Investigating Wrench Attacks: Physical Attacks Targeting Cryptocurrency Users

Marilyne Ordekian
Department of Computer Science, University College London, UK

Gilberto Atondo-Siu
Department of Computer Science, University of Cambridge, UK

Alice Hutchings
Department of Computer Science, University of Cambridge, UK

Marie Vasek
Department of Computer Science, University College London, UK

Abstract

Cryptocurrency wrench attacks are physical attacks targeting cryptocurrency users in the real world to illegally obtain cryptocurrencies. These attacks significantly undermine the efficacy of existing digital security norms when confronted with real-world threats. We present the first comprehensive study on wrench attacks. We propose a theoretical approach to defining wrench attacks per criminal law norms, and an interdisciplinary empirical approach to measure their incidence. Leveraging three data sources, we perform crime script analysis, detecting incidents globally across 10 interviews with victims and experts, 146 news articles, and 37 online forums. Our findings reveal diverse groups of attackers ranging from organized crime groups to friends and family, various *modi operandi*, and different forms of attacks varying from blackmail to murder. Despite existing since Bitcoin's early days, these attacks are underreported due to revictimization fears. Additionally, unlike other cryptocurrency crimes, users with advanced security experience were not immune to them. We identify potential vulnerabilities in users' behavior and encourage cryptocurrency holders to lean into digital as well as physical safety measures to protect themselves and their cryptocurrency. We offer actionable recommendations for the security community and regulators, highlighting the double-edged sword of Know Your Customer policies.

2012 ACM Subject Classification Applied computing → Law; Applied computing → Digital cash; Security and privacy → Social aspects of security and privacy; Social and professional topics → Financial crime

Keywords and phrases cryptocurrency, Bitcoin, crime, wrench attack, physical attack

Digital Object Identifier 10.4230/LIPIcs.AFT.2024.10

Funding *Marilyne Ordekian*: UK Engineering and Physical Sciences Research Council (EPSRC), grant No EP/S022503/1.
Gilberto Atondo-Siu: European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme, grant No 949127.
Alice Hutchings: European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme, grant No 949127.

1 Introduction

Since the launch of Bitcoin in 2009, cryptocurrency owners have faced a constant threat of cyberattacks, financial crimes, and emerging risks threatening the safety and security of their funds [29, 10, 47, 4]. In 2022 alone, $3.8B was reportedly stolen from cryptocurrency users and service providers [15].

While cryptocurrencies may open users up to cyberattacks, the threat of physical attacks has not diminished. Hal Finney, a highly influential cypherpunk and computer scientist, and

6th Conference on Advances in Financial Technologies (AFT 2024).
Editors: Rainer Böhme and Lucianna Kiffer; Article No. 10; pp. 10:1–10:30
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

the first user to download and receive Bitcoin in 2009, was a victim of such attack [44]. Unlike other forms of cryptocurrency-specific/facilitated crime [10, 57], this threat targets users physically outside the cyber world. These attacks, also known as "wrench attacks," target users in the real world to illicitly acquire their cryptocurrencies or the means of access.[1][2]

The term **$5 wrench attack** first appears in the webcomic, XKCD [64]. The comic describes two characters discussing a physical attack using a $5 wrench to force the victim to provide information rather than orchestrating a cyberattack. This term has been adopted in the cryptocurrency space [38], hence the terminology we use throughout this paper.

Five aspects distinguish cryptocurrency wrench attacks from their digital counterparts and make them a serious threat requiring attention. First, the crime scene is in the physical world rather than the digital, thereby endangering the physical security and safety of users. Second, the conventional *modi operandi* distinguish these, as attackers forgo the technical skills required to bypass cybersecurity measures and revert to primitive tools and methods reminiscent of conventional crimes, such as violence, robberies, extortion, etc. Third, wrench attacks are crimes against persons and property; targets are not just property and ownership, but also people (users). Fourth, wrench attacks challenge existing cybersecurity measures, as no existing security measure can ensure that the funds of a victim with a gun pointed at them are secure. Fifth, everyone is a potential victim, as attackers do not distinguish between old and new users, professional traders and amateurs, or levels of security awareness.

To deeply understand this emerging threat, we investigate the following research questions:

RQ1: What are wrench attacks? What distinguishes them from other crimes?

RQ2: How do wrench attacks work? Considering the different types, stages, *modi operandi*, attackers, and repercussions.

RQ3: How do users perceive this threat? How can they and the cryptocurrency industry best defend against wrench attacks?

We take an interdisciplinary approach to answer these research questions. We collect three separate datasets and implement data triangulation to overcome biases that may be present in a single dataset. First, we collect *forum posts* from 37 online forums and programmatically parse out wrench attack-related content. We also conduct in-depth semi-structured *interviews* with 10 victims and experts. Finally, we analyze 147 incidents reported in 146 *news articles*.

Contributions. To our knowledge, this is the first investigation of cryptocurrency wrench attacks. Our contributions are the following:

- We collect three novel datasets: interviews, news articles, and forum posts. We combine common analysis methods from computer science along with legal and crime science methods in a way new to the computer science audience.
- In the absence of legal and scholarly definitions, we craft the first definition of a wrench attack. Each form of a wrench attack involves at least one form of traditionally recognized crime, e.g. robbery; we systematically contextualize these crimes within a wrench attack. Our definition allows wrench attacks to be separately measured and studied.
- We perform a crime script analysis and identify seven forms of wrench attacks dating back to 2014, including violent crimes, aggravated thefts, and a new form of domestic abuse we pin as cryptocurrency-facilitated domestic economic abuse.

[1] Acquiring cryptocurrencies often happens when a victim is forced to transfer their cryptocurrencies to the attacker; whereas acquiring the means of access is where an attacker gains direct access to a user's wallet. We discuss this distinction further in §3.

[2] "Means of Access" incorporates digital means (e.g. private key, wallet password) and physical means (e.g. hardware devices like cold wallets or computers) allowing access and/or control of cryptocurrencies.

- We identify new physical and cyber security vulnerabilities in cryptocurrency users' behaviors. Accordingly, we devise recommendations for users, policymakers, software designers, and other stakeholders.

2 Background

In Section 2.1 we overview prior work which touches upon cryptocurrency physical attacks. Then in Section 2.2 we explain our methodology, crime script analysis.

2.1 Cryptocurrencies and Physical Attacks

Cryptocurrency users encounter a diverse range of threats, with prior work categorizing these threats based on varied levels of risk [29, 1]. These user-centered threats span cybersecurity and technical risks, financial and economic risks, and social and legal risks [29, 1, 10, 51].

Physical attacks have been briefly acknowledged in prior work as a source of threat to users, however, none comprehensively and specifically investigate wrench attacks or physical attacks targeting cryptocurrency users. Froehlich et al. identify physical attacks as one of six threats faced by cryptocurrency users; they focus on the devices or physical objects, without considering the harms or attacks directed towards users [29]. Voskobojnikov et al. explore the concerns of cryptocurrency users, including physical safety and the fear of a gun being held to their heads [62]. Other works explore the reasons for the non-adoption of cryptocurrencies, highlighting the fear of physical safety as a factor for avoidance [61]. Empirical work examining mobile wallets identifies physical safety concerns as well like the fear of phones being snatched whilst making mobile payments [63]. There has been some work into making Bitcoin wallets more secure, including against physical attacks [32, 6], though the threat models for these improved techniques are often not robust against a coercive physical attacker.

2.2 Crime Script Analysis

Crime script analysis is a methodology from the crime science field used to systematically identify the stages carried out when committing a specific crime. These stages include actions preceding, during, and following the commission of a crime [19, 20] where a criminal event encompasses specific actors, tools, actions, locations, and motivations. By unraveling the necessary processes to commit a crime, this approach provides a deeper understanding of how crimes are committed, situational factors, and other influences. Crime scripting is an emerging method for identifying intervention approaches derived from different fields. Crime scripts can be developed with a diverse range of data, including police reports and interviews, and are developed by explicitly recording the steps and stages involved in the process.

Researchers can use crime scripts to understand various types and classes of crimes [23]. These include complex crimes like organized crimes or financial crimes which incorporate a longer process, more actors, more preparation, and often a mixture of a few different classes of crimes [37, 31, 18].

3 Definition and Crime Steps of Wrench Attacks

There is currently no definition of a wrench attack in legislation or academic work, making it difficult to measure the scope of such attacks. Other work investigates threats with measurable, technical definitions (e.g. malware is determined by analyzing network traffic, files changed, etc., or some signature found in the code itself [5]), however, physical crime does not yield itself to technical definitions. Instead, we use legal methods derived from criminal law to formally define these attacks committed in the physical world. This assists in the subsequent measurement of the incidents.

Criminal courts and law enforcement agencies utilize national criminal codes or laws to break down an act into steps; this process determines whether an act is punishable by law, and if so, what type of punishment it entails. According to criminal law principles, an act is considered "criminal" only if it is defined in the law and its steps are outlined [65]. This is the universal concept of "no punishment without law".[3] These defined steps are referred to as crime elements; they constitute a checklist used to determine whether an act follows predetermined steps and requires penalizing the perpetrator.

Crime elements consist of two main components: the *Mens Rea* element, also known as the "guilty mind", represents the criminal intent of a perpetrator; and the *Actus Reus* element, or the "guilty act", refers to the physical element of a crime, i.e. physical conduct(s) that constitutes a crime [34]. The *Actus Reus* requires a 1) act, 2) result, and 3) causation [34].

We propose a definition outlining the steps (crime elements). To craft this definition, a criminal law expert on our team examined the English common law and French civil law, both key references for legal systems worldwide. Analyzing the French "code pénal" and English criminal law, provides insights into crime elements and how they can be adapted and distilled into steps; hence a checklist [39, 55]. Using this method, we propose our definition of a wrench attack, create its specific crime elements and aid in understanding how it unfolds from planning to execution.

Definition. We define wrench attacks as the physical targeting of cryptocurrency owners with the intention to gain unlawful possession and ownership of their cryptocurrencies by means of physical force or threat of force or harm. The act combines offences against property, and offences against natural persons.

Elements. Our proposed elements for wrench attacks are detailed in Table 1; we define these elements per legal norms and provide a loose understanding for a general audience.

Wrench attacks are intentional crimes and cannot occur accidentally. Furthermore, similar to many crimes, they have additional unique requirements, such as "property" and the property "belonging to another" (here the victim's cryptocurrency or means of access). The targeted "property" is owned or possessed by someone other than the attacker, as the attack itself will shift that possession from the victim to the attacker. Finally, wrench attacks can take seven different forms (Table 3), yet not all can result in success; some are failed attempts i.e. for reasons not intended by the perpetrator, the desired outcome does not occur. Though, as demonstrated in Table 4, most of the attacks were successful.

Anatomy of a Wrench Attack. We translate this definition and elements into a step-by-step systematic guide on how wrench attacks are committed. This anatomy is presented in Figures 1 and 2, which break up the attack into events precursing the physical attack (Fig. 1) and events occurring during the attack resulting in the outcome (Fig. 2).

Exclusion Criteria. Our proposed definition acts as an inclusion criterion as it outlines what qualifies as a wrench attack. By following this definition, we exclude scenarios like insider threats (not targeting an individual's cryptocurrency) and attacks on physical infrastructure (not targeting a person). Appendix D outlines the excluded scenarios.

[3] This is also known as the Principle of Legality in criminal law. It was developed in the 18th century by Cesare Beccaria [7].

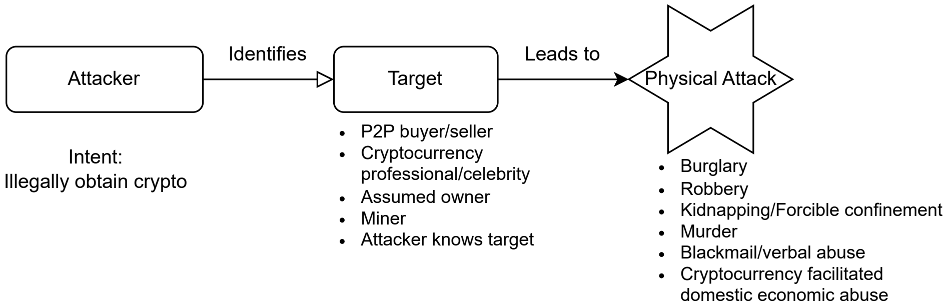

Figure 1 Anatomy of a Wrench Attack: Preparation.

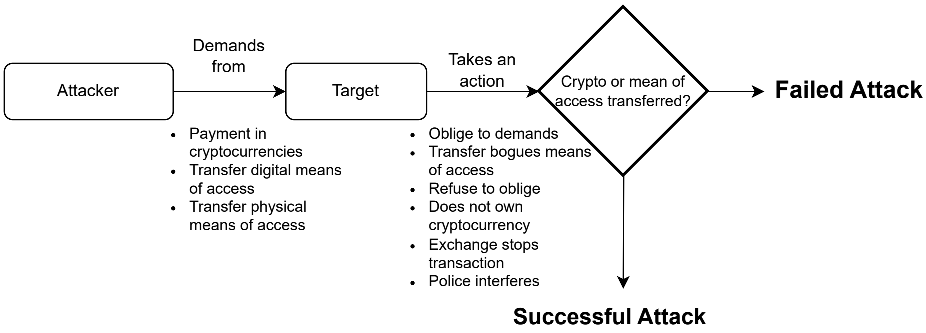
Attacker
Demands from
Target
Takes an action
Crypto or mean of access transferred?
Failed Attack
Successful Attack
Payment in cryptocurrencies
Transfer digital means of access
Transfer physical means of access
Oblige to demands
Transfer bogues means of access
Refuse to oblige
Does not own cryptocurrency
Exchange stops transaction
Police interferes

Figure 2 Anatomy of a Wrench Attack: During and After.

4 Methodology

Informed by the definition outlined in §3, we use data triangulation, a research method that uses multiple datasets, methods, and approaches to answer a research question [14, 58, 24]. The goal of data triangulation is to enhance validity and credibility. Therefore, we implement three different research designs and data sources to present a comprehensive understanding of wrench attacks; these three datasets are later used to perform the crime script analysis in §5. We present a mixture of qualitative and quantitative research designs, collecting data via interviews §4.1, forum posts §4.2, and news articles §4.3. Table 2 summarizes our datasets.

4.1 Interviews

We conducted semi-structured interviews to gain a deeper understanding of wrench attacks, victimization process, user susceptibility and security behaviors that either ignite or prevent wrench attacks. We interviewed three groups of users: 1) victims, 2) people who personally know a victim, and/or 3) academics or industry personnel actively involved in the cryptocurrency ecosystem.

4.1.1 Recruitment

Cryptocurrency owners in general are difficult to survey [3, 2]. Identifying participants for wrench attacks is even more challenging due to the sensitive nature of these incidents. We took measures to ensure potential victims felt safe coming forward and speaking with us while maintaining their privacy during initial contact. When advertising the interviews,

Element	Definition	Loose Understanding
Property	Funds in possession (i.e. cryptocurrencies) or the means of access that provide the right to access and transfer funds, such as keys, passwords, and seed phrases.	What the attackers desire to get through the attack (cryptocurrency).
Belonging to Another	The perpetrators are aware that the property subject of the attack, at the time of the attack, is under the possession or control of another "person" (natural or legal person).	Perpetrators are aware that the funds belong to someone else.
Act	Willed and controlled bodily movements [45]. Acts are detailed in Table 3.	What the attacker did.
Result	Appropriation; in this case, transfer of possession (of the funds) i.e. the victim is permanently or for a prolonged period deprived of their ownership, as offenders assume the legal rights over the victim's property (i.e. cryptocurrencies or the means of access).	Attacker must take (or forcibly lend from) the victim's cryptocurrency.
Causation	The conduct of using force or threat of force or harm caused the acquisition of the means of access and/or the transfer of funds.	The attacker's conduct itself caused the harm or damage to the victim and led to their loss of funds.
Mens Rea	Wrench attacks are intentional acts. We consider: 1) general intention where the offender is aware of the nature of the conduct and has a desire to perform it, 2) specific intention where the offender intends to permanently deprive the victim of their funds or means of access.	Attacker must intend to steal cryptocurrency.
Attempt	1) Acquiring the means of access, but failing to transfer the coins, 2) acquiring means of access, but the wallet contains no funds, 3) failure to acquire genuine means of access from the victim; i.e., faulty means of access, 4) the victim does not give in to the threats or assault, 5) the victim does not or no longer has a wallet(s)/funds/or access to the means of access.	The attacker's conduct failed to deliver the desired outcome i.e. acquiring the cryptocurrencies.

Table 1 Crime elements of wrench attacks per our proposed definition and scope.

we initially advertised to people who knew a victim and cryptocurrency experts. This was crucial. All victims we interviewed initially signed up to participate as experts, but during the interviews, they disclosed that they were victims.

We followed a multi-step recruitment process. We reached out to academics and cryptocurrency experts, securing five interviews. We contacted 98 attendees of an academic information security conference, obtaining a further 5 interviews. Despite efforts to engage public figures, we received no responses here. Finally, we posted interview invitations on Bitcointalk [8]; this yielded eight comments but no participants.

We outlined our rigorous security measures and spent weeks building trust with participants to gain their consent to participate. Our recruitment focused on gathering personal experiences, excluding participants informed of wrench attacks solely by news reports. In total, we conducted 10 interviews both online and in person.

Source	Dataset Size	Reported Incidents	Wrench Attacks
Interviews	10	11	11
News articles	146	147	105
Forum posts	672	54	3

Table 2 Summary of wrench attack data sources and incidents. Reported incidents are filtered via our criteria to yield our wrench attack dataset.

Act	Africa	Asia	Europe	N America	Oceania	S America	Unspecified	Total
Burglary	0	9	20	7	1	1	0	38
Kidnapping	1	12	8	1	0	2	0	24
Robbery	0	9	4	9	0	1	0	23
Forcible Confinement	1	2	2	2	0	0	0	7
Murder	1	3	2	0	0	0	0	6
Blackmail	0	2	0	1	0	0	0	3
Cryptocurrency Facilitated Domestic Economic Abuse	0	1	0	1	0	0	1	3
Fraud	0	0	1	0	0	0	0	1

Table 3 The main acts involved in the wrench attacks from our dataset of news articles. The majority involved more than one act, but incidents are sorted here based on the dominating act.

4.1.2 Interview Schedule

We employ a semi-structured interview schedule. The interview schedule comprises 7 sections and 2 main categories: establishing and identifying the occurrence and characteristics of a wrench attack, and a series of questions about the security behavior and risk assessment of participants, general and cryptocurrency-specific demographics, and recommendations for mitigating wrench attacks. Overall, the final schedule includes 59 questions with a duration ranging from 35 to 60 minutes. The interview schedule is included in Appendix B.

4.1.3 Profile of Participants

Our sample of 10 interviews includes industry/academic experts, out of which 6 were victims or directly associated with victims, reporting 11 wrench attacks. General demographics are summarized in Appendix C. As for **cryptocurrency-specific demographics**, most participants have over four years of experience with cryptocurrencies, with about half being early adopters. Three report using peer-to-peer (P2P) in-person transactions, which we outline as a major risk factor in §5.1.1, while a minority (two) use ATMs. Notably, all use centralized exchanges such as Binance, hence all underwent Know Your Customer (KYC) verification. Half the participants knew of specific breaches on exchanges they used; the rest either assumed their exchange had been breached or were entirely unaware.

Half the sample, especially those residing in financially unstable countries, rely on cryptocurrencies as an alternative payment method. Three use cryptocurrencies for research or as a store of value. Nearly all participants own multiple cryptocurrencies, with Bitcoin being the most common.

4.2 Forum Posts

In order to ensure comprehensiveness, we search for additional reports on social media.

Our first data source is the CrimeBB dataset [49], created in 2018, which amalgamates underground forum data. This dataset is available for academic research use under a data-sharing agreement with the Cambridge Cybercrime Centre. We search through ∼110 million posts made by 6 million members from 36 underground forums (some of which have been active since 2007) including HackForums and Dread. This yielded no wrench attack reports.

We additionally use the online forum Bitcointalk. Satoshi created this in February 2009 and it is the largest cryptocurrency-focused forum with more than 3.5M members as of January 2024. We crawl through over 45M posts from July 2010 until August 2023. After annotating a random sample, we use machine learning methods to classify the collected data as described in Appendix A. Our classification yielded 672 posts about wrench attacks including 3 victim narratives. We also parsed out links to news articles yielding two additional news articles not already included in Section 4.3. One of these articles referred to two different wrench attacks, therefore three incidents were added to our news article dataset (§4.3).

4.3 News Articles

We use an up-to-date list of news articles curated by cryptocurrency expert Jameson Lopp [40]. The list includes publicly reported physical attack cases involving cryptocurrencies. We collect 144 news articles available from December 2014 through October 2023, reporting 144 unique incidents. As outlined in §4.2, our analysis of Bitcointalk yields 2 additional news articles reporting 3 incidents. This yields a total of 146 news articles reporting 147 incidents.

We apply our definition (§3) as a selection criterion. This excludes 42 articles, leaving 104 news articles reporting 105 wrench attacks, which we use in our analysis. Appendix D details incidents excluded based on our criteria.

4.4 Coding and Analysis

We analyze the three datasets qualitatively. Qualitative analysis provides deep insights into a subject matter beyond mere quantification. The coding of the data was inductive and data-driven, with codes and themes derived directly from the data [30]. Coding of wrench attack-related sections of data followed Cornish's universal crime script scenes [19]. There is no single universal script, as it can be adapted and used diversely, depending on the complexity of the crime and its composition. In conducting this crime script, we borrow from Hutchings et al. [36], where the script is adapted and divided into three acts tacitly reflecting the original nine tracks as proposed by Cornish [20, 19].

4.5 Ethics

This work uses data obtained through interviews, online forums, and news articles. The ethics committee at the Department of Computer Science & Technology, University of Cambridge, approved this research. Our recruitment process was covered by this remit. Interview participants were provided with an overview of the research before providing informed consent. All interview data was stored locally until transcription. Transcripts exclude any information identifying the participant or third parties, and the recordings were deleted along with emails and any other records that contained participants' personal data. Participants were advised that they were free to withdraw from the study at any time and could opt to not answer any of the questions asked.

Our forum data and news articles were extracted from publicly accessible sources. In our analysis, we paraphrased any quoted text to limit searchability. Furthermore, this work focuses on analyzing aggregate information and collective behavior of online communities using publicly available data and under the British Society of Criminology's Statement of Ethics, it falls outside the requirement of informed consent [13].

4.6 Limitations

Crime research tends to have limitations due to the hidden nature of offenses, with victims often being unwilling to report, and incidents that are reported are not necessarily similar to those that are not. We aim to reduce these limitations by triangulating three data sources, using data relating to public disclosures of attacks (media reports), anonymous disclosures (forum posts), and victim accounts (interviews).

Additional limitations include privacy and personal safety concerns led some potential participants (victims) to opt against participating, this limited the variety of perspectives included in the study. Furthermore, while the captured experiences of the victims vastly enriched the dataset, and the recruitment process proved to be immensely challenging, the generalizability of the sample is constrained.

There are additional limitations related to the forum analysis. Our Bitcointalk dataset represents approximately 75% of the forum (as of August 2023). We crawl historic forums, so removed posts are excluded. Our use of specific keywords to create our training sample may add an inherent bias. Thus, we might not include all posts that are wrench attack-related.

5 Crime Script Analysis

Wrench attacks involve a combination of crimes, with the main aim being financial gain. The key element that facilitates this goal is targeting individuals. Thus, wrench attacks are possible by a combination of actions targeting both individuals and their personal property. We analyze these attacks using three datasets, dividing each incident into 3 parts: Preparation (Act 1), attack (Act 2), and the aftermath (Act 3). This allows us to encompass all crimes documented in our datasets.

5.1 Act 1: Preparation

When preparing a physical attack against a victim, the physical location and the primitive tools and methods utilized in perpetrating the offense play a pivotal role.

5.1.1 Actors

There are two main actors identified in wrench attacks, the victim(s) and the offender(s). Actor roles differ depending on circumstances. We find no notable distinction or a pivot on a specific type of users. Our three datasets reveal a variety of offending actors, indicating the absence of a singular or specific type of dominant perpetrators for wrench attacks. However, we do note the prevalence of co-offending compared to solo offending (Table 3b).

Over the Counter (OTC) brokers or peer-to-peer (P2P) transactors. In-person P2P operations are a prevalent method of exchanging cryptocurrencies with fiat or other cryptocurrencies. P2P transactions usually take place in person and do not require service providers or KYC verification, nor does it necessarily engage the banking system. It is also a prevalent approach embraced by those who are unbanked or underbanked, allowing them an alternative to transfer funds locally and globally.

Tool	Burglary	Kidnapping	Robbery	Forcible Confinement	Murder	Blackmail	Domestic Violence	Fraud
Physical Violence	19	15	7	6	2	0	0	0
Firearm	13	5	6	0	1	0	0	0
Offensive Weapon	2	0	5	0	1	0	0	0
Spiking	1	0	0	0	0	0	3	0
Legal Extortion	0	0	0	1	0	1	0	0
Swatting	0	0	0	0	0	1	0	0
Unspecified	3	4	5	0	2	1	0	1

(a) Tools used per each crime type.

	Solo	Group	Total
Strangers	13	91	104
Non strangers	2	9	11
Total	15	100	

(b) Type of offender carrying out wrench attack and their relationship. Each victim outlined independently so numbers add to more than 105.

Figure 3 Factors in different wrench attacks (news articles).

Based on our interview sample, in three instances the offender(s) were either OTC brokers or P2P transactors. Of the 104 inspected news articles, 25 reported incidents involving P2P transactions, while we found two victims with similar encounters on Bitcointalk.

However, OTC brokers can also be targeted by attackers. One of the authors informally spoke to an OTC broker whose shop was targeted on multiple occasions. The victim preferred not to be interviewed for security reasons.

Accepting payments in cryptocurrencies. The offender here is a person accepting cryptocurrencies in exchange for goods. In our interview sample, the victim was in a bar, reimbursed a person in Bitcoin for buying them a round of beer, only for this person to attack the victim and snatch their phone after learning about their Bitcoin ownership.

Family, friends, and business partners. Offenders may also be acquaintances, business partners, family members, and romantic partners; i.e. persons who know the victims and are aware of their involvement with cryptocurrencies. The involvement of these individuals might either be as a principal perpetrator, or by being a secondary party (accessory) that aids, abets, procures or counsels the principal(s) offenders. This applies to five incidents in our interview dataset but only eleven in the news articles study (Table 3b).

Organized crime groups. There are indications that crime groups are involved in wrench attacks. We note that the role of organized crime groups in technology-related crime can often be overstated [35, 41], so we refrain from quantifying this to avoid inaccurate assumptions about group offenders.

Victims as offenders. We record one incident in our interviews and three in the news articles where the offenders were former victims seeking revenge through their attack.

Corrupt law enforcement agents as offenders. Corrupt law enforcement agents could either abuse their badges or misuse confidential information gained through police records. Our news articles dataset includes five such incidents.

5.1.2 Crime Location

Real physical world. A factor setting wrench attacks apart from other cryptocurrency-related crimes is their occurrence in the physical realm. This entails direct physical contact between the offender and the victim, involving face-to-face or direct contact like calling the victim on their private number.

No favorable environment. Wrench attacks manifest across a diverse spectrum of locations and environments. Crime scenes span populated public streets, commercial establishments like shops, private residences, and secluded locales. This was unexpected, particularly the number of instances of violent crimes on busy streets in broad daylight.

Geographically. The attacks in our interview series span South America, Europe, Asia, and the Middle East. In the news article dataset, we find attacks occurring in all continents, with the predominant ones being Europe and Asia (Table 3).

5.1.3 Target Selection

We differentiate between random and non-random selection, whether victims are chosen specifically because of an identified association with cryptocurrencies or entirely at random. In our interview dataset, all targets were selected non-randomly. Offenders had varying degrees of knowledge or familiarity with victims, choosing them based on a presumed holding of cryptocurrencies. This prior knowledge could stem from acquaintanceship, transactional meetups, investigation of assumed ownership, and publicly available information e.g. the victim is a known cryptocurrency professional/figure.

In the news articles dataset, detailed information on the victim selection process or prior relationship was inconsistent. Hence, we omit implied information on the randomness of the selection, and only record cases where either a prior relationship existed between the victim and the offender (11) or the victim is a professional/public figure in the space (27).

5.1.4 Attacks over Time

Interviewees refrained from disclosing precise dates of attacks to avoid identification, but indicated timeframe; spanning from the early days (2011-2012) to the 2017/18 ICO boom and beyond. Despite a broad distribution of attacks over the years, the rate of attacks increased notably at the end of 2017; this coincides with Bitcoin reaching (at the time) an all-time high. This trend is evident in both the interview and articles datasets, with the second-highest recorded articles (20) reported in 2018. The highest number of attacks (25) is noted in 2021, following the return from Covid-19 lockdowns and the all-time high price of Bitcoin nearing $65,000.

5.1.5 Tools or Attack Methods

Wrench attacks rely on conventional methods of committing crime. Many wrench attack offenders resort to physical assault (crimes against persons). The majority of incidents involved weapons, tools, or objects that could inflict harm. Other methods involved imposing physical restrictions, spiking, etc. Table 3a outlines tools used per each crime type. Physical violence and firearms are mostly used in burglaries and kidnapping; robberies use both as well as offensive weapons (usually knives). Spiking is only used in domestic violence cases.

5.1.6 Motivation

The overarching aim of wrench attacks is to secure substantial funds. The resort to physical attacks originates from two primary motivations. First, some find it easier to illegally acquire cryptocurrencies through physical means rather than resorting to sophisticated cyberattacks.

Second, targeting affluent individuals outside the cryptocurrency space is challenging as forcing victims to make large bank payments is difficult. Unlike bank payments, there is no threshold for transferred funds in a single transaction. Additionally, offenders benefit from the absence of comprehensive and global regulatory requirements, simplifying the unrestricted transfer and cash-out process of cryptocurrencies.

5.2 Act 2: Methods

Wrench attacks are mostly perpetrated in line with other crimes. The current act explores the various methods (tracks) by which wrench attacks are committed. As a reminder, the primary goal of the attackers is financial gain, particularly to illicitly gain cryptocurrencies. Section 5.2.2 details the demands made by attackers to achieve their goal.

5.2.1 Tracks

These tracks outline variations in the wrench attack crime script found in our three datasets. We summarize the findings from the news articles in Table 3.

Track: Attacks on personal liberty. Kidnapping and forcible confinement violate the personal liberty of the victim. Kidnapping requires abducting and relocating someone by force or deception [59]; in forcible confinement, the victim's freedom of movement is confined, i.e. they are not relocated nor abducted [42]. In both cases, the aim is financial gain, either directly through the victim or by demanding a ransom from family members. Offenders primarily use physical violence, among other methods to commit this (Table 3a).

One of our interview participants was kidnapped and cuffed by acquaintances, and was forced to hand over a hardware wallet under verbal threats. Notably, five incidents in the news data involved corrupt law enforcement agents, with victims being forcibly taken to police stations and extorted by fake police reports and accusations in return for cryptocurrencies.[4] Another notable method involved offenders impersonating law enforcement agents or posing as fake investors and kidnapping victims during a business meeting in a foreign country.

Bitcointalk users express fears of kidnapping, especially fears of loved ones being kidnapped for a Bitcoin ransom or corrupt government officials leaking information to criminals.

Track: Violent crimes. Some wrench attacks have resulted in **murder**. In our interviews, an interviewee describes a wrench attack involving a murder, where the victim was kidnapped into a jungle by a contract killer hired by the victim's business partner. The news articles dataset includes six murder cases, all occurring after the 2017 ICO boom. Notably, two cases involved victims of investment scams turning into wrench attack offenders, murdering scammers who had deceived them into investing in cryptocurrencies.

Track: Crimes against property. Burglary, which entails trespassing a private premise to commit theft [33], is the most common form of a wrench attack reported in the media. As seen in Table 3a, burglaries can be hostile as they are the crime type mostly associated with physical violence and possessing firearms. In three distinct cases, the wrench attack took the form of a heist, where offenders broke into cryptocurrency firms or service providers (e.g. exchange), and assaulted employees. In the remaining incidents, the victims in most cases were either cryptocurrency experts, consultants, miners, or bloggers who publicly discussed cryptocurrencies.

In our interview dataset, a burglary incident involves breaking into a cryptocurrency user's home to take over their funds. Bitcointalk users have also been concerned about burglary as early as 2014, even though a user refers to the idea as "absurd", stating: *"How would a*

[4] We examine the Corruption Perceptions Index (CPI) rank for the countries involving these corrupt law enforcement agents [56]. These incidents occurred in India (rank 85), Ukraine (rank 116), and Nigeria (rank 150).

potential attacker with a gun even identify which house to break in? This scenario seems more like fiction and spreads unnecessary fear." **Robberies** are also committed with the use of firearms or physical force (Table 3a), but unlike burglaries, they can occur anywhere. We see a direct relation between these incidents and P2P transactions. Our interviews reveal two cases of armed robberies, in Europe and the Middle East. Both were involved in public P2P transactions between buyers/sellers during which the victims were held at gunpoint. In one case, the armed robbery escalated further into a car chase. Our interviews also include a victim who was mugged in a pub while making a Bitcoin payment with their phone. The offender upon seeing the displayed amounts of Bitcoin on the screen, stabbed the victim and fled with the phone. The news media includes 23 incidents of robberies, 17 occurring during P2P transactions in North America and Europe. One Bitcointalk post recounts an armed robbery by a gang during a P2P transaction in Europe. Another Bitcointalk user reports an attempted mugging during a P2P transaction, where the offender failed to successfully snatch their phone whilst transferring Bitcoin.

Track: Blackmail or verbal abuse. Many of the tracks also involve the use of blackmail/extortion and verbal abuse. Here, we only report instances occurring independently of any other crimes. **Blackmail** here ranges from threatening to reveal private, damaging, or embarrassing information about the victim, or threatening to harm them or a relative or a friend, unless they comply with their demands [28]. There also exists "legal" tools used in extortion, such as threatening to report someone to the police or sue them in court.

Our interview participants reported several instances of blackmail and threats. Victims report being extorted with old and/or intimate pictures of them that could damage their reputation. The offenders were previous friends, previous romantic partners, and random strangers claiming to possess such images. In one incident, the offender used the victim's family to exercise pressure. In another case, the offender extorted and threatened the interviewee with legal actions promising to get them into legal trouble.

Verbal abuse takes many forms, ranging from harassment, threats, hate speech, to insulting or abusive language. The intent is to cause the victim distress and intimidation, harass them, and/or create an unpleasant and unsafe environment. In wrench attacks, the offender has ulterior motives, i.e. obtaining the victim's cryptocurrencies. The victims we interviewed disclosed instances of verbal abuse, mostly by friends, distant family members, or acquaintances who knew the victim owned cryptocurrencies. One victim was stalked by their harasser; another incident involved the harassment of a woman during P2P transactions.

Both blackmail and verbal abuse were reported more frequently in our interview dataset (six incidents) compared to the news articles dataset (three incidents). One reason for this difference may be that news articles recount crimes that have been reported to law enforcement, and blackmail and verbal abuse might be under-reported or not taken seriously.

Track: Cryptocurrency-facilitated domestic economic abuse. When an intimate partner or family member exercises economic abuse to take over their victim's cryptocurrencies, we are faced with a combination of acts: a wrench attack and a new term we pin as cryptocurrency-facilitated domestic economic abuse. In our interview dataset, an intimate partner coerces and/or harms their partner to take unlawful possession of their cryptocurrencies. This form of economic abuse cases also occurs outside long-term intimate partner relations, such as in family settings or new romances. The news articles dataset records three cases of such abuse. In two cases, the offender and victim had a short romantic relationship after meeting on an online dating app. The other case involves a son stealing his father's funds. Notably, this track primarily occurs through spiking (Table 3a).

Attacker Demand(s)	Count	Crime Outcome	Count
Cryptocurrencies (no specification)	40	Successful	70
Means of access (private keys, storing device, etc.)	30	Failed	29
Specifically requested only Bitcoin	26	Unspecified	6
Unspecified	9		

Table 4 The distinct demands made by wrench attackers in our news articles dataset, and the outcome of the attack divided between failed attempts and successful ones.

5.2.2 Offender Demands

The primary goal of wrench attackers is to illegally acquire cryptocurrencies through physical means. However, not all attackers coerce their victims to transfer cryptocurrencies, instead, we find in our datasets a variety of requests made by offenders, as shown in Table 4.

Demanding the transfer of cryptocurrencies. In person, the offender(s) coerces the victim to personally transfer cryptocurrencies. In a successful attempt, the victim under duress, transfers cryptocurrencies to a designated address. Many offenders specifically ask for Bitcoin, however, other cryptocurrencies are demanded as well.

Demanding means of access: Storage device. The victim is coerced in person to transfer the storage device, e.g. a hardware wallet, a mobile phone, or a computer. Often the offender(s) has prior knowledge that a device exists. Consequently, the device holding cryptocurrencies is transferred.

Demanding means of access: Access information. The victim is coerced in person to reveal the private key and/or any other digital security layer that grants full access and control of the funds. Access demands are not limited to a specific type of wallet, e.g. if the victim uses a mobile wallet, the offender(s) ask for the phone PIN and the wallet app credentials. Here, there is a reveal of access/control information.

Fraud during P2P transactions. Unlike the previous scenarios, the perpetrator resorts to deception here. The perpetrator and victim meet in person to exchange cryptocurrencies/fiat. Once the victim makes a transfer, the perpetrator refuses to transfer the equivalent funds they had initially agreed on. The offender often verbally abuses or threatens the victim if they refuse to oblige.

5.3 Act 3: Attempt or Completion

The third Act includes the actions that take place following the commission of the crime, as detailed in Act 2.

5.3.1 Crime Outcome

Successful appropriation - successful wrench attack. A successful wrench attack involves the successful transfer of funds to offenders, or their acquisition of either a storage device(s) or means of access.

Failed attempt - failed wrench attack. Failed attempts occur when for any reason, the offenders do not end up with the victim's cryptocurrencies or the means of access. While not all media articles provide information on the outcome of the crime, of those that did, 28 incidents resulted in failed attempts. Attempts are typically thwarted through no funds being available in the targeted wallet, fictitious means of access, or the victim not submitting to the offender's demands.

5.3.2 Role of Law Enforcement

Under reporting. The media reports include just 105 incidents reported between 2014 and October 2023. Of the 11 incidents discussed in the interviews, only two incidents were reported to the police. Our interview participants had decided not to report due to a number of concerns. These included privacy and security considerations, as they were concerned that exposing themselves as cryptocurrency owners could create further risks. Others wanted to avoid future complications with the same offenders, as they lacked confidence in law enforcement agencies. Some victims highlighted that they thought their case might not be taken seriously, or they were hesitant about the outcome. This under-reporting is consistent with other research on online property crime [54].

Shortcoming in involvement. Law enforcement involvement varies, which can be ascribed to several factors. During the early days of Bitcoin, cryptocurrencies were often trivialized as "magic Internet money" which led to minimal law enforcement interest. One interviewee held at gunpoint in public, reported the incident to authorities. As they state: *"From the start, it was ignored."* Another early-day victim, posting their experience with attempted street robbery on Bitcointalk, questioned the usefulness of law enforcement: *"I'll report the incident to the police, but I'm doubtful anything good will come out of it."*

In recent years, the involvement of law enforcement seems to increase due to cryptocurrencies gaining more popularity and value. We can conclude this from the reporting in media (§5.1.4). Yet, not all law enforcement agencies have the capabilities or access to tools that assist in dealing with cryptocurrency crime. This can be extended to wrench attacks.

The limited role of law enforcement in usefully addressing wrench attacks helps motivate our effort in thoroughly defining wrench attacks. While all of the attacks we study were crimes and therefore under the purview of law enforcement, few were reported and even fewer still were investigated. One role of definitions is to highlight attention in understudied areas.

5.3.3 Post Attack Alert

Among the victims we interviewed, a minority chose to alert the community, the rest were hesitant. This hesitancy is observed in our online forum posts dataset, as a minority chose to share their experience. The methods of alerting others varied. Some opted to post on online cryptocurrency communities such as Bitcointalk, or other public platforms such as podcasts. Others notified local groups through Telegram or WhatsApp. Nevertheless, most were inclined to preserve their status as cryptocurrency users and decided to remain silent.

6 Security Behaviors and Risk Perception

The cryptocurrency userbase has become more diverse over time [9, 50, 3]. Abramova et al. [3] suggest a new typology that groups users into three clusters (cypherpunks, hodlers, and rookies) based on their risk perceptions and security behavior. Contrary to this, we find no relationship between user experience or security awareness and wrench attack victimization.

During the interviews, we were interested in understanding participants' security behaviors, threat assessment, and perceptions of past/future wrench attacks. This could assist in recognizing behaviors or knowledge gaps among users that increase risk or make them more favorable targets for attack. Our objective is not to engage in victim blaming, but rather discern proactive measures to counteract potential attackers.

6.1 Threat Assessment

We explore users' threat assessment relating to their cryptocurrency ownership. Participants communicated concerns about the potential exploitation of personal data as a precursor to a wrench attack. Here, they expressed distrust towards cryptocurrency service providers (e.g. exchanges) collecting excessive personal data including government IDs, biometrics, etc., necessary for KYC verification. Ordekian et al. highlight that existing AML/CFT policies applied within the cryptocurrency space have inadequacies that could cause more harm than good, especially relating to the security of personal information gathered for KYC verification [48]. An interviewee expressed these concerns, stating: *"... I have to provide a driver's license to buy a $10 NFT... But if my identity gets compromised as a result of making a transaction, it's a much higher risk, and that's purely created by the government."*

6.2 Wrench Attack Risk Perception

Existing literature identifies vulnerable groups and behaviors that predispose users to vulnerabilities in the cryptocurrency ecosystem: security breaches, poor security behavior, and self-inflicting errors. Understanding one's vulnerability to potential security threats, coupled with precautionary security behavior, influences informed security decision-making [60]. Hence, we investigate two key aspects: 1) the risk perceptions of both users and victims, and 2) their confidence in their existing security measures in thwarting future wrench attacks.

Risk perception. We asked participants about the likelihood they would experience a wrench attack in the future. For victims, we inquired if they anticipate experiencing a wrench attack again. Half anticipate the possibility, with the remaining feeling secure for diverse reasons. One participant felt secure as they resided in a jurisdiction with a low crime rate. Others believe they are unlikely targets as they own insignificant amounts of cryptocurrencies, primarily for research and curiosity purposes. However, we note many wrench attack victims are targeted because of their affiliation with the cryptocurrency sector, as attackers presume ownership. Hence, we challenge the assumption that limited funds ownership reduces susceptibility when affiliation exists.

Confidence level in security practices. Participants varied in their confidence that their security practices were effective against wrench attacks. Three expressed confidence, while others emphasized situational nuances, like the type of attack or the attacker's knowledge and skill level. A security expert was also concerned that attackers might target family members as an easier route to reach them.

Geographical location was identified by two participants as a key factor affecting their confidence level; one avoided certain countries due to security concerns. Moreover, confidence levels varied based on the wallet type. Online or mobile wallets were considered less secure and easier to steal.

Perpetrators possessing key information. In a scenario where attackers possessed information enabling fund access, 7 out of 10 participants doubted their security measures. Concerns were voiced again about the security of user information held by service providers, with participants noting that if an exchange is breached, a successful wrench attack would be possible. These concerns of exchange data breaches [3] align with prior work investigating the adverse consequences, like social engineering attacks users face due to leaked data [2].

6.3 Repeat and Multiple Victimization

Victims with a history of victimization may be at a higher risk of future victimization [21]. Understanding this and identifying patterns in victimization, such as crime types, specific environments, and the dynamics of victimization, assists in informing preventative measures.

Repeat victimization. We find being a wrench attack victim does not grant immunity against future incidents. Though a sensitive topic, two participants reported multiple wrench attack incidents, suggesting their public figure status and being early adopters as contributing factors to this.

Multiple victimization. Our interviewees report being the victims of non-cryptocurrency cybercrime. Three wrench attack victims recounted constant phishing attacks via email or SMS attempts to gain unauthorized access. Another victim reports a smart contract exploit having their NFT wallet drained. One victim thwarted a romance scam attempt. Two of the wrench attack victims attributed their multiple targeting to their fame, with one reporting online stalking and the other being impersonated with fake cryptocurrency projects and scams being promoted in their name.

6.4 Post Wrench Attack Changes

Following an attack, two participants spoke openly about behavioral changes. The first emphasized the significance of alertness, awareness, and openly discussing incidents to alert the community. The second participant mentioned avoiding carrying significant cryptocurrency amounts, especially during P2P transactions.

7 Recommendations and Intervention Areas

In this section, we outline several recommendations for interventions to help prevent wrench attacks. These recommendations are informed by suggestions made by security experts we interviewed as well as our expertise. Cryptocurrency holders may have different risk appetites and exposure, so they may choose to implement what makes sense to their individual situation. We also address intermediaries who can help prevent or mitigate wrench attacks.

7.1 Precautionary Measures for Users

In this section, we outline recommendations for users that could aid them in protecting against wrench attacks.

7.1.1 Keeping a Low Profile

Eight out of ten interviewees emphasize keeping a low profile to avoid targeting. This includes refraining from bragging, flashing wealth, and disclosing financial details. Some advise not disclosing holding funds entirely, others suggest not specifying the held amount. An interviewee explained: *“We disclose we hold, we disclose we deal, but we never disclose the amount so that we don’t become more of a target.”*

Besides maintaining secrecy, users should be careful when discussing cryptocurrencies, since eavesdroppers and discussants have turned into adversaries. Users are recommended to discuss cryptocurrencies only with trusted persons and refrain from public advertisement of their ownership, even on online forums with pseudonyms which can still be identifiable.

7.1.2 Fund Management

To prudently manage funds, strategic approaches encompass wealth distribution and storage. Geographical distribution of funds or means of access was recommended. This practice involves spreading wealth across regions to mitigate localized threats and reduce losses.

Storage diversification adds an extra layer of protection, minimizing exposure to a single point of failure and enhancing overall resilience. Using multifaceted approaches by mixing hot and cold wallets helps users avoid losing everything at once. Three interviewees describe this as *"not keeping your eggs in one basket."*

7.1.3 Digital and Physical Safety

Considering the nature of wrench attacks, a combination of digital and physical security measures can best protect against them.

Digital safety. Multisignature wallets are recommended for securely storing cryptocurrency. This method mandates m signatures out of a possible n to access funds. Regarding wrench attacks, these wallets could give victims plausible deniability that the victim would be unable to transfer the funds. The tradeoff here is that while requiring more signatures could make it harder for attackers to steal funds, it can be harder for users to set up and potentially easier for a user to lose their funds. Other digital safety measures include using 2FA on cryptocurrency online platforms or creating read-only wallets. Both of these measures would allow victims to be unable to transfer funds or otherwise add time/friction.

Physical safety. Physical security is crucial in addressing wrench attacks. Situational awareness is key, considering that different geographical locations pose varying risk levels. By staying attuned to these risks, users can adjust their behaviors to reduce potential exposure to threats. Some interviewees feel safer discussing cryptocurrencies in a country with generally low crime rates; emphasizing that the risks associated with wrench attacks are similar to other crimes, as it all depends on location. Others consider being in countries with wider and massive cryptocurrency adoption increases risk exposure, requiring extra caution.

Safety measures are necessary. In addition to keeping a low profile more generally (§7.1.1), users are recommended to avoid revealing their location in advance of travel and limit sharing personal information. Additionally, it is important to ensure personal safety during in-person cryptocurrency gatherings, particularly around due diligence on the identities and intentions of individuals attending these gatherings to minimize the risk of malicious encounters.

7.1.4 Peer-2-Peer Specific Measures

In-person cryptocurrency transactions are quite common, especially in countries with limited access to banking, financial crises, or under international sanctions [16]. Yet, this method carries risks due to direct physical contact between transactors. In the incidents reported in the news articles, 25% of cases occurred during P2P transactions.

There are two primary precautions for P2P transactions. First, exercise diligence with the seller/buyer by assessing trustworthiness before the meet-up. Users should avoid meeting random or potentially risky individuals, especially alone, have an escape plan, and choose crowded public areas with access to police. Second, exercise diligence with transactions, starting with smaller transactions to build mutual trust. Users are advised to avoid carrying large sums of funds, and only bring what is necessary. An additional recommended layer of diligence is validating large transactions and considering time-delaying transfers.

7.2 Collaborative Initiatives and Interventions

Stakeholders including governments, the cryptocurrency industry, and the community, can help protect users against wrench attacks. This section details intervention strategies.

7.2.1 Know Your Customer Policies

KYC processes are increasingly imposed by governments on cryptocurrency service providers (e.g. exchanges) to combat money laundering and terrorist financing. KYC verification involves collecting/storing/sharing personal information including physical addresses, government IDs, financial data, etc. [26, 27]. Yet, the porous security of these businesses made them highly susceptible to data breaches [46, 47, 43]. This increases the risk for users, making them potential targets for both cybercrime and wrench attacks [2].

One participant expresses how KYC verification could ignite wrench attacks: *"[...] government requirements for KYC, AML [with centralized exchanges], I would say your criminal organization that's operating in some country that has essentially ability to act in an area, they would get a list of customers of exchanges that are in that area and then they have to know which of these people [exchange customers] are approachable and everything else [...] So the government requirements that you provide identity [KYC process] actually creates like a shopping list for criminals for those kinds of stuff [wrench attacks]."*

Cryptocurrency users have voiced privacy fears over KYC verification and the substantial collection of personal information, as a minority have already been targets for physical threats following data leaks [63, 2]. Legal academics also argue that the extensive information collected by cryptocurrency service providers for KYC compliance poses a security risk to users, highlighting the unsuitability of already existing anti-money laundering regulations for the cryptocurrency industry [48]. Hence, governments should either reconsider some of these policies that are criticized in the banking system for not ideally achieving required aims [11], or impose higher security standards on these service providers.

7.2.2 Cryptocurrency Exchanges

Cryptocurrency exchanges play the role of an intermediary. They can delay or stop certain transactions going through their services. In two incidents from the news articles dataset, the wrench attackers, who successfully coerced the victims to initiate a transfer, failed to fully receive the cryptocurrencies as the transactions went through exchanges. The latter exchanges had a 24-hour delay/verification feature which enabled victims to flag the transactions and stop them. While some exchanges implement this process for large transactions in compliance with AML/CFT policies, these processes are not standard.

7.2.3 Educational Efforts

Educational resources and awareness could help non-tech-savvy users understand basic concepts like fund/key management, safe storage, and protective security measures. Participants stressed the importance for the public to be aware of emerging risks, such as wrench attacks.

7.3 System Design Change

This section proposes areas for system design changes.

7.3.1 Cryptocurrency Protocols

Cryptocurrencies themselves can be designed to keep their users safe against wrench attacks. Better protocol properties like zero knowledge protocols can assist in hiding how much a user holds. If implemented and used broadly, these can also increase privacy on a protocol level where it is impossible to tell which users are a part of which transactions. This limits information attackers can glean on potential victims.

7.3.2 Wallet Software Underpinnings

Wallet software could, for instance, allow the user to create wallets with false proofs of no funds. This could thwart potential attacks where a victim could show the false proof which could be validated by the attacker. Mechanisms for easy recovery of wallets could allow users to take back their money before the transaction is on the network. Making the software of hardware wallets seamless and changing how seed phrases are handled would make the use of backup wallets more straightforward. While this might not fully thwart known attackers, it could help mitigate the impact, particularly with users who currently rely on online or mobile wallets to store all their funds.

7.3.3 Wallet Interface Design

The user interface of cryptocurrency wallets could be changed to allow more security for the users against physical attacks. For instance, not showing transaction history/details would allow users to hide their behavior. Similarly, displaying on the main screen of the app/service the amount that a user has in their wallet is a known threat (we have a victim in our interviews who got stabbed because the offender saw their Bitcoin holdings on their phone screen). Early research demonstrates that users are rightly concerned here [63]. Not all victims are necessarily tech-savvy – a user-friendly interface while broadly useful, could help thwart attacks, since many users struggle with cryptocurrency wallet user interfaces [63, 62, 25].

8 Conclusion

There have been substantial recent efforts towards securing cryptocurrency infrastructure against digital threats. This has caused some offenders to pivot towards more antiquated methods of stealing, namely by physical force or threat.

Wrench attacks are a novel, yet unsophisticated, type of crime that is increasing in frequency. While compared to other forms of cryptocurrency crimes, wrench attacks are less prevalent, yet, their outcome is more hazardous. This not only imperils users but also impacts the trust in the space. This is particularly worrying for users residing in countries experiencing financial unrest, who have sought refuge in cryptocurrencies as an alternative [16].

The media primarily reports cryptomillionaires or dramatic incidents, but we find many attacks go unreported. There is no adequate regulatory landscape here, and existing technical defenses seem obsolete. Hence, this paper is an urgent plea to tackle this issue. Our contributions extend beyond identifying this issue; they serve as the foundation for regulators, researchers, and stakeholders to collaborate in developing strategies to mitigate the adverse risks posed by these attacks.

Wrench attacks are an example of criminals eschewing sophisticated methods of committing crime, and reverting to old-school tactics to exploit new technologies. By acknowledging these methods, we can better protect users and alleviate the spread of these attacks. Future work should investigate how regular users are being identified and whether there is a relation with data breaches.

References

1 Svetlana Abramova and Rainer Böhme. Perceived benefit and risk as multidimensional determinants of bitcoin use: A quantitative exploratory study. In *Proceedings of the International Conference on Information Systems - Digital Innovation at the Crossroads*, 2016.

2 Svetlana Abramova and Rainer Böhme. Anatomy of a High-Profile data breach: Dissecting the aftermath of a Crypto-Wallet case. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, 2023.

3 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 *Conference on Human Factors in Computing Systems*, pages 1–19, 2021.

4 Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Carlos Gañán, Tom Grasso, Michael Levi, Tyler Moore, Stefan Savage, and Marie Vasek. Measuring the changing cost of cybercrime. In *18th Workshop on the Economics of Information Security (WEIS)*, 2019.

5 Michael Bailey, Jon Oberheide, Jon Andersen, Z Morley Mao, Farnam Jahanian, and Jose Nazario. Automated classification and analysis of internet malware. In *Recent Advances in Intrusion Detection*, pages 178–197. Springer, 2007.

6 Tobias Bamert, Christian Decker, Roger Wattenhofer, and Samuel Welten. Bluewallet: The secure bitcoin wallet. In *Security and Trust Management: 10th International Workshop*, pages 65–80, 2014.

7 Cesare Beccaria. *On crimes and punishments*. Transaction Publishers, 2016.

8 BitcoinTalk. `https://bitcointalk.org/`.

9 Apolline Blandin, Gina C Pieters, Yue Wu, Anton Dek, Thomas Eisermann, Damaris Njoki, and Sean Taylor. 3rd global cryptoasset benchmarking study. *Cambridge Centre for Alternative Finance Reports*, 2021. URL: `https://www.jbs.cam.ac.uk/wp-content/uploads/2021/01/2021-ccaf-3rd-global-cryptoasset-benchmarking-study.pdf`.

10 Rainer Böhme, Nicolas Christin, Benjamin Edelman, and Tyler Moore. Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, 29(2):213–238, 2015.

11 Rainer Böhme, Johanna Grzywotz, Pesch Paulina, Christian Ruckert, and Christoph Safferling. Bitcoin and alt-coin crime prevention, 2017. `https://www.bitcrime.de/presse-publikationen/pdf/BITCRIME-RegulRep.pdf`.

12 Bernhard E. Boser, Isabelle M. Guyon, and Vladimir N. Vapnik. A training algorithm for optimal margin classifiers. In *Fifth Annual Workshop on Computational Learning Theory*, COLT '92, page 144–152, New York, NY, USA, 1992. Association for Computing Machinery.

13 British Society of Criminology. Statement of ethics, 2015. `https://www.britsoccrim.org/ethics/`.

14 Nancy Carter, Denise Bryant-Lukosius, Alba Dicenso, Jennifer Blythe, and Alan Neville. The use of triangulation in qualitative research. *Oncology Nursing Forum*, 41:545–547, September 2014.

15 Chainalysis. 2023 crypto crime trends: Illicit cryptocurrency volumes reach all-time highs amid surge in sanctions designations and hacking, 2023. `https://blog.chainalysis.com/reports/2023-crypto-crime-report-introduction/`.

16 Chainalysis. The 2023 global crypto adoption index, 2023. `https://www.chainalysis.com/blog/2023-global-crypto-adoption-index/`.

17 Nitesh V. Chawla, Kevin W. Bowyer, Lawrence O. Hall, and W. Philip Kegelmeyer. Smote: Synthetic minority over-sampling technique. *Journal of Artificial Intelligence Research*, 16:321–357, June 2002.

18 Yi-Ning Chiu, Benoit Leclerc, and Michael Townsley. Crime script analysis of drug manufacturing in clandestine laboratories: Implications for prevention. *The British Journal of Criminology*, 51(2):355–374, March 2011.

19 Derek B Cornish. Crimes as scripts. In *International Seminar on Environmental Criminology and Crime Analysis*, volume 1, pages 30–45. Florida Criminal Justice Executive Institute, 1994.

20 Derek B Cornish. The procedural analysis of offending and its relevance for situational prevention. *Crime prevention studies*, 3(1):151–196, 1994.

21 Sara Giro Correia. Patterns of online repeat victimisation and implications for crime prevention. In *2020 APWG Symposium on Electronic Crime Research (eCrime)*, pages 1–11. IEEE, 2020.

22 Corinna Cortes and Vladimir Vapnik. Support-vector networks. *Machine Learning*, 20(3):273–297, September 1995.

23 Hashem Dehghanniri and Hervé Borrion. Crime scripting: A systematic review. *European Journal of Criminology*, 18(4):504–525, 2021.

24 Norman K Denzin. Triangulation. *The Blackwell encyclopedia of sociology*, 2007.

25 Shayan Eskandari, David Barrera, Elizabeth Stobert, and Jeremy Clark. A first look at the usability of bitcoin key management. *Workshop on Usable Security (USEC)*, February 2015.

26 European Union. Regulation (EU) 2023/1113 of the european parliament and of the council of 31 may 2023 on information accompanying transfers of funds and certain crypto-assets and amending directive (EU) 2015/849, 2023.

27 FATF. Guidance for a risk-based approach to virtual assets and virtual asset service providers, 2019. `https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html`.

28 George P Fletcher. Blackmail: The paradigmatic crime. *University of Pennsylvania Law Review*, 141(5):1617–1638, 1993.

29 Michael Froehlich, Philipp Hulm, and Florian Alt. Under pressure. a user-centered threat model for cryptocurrency owners. In *4th International Conference on Blockchain Technology and Applications*, page 39–50, 2021.

30 Graham R Gibbs. *Analyzing qualitative data*. SAGE Publications Ltd, 2018.

31 Nicholas Gilmour. Understanding money laundering. a crime script approach. *The European Review of Organised Crime*, 1(2):35–56, 2014.

32 Andriana Gkaniatsou, Myrto Arapinis, and Aggelos Kiayias. Low-level attacks in bitcoin wallets. In *International Conference on Information Security*, pages 233–253, 2017.

33 Wim Hardyns and Anneleen Rummens. Predictive policing as a new tool for law enforcement? recent developments and challenges. *European journal on criminal policy and research*, 24:201–218, 2018.

34 Jonathan Herring. *Criminal law: Text, cases, and materials*. Oxford University Press, USA, 2014.

35 Alice Hutchings. Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change*, 62:1–20, 2014.

36 Alice Hutchings. Leaving on a jet plane: the trade in fraudulently obtained airline tickets. *Crime, Law and Social Change*, 70(4):461–487, 2018.

37 Alice Hutchings and Thomas J Holt. A crime script analysis of the online stolen data market. *British Journal of Criminology*, 55(3):596–614, 2015.

38 James Jones. Protect yourself against $5 wrench attacks, 2017. `https://steemit.com/bitcoin/@jamesjones/protect-yourself-against-usd5-wrench-attacks`.

39 Légifrance. Code pénal, 1992. `https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/2024-05-23`.

40 Jameson Lopp. Known physical bitcoin attacks. `https://github.com/jlopp/physical-bitcoin-attacks/`.

41 Jonathan Lusthaus. How organised is organised cybercrime? *Global Crime*, 14(1):52–60, 2013.

42 Donna L Mailloux and Ralph C Serin. Sexual assaults during hostage takings and forcible confinements: Implications for practice. *Sexual abuse: a journal of research and treatment*, 15:161–170, 2003.

43 Patrick McCorry, Malte Möser, and Syed Taha Ali. Why preventing a cryptocurrency exchange heist isn't good enough. In *Security Protocols XXVI: 26th International Workshop*, pages 225–233. Springer, March 2018.

44 Robert McMillan. An extortionist has been making life hell for bitcoin's earliest adopters, 2014. https://www.wired.com/2014/12/finney-swat/.

45 Michael S Moore. *Act and crime: The philosophy of action and its implications for criminal law*. Oxford University Press, 2010.

46 Tyler Moore and Nicolas Christin. Beware the middleman: Empirical analysis of bitcoin-exchange risk. In *Financial Cryptography and Data Security*, pages 25–33. Springer, April 2013.

47 Tyler Moore, Nicolas Christin, and Janos Szurdi. Revisiting the risks of bitcoin currency exchange closure. *ACM Transactions on Internet Technology (TOIT)*, 18(4):1–18, 2018.

48 Marilyne Ordekian, Ingolf Becker, and Marie Vasek. Shaping cryptocurrency gatekeepers with a regulatory "trial and error". In *Workshop on the Coordination of Decentralized Finance*, pages 113–133. Springer, May 2023.

49 Sergio Pastrana, Daniel R Thomas, Alice Hutchings, and Richard Clayton. Crimebb: Enabling cybercrime research on underground forums at scale. In *Proceedings of the 2018 World Wide Web Conference*, pages 1845–1854, 2018.

50 Michel Rauchs, Apolline Blandin, Kristina Klein, Gina C Pieters, Martino Recanatini, and Bryan Zheng Zhang. 2nd global cryptoasset benchmarking study. *Cambridge Centre for Alternative Finance Reports*, December 2018. URL: https://ideas.repec.org/p/jbs/altfin/201812-sgcbs.html.

51 Corina Sas and Irni Eliana Khairuddin. Design for trust: An exploration of the challenges and opportunities of bitcoin users. In *Conference on Human Factors in Computing Systems*, pages 6499–6510, May 2017.

52 Reena Shaw. Xgboost: A concise technical overview, 2017. https://www.kdnuggets.com/2017/10/xgboost-concise-technical-overview.html.

53 Karen Sparck Jones. A statistical interpretation of term specificity and its application in retrieval. *Journal of documentation*, 28(1):11–21, 1972.

54 Maria Tcherni, Andrew Davies, Giza Lopes, and Alan Lizotte. The dark figure of online property crime: Is cyberspace hiding a crime wave? *Justice Quarterly*, 33(5):890–911, 2016.

55 Theft act, 1968. https://www.legislation.gov.uk/ukpga/1968/60.

56 Transparency International. Corruption perception index, 2022. https://www.transparency.org/en/cpi/2022.

57 Arianna Trozze, Josh Kamps, Eray Arda Akartuna, Florian J Hetzel, Bennett Kleinberg, Toby Davies, and Shane D Johnson. Cryptocurrencies and future financial crime. *Crime Science*, 11:1–35, 2022.

58 Scott F Turner, Laura B Cardinal, and Richard M Burton. Research design for mixed methods: A triangulation-based framework and roadmap. *Organizational Research Methods*, 20(2):243–267, 2017.

59 Rodanthi Tzanelli. Capitalizing on value: Towards a sociological understanding of kidnapping. *Sociology*, 40(5):929–947, 2006.

60 Paul Van Schaik, Debora Jeske, Joseph Onibokun, Lynne Coventry, Jurjen Jansen, and Petko Kusev. Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, 75:547–559, 2017.

61 Artemij Voskobojnikov, Svetlana Abramova, Konstantin Beznosov, and Rainer Böhme. Non-adoption of crypto-assets: Exploring the role of trust, self-efficacy, and risk. In *European Conference on Information Systems*, 2021.

62 Artemij Voskobojnikov, Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. Surviving the cryptojungle: Perception and management of risk among north american cryptocurrency (non) users. In *Financial Cryptography and Data Security*, pages 595–614. Springer, 2020.

63 Artemij Voskobojnikov, Oliver Wiese, Masoud Mehrabi Koushki, Volker Roth, and Konstantin Beznosov. The u in crypto stands for usable: An empirical study of user experience with mobile cryptocurrency wallets. In *Conference on Human Factors in Computing Systems*, pages 1–14, 2021.

64 XKCD. Security, 2009. `https://xkcd.com/538/`.

65 Lucia Zedner. *Criminal justice.* Oxford University Press, 2004.

A Appendix

A.1 Forum Data Processing

We start our annotation process by identifying a set of 18 keywords that could potentially be related to wrench attacks, namely: assault, blackmail, extortion, firearm, force, gunpoint, harass, hostage, kidnap/kidnapping, mugging, physical attack, physical threat, robbery/robbed, theft, torture, victim, weapon, and wrench. We obtain 100 random posts that contain each of these keywords and analyse their content. Through this exercise, we identify three main topics being discussed:

1. Victim warning. The user provides an account of their wrench attack experience to warn other users. For example: *"Somebody just attempted to rob me of my phone after setting up a local trade. Be careful out there if trading in person. I'm in a ... city (not ...) and somebody contacted me over localbitcoins for an in person trade. He wanted to buy 500 ... worth of BTC."*
2. General knowledge. The user talks about wrench attacks in a general context that is not related to cyber security. They sometimes refer to news of wrench attacks. For example: *"... firefighter kidnapped, robbed and stabbed by crypto thieves..."*
3. Cyber Security. The user talks about wrench attacks in a cyber security related context. For example: *"I plan to use said ... on a ... soon. Then I don't need to make sure the hardware, drivers, linux, additional software, encryption algorithms, bitcoind and ... are without bugs and backdoors, as I have (more or less) removed any possible way for data to leak out at all. If then someone does the $5 wrench attack on me, I'll happily surrender the one bitcoin I own."*
4. Not Wrench Attack related. The post content does not include information associated with wrench attacks.

We use these three topics as annotation guidelines to annotate a random sample of 1,142 threads.

A.1.1 Data classification

One of our objectives is to identify wrench attack-related discussions. Therefore, we categorize all data posts with machine learning methods. We test the performance of two models: Support Vector Machines (SVM) [12, 22], and XGBoost [52]. We pre-process and tokenize all input text, then we use the NLTK library to perform word lemmatization. We then obtain the vector of lexical features by using the Term Frequency-Inverse Document Frequency (TF-IDF) words weighting [53].

We use the annotated posts (as described in A.1) and split the data for training and testing using a ratio of 67/33 correspondingly. The training data is unbalanced because the majority of posts in the forum are not related to wrench attacks. We oversample the training data using SMOTE [17] to deal with the skewed data distribution. We tune the models' hyperparameters and use ten-fold crossvalidation to avoid overfitting the training data.

A.1.2 Examination of wrench attack-related posts

After classifying all posts from both datasets, no wrench attack-related posts were found on CrimeBB posts. This is surprising since underground forums do contain cryptocurrency-related conversations. However, the majority of these conversations are related to cryptocurrency trading and its use in money laundering.

The classification of Bitcointalk posts predicts that 672 threads are wrench attack-related. This represents 0.06% of all 1,091,890 English only collected threads.

We analyze the content of posts related to wrench attacks and find the following observations. First, posts identified as 'Victim warnings' are extremely rare since only 12 posts were classified under this category in the dataset extracted. This could indicate that very few Bitcointalk users have experienced a wrench attack or, if they have, are reluctant to talk about their experience as a victim. A larger number of posts were identified as 'General knowledge' or 'Cyber security' related. We use URL patterns and the python 're' library to extract linked websites that are mentioned within posts identified under these two categories and find a total of 54 unique URLs. We analyze these URLs' websites and identify that the news content (i.e. the wrench attack story behind them) 52 of them overlap with those in §4.3 and only two of them were not already mentioned in that list. We process these, as described in §4.2.

B Interview Schedule

B.1 Cryptocurrency Demographics

1. What field is your career in? what is your current occupation/position?
2. What year did you first start using cryptocurrencies?
3. Tell us about any experiences you have had or have working within the cryptocurrency ecosystem.
4. Tell us about any experiences in contributing to open-source projects, repositories, or writing code.
5. Do you consider yourself to be a known figure in the cryptocurrency ecosystem?
6. What cryptocurrencies do you currently own/hold?
7. In what ways have you been using cryptocurrencies?
8. Specify if you publicly declare or imply that you own cryptocurrencies.
9. How often do you discuss cryptocurrencies in public, either in person or on online forums?
10. How much in terms of the market value are you currently holding in cryptocurrencies?
    - Less than USD 1,000
    - USD 1,000 - USD 5,000
    - USD 5,000 - USD 10,000
    - USD 10,000 - USD 100,000
    - More than USD 100,000
    - Prefer not to say
11. Specify how often you use or have used peer-to-peer platforms to buy cryptocurrencies.
12. Specify how often you use or have used ATMs to buy cryptocurrencies.
13. Can you tell us about the cryptocurrency exchanges that you have used or regularly use to buy cryptocurrencies?
14. Specify if you conduct or used to conduct your operation(s) with a KYC verified account.
15. Are you aware if any of the services that you use or have used, been the targets of security breaches or leaks?

B.2 Physical and Digital Security Practices and Habits

1. What type of wallets do you use?
2. How many wallets do you have?
3. How does the fund distribution looks like in these wallets?
4. What factors influenced your decisions in taking the above-mentioned measures?
5. Do you share the means of access to your funds with other people?
6. Do other people have access to the devices that you use to whether access or store your funds?
7. What digital security measures do you implement to ensure the protection of your funds, the means or access, or the devices?
8. What physical security measures do you implement to ensure the protection of your funds, the means or access, or the devices?
9. What safety measures do you or have you implemented when buying cryptocurrencies from an ATM/P2P?
10. How (physically) safe do you or have you felt when buying cryptocurrencies from an ATM/P2P?

B.3 Establishing if a $5 Wrench Attack Occurred

The purpose of this section is to make sure that the participant was actually a victim of a $5 wrench attack and not something else. We provide a simple and brief definition and explanation of what constitutes a $5 wrench attack.

1. A successful $5 wrench attack is an attack that targets a cryptocurrency owner physically with the purpose of forcing the owner to transfer cryptocurrency to the attacker(s) or give out the means of access. This can include any physical assault or the threat of using force or causing any type of harm.
   Have you fully/or partially experienced any of the following scenarios that you suspect was a $5 wrench attack? Please state all that is relevant:
   - Kidnapped or held against your will;
   - Blackmailed or extorted;
   - Verbally abused or harassed;
   - Threatened;
   - Got stalked;
   - Held at gunpoint in public;
   - Physically assaulted in public;
   - Physically assaulted on your private property (house, vehicle, etc.)
2. If you have not experienced any of the above mentioned personally, can you specify if you know anyone *Personally* who encountered any of these scenarios? *(We are only interested in persons they know personally, and not incidents they heard on the news, etc.)*
3. For an attack to be classified as $5 wrench attack, the attacker must not initially ask you for fiat, but rather for cryptocurrencies or the means of access (such as private keys, passphrases, hardware wallet, etc.). Can you specify what the attacker(s) first asked for? *(Only asked if the occurrence of a wrench attack has been established in prior questions.)*
4. Not all attacks can be successful, some can be failed attempts. Here are some scenarios of such attempts, please specify those that apply:
   - The attacker(s) got the means of access, but failed to transfer the stored funds;
   - The attacker(s) got the means of access, but the wallet had no funds or was bogus;

- The attacker(s) failed to get the genuine means of access; for example, they obtained fake or false means of access;
- At the time of the attack, you no longer had any cryptocurrencies or had the means of access; e.g. you had lost your private keys.
- For any reason, the use of force or threat of force or harm did not lead to you being deprived of your cryptocurrencies; e.g. a police car passed by, or you managed to get help, or you escaped, etc.

B.4 Attack Details

(Only asked if the occurrence of a wrench attack has been established in prior sections.)

1. Describe in your own words, and with detail, the attack in question.
2. Describe the environment where the attack occurred, including if possible, details such as the country/city, whether it was a public or private place, and whether it was a crowded or isolated area.
3. State the month, year, and time of day the attack occurred.
4. Specify any demands made by the attacker(s), such as the requests for certain amounts of funds or specific cryptocurrencies.
5. Can you tell us about any negotiation or circumvention techniques that were used?
6. What information can you provide about the perpetrators?
7. Did the attacker(s) have any prior knowledge about the held funds, location, or how they were secured?
8. Following the attack, were the authorities informed about the attack? If yes, can you share the overall experience with the initial response, and the current stage of the investigations?
9. Following the attack, was the community alerted?
10. Following the attack, can you tell us about digital and/or security measures that were taken or changed?
11. Can you tell us about any previous experiences where you were a target or a victim of a cryptocurrency related crime? If yes, would you be comfortable sharing any details about the incident?
12. Can you tell us about any previous experiences where you were a target or a victim of a non-cryptocurrency related financial crime? If yes, are you comfortable sharing any details with us?
13. Do you have any knowledge whether the victim in question has been previously the victim of a cryptocurrency related crime?
14. Do you have any knowledge whether the victim in question has been previously the victim of a non-cryptocurrency related financial crime?

B.5 Risk Perception and Susceptibility

1. How likely do you think you are to experience a $5 wrench attack in the future?
2. How likely do you think you are to experience a $5 wrench attack in the future, again? *(if victim)*
3. How confident are you in the effectiveness of the security measures you currently implement, in thwarting a successful $5 wrench attack?
4. Suppose someone without your consent, acquired your means of access. In your opinion, what is the likelihood that they will succeed in transferring all the stored funds without obtaining further information from you?
5. What precautionary measures would you take to:

  5.1 avoid being a target in the first place;
  5.2 avoid losing significant amounts of funds.
6. What do you consider a major threat or risk to the safety of your funds and/or means of access?
7. Do you have any type of relevant insurance?

B.6 Recommendations

1. What recommendation do you have for users to help them avoid being a target or a victim of a $5 wrench attack?
2. What precautionary measures do you advise users to implement to mitigate their losses?
3. In your opinion, how can the community, authorities, and academics work together to combat or reduce: 1. the occurrence of such attacks, 2. minimize the losses.
4. What modifications do you see necessary in applications and UI design for wallets that could minimize exposing users to risk?

B.7 Demographics

1. Age group
   - Younger than 24
   - 25-34 years
   - 35-44 years
   - 45-54 years
   - 55-64 years
   - Older than 65
2. Education Level
3. Country of residence
4. Gender
5. Race or ethnicity

B.8 Concluding

- Do you have any questions for us?

C Interviewee Demographics

Demographic	Respondents
Man	8
Woman	2
<24	1
25-34	2
35-44	7
High School Diploma	1
Bachelor’s Degree	2
Master’s Degree	4
PhD	3
East Asia	2
Europe	4
Middle East and West Asia	2
North Africa	1
North America	1
<1k in funds	2
1-5k in funds	1
5-10k in funds	1
10-100k in funds	1
100k+ in funds	1
Prefer not to say	4
First active before 2015	4
First active between 2016 and 2019	5
First active between 2020 and 2021	1
Publicly declare ownership	2
Privately declare ownership (certain communities)	3
Do not declare ownership	5
Academic fame	2
Industry fame	4
No perceived fame	4
Used ATMs	2
Technical Contributor	5
Conducted KYC	8

Table 5 General demographics of our interviewees.

D Exclusion Criteria

Excluded News Articles	Reason	Count
Attack on ATM	Not against person(s)	14
Attackers only demanded fiat cash from cryptocurrency users	Not demanding cryptocurrency or means of access	13
Attack on mining equipment	Not against person(s)	7
Attackers only demanded expensive goods from cryptocurrency users	Not demanding cryptocurrency or means of access	4
Attack on cryptocurrency company servers	Not against person(s)	1
Attackers did not intend to steal	No intent	1
Unspecified		2
Total		42

Table 6 Excluded news articles per the set exclusion criteria in §3. The table details different categories of physical attacks not qualifying as a wrench attack.