdao whitepaper. https://makerdao.com/en/whitepaper. Accessed 2023.

[45] 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.

[46] 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.

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

[48] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*, page 21260, 2008.

[49] OpenAi. Introducing chatgpt.

[50] Ingolf Gunnar Anton Pernice. On stablecoin price processes and arbitrage. 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 124–135. Springer, 2021.

[51] Microsoft Presidio. Presidio: Data protection and de-identification sdk.

[52] Reuters. Stablecoin usdc breaks dollar peg after revealing $3.3 billion silicon valley bank exposure. https://edition.cnn.com/2023/03/11/business/stablecoin-circle-silicon-valley-bank/index.html, 2023.

[53] Mehdi Salehi, Jeremy Clark, and Mohammad Mannan. Red-black coins: Dai without liquidations. 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 136–145. Springer, 2021.

[54] 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.

[55] Janice Jianing Si, Tanusree Sharma, and Kanye Ye Wang. Understanding user-perceived security risks and mitigation strategies in the web3 ecosystem. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–22, 2024.

[56] Terra. Terra money. https://www.terra.money/. Accessed 2023.

[57] Tether. How tether works. https://tether.to/en/how-it-works. Accessed 2023.

[58] VAN TRAN. Crypto firm paxos faces sec lawsuit over binance usd token. https://coinculture.com/au/business/crypto-firm-paxos-faces-sec-lawsuit-over-binance-usd-token/, 2023.

[59] Fiona van Echelpoel, Maria Teresa Chimienti, Mitsutoshi Adachi, Phoebus Athanassiou, Irina Balteanu, Thomas Barkias, Ioannis Ganoulis, Danielle Kedan, Holger Neuhaus, Adam Pawlikowski, et al. Stablecoins: Implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area. Technical report, ECB Occasional Paper, 2020.

[60] Artemij Voskobojnikov, Svetlana Abramova, Konstantin Beznosov, and Rainer Böhme. Non-adoption of crypto-assets: Exploring the role of trust, self-efficacy, and risk. In *ECIS*, 2021.

[61] 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 *International conference on financial cryptography and data security*, pages 595–614. Springer, 2020.

[62] Wang Chun Wei. The impact of tether grants on bitcoin. *Economics Letters*, 171:19–22, 2018.

[63] 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.

[64] 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.

[65] Chenhang Zhou, Yu Chen, Roger Wattenhofer, and Ye Wang. Print your money: Cash-like experiences with digital money. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–7, 2023.

[66] 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.

[67] Liyi Zhou, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, Kaihua Qin, Roger Wattenhofer, Dawn Song, and Arthur Gervais. Sok: Decentralized finance (defi) attacks. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 2444–2461. IEEE, 2023.

Appendix A. Interview Study

A.1. Interview Protocol

A.1.1. ***Part 1: Opening*.** Thank you so much for taking the time to participate in our user study. My name is *** and I'm a researcher from the ***. Our research is trying to understand users' experience and practices with stablecoins. Throughout our discussion, I'll be asking you a series of questions. Remember, there is no right or wrong answer. We are keenly interested in your unique experiences and opinions.

Would it be okay if I audio record our session for note-taking accuracy? Please be assured that your identity will be kept confidential, and your real name won't be mentioned in any of our publications or presentations. You're free to ask questions or pause the interview at any point. May I have your consent to record this call?

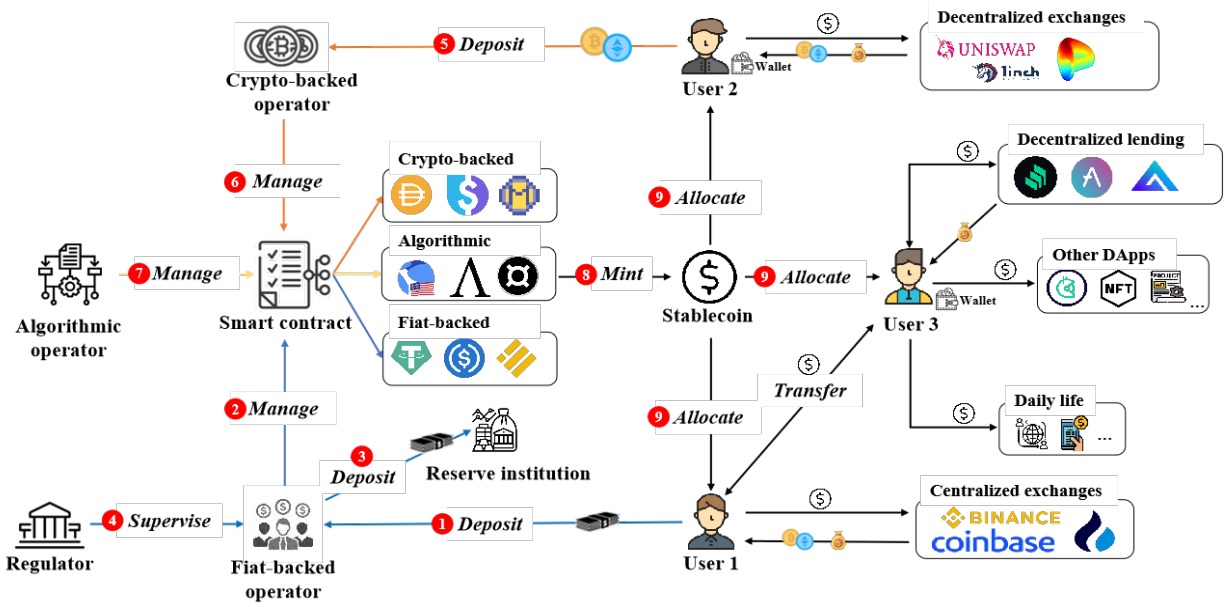

Figure 2: An Interaction Framework of Stablecoin within the Crypto Ecosystem. The issuance process of fiat-backed stablecoins corresponds to reference points ❶-❹ and ❽-❾. Take USDT as an example, ❶ User 1 deposits 100 dollars into Tether's bank account, and then ❷ Tether uses a smart contract to ❽ mint 100 USDT and ❾ allocates to the user. ❸ The operator (issuer) deposits the fiat collateral in a reserve institution like a bank. Stablecoin reserves are maintained by central entities that regularly audit their funds and ❹ work with regulators to ensure that the entities holding stablecoin reserves remain compliant. The issuance process of crypto-backed stablecoin corresponds to reference points ❺-❻ and ❽-❾. Take DAI as an example, ❺ User 2 deposits $150 worth of ETH into a collateralized debt position (CDP) [44] set up by Maker. ❻ The collateralized vault triggers a smart contract to ❽ mint $100 worth of DAI and ❾ sends it to the user [44]. The issuance process of algorithmic stablecoin corresponds to reference points ❼-❽. Algorithmic operator ❼ manages to set the conditions for the stablecoin's stability mechanisms. Following this, ❽ the stablecoin is minted automatically by the smart contract based on these predefined rules. ❾ The newly created stablecoins are allocated to users.

A.1.2. *Part 2: Experience with Stablecoin.*

- In your opinion, what are stablecoins? Can you describe them in your own words?
- How do you think stablecoins differ from other cryptocurrencies like BTC?
- What is your primary purpose for using stablecoins?
- Can you share some specific scenarios in which you typically use stablecoins?
- Do you know how many different stablecoins are available in the market?
- Can you give some examples of stablecoins you are familiar with?
- Do you know the differences between these different stablecoins? Could you describe them in your own words?
- Do you hold any of these types of stablecoins? If so, could you list the stablecoins you have used?
- What made you choose to use [specific stablecoins mentioned by the participant]?
- What made you decide not to use [specific stablecoins mentioned by the participant]?
- Would you consider using [specific stablecoins mentioned by the participant]? If yes, please explain why; if not, what are the reasons?
- If it is convenient, could you share the total amount you have invested in stablecoins?
- How frequently do you use stablecoins?
- Has your usage frequency changed compared to other cryptocurrencies?
- What factors have influenced the changes in your usage frequency?

A.1.3. *Part 3: Risk Perception and Mitigation.*

- When using stablecoins in [the scenario mentioned by the participant], have you ever been concerned about the price instability of stablecoins? What are those concerns?
- Why are you concerned about these issues?
- How do you manage those concerns?
- Have you personally experienced a situation where the price of a stablecoin became unpegged? Could you share that experience with us?
- How did you handle that situation?
- How did this event influence your future behavior regarding stablecoin usage?
- In recent years, there have been reports of some stablecoin projects collapsing in the cryptocurrency market. Have you heard of these events?

- Can you provide examples of the news you've heard?
- How do you personally view these failures?
- Have these security issues affected your overall trust in stablecoins? If so, in what ways?
- Have you taken any specific measures to protect the security of your stablecoin assets? If so, what measures have you taken?

A.2. Demographics of the Interviewees

Table 3 shows the interview participants demographics.

Appendix B. Details in Empirical Analysis on Reddit

B.1. Data Collection

We examined the top five hundred subreddits on the Reddit platform, subsequently selecting subreddits tagged as "crypto". A total of seven such communities were identified: r/CryptoCurrency, r/ethereum, r/bitcoin, r/dogecoin, r/NFT, r/CryptoMarkets, r/Crypto-Technology.

To construct our dataset, we initially extracted all posts from the targeted subreddits using relevant keywords. The extraction process was facilitated by the Python Pushshift.io API Wrapper (PSAW) [10]. Our selection of keywords included notable stablecoin projects such as "*USDT*", "*USDC*", "*DAI*", and the names of the stablecoin issuer such as "*Tether*", "*Circle*". Following the data extraction, we conducted a manual review of the collected posts to ensure each contained at least one of the specified keywords. We scratched 9,326 posts initially.

B.2. Data Preprocessing

Sensitive information removal: Prior to uploading our scraped data to GPT-4 [49], we performed local anonymization of sensitive information within the dataset. For this task, we utilized the open-source toolkit Microsoft Presidio, specifically designed to ensure sensitive data identification and anonymization [51]. Previous studies have validated its effectiveness, with an accuracy rate of up to 99% in identifying Personally Identifiable Information (PII) [21].

B.3. Post Classification

We categorized Reddit posts to investigate user discussions about stablecoins. Initially, we randomly selected 100 posts for thematic analysis. Two researchers independently analyzed 20% of the selected posts, developed an initial coding framework, and refined it through iterative comparison until a consistent codebook was established. This finalized codebook was then applied to the remaining posts by the two researchers, followed by a final consistency check after all posts were coded. Subsequently, the codebook was organized into classification criteria through thematic analysis, which served as prompts for GPT-4 to analyze the posts. In this process, GPT-4 first categorized the same 100 posts that had been manually classified by the researchers. The results were compared, and the accuracy rate reached 89%, the same standard was used to allow ChatGPT-4 to continue classifying the remaining posts. For posts that could not be automatically classified, the researchers conducted manual reviews. The results indicated that Category 1 (*Introduction and security issues of stablecoins*) contained 5403 posts, with 1192 posts broadly discussing stablecoins and 4211 posts discussing risks. Category 2 (*Requests for assistance with cryptocurrency operations*) included 1214 posts, and Category 3 (*Cryptocurrency investment advertisements*) included 2243 posts (with 12 posts requiring manual classification due to GPT-4's inability to classify them), and 466 posts were found to be unrelated to stablecoins (verified manually). Our research goal is to analyze users' perceptions and security awareness of stablecoins, so we focus on posts in Category 1. Although the content of Categories 2 and 3 is related to the broader cryptocurrency ecosystem, we exclude them to maintain the research focus and reduce potential bias.

Then we used the same classification method to classify posts on the theme of discussing stablecoins (excluding risk-related topics). The accuracy of classification using GPT-4 reached 87%. Table 4 presents the classification results. We found that discussions primarily focus on the necessity and specific uses of stablecoins, such as a medium of exchange, payment method, and investment tool.These findings are partially consistent with Section 4 and support conclusions from our semi-structured interviews.

For classifying posts on the theme of stablecoin security concerns, we employed the same method to categorize the posts. We initially selected 100 posts for thematic analysis and then used GPT-4 for reclassification to verify accuracy. GPT-4 correctly categorized 91 posts, achieving an accuracy rate of 91%. This standard was subsequently applied to the remaining posts using GPT-4, with results presented in Table 5. Our analysis revealed that online discussions prominently feature users' concerns about operators and regulatory issues. Users are generally worried about stablecoin operators' ability to ensure stability and security, as well as their transparency and credibility to maintain trust. Additionally, users expressed significant concerns about regulatory issues, such as the impact of government crackdowns on the use and circulation of stablecoins, which could lead to a decline in market value and user confidence. Discussions about third-party institutions are less frequent, indicating relatively low user awareness of these entities. In our interviews, some interviewees mentioned that they only become aware of this issue when reserve institutions, such as SVB, encounter problems. This further suggests that although third-party institutions play an important role in the stablecoin ecosystem, users' understanding and awareness of their potential risks still need to be improved.

TABLE 3: Demographics of the Interviewees. NA indicates that the interviewee was unwilling to provide this information.

ID	Age	Gender	Occupation	Country	Exp. (yrs)	Stablecoins Usage
P1	25-34	Male	Engineer	China	2-3	USDT
P2	18-24	Male	Student	China	>3	USDC, USDT
P3	25-34	Male	Freelancer	Montenegro	>3	USDT, USDC, DAI
P4	25-34	Male	Investor	China	>3	USDT, USDC, DAI, UST
P5	25-34	Male	Crypto researcher	Singapore	>3	USDT, USDC, DAI, UST, FRAX
P6	25-34	Male	Software engineer	China	>3	BUSD, USDT
P7	25-34	Male	Assets manager	China	>3	USDT
P8	18-24	Male	Software engineer	Singapore	>3	USDT, USDC, LUSD, RAI
P9	25-34	Male	NA	United States	>3	USDC
P10	18-24	Male	Student	United States	2-3	USDC, DAI
P11	18-24	Female	Analyst	Singapore	2-3	USDT, USDC
P12	35-44	Male	Entrepreneur	United Kingdom	>3	USDT, DAI, USDP
P13	25-34	Female	Student	China	>3	USDC, USDT, DAI
P14	35-44	Male	Software engineer	China	1-2	USDT
P15	25-34	Male	Student	China	1-2	BUSD, USDT, USDC
P16	18-24	Male	Student	Australia	>3	USDT, USDC, UST
P17	25-34	Female	Accountant	Australia	1-2	USDT, BUSD, UST
P18	25-34	Male	Software engineer	Malaysia	>3	USDT, USDC, BUSD, UST
P19	18-24	Male	Web3 practitioner	United Kingdom	2-3	USDT, USDC, DUSD
P20	18-24	Male	Student	United States	2-3	USDT, USDC
P21	18-24	Male	Assets manager	United Kingdom	>3	USDT, USDC, DAI

TABLE 4: Classification of Stablecoin Discussions from the Reddit Platform (Excluding Risk-Related Topics)

Topic	**Explanation**	**Post Quantity**	**Percentage(%)**
Introduction of Stablecoin	Introduce the basic concepts of stablecoins, explaining how they maintain their value stability, the entities that issue them, and how they operate in the market.	104	8.72%
Concerns and Discussions About Using Stablecoins	Discuss the concerns and questions about using stablecoins, including why people choose to use them and a comparison of different stablecoins.	171	14.35%
Using Stablecoins as a Means of Payment	Discuss the use of stablecoins for making payments, including their acceptance by merchants, transaction speed, and cost efficiency compared to traditional payment methods.	331	27.77%
Using Stablecoins as a Medium of Exchange in the Crypto Market	Discuss how stablecoins are used as a trading pair in the cryptocurrency market, facilitating the exchange of other digital assets and providing liquidity.	317	26.59%
Using Stablecoins as an Investment Asset	Discuss the potential of stablecoins as an investment asset, including their use in yield farming, interest-earning accounts, and other investment strategies.	231	19.38%
Tax Implications and Considerations for Stablecoins	Discuss the tax considerations associated with stablecoins, including how they are treated under different tax jurisdictions, reporting requirements, and potential tax liabilities.	38	3.19%

TABLE 5: Classification of Stablecoin Security Risk Discussions on the Reddit Platform

Topic	**Explanation**	**Post Quantity**	**Percentage(%)**
Operator Risk	Discussions on the risks associated with the issuers or operators of stablecoins, including potential mismanagement and lack of transparency.	1449	34.41%
Collateral Risk	Discussions on the risks related to the backing reserves of stablecoins, such as the liquidity of collateral assets, overcollateralization, and the potential for collateral value fluctuations.	638	15.15%
Operational Risk	Discussions on the risks inherent in the operational mechanisms of stablecoins, including technological vulnerabilities and smart contract bugs.	387	9.19%
Third-party Risk	Discussions on the risks associated with third-party institutions involved in stablecoin transactions, such as exchanges, custodians, and other intermediaries.	293	6.96%
Regulation Risk	Discussions on legal and regulatory issues impacting stablecoins, including compliance requirements, regulatory scrutiny, and the potential for legal restrictions by governmental authorities.	1444	34.29%