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

Conference Paper · December 2021

DOI: 10.1145/3510487.3510494

CITATIONS
12

READS
233

3 authors:

Michael Froehlich
Center for Digital Technology and Management
16 PUBLICATIONS **105** CITATIONS
SEE PROFILE

Philipp Hulm
Technische Universität München
1 PUBLICATION **12** CITATIONS
SEE PROFILE

Florian Alt
Universität der Bundeswehr München
313 PUBLICATIONS **7,723** CITATIONS
SEE PROFILE

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

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

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

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

ABSTRACT

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

CCS CONCEPTS

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

KEYWORDS

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

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

1 INTRODUCTION

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

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

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

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

2 BACKGROUND

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

2.1 Cryptocurrency and HCI

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

2.2 Threat Modeling

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

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

2.3 Cryptocurrency Security and Threats

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

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

2.4 Summary

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

3 METHOD

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

3.1 Participant Recruiting

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

3.2 Focus Group

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

3.3 Delphi Study

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

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

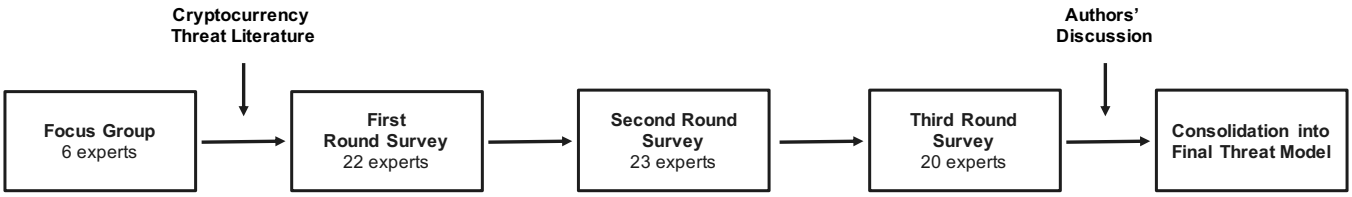

Figure 1: The threat model was developed in five steps. First, we conducted a focus group (n=6). Second, we combined the outcomes with existing research on cryptocurrency threats into the first version. Third, in steps 2-4, we used a three-round Delphi process (n=25) to validate and iterate the model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

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

3.4 Limitations

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

4 RESULTS

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

4.1 Threat Model Overview

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

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

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

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

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

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

4.2 Accidental Threats

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

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

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

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

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

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

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

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

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

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

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

4.3 Privacy Threats

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

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

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

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

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

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

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

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

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

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

4.4 Physical Threats

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

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

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

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

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

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

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

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

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

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

4.5 Financial Fraud Threats

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.6 Social Threats

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

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

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

All sub-forms share the following threat characteristics:

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

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

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

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

All sub-forms share the following threat characteristics:

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

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

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

4.7 Technical Threats

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

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

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

All sub-forms share the following threat characteristics:

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

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

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

All sub-forms share the following threat characteristics:

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

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

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

All sub-forms share the following threat characteristics:

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

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

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

All sub-forms share the following threat characteristics:

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

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

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

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

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

All sub-forms share the following threat characteristics:

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

5 DISCUSSION

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

5.1 Summary

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

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

5.2 Relevance

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

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

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

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

5.3 Design Challenges and Future Work

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

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

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

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

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

6 CONCLUSION

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

ACKNOWLEDGMENTS

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

REFERENCES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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