This is an Accepted Manuscript of a book chapter published by Routledge/CRC Press in The Economics of Cryptocurrencies on 4 December 2020, available online: https://doi.org/10.4324/9780429200427

Ch. 6 The sources of cybersecurity threats in cryptocurrency

by Valtteri Kaartemo and Marius Kramer

Cryptocurrencies and the blockchain technology behind them have been hailed for overcoming many of the challenges of fiat money. While people interested in cryptocurrencies have also heard about potential security threats, they are relatively little known by average cryptocurrency users. However, they are important, as cybersecurity attacks on cryptocurrencies can significantly influence the use and value of any cryptocurrency. Various criminal activities cause loss of over USD 1 billion annually (Europol, 2019). And even if a fork might save the system, attacks can have a long-term impact on the future of a cryptocurrency.

The purpose of this book chapter is to increase the understanding on the sources of cybersecurity threats in cryptocurrency. We review the extant literature to identify the most common sources of cybersecurity threats in cryptocurrency literature, more specifically those of 51% attacks, sybil attacks, eclipse attacks, and spam attacks, as well as introduce one attack that is not discussed in the academic literature, namely GitHub attacks. In addition to reviewing the literature, we provide illustrative examples of the attacks and methods to prevent the attacks. We also contribute by suggesting future research avenues to improve cybersecurity in cryptocurrency. Due to space limitations, we are not able to discuss all cybersecurity threats in cryptocurrency. For the readers interested in wider reviews, we recommend referring to reviews of blockchain security in general (Li, Jiang, Chen, Luo, & Wen, 2017; Saad et al., 2019; Zhu et al., 2018), security and adversarial strategies of proof of work (PoW) cryptocurrencies (Gervais et al., 2016), or vulnerabilities of smart contracts (Atzei, Bartoletti, & Cimoli, 2017; Chen, Pendleton, Njilla, & Xu, 2019).

51% attacks. In 51% attacks a hostile node gets a majority of voting power and can introduce changes to the blockchain. This enables, for instance, double spending of coins, when the node in power can alter the transaction history. This requires people to trust that the actor behind 51% of hashing power has good intents.

For PoW coins there are basically three ways to get into the majority position. First, one can buy enough equipment to get the majority of hashing power. For Bitcoin, the hardware cost is estimated around 20 billion (“Cost of a 51% attack,” 2020). While this might be too much for a criminal attempt, it is also possible to rent enough hashing power. Crypto 51 (2020) shows how much it theoretically costs to run a 1 hour attack against a cryptocurrency. The price varies from less than USD 1 (Euno, Straks, Halcyon) to close to USD 1 million (Bitcoin) as of early 2020.

Second, majority position might result from the willingness of cryptocurrency miners to join their forces. Due to high difficulty, solo miners (those not partaking in a mining pool or building a mining farm) of PoW cryptocurrencies would take hundreds of years on average to solve a block even with the latest, specialized equipment. Therefore, the miners tend to join the mining pool with the highest hash power. In these pools, the profits from mining are shared with the miners. While these pools are in general useful for individual miners, they can be a cybersecurity threat for the system, as pool operators can perform certain attacks on the network as soon as their pool reaches a majority of the voting power (Bastiaan, 2015). With 51% of

voting power, miners are able to make changes to the original blockchain and double spend the coins. This centralization of PoW coins is dangerous for their security. For instance, Bitcoin is extremely centralized and has faced a situation in which Bitmain had a majority of the voting power. The only factor currently still protecting Bitcoin is a social one.

Third, it is possible to that one malicious intern of a pool with a minimal amount of skills takes over a large pool with 51% for a short amount of time and launch a double spend attack. Therefore, it is not enough that we rely on a good faith of these mining pools. 51% attack could be initiated through social engineering, blackmail, coercion or hacking. Given that you could take over a cryptocurrency worth billions of dollars, the criminals might be willing to spend several millions for this. While we do not know how many times this has been attempted, this is a serious concern that would have a serious impact on Bitcoin, which would be forked to BTC classic and BTC, and in the case of Bitcoin this would have a tremendous impact to the whole cryptocurrency market.

The threat of 51% attack can be fixed with new hybrids that combine PoW with PoS (VeriCoin & Verium. Decred, Ethereum's Casper). There can also be side-chain scaling that prevents 51% attacks (Cardano, Skycoin, Elastos, Lisk, Ark, and Ardr) or more voting power can be given to trustworthy nodes (IOST's Proof-of-Believability). Finally, PoW-only coins can introduce new rules that restrict the size of large mining pools to 5% of the entire hash rate.

Sybil attacks. Sybil attacks are considered to be the most challenging threat for security in permissionless architectures (Otte, de Vos, & Pouwelse, 2017). Peer-to-peer networks are typically designed in a way that independent remote entities mitigate the threat of hostile peers. In the Sybil attack, individuals present several identities simultaneously to gain unreasonably large influence over the system, and thus a hostile peer overcomes the power of friendly peers (Douceur, 2002). In other words, when one actor should present only node at a time, there are several nodes that are controlled by a single person. In these attacks, the system cannot tell, if the tasks in the systems are distributed to different remote entities. As a result, attackers can block honest nodes from partaking in the system and can even control the majority of the voting power (51% attack) in a large-scale sybil attack. A typical solution to the problem is to rely on a trusted identification authority but as many cryptocurrencies are built on the idea of decentralization and trustlessness, these systems are typically designed to avoid the need to trust any identification authorities, and are thus vulnerable to sybil attacks.

Proof-of-Work and Proof-of-Stake are classic examples of how blockchains have designed avoiding sybil attacks. Here, it is considered that independent remote entity needs to work or put something on stake to partake in the system. As a result, the friendliness to the system is proven. While this is not enough to avoid sybil attacks, these consensus mechanisms make the attacks impractical (difficult and expensive) ("Sybil Attacks Explained," 2020).

Eclipse attacks. Eclipse attacks refers to an attempt to isolate certain users from the network, rather than attacking the whole system (as in sybil attack). By isolating the user from the network, the victim cannot see the current picture of the real network and the ledger. This is possible as cryptocurrencies limit the number of

outgoing connections. By default, Bitcoin node randomly picks eight nodes to establish connections. By hijacking all these connections, an attacker can control the victim's connections and take advantage by, for instance, carrying out a 0 confirmation double spend attack. In other words, resend already spent coins to an isolated user. This is also possible as a so-called N-confirmation double spending in which a merchant requires a certain amount of confirmations before accepting the transaction. If the attacker sends the transaction to eclipsed miners, it is possible to show their confirmations to the eclipsed merchant. The merchant sees the true ledger only after sending the goods.

In addition to 0/N confirmation double spending, Heilman, Kendler, Zohar and Goldberg (2015) discuss engineering block races and selfish mining that are possible through eclipse attacks. A block race happens, when a block is mined simultaneously by two miners. The other block will be followed and the other will be 'orphaned'. Thus, an eclipse attack can be used for directing the eclipsed miners to waste effort on orphan blocks, and thus engineer the block race. With selfish mining the eclipse attacker changes the perception of the ratio of mining power controlled by the attacker and the ratio of honest mining power that will mine on the attacker's blocks during a block race by eclipsing other miners. Thus, the attacker is able to win more than a fair share of the mining reward.

Eclipse attacks are relatively easy to conduct in structured networks when attackers can run several nodes from the same IP address. As a result, Marcus, Heilman and Goldberg (2018) argue that it is easier to conduct eclipse attack on Ethereum network than it is on Bitcoin. Therefore, it is possible to avoid eclipse attacks through random node selection, limiting the number of nodes from a single IP address, white labeling nodes, and increasing the number of outgoing connections, which would make it more probable that a node is not eclipsed from the network. Recently, Xu et al. (2020) introduced a design for an eclipse-attack detection model that identifies malicious actors in the network.

Spam attacks. A spam attack refers to an introduction of several simultaneous small transactions that decelerate the network, delay the creation of new blocks in the blockchain, and result in losing the computing power for maintaining the system for real transactions. Spam attacks diminish the number of connected peers in the system, and may also result in network outage (Moubarak, Filiol, & Chamoun, 2018). While these attacks may be vulnerable to the system, it is not always easy to identify unnecessary transactions.

Over the years, there have been rumors on spam attacks on Bitcoin (Suberg, 2019) and Ethereum (Memoria, 2018). While it is not always clear, if there has been a spam attack for real, it is clear that the average fees and block sizes have spiked from the introduction of small transactions in the network. This illuminates the potential vulnerability of cryptocurrencies to spam attacks.

Transaction fees are one way of avoiding spam attacks, as the fees make attacks expensive. For instance, Bitcoin prioritizes high-fee transactions. However, many cryptocurrencies are designed to enable inexpensive transactions. In these systems, other methods are needed to prioritize legitimate transactions over spam. For instance, cryptocurrencies may introduce larger block sizes to decrease the burden of spam transactions. IOTA, on the other hand, requires that all transactions require

PoW to secure two other transactions. As a result, spammers are incentivized to partake in the systems, as they increase the speed and security of the system ("IOTA Spam Fund," 2020). However, this may increase the difficulty of mining, and thus cause economic burden on keeping up the system. Some other cryptocurrencies have two mechanisms for different tiers, similar to night clubs: no transaction fees for users with high reputation, and transaction fees for non-priority users.

GitHub attacks. GitHub attacks are probably the least known attacks presented in this book chapter. They refer to the attacks made on GitHub, the software development platform used for many cryptocurrency projects, to misuse the developers for personal intentions. In brevity, a charismatic person can take over a cryptocurrency, and introduce several things that would benefit the individual but not necessarily improved the viability of the project.

There can be both technical and social solutions for preventing GitHub attacks. Nevertheless, these may be challenging to operationalize in practice. For instance, one could tie the suggestion power to the voting power, which would guarantee that the miners are taken into consideration in the development. This could result in large miners taking over the development work. As another example, there could be rules for limiting the new suggestions by a single individual. However, the real identities are not always known on GitHub. Moreover, these rules might slow down the development process, as the activities of the most active, and sincere people were hindered.

Conclusion

In this book chapter, we have presented several sources of cybersecurity threats that are common in the field of cryptocurrency. We highlight that too many cryptocurrency projects still rely on trust and good faith in lead developers and pools. As a contribution, we bring together ideas from academic literature on the most common threats and introduce the discussion on GitHub attacks, which is a less known cybersecurity threat in cryptocurrency. Particularly, we hope that the book chapter helps people in making their own research on whether it is safe to buy and use certain cryptocurrencies. While many of the threats can be solved by the developers, it is important that the cryptocurrency users are able to assess how well the system has been designed against the most common security threats.

In this chapter, we focused on 51% attacks, sybil attacks, eclipse attacks, spam attacks, and GitHub attacks. While there is some academic literature on the first four attacks, it would be important to have more studies that would describe how these attacks have been prevented, and how they can be avoided in the future by designing more robust systems.

Moreover, we call for more research on cybersecurity threats in cryptocurrency. It is important to identify the threats and develop solutions to these threats. Many of the threats in cryptocurrency, particularly in more centralized systems, are social by nature. Therefore, it would be important to develop technical solutions that would make cryptocurrencies less vulnerable to individual misbehavior.

References

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A Survey of Attacks on Ethereum Smart Contracts (SoK). In M. Maffei & M. Ryan (Eds.), *Principles of Security and Trust. POST 2017. Lecture Notes in Computer Science* (Vol. 10204). Berlin, Heidelberg: Springer.

Bastiaan, M. (2015). Preventing the 51%-Attack: a Stochastic Analysis of Two Phase Proof of Work in Bitcoin, 10. Retrieved from http://referaat.cs.utwente.nl/conference/22/paper/7473/preventing-the-51-attack-a-stochastic-analysis-of-two-phase-proof-of-work-in-bitcoin.pdf

Chen, H., Pendleton, M., Njilla, L., & Xu, S. (2019). A Survey on Ethereum Systems Security: Vulnerabilities, Attacks and Defenses. *ArXiv*, 1–29. Retrieved from http://arxiv.org/abs/1908.04507

Cost of a 51% attack. (2020). Retrieved January 13, 2020, from https://gobitcoin.io/

Crypto 51. (2020). Retrieved January 13, 2020, from https://www.crypto51.app/

Douceur, J. R. (2002). The Sybil Attack. In *International workshop on peer-to-peer systems* (pp. 251–260). Berlin, Heidelberg: Springer. https://doi.org/10.1145/984622.984660

Europol. (2019). Internet Organised Crime Threat Assessment (IOCTA). *IOCTA Report*, 1–63. Retrieved from https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Čapkun, S. (2016). On the security and performance of proof of work blockchains. In *Proc. of Conference on Computer and Communications Security* (pp. 3–16). Retrieved from https://bitcoin.org/en/developer-reference#data-messages

Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (2015). Eclipse Attacks on Bitcoin's Peer-to-Peer Network. *USENIX Security Symposium*, (August), 129–144.

IOTA Spam Fund. (2020). Retrieved from https://ecosystem.iota.org/projects/iota-spam-fund

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.08.020

Marcus, Y., Heilman, E., & Goldberg, S. (2018). Low-Resource Eclipse Attacks on Ethereum's Peer-to-Peer Network. *IACR Cryptology EPrint Archive*, *2018*(January), 236.

Memoria, F. (2018). EOS Whales Behind Spam Attack on Ethereum Network, Claims DApp Developer. Retrieved from https://www.cryptoglobe.com/latest/2018/07/os-whales-behind-spam-attack-on-ethereum-network-claims-dapp-developer/

Moubarak, J., Filiol, E., & Chamoun, M. (2018). On blockchain security and relevant

attacks. *2018 IEEE Middle East and North Africa Communications Conference, MENACOMM 2018*, 1–6. https://doi.org/10.1109/MENACOMM.2018.8371010

Otte, P., de Vos, M., & Pouwelse, J. (2017). TrustChain: A Sybil-resistant scalable blockchain. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.08.048

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, A. (2019). Exploring the Attack Surface of Blockchain: A Systematic Overview, 1–30. Retrieved from http://arxiv.org/abs/1904.03487

Suberg, W. (2019). Spam Attack? Bitcoin Average Block Size Suddenly Spikes to Over 3MB. Retrieved January 13, 2020, from https://cointelegraph.com/news/spam-attack-bitcoin-average-block-size-suddenly-spikes-to-over-3mb

Sybil Attacks Explained. (2020). Retrieved January 13, 2020, from https://www.binance.vision/security/sybil-attacks-explained

Xu, G., Guo, B., Su, C., Zheng, X., Liang, K., Wong, D. S., & Wang, H. (2020). Am I eclipsed? A smart detector of eclipse attacks for Ethereum. *Computers and Security*, *88*, 101604. https://doi.org/10.1016/j.cose.2019.101604

Zhu, L., Zheng, B., Shen, M., Yu, S., Gao, F., Li, H., … Gai, K. (2018). Research on the Security of Blockchain Data: A Survey. Retrieved from http://arxiv.org/abs/1812.02009