The Security of Cryptocurrency

Carlos Hernandez

Department of Information Science, USF

ENC 3249: Communication for I.T

Dr. Michael Shuman

April 30, 2021

Abstract

This pandemic, among other things, has impacted the U.S currency, the currency used as the de facto global reserve currency, due to high levels of inflation and increased debt in an effort to combat the social and economic effects of the aforementioned Covid-19. Due to this perception, many institutions have shifted from using the U.S currency to bitcoin, a cryptocurrency that is not controlled by any institution or central bank and embraced the benefits of this technology. As a result, the price of bitcoin has increased from 4,857 dollars on March 12 of 2020 to 59,031.98 dollars as of today's writing. This price increase, which is evidence of a demand for bitcoin, creates questions about whether the security behind this technology could accommodate this sharp appreciation in value. In my opinion, these security concerns are related to three features of the technology. These features, which include the international nature of the technology, infrastructure deficiencies, and securities issues associated with blockchain technology (technology that forms the foundation of famous cryptocurrencies such as Bitcoin and Ethereum), could restrict the growth of this technology. Thus, this paper seeks to study the security implications of this technology amidst this dramatic change in the market. To do this, variables such as the bibliographic history of cryptocurrency in academic literature, the relationship between the U.S dollar and cryptocurrency, and the way in which people store the keys for the storage system of this technology will be explored. This would create a comprehensive picture of this recent event and what steps the market must take to protect this valuable asset.

The Security of Cryptocurrency

This pandemic, among other things, has impacted the U.S currency, the currency used as the de facto global reserve currency, due to high levels of inflation and increased debt in an effort to combat the social and economic effects of the aforementioned Covid-19. Due to this perception, many institutions have shifted from using the U.S currency to Bitcoin, a cryptocurrency that is not controlled by any institution or central bank and embraced the benefits of this technology. As a result, the price of bitcoin has increased from 4,857 dollars on March 12 of 2020 to 57,023.4 dollars as of today's writing. This monumental price increase, which is evidence of a demand for bitcoin, led me to speculate in this sister's project whether a global economy with a decentralized electronic currency was possible. I concluded in that project that is unlikely that this technology would be embraced as a global currency. Among one of the reasons for this conclusion was the security issues associated with this technology. Although this technology is considered relatively safe, there are some security issues associated with this technology that could be exploited to the detriment of this tool. Thus, it is important to recognize these issues in order to mitigate them in the future.

Prior to discussing these issues, however, I think it is important to cover the technology behind this currency since the benefits and faults of this system are derived from its idiosyncrasies. Central to the concept of cryptocurrencies is the implementation of a set of rules, a protocol, that aims to create a reliable payment technology without a central authority (İçellioğlu & Öner, 2019, p.914). This protocol, in turn, sets up the supply of the currency and ensures that its users follow the rules laid out by it (p.914). This technology keeps track of the operation of its user through a distributed ledger, or a file that keeps track of the distribution of cryptocurrencies and the history of these transactions (pp.914-915). It is important to note that

this system necessitates that an up-to-date ledger is kept by each user and that verification with the currency's network takes place to avoid double-spending or, the act of using the same currency in two transactions (p.914).

Cryptocurrencies are broadly categorized into two groups depending on how their ledger is updated. The first group uses permissioned distributed ledger technology, in which trusted participants are able to change the ledger and this process is controlled by a central authority who decides what participants ought to be trusted (İçellioğlu & Öner, 2019, p.914). On the other hand, the second group utilizes a system called permissionless distributed ledger technology, in which the ledger is updated by the consensus of the participants (p.914). Bitcoin belongs to the second category; however, the ledger of block-chain technology is unique in that it is divided into groups, called blocks, which must be chained chronologically through the use of cryptography (p.915). This system is also unique in that users and their computers serve as the way that this system keeps track of and transfers these blocks (p.915). This principle of decentralization is the reason why this technology is immune to government interference or market manipulation; however, this also means that there are some inherent risks while using this technology. One of these risks is the possibility of a cyber-attack bringing down the whole system (p.915). Although this is unlikely due to the decentralized nature of the system, a successful cyberattack could leave its users vulnerable to losses which they would not be able to recuperate. An example of an attack that might be effective at targeting this system is a Distributed Denial of Service attack. In this attack, the aggressor targets the miner's pools (a group of people who act as bookkeepers of Bitcoin transactions) to slow down the operations of the group and discourage individuals from participating (Soni, 2020, p.227). It is important to note that this behavior is mitigated by this technology naturally by having a block capacity of

1MB (Dai, 2017, p.977). This type of attack can also be mitigated using Traffic Monitoring and botnet detection (Soni, 2020, p. 227). Nevertheless, this attack can occur and is a direct result of the architecture of this technology. A similar attack that targets the architecture of Bitcoin is called the Sybil threat. In this attack, an aggressor could potentially make several Sybil pirated identities, which are later used to deny the receival and transmission of Bitcoin by other users (p.227). It is important to note that if a person is able to create fake accounts and take over most of the network, they are able to perform a 51 percent attack (p.227). This type of attack only occurs when an attacker has a mining power that is more than 50 percent of the mining hash rate of a network and results in the attacker taking control over the whole network (p. 226). This attack can later be combined with the aforementioned attacks to maximize its damage. Although this type of attack has not been successful on the Bitcoin currency, it is important to note that in 2019 an attack on Ethereum Classic (a spinoff currency of the second most famous cryptocurrency) succeeded and allowed criminals to steal 1.5 million dollars worth of this currency (Cuthbertson, 2019). It is important to note that this type of attack discriminately targets smaller networks more than larger networks since the attacker has to invest less money on acquiring the computational power required for this type of attack (Gupta et al., 2019, p.398). Nevertheless, it is important that Bitcoin (the most popular cryptocurrency on the planet) is protected from these types of attacks by mitigation strategies. An article that tries to mitigate one of these proposed strategies is titled *A Hybrid POW-POS Implementation Against 51% Attack in Cryptocurrency System* and was coauthored by multiple authors. This article proposes a hybrid solution that utilizes a combination of different strategies such as Proof of Work and Proof of Stake and regulates them with strict time spacing to mitigate this attack (Gupta et al., 2019, p.403). Although a detailed explanation of this integration process was given in this article, I will

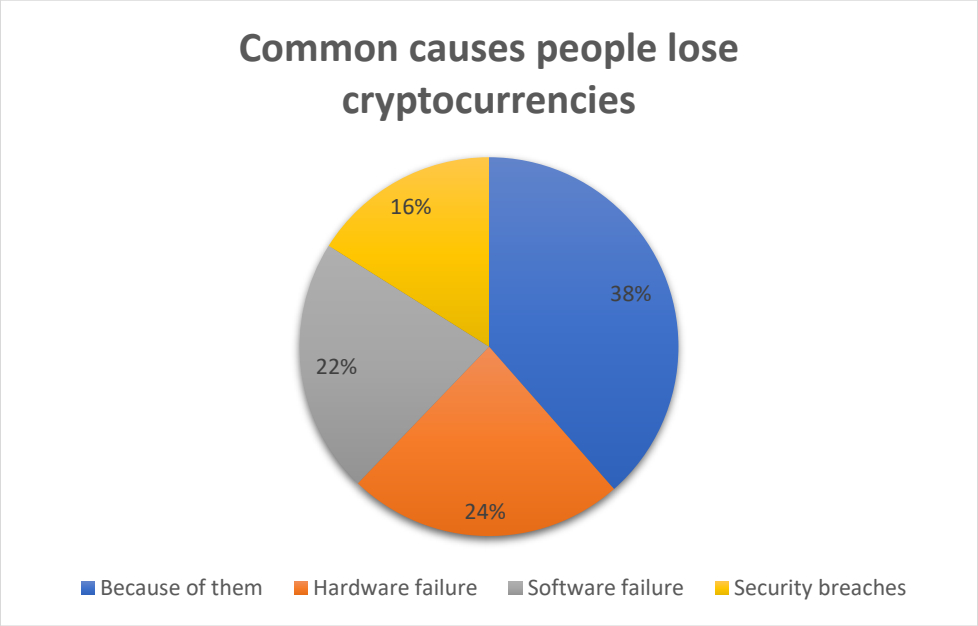
refrain from these details since they are out of the scope of this paper. Nevertheless, it is important to note that they were able to implement this security scheme successfully. It is also vital to mention that although more research is necessary for the improvement of this solution, this article promises that a person with a large amount of hash rate will not guarantee to generate a block of Bitcoin (p.403). In turn, a person with a lot of money will not be able to dominate the network (p.403). Thus, eliminating this type of attack. Although this type of protection would not be deployed anytime soon, I mention this development to demonstrate that cryptocurrency is a new industry that is constantly creating threats and solutions to mitigate these threats.

Other challenges arise when considering other characteristics of this technology. For example, since this technology provides high levels of anonymity to its users, cryptocurrencies are susceptible to money laundering and terrorist financing activity (İçellioğlu & Öner, 2019, p.915). Although this doesn't make any statement about the technology itself, these reasons might incentivize governments to restrict or make illegal the use of this technology. Examples of countries that have made cryptocurrencies illegal include Afghanistan, Bolivia, Ecuador, Russia, etc. (p. 915). This creates a restriction on the natural growth of this technology. This concentration of anonymity also makes criminals attracted to this currency since no personally identifiable information is collected linking sellers and buyers of these transactions (Irwin & Dawson, 2019, p.122). This, in turn, create situations such as the one presented in this article where the currency is used to enhance criminal activities such as ransomware. Such is the case during the WannaCry attack, a ransomware attack that spread in May 2017 to 150 countries and affected more than 300,000 computers (p.112). Besides being the biggest ransomware attack of the time, this event was devastating because this malware also contained a worm that looked for other computers to infest (p.112). This malware program acted by encrypting all of the files of

the system it infected and making it unavailable until the victim paid 300 dollars' worth of Bitcoin (p.112). This ramson was collected on three wallets and totaled a 144,010-dollar amount as of this article publication (p.112). It is important to note that even though officials knew what account collected the funds of these wallets, it was impossible to track this criminal's activity due to the aforementioned reasons. It is important to specify that although officials couldn't track the criminal in this case, there are examples of where Bitcoins can be traced by careful analysis and examination (p.122). For example, there is software that maps user transactions across a network, analyze the specific use of public keys, and pair transactions to find individual networks (p.122). This, in turn, has created technology where criminal activity is identified. For example, a Bitcoin tracking firm, aptly named Chainanalysis, has been working on a tool that tracks services criminals are using to convert Bitcoin to cash or digital currencies (p.122). These advancements, however, are mitigated by technologies such as Dark Wallet and Bitcoin Fog, which allows currency related to illicit activity to be processed alongside non-illicit transactions (p.122). It is important to note that the novelty of this technology is the reason for the state of this tool, but also for comprehensive international legislation that is verily nonexistent.

These characteristics of anonymity not only have ramifications for the criminals, but also for the average consumer. Due to the cryptocurrency's systems of cryptography and privacy, users are responsible for the protection of their private key, a variable used in cryptography to confirm a user's identity and complete payment transactions (Dai et al., 2017, p.978). This means that if a person loses his or her key, they lose all access to the cryptocurrency (p.978). The decentralized nature of this technology creates a situation where the person not only has to be aware of any malicious activity by a malicious actor, but they have a fear of being betrayed by another stakeholder (Frohlich et al., 2020, p.5). This anxiety also expands to the hardware

utilized for the management of this technology and any potential human error (p.5). This anxiety is not unsubstantiated, however, since a study presented in this article found that 22.5 percent of the people they sampled had lost cryptocurrencies (as cited in Frohlich et al., 2020, p.5). Of these people, 43.2 percent of them lost these currencies on account of their person, 26.5 to a hardware failure, 24.4 to a software failure, and 18 percent to security breaches (as cited in Frohlich et al., 2020, p.5). I mention this finding to demonstrate that due to the characteristics of this currency, a point of insecurity of it is the people who have them and the actions they perform with them. (Below is a pie chart to visualize the aforementioned information)



Other points of insecurity exist within the platforms that surround these cryptocurrencies. This is apparent in the article titled *Security Analysis of Cryptocurrency Wallets in Android-based Applications* which outlines some security issues created by the vulnerabilities of the wallets, in which this cryptocurrency resides, and the operating system of the devices utilized (He et. al, 2020, p.114). Examples of these vulnerabilities are presented in this paper's experiment where the authors use common vulnerability with the intent of capturing the private

key of a bitcoin account. For instance, they utilized key management and transaction vulnerabilities found in cryptocurrency wallets (a piece of software that can generate, store, and manage private keys) and common Android OS features, such as root privilege and a USB debugging feature to accomplish this task. The result was that they were able to capture sensitive information of the key from the screen display of the device, and capture user input using this USB function (pp.117-118). It is significant to note that the articles go into great detail about how these actions were performed, however, I will abstain from such details since they are not necessary for the scope of this article. Nevertheless, this article demonstrates that cryptocurrency's security not only depends on its characteristics but also on the devices surrounding it.

The last point that I want to make on this issue is that not all of the characteristics associated with Bitcoin lead to security issues. A sentiment that was echoed throughout these resources was that this technology had other challenges. These challenges included the size and bandwidth requirements of this tool, latency issues associated with it, challenges with throughput, and the need for a system in which resources are processed more efficiently (Ghosh et al., 2020, p.20). Although these challenges might bring security issues in their own right, they also give Bitcoin a natural immunity to some attacks. This is demonstrated by the creation of IOTA Tangle, an architecture inspired by block-chain technology (Bitcoin) that sought to apply the concepts of cryptocurrencies to internet of things devices (Cullen et al., 2019, p.2). However, due to the features of these devices, many of the challenges that I mentioned before were transgressed by creating an architecture that seemed to simplify these processes and make it more suitable for these devices. This, however, resulted in an architecture that is susceptible to a parasite chain attack that works by disrupting the immutability and irreversibility of the ledger

(Cullen et al., 2019, p.1). Thus, I mention this example to show that even though Bitcoin has some vulnerabilities, it also contains some ingenious solutions to protect itself and its assets.

In conclusion, even though I don't think cryptocurrencies will become the de facto currency of the world, I still think this invention will play an important role in the financial systems of the future. However, in order for this system to become more pronounced in our financial system, there are some security issues that must be addressed. These security risks are broadly associated with this currency's architecture, the people who use it, and the devices that surround it. Nevertheless, I believe the current price of this technology shows that the advantages of this tool outweigh its potential deficiencies.

References

İçellioğlu, C. Ş., & Öner, S. (2019). An Investigation on the Volatility of Cryptocurrencies by means of Heterogeneous Panel Data Analysis. *Procedia Computer Science*, *158*, 913–920. https://doi.org/10.1016/j.procs.2019.09.131

Ghosh, A., Gupta, S., Dua, A., & Kumar, N. (2020). Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects. *Journal of Network and Computer Applications*, 163. https://doi-org.ezproxy.lib.usf.edu/10.1016/j.jnca.2020.102635

Cuthbertson, A. (2019, January 8). Cryptocurrency: What is a 51 percent attack and how could hackers bring down bitcoin?. *Independent, The/The Independent on Sunday: Web Edition Articles (London, England)*. Available from NewsBank: Access World News – Historical and Current: https://infoweb-newsbank-com.ezproxy.lib.usf.edu/apps/news/document-view?p=WORLDNEWS&docref=news/170D7B2725DF0D98.

Cullen, A., Ferraro, P., King, C., & Shorten, R. (2019). *Distributed Ledger Technology for IoT: Parasite Chain Attacks*. https://doi.org/10.1109/JIOT.2020.2983401

Dai, F., Shi, Y., Meng, N., Wei, L., & Ye, Z. (2017). From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues. *2017 4th International Conference on Systems and Informatics (ICSAI), Systems and Informatics (ICSAI), 2017 4th International Conference On*, 975–979. https://doi-org.ezproxy.lib.usf.edu/10.1109/ICSAI.2017.8248427

Angela S.M. Irwin, & Caitlin Dawson. (2019). Following the cyber money trail : Global challenges when investigating ransomware attacks and how regulation can help. *Journal*

of Money Laundering Control, *22*(1), 110–131. https://doi-org.ezproxy.lib.usf.edu/10.1108/JMLC-08-2017-0041

Fröhlich, M., Gutjahr, F., & Alt, F. (2020). Don't lose your coin! investigating security practices of cryptocurrency users. *Proceedings of the 2020 ACM Designing Interactive Systems Conference.* https://doi.org/10.1145/3357236.3395535

Soni, D. K., Sharma, H., Bhushan, B., Sharma, N., & Kaushik, I. (2020). Security Issues & Seclusion in Bitcoin System. *2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), Communication Systems and Network Technologies (CSNT), 2020 IEEE 9th International Conference On*, 223–229. https://doi-org.ezproxy.lib.usf.edu/10.1109/CSNT48778.2020.9115744

Gupta, K. D., Rahman, A., Poudyal, S., Huda, M. N., & Mahmud, M. A. P. (2019). A Hybrid POW-POS Implementation Against 51 percent Attack in Cryptocurrency System. *2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Cloud Computing Technology and Science (CloudCom), 2019 IEEE International Conference On*, 396–403. https://doi-org.ezproxy.lib.usf.edu/10.1109/CloudCom.2019.00068

He, D., Li, S., Li, C., Zhu, S., Chan, S., Min, W., & Guizani, N. (2020). Security Analysis of Cryptocurrency Wallets in Android-Based Applications. *IEEE Network, Network, IEEE*, *34*(6), 114–119. https://doi-org.ezproxy.lib.usf.edu/10.1109/MNET.011.2000025