How do Bitcoin Users Manage Their Private Keys?

Gunnar Lindqvist[1], Joakim Kävrestad[1], Dennis Modig[1] and Ali Padyab[1]

[1]*University of Skövde, Högskolevägen 1, 541 28 Skövde, Sweden*

Abstract

Bitcoin has emerged as the most recognisable cryptocurrency due to its usages as a speculative asset, medium of exchange and store of value. The fundamental characteristics of trustless and secure sound money have made it appealing to people. As a result of the immutability of Bitcoin, monetary losses caused by user security mistakes such as lose possession of private keys may hinder Bitcoin usage. We surveyed 339 Bitcoin users to explore the interaction between individuals and the technology of Bitcoin of how they safeguard their Bitcoin private keys. The results showed that users employed technologies to enhance the protection of their Bitcoin private keys, such as encryption and multi-signature. However, a proportion of users employed less secure approaches. The study results suggest that users prefer encrypting their private keys rather than multi-signature due to convenience and ease of use. Hardware wallets were moreover the most used wallet by the participants.

Keywords

Bitcoin, Cryptocurrency, Private key, Wallet, Backup

1. Introduction

Bitcoin was first introduced in 2008 by the alias Satoshi Nakamoto where a proposal for a peer-to-peer version of electronic cash based on several concepts and technologies was presented in a white paper [1]. This digital currency is based on public-key cryptography, where all transactions are registered on a public open blockchain and secured by the consensus algorithm proof-of-work. Bitcoin is the first digital currency that solves the problem of double-spending and makes it possible to send and receive currency without a third party involved [1]. It is estimated that over half a million transactions take place per day and that Bitcoin is used by more than 48 million users around the globe [2]. Bitcoin consists of the technologies of public-key cryptography, blockchain and the consensus algorithm proof-of-work. Combined, they allow unique technological properties of immutability, decentralisation, trustless, and permissionless. Private keys provide bitcoin ownership and can create Bitcoin addresses and digital signatures for transactions on the Bitcoin blockchain. The private keys are not stored on the Bitcoin network but are created and stored through Bitcoin wallets. A Bitcoin wallet makes it possible to receive, send and see the sum of all UTXOs (unspent transaction outputs) for the private keys that the wallet manages. Different wallets offer different levels of ease of use and security [3]. Private keys enable the technological properties of Bitcoin transactions to be pseudonymous, borderless and censorship-resistant. The Bitcoin network does not differentiate

7th International Workshop on Socio-Technical Perspective in IS development, October11-12, 2021 (STPIS'21)

lindqvist.gunnar@protonmail.com (G. Lindqvist); joakim.kavrestad@his.se (J. Kävrestad); dennis.modig@his.se (D. Modig); ali.padyab@his.se (A. Padyab)

between correctly signed transactions [4]. As described by [5], Social-Technical Systems (STS) consists of the dynamic of human, social, organisational and technical components. The Bitcoin ecosystem relies on a technical foundation but requires human users as well as organisational support and can be viewed as an STS. Bitcoin is seen as a social construct since the users agree that it has value. Bitcoin has become a social and technical phenomenon where its use has increased significantly. Furthermore, Bitcoins' governance for how rules are decided, implemented, and enforced makes it a social-technical system where a complete consensus is agreed among all users. For users to socially interact with the exchange of the value of bitcoin, a Bitcoin wallet is needed. This study addresses how users manage their private keys for Bitcoin and is aligned towards the social end of the Bitcoin ecosystem. In order to send Bitcoin, a private key is used in conjunction with a wallet, and it is therefore vital that private keys are handled with security in mind [4]. Moreover, the choice of the wallet, which manages the private keys, is essential. As described by [6], there are various types of wallets, and they differ in usability and security. In contrast, usability is likely to influence the users' decision on what wallet to choose. Security, as well as integral, both in terms of availability and confidentiality of the private key, are important [7]. Disclosing the private keys means giving away complete control over the spendable bitcoin corresponding to those private keys. As such, sustainability relies on strong security measures to handle private keys. The protection includes ensuring the confidentiality of private keys while making unauthorised access impossible.

We consider both cybersecurity and the Bitcoin environment to be socio-technical properties that are dependant on technical and social factors. It is essential to acknowledge both aspects to help people interact with the Bitcoin network in a secure way [8]. Previous research has focused on wallets from a technical point of view where improvement proposals have been put forward to develop the security of key management [9]. Previous research on users has only examined a small group of beginners regarding their perception of security and use [7], which makes our understanding of Bitcoin private key management relatively narrow. There is scant research on key management practices from the perspective of Bitcoin users. Further, we are unaware of a study that examines how Bitcoin users manage their private keys. The current study helps answer the response to unexplored areas within Bitcoin by examining the security practices of experienced Bitcoin users.

The purpose of this study is to understand the strategies that Bitcoin users employ in the socio-technical system of Bitcoin to back up their private keys and provide an overview of the types of wallets used. Besides, the study focus on the social-technical aspects through what strategies and techniques can be helpful for future research and practice for users regarding the use of Bitcoin. A survey was distributed to Bitcoin users to determine their private key management strategies to address the study's aims. The results show that users make security-conscious choices when it comes to Bitcoin. Most users are willing to invest in security and perform backups for the possibility of recovery. We believe that this study presents new and valuable insights to researchers and practitioners regarding how Bitcoin users manage their private keys. In extension, this research studies user's security behaviour in a context where security can be assumed to be of great importance to the users since a Bitcoin wallet holds a monetary value and is best compared to a bank account. As such, this research complements existing research into security behaviour which is typically conducted in domains where security is assumed to be a secondary target for the users [10].

2. Related work

Previous research has focused on providing suggestions for how different implementations can increase the security of wallets and backups and evaluate and identify security issues that exist. While Bitcoin wallets are considered as STSs, previous research has focused on technical aspects. A study by [11] surveyed the number of active users and downloads for different types of wallets and compared that to other cryptocurrencies. The study showed that there were between 2.9 million and 5.8 million unique active users of cryptocurrency wallets, and 5.8 million to 11.5 million wallets are likely to be active. The study indicated that the mobile wallet is the most common type of wallet used.

Research conducted by [9] suggested how a key management scheme can be used to sign transactions via a password phrase and personal questions that can reset the private key in case of a loss. Only a bit of the private key is stored locally for increased security in their proposed scheme. The research concluded that storing private keys on local devices enabled the possibility of theft, where the key management scheme could reduce that risk. The suggested method can help novice users manage their private keys.

The report [12] focused on an easier way to back up private keys. Nearly all existing wallets use a seed phrase for backup, which can be inconvenient and problematic. A proposal relying on a side-channel via visual verification by a screen was made as a suggestion. With the help of a hardware card that can store the backup, users did not have to write down the private key. The proposal used NFC as the transfer method between wallets and the hardware card to transfer the private key. The research presented a proof-of-concept where the goal was to create a secure backup transferring mechanism.

Several research efforts have been made regarding the security deficiencies of the different types of wallets. The research report of [13] explored the security problems that exist for mobile wallets and cryptocurrency exchanges. The research exposed the risks that come by the use of those applications [14]. Both reports concluded that users need to know the possible risks involved and the present potential vulnerabilities.

Authors of [15] conducted a study aimed at hardware wallets that are currently on the market and reviewed the shortcomings and attacks that existed. In the same area, [16] conducted a similar study aimed at a software wallet for computers, an SPV wallet and cryptocurrency exchanges to report the risks and security problems that existed. Even though Bitcoin is tamper-proof, well-known attacks were still possible, but against users of Bitcoin, both journals show.

When it comes to social aspects of Bitcoin wallets, in a survey about Bitcoin users, authors of [7] have investigated what beginners think about the security and use of Bitcoin. The survey showed that Bitcoin as a cryptocurrency was a significant challenge for many users and indicated the need for further investigation to understand usability and security issues better.

Our study is different from previous research in that it reported on what types of wallets users utilise. Another aspect that distinguishes the study is that it focused on the types of available wallets and not on a single solution. Moreover, our aim in this study was to investigate the private key management strategies of Bitcoin users, as opposed to the previous literature in which technical aspects of cryptocurrency wallets has been investigated. The effort has implications for the designers and researchers of cryptocurrency wallets in helping users increase private keys' security.

3. Background

Bitcoin allows people to participate in an economic, political, and social life without hindrance from a third-party actor. Bitcoin consist of properly socio-technical assemblages. With blockchain as the underlying technology, socio-technical arrangements of human and non-human are made [17]. The peer-to-peer exchange of bitcoin between people is made through asymmetric cryptography where the private key enables Bitcoin transactions, and the public key derives Bitcoin addresses. A wallet is an application and serves as the primary interface for a user. A Bitcoin wallet (with the paper wallet as an exception) manages a user's keys and allows for the generation of addresses, tracks inputs and outputs, creates and signs transactions [4]. Research categorises several different wallet formats into four categories: software wallets, hardware wallets, paper wallets, and web wallets.

A software wallet is an application that runs on a computer or smartphone. The private keys are stored locally on the device and provides users with complete control of their wallet [13]. Hardware wallets store the private keys on a separate physical device [9]. Signatures are created locally on the device and then sent to the medium device [18]. Paper wallets have the private key and corresponding public key written down on a physical item. The private key needs to be imported if a transaction is to be carried out where one must be aware of the change address [19]. Web wallets are either custodial or non-custodial, also known as hosted or non-hosted, which an external provider operates via a web browser. The differences are that hosted web wallets store the private keys, whereas, in a non-hosted web wallet, the private keys are stored on the user's local device [14]. Table 1 gives an overview of wallets types with an assessment of their security, accessibility and cost, which can influence users regarding their choice of wallet.

Table 1
Types of Bitcoin wallets

Wallet type	Security	Accessibility	Cost
Software wallet	Sufficient for lower amount	Generally easily accessible	Freely available
Web wallet	Generally not secure	Easily accessible	Freely available
Paper wallet	Good offline security	Hard to access	Costs only to print
Hardware wallet	Good security	Can be cumbersome	Not free

There is plenty of free information available and resources for helping users choose a well-suited wallet regarding their needs and intentions. Information and education for how to securing a wallet are also available. The registered Bitcoin.org domain used for the white paper is one example that offers guidance for how to use Bitcoin [20]. Users can search the web for several courses that are available online, both free and paid. Due to the extensive ecosystem of Bitcoin, a tremendous amount of information is available. However, a great responsibility lies with the users to seek out this information.

4. Methodology

The aim of the study was met using a web-based survey that intended to understand Bitcoin user's security behaviour regarding their selection of wallet type, backup procedures for private keys and practices for signing transactions. The survey was developed and piloted to ensure that participants could easily understand it, as suggested by [21]. The pilot test was first done to clarify ambiguities. The pilot test was published on the Facebook group ”Bitcoin Sweden” 2020-04-15, where the group at the time of publication consisted of 8348 members. Communities of Bitcoin users were used in the pilot and the final sampling because of the surveys outspoken objective of measuring the actions of Bitcoin users.

The final questionnaire was distributed via the survey web app LimeSurvey, which was installed on a virtual machine. It consisted of five questions, and several predefined response options were sent out. The following five questions were asked in the survey. 1) What kind of wallet do you use to store the majority of your bitcoin? 2) Do you use multi-signature to sign transactions for that wallet? 3) Do you have a backup(s) of your private key for that wallet? 4) If yes, in what ways is the key backed up? and 5) Is your backup encrypted?. The survey began with a welcome page that explained the purpose, what all data would be used for and how personal data would be handled. The survey was completely anonymous, where no personal data such as IP address, email or geographical location was collected. The survey was designed to be conducted quickly and had a simple language to remove confusion. A reward in bitcoin was offered to increase the number of responses and validity. The survey was published on ”/ r / Bitcoin /” 23-04-2020 at 12:00 and was closed on 27-04-2020 at 23:59.

For data analysis, the gathered data was treated as nominal data, and the frequency of respondents in each category reported as described by [22]. Confidence Intervals (CI) was calculated to identify what categories that were separated from easy other with statistical significance as described by [23]. Thus, categories with overlapping CI were considered to be equally favoured by the respondents. The common significance level of 95% was adopted in this study.

5. Survey results

The survey page had 553 visits during the time the survey was open and was completed by 339 respondents. The first question was ”What kind of wallet do you use to store the majority of your bitcoin?” and intended to provide an overview of the most common wallet types, which in turn indicates what wallet types are perceived as most secure by the community. The answer options and results are presented in Table 2.

As seen in Table 2, Hardware wallets are the most used wallet types and are used as the primary wallet by 46.6% of the respondents. Software wallets stored locally on a mobile or computer or stored on a hosted service share a second-place since they all have overlapping CI and each of them is the primary wallet type of about 15% of the respondents. The second question was ”Do you use multi-signature to sign transactions for that wallet?” and intended to provide insight into how frequently Bitcoin users use multiple signatures to sign transactions as an added layer of security. The results of this question are presented in Table 3, which suggests

Table 2
Results and Confidence Intervals for question 1: What kind of wallet do you use to store the majority of your bitcoin?

Option	Frequency	Percentage	CI(+-)
Software wallet on mobile	59	17.4	4
Software wallet on computer	54	15.93	3.9
Hosted web wallet	42	12.39	3.5
Non-hosted web wallet	3	0.88	1
Paper wallet	21	6.91	2.6
Hardware wallet	158	46.61	5.3
(Other) Self-generated	1	0.29	0.6
(Other) Bitcoin node	1	0.29	0.6

that a minority of the participants only employs multi-signature.

Table 3
Results and Confidence Intervals for question 2: Do you use multi-signature to sign transactions for that wallet?

Option	Frequency	Percentage	CI(+-)
Yes	117	34.5	5.1
No	222	65.5	5.1

The third question and fourth questions were ”Do you have a backup(s) of your private key for that wallet?” and ”If yes, in what ways is the key backed up?”. 88.20% of the respondents do back up their wallets, and the types of backups used by the participants are displayed in Table 4, note that participants could pick several answers.

Table 4
Results and Confidence Intervals for question 4: Do you have a backup(s) of your private key for that wallet?

Option	Frequency	Percentage	CI(+-)
On a piece of paper	238	54.84	4.7
On an external drive	71	16.36	3.5
On an internal drive	25	5.76	2.2
On a cloud service	33	7.60	2.5
On an email	10	2.30	1.4
Stored in brain memory	37	8.53	2.6
(Other) Private cloud	1	0.23	0.5
(Other) Engraved on metal plate	17	3.92	1.8
(Other) Custodial	1	0.23	0.5
(Other) 3-2-1 backup	1	0.23	0.5

The results from question three and four suggest that the vast majority of the respondents back up their wallets. Further, as demonstrated by the fact that there are 434 answers to question four, many respondents use more than one means of backup with papers-based backups as the, by far, most prominent method. The final question was whether or not the participants encrypt their backups. It was found that 20 (59.9%) of the respondents answered that they did not encrypt their backups. However, that result should be interpreted in light of most participants using paper-based backups, which are hard to encrypt.

6. Analysis

The results show that socio-technical choices of Bitcoin users regarding handling their wallets are interwoven. Below, we elaborate on the interaction between the technological properties of Bitcoin and the strategies that users employ for their choices. The survey indicates that Bitcoin users are security-aware when managing private keys, especially regarding the backup them. The reason is that losing the private key means losing the Bitcoin it can transact. The difference from ordinary fiat currency (Traditional government-issued currency) is that the security is based on one's own choices dependent on technical and social factors. With a bank, one does not have complete control of the security, but on the contrary, the responsibility lies with the user with Bitcoin. Further, a property that Bitcoin possesses compared to fiat currency is immutability which can also be a significant factor in taking security measures. A signed Bitcoin transaction cannot be reversed once it is broadcast and accepted to a block on the Bitcoin blockchain. These reasons are likely to make people willing to make well-thought-out security decisions and explain why so many participants in the survey had bought hardware wallets. Regarding the choice of wallets, the results show that hardware wallets are the most widely used type of wallet for managing private keys that corresponds to the most spendable bitcoin. The reason is that a hardware wallet can be seen as the wallet that has the best ratio between security, functionality [24] and availability in the market. A large portion of the respondents also uses software wallets, and a possible reason can be that they are often free to use where there is a large selection of different types which one can choose based on their preference. It is possible that more respondents would prefer to use a hardware wallet but may not consider it due to their costs. Many day-traders and non-technical users may use such platforms as hosted web wallets. Since many hosted web wallets act as a cryptocurrency exchange, they are more similar to the banking systems, which enable easier trading and a more familiar interaction. Those factors could be why web wallets are often used despite users not owning their private keys. The low percentage of paper wallets could be because of the low availability and knowledge for creating one correctly. A paper wallet is prone to be easily destroyed since it is made of paper.

Results show that the majority of Bitcoin users make backups of their keys, which is seen as both positive and troublesome since it can make the recreation of keys possible. The issue was further explored regarding backup practices. The results suggest that backing up to something physically writable is the most popular method. The probable reason for this is that this type of backup can be cheap to do in the form of paper and pen. The results suggest that the participants are aware that losing the private key means losing spendable bitcoin. The result of this survey suggests that Bitcoin users back up their private keys to a higher degree than with which general users tend to back up data, as exemplified by [25] and [26]. A possible explanation can be that the community of active Bitcoin users make up only a few percent of all computer users [27, 28].

It can be assumed that users possessing bitcoin are more prone to safeguard their possession than other users in safeguarding regular data. A possible problem that the survey suggests is the usage of many different types of backups since a specific backup can become a weak link. It can also be problematic since one could forget that a weaker backup was made where a security breach could happen.

As for encryption of backed up private keys, encryption of backups is only used by about 40% of the respondents. However, encrypting paper-based backups can be cumbersome, and most respondents who stated to use paper write their private keys or seed phrases directly in plain text where they then hide the backup from access. Encryption can be seen as more relevant for hard drives, but above all, email and cloud services as the backups are stored with a third party. Something that may have made the question unclear is whether encryption can occur on a written paper or piece of metal.

Multi-signature, which can reduce the likelihood of theft and loss rather than the availability, was used by 34.5% of the respondents. The percentage is far less than the almost 90% who use some form of backup. The results suggest that Bitcoin users primary concern is to ensure that they can spend their bitcoin and not hassle with many private keys for signing transactions. The lower usage of multi-signature could also be possible due to its technical difficulty and that not all wallets use this technology. Multi-signature also contributes to lower availability since all key pairs for the set relation needs to be accessible [9].

The paper's limitation is that the survey may have missed a large sample of users who are not actively searching and reading about Bitcoin. The reason for this is that the survey was published on a forum for Bitcoin users. People who apply to forums tend to be interested in the topic and spend time gathering information and discussing it. In addition, the posts in the forum could have affected users' choice of wallets and backup methods. Furthermore, the study does not cover if users backup a nondeterministic or deterministic wallet. A deterministic wallet only requires one backup. In contrast, a nondeterministic wallet can contain several random private keys resulting in a more demanding backup [4]. Another issue that would have provided more information is whether users use a passphrase for an extra layer of security.

7. Conclusions and future work

This paper aimed to investigate how Bitcoin users managed their private keys and illustrate users social-technical interactions with Bitcoin wallets and backups of private keys. The results from the survey of 339 Bitcoin users show that users make security-conscious choices by using hardware wallets and backup. The results also show that 34.5% of the respondents use multi-signature technology. An influential factor that can affect the choice of wallet is the amount of bitcoin that the user owns. Hardware wallets and advanced solutions such as a multi-signature are arguably used for users possessing a large amount of bitcoin. One interesting result showed that more than half of respondents make a backup of their keys on a piece of paper, and about half of those who make backups of their keys do not encrypt their backed up keys. Our research calls for more research on ways in which private keys could be secured.

This research concludes that Bitcoin users are security-aware when it comes to the management of their private keys. This is in contrast to research into security behaviour in general which suggests that users often select not to use security features and functions voluntarily [29]. While the survey data does not allow for an investigation of the reason for this discrepancy, we offer three possible explanations. First, it is possible that this sample, by accident, contains users that are more prone to secure behaviour than the average user. However, a more likely explanation could be that Bitcoin users are prone to secure behaviour than the average computer user. While researching the demographic aspects of the users in the Bitcoin ecosystem is made hard by the anonymous nature of it, some research suggests that computer professionals and criminals make a large part of the user base [30]. Those users can perhaps be assumed to be more cautious than the average computer user. A third explanation could be that Bitcoin users are careful about their wallets since they hold a monetary value, and therefore ready to make efforts to keep it secure. The last explanation would suggest that users are ready to put effort into security in cases where security is perceived as important.

For future work, there are many opportunities to pursue. Cryptocurrencies are reasonably young digital assets that will most likely evolve and gain more significant usage. Similar surveys can be conducted in the form of a correlational study of the security choices and the features of the wallets and security features and wallet adoption. Additional research regarding the use of passphrases can also be explored. Further research can be done where a comparison between different cryptocurrency wallets can take place.

Acknowledgments

Thanks to the developers of ACM consolidated LaTeX styles https://github.com/borisveytsman/acmart and to the developers of Elsevier updated LaTeX templates https://www.ctan.org/tex-archive/macros/latex/contrib/els-cas-templates.

References

[1] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008. URL: https://bitcoin.org/bitcoin.pdf.

[2] Blockchain.com, Wallets, 2020. URL: https://www.blockchain.com/charts/my-wallet-n-users.

[3] M. Conti, E. S. Kumar, C. Lal, S. Ruj, A survey on security and privacy issues of bitcoin, IEEE Communications Surveys & Tutorials 20 (2018) 3416–3452. doi:10.1109/COMST.2018.2842460.

[4] A. M. Antonopoulos, Mastering Bitcoin: Programming the open blockchain, " O'Reilly Media, Inc.", 2017.

[5] G. Baxter, I. Sommerville, Socio-technical systems: From design methods to systems engineering, Interacting with Computers 23 (2011) 4–17. doi:10.1016/j.intcom.2010.07.003.

[6] S. Eskandari, J. Clark, D. Barrera, E. Stobert, A first look at the usability of bitcoin key management, 2015. doi:10.14722/usec.2015.23015.

[7] A. Alshamsi, P. Andras, User perception of bitcoin usability and security across novice

users, International Journal of Human-Computer Studies 126 (2019) 94–110. doi:10.1016/j.ijhcs.2019.02.004.

[8] C. Tarimo, J. Bakari, L. Yngström, S. Kowalski, A social-technical view of ict security issues, trends, and challenges: Towards a culture of ict security the case of tanzania., 2006, pp. 1–12.

[9] Y. Liu, R. Li, X. Liu, J. Wang, L. Zhang, C. Tang, H. Kang, An efficient method to enhance bitcoin wallet security, in: 2017 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID), IEEE, 2017, pp. 26–29. doi:10.1109/ICASID.2017.8285737.

[10] A. Whitten, J. D. Tygar, Why johnny can't encrypt: A usability evaluation of pgp 5.0., in: USENIX Security Symposium, volume 348, 1999, pp. 169–184.

[11] G. Hileman, M. Rauchs, 2017 global cryptocurrency benchmarking study, Available at SSRN 2965436 (2017). doi:10.2139/ssrn.2965436.

[12] H. Rezaeighaleh, C. C. Zou, New secure approach to backup cryptocurrency wallets, in: 2019 IEEE Global Communications Conference (GLOBECOM), IEEE, 2019, pp. 1–6. doi:10.1109/GLOBECOM38437.2019.9014007.

[13] A. R. Sai, J. Buckley, A. Le Gear, Privacy and security analysis of cryptocurrency mobile applications, in: 2019 Fifth Conference on Mobile and Secure Services (MobiSecServ), IEEE, 2019, pp. 1–6. doi:10.1109/MOBISECSERV.2019.8686583.

[14] C. Y. Kim, K. Lee, Risk management to cryptocurrency exchange and investors guidelines to prevent potential threats, in: 2018 International Conference on Platform Technology and Service (PlatCon), IEEE, 2018, pp. 1–6. doi:10.1109/PlatCon.2018.8472760.

[15] A. Gkaniatsou, M. Arapinis, A. Kiayias, Low-level attacks in bitcoin wallets, in: International Conference on Information Security, Springer, 2017, pp. 233–253. doi:10.1007/978-3-319-69659-1_13.

[16] P. K. Kaushal, A. Bagga, R. Sobti, Evolution of bitcoin and security risk in bitcoin wallets, in: 2017 International Conference on Computer, Communications and Electronics (Comptelix), IEEE, 2017, pp. 172–177. doi:10.1109/COMPTELIX.2017.8003959.

[17] A. Hayes, The socio-technological lives of bitcoin, Theory, Culture Society 36 (2019) 1–16. doi:10.1177/0263276419826218.

[18] A. G. Khan, A. H. Zahid, M. Hussain, U. Riaz, Security of cryptocurrency using hardware wallet and qr code, in: 2019 International Conference on Innovative Computing (ICIC), IEEE, 2019, pp. 1–10. doi:10.1109/ICIC48496.2019.8966739.

[19] S. He, Q. Wu, X. Luo, Z. Liang, D. Li, H. Feng, H. Zheng, Y. Li, A social-network-based cryptocurrency wallet-management scheme, IEEE Access 6 (2018) 7654–7663. doi:10.1109/ACCESS.2018.2799385.

[20] bitcoin.org, Bitcoin - open source p2p money., 2021. URL: bitcoin.org.

[21] F. J. Fowler Jr, Survey research methods, Sage publications, 2013.

[22] H. T. Reynolds, Analysis of nominal data, 4-7, Sage, 1984.

[23] C. Wheelan, Naked statistics: Stripping the dread from the data, WW Norton & Company, 2013.

[24] M. Gentilal, P. Martins, L. Sousa, Trustzone-backed bitcoin wallet, in: Proceedings of the Fourth Workshop on Cryptography and Security in Computing Systems, 2017, pp. 25–28. doi:10.1145/3031836.3031841.

[25] E. M. Redmiles, E. Hargittai, New phone, who dis? modeling millennials' backup behavior,

ACM Transactions on the Web (TWEB) 13 (2018) 1–14. doi:10.1145/3208105.

[26] F. Breitinger, R. Tully-Doyle, C. Hassenfeldt, A survey on smartphone user's security choices, awareness and education, Computers & Security 88 (2020) 101647. doi:10.1016/j.cose.2019.101647.

[27] C. S. Henry, K. P. Huynh, G. Nicholls, Bitcoin awareness and usage in canada, Journal of Digital Banking 2 (2018) 311–337.

[28] C. Tsanidis, D.-M. Nerantzaki, G. Karavasilis, V. Vrana, D. Paschaloudis, Greek consumers and the use of bitcoin, The Business & Management Review 6 (2015) 295.

[29] M. Lennartsson, J. Kävrestad, M. Nohlberg, Exploring the meaning of usable security–a literature review, Information & Computer Security (2021).

[30] A. Yelowitz, M. Wilson, Characteristics of bitcoin users: an analysis of google search data, Applied Economics Letters 22 (2015) 1030–1036.