Article

A Taxonomy of Blockchain Threats and Vulnerabilities

Ayman Alkhalifah [1,†,‡], Alex Ng [2,‡] A.S.M Kayes [3,‡] Jabed Chowdhury [4,‡] Mamoun Alazab [5,‡] and Paul A. Watters [6,*]

1 La Trobe University; 19545133@students.latrobe.edu.au
2 La Trobe University; alex.ng@latrobe.edu.au
3 La Trobe University; a.kayes@latrobe.edu.au
4 La Trobe University; m.chowdhury@latrobe.edu.au
5 Charles Darwin University; mamoun.alazab@cdu.edu.au
6 La Trobe University; p.watters@latrobe.edu.au
* Correspondence: alex.ng@latrobe.edu.au; Tel.: +61 03 94793739
† Current address: Computer Science IT, La Trobe University, VIC 3086 Australia
‡ These authors contributed equally to this work.

Abstract: Blockchain technology has become one of the most popular technologies for maintaining digital transactions. From the foundation of Bitcoin to the now predominant smart contract, blockchain technology promises to induce a shift in thought about digital transactions in many fields, such as energy, healthcare, Internet of Things, cybersecurity, financial services and the supply chain. Despite blockchain technology offers many cryptography advantages such as immutability, digital signature and hashing; it has suffered from several critical cybersecurity threats and vulnerabilities. In this paper, we build upon the previous studies on vulnerabilities and investigates over 60 real cybersecurity incidents that have been happening on the blockchain networks between 2009 and 2019. We categorise those incidents against the key cybersecurity vulnerabilities in blockchain technologies; and have developed a taxonomy that captures five types of cybersecurity threats and vulnerabilities based on five main players in b lockchain. The outcome of this research prompted concerns and research direction in developing countermeasures to alleviate these risks.

Keywords: blockchain; cybersecurity; attack; threats; vulnerability

1. Introduction

Blockchain technology (BT) - promises a new dimension of conducting business transactions among untrusted entities; its features that support verification, identification, authentication, integrity and immutability are guaranteed through cryptography, transparency and decentralised smart contracts and smart ledgers. BT offers chronologically linked and replicated digital ledgers in a decentralised database and a sharing of transactions in an extensive network of untrusted entities. BT provides independent verification guarantees which eliminate the need to rely on a central authority. Furthermore, given the absence of central authorities, blockchain services are able to provide better security properties for systems that are distributed among different entities and can apply immutability against abuse and supervision even if there is a malicious insider.

However Given that BT is a cutting edge technology with many promises, there are concerns about its robustness [1]. If such an authority exists in a system, tampering with blockchain or hindering the broadcast of its contents is possible with a collusion between the most powerful entities. There

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 September 2019 doi:10.20944/preprints201909.0117.v1

have been many reported cyber attacks, and several cybersecurity vulnerabilities have been identified in blockchain implementations. The growing use of blockchain technology as a service delivered by governments or large firms, such as the financial technology industry, has raised users' concerns about its security. Recently, several reports have been published about cyber attacks and cybersecurity vulnerabilities in blockchain technology. For instance, 8,833 existing Ethereum smart contracts are vulnerable, and their total balance is 3,068,654 million Ethers, which is equal to about US$30 million [2]. Financial losses are possible because of the vulnerabilities in the smart contracts. For example, an attacker attacked Mt Gox in 2014—the largest platform for Bitcoin trading—and stole Bitcoins equal to US$450 million, which led to the collapse of Mt Gox. Another example is when a hacker managed to exploit a vulnerability and steal Ethers which were equal to more than US$60 million in 2016 from the DAO, a smart contract in Ethereum blockchain [3].

2. Cybersecurity Threats and Incidents on Blockchain Network

We have identified 65 real-world cybersecurity incidents occurred between 2011 and first half-year 2019 that have adversely impacted blockchain systems. We calculate the impact figures reported from the source which are based on the price of the lost coins at the time the attacks were discovered. The reported cases may not be complete since our research is based on publicly available information on forums, news feeds and other journal articles. Most incidents are lacking in details about the real circumstances surrounding the incidents. Thus, we provide a high-level classification of three types, namely hack, scam and smart contracts flaws. The total impact of the cybersecurity incidents between 2011 and 2019 has been more than US$3 billion. The highest loss relates to hacking, which is equal to more than US$1.6 billion followed by the scam, which is equal to more than US$1.1 billion and smart contracts flaws, which is equal to more than US$289 million.

Blockchain technology suffers from several cybersecurity vulnerabilities. Some of these vulnerabilities are specific to particular blockchain implementations, while the others are general. The blockchain cybersecurity vulnerabilities are divided into five categories.

- Clients' Vulnerabilities: they are concerned with how humans interact with blockchain since blockchain addresses are not tied to a person and all conducted transactions do not require the disclosure of participant identities in the transaction process. The vulnerabilities may include Digital Signature Vulnerability;Hash Function Vulnerability; Mining Malware; Addresses Vulnerability; and Software's Flaws [4].
- Consensus Mechanisms Vulnerabilities: they are related to Blocks requiring an efficient and secure consensus algorithm to establishes a decentralised, distributed and public digital ledger across a vast number of nodes. The vulnerabilities may include 51% Vulnerability; Alternative History Attack [5], Finney Attack [6], and so on.
- Mining Pool Vulnerabilities: Mining pools use "shares" to track activities of each miners. Attackers may apply different tactics to gain more shares as such will receive a greater portion of the reward. There are issues such as Block Withholding (BWH) Attack [7], Bribery Attack [8], and so on.
- Network Vulnerabilities: There are many tactics that attackers can disrupt the normal operation of a blockchain network, such as Transaction Malleability Attack where the adversary alters the transaction identifier (TXID) without revoking the transaction. Thus, the adversary can continuously withdraw [9]. Mt. Gox was one of the largest exchanges in Bitcoin history, which declared bankruptcy due to losing coins valued over US$450 million. The attackers performed a transaction malleability attack to steal coins from the exchange, which forced the exchange to freeze users' account and halt withdrawals [10].
- Smart Contract Vulnerabilities : This includes Ethereum Virtual Machine (EVM) Bytecode Vulnerabilities [11] and Solidity Vulnerabilities [11].

 doi:10.20944/preprints201909.0117.v1

3. Conclusion

This paper analysed 65 cybersecurity incdents and over 25 attack mechanisms in the blockchain technology systems which shows the following key findings:

- No actor on the blockchain network is immune to attacks.
- Blockchain exchanges suffer most of the attacks with significant amount of loss.
- Blockchain network is being used actively for scamming.
- We have seen an upward trend in attacks targeting the Ethereum Smart Contract Flaw from 2016.

We have developed a taxonomy of five differnt classifications capturing all of the identifiable blockchain attacks based on 31 documented real-world attacks and vulnerabilities.

These issues have arisen because concerns in blockchain conceptualisation, blockchain network implementation, the functionality of smart contracts, the process of mining and consensus mechanisms. Although Some of these vulnerabilities might become obsolete in the future, new ones may be discovered; however, we believe this taxonomy we have developed describes a more general set of vulnerabilities that are likely to persist into the future.

References

1. Natarajan, H.; Krause, S.K.; Gradstein, H.L. Distributed Ledger Technology(DLT) and blockchain. FinTech note; no. 1. Washington, DC: World Bank Group, 2017.
2. Luu, L.; Chu, D.H.; Olickel, H.; Saxena, P.; Hobor, A. Making Smart Contracts Smarter. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security; ACM: New York, NY, USA, 2016; CCS '16, pp. 254–269. doi:10.1145/2976749.2978309.
3. del Castillo, M. The dao attacked: Code issue leads to $60 million ether theft. *Saatavissa (viitattu 13.2. 2017): http://www. coindesk. com/dao-attacked-code-issue-leads-60-million-ether-theft* **2016**.
4. Hoch, J.J.; Shamir, A. On the Strength of the Concatenated Hash Combiner When All the Hash Functions Are Weak. Automata, Languages and Programming; Aceto, L.; Damgård, I.; Goldberg, L.A.; Halldórsson, M.M.; Ingólfsdóttir, A.; Walukiewicz, I., Eds.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2008; pp. 616–630.
5. Mechkaroska, D.; Dimitrova, V.; Popovska-Mitrovikj, A. Analysis of the Possibilities for Improvement of BlockChain Technology. 2018 26th Telecommunications Forum (TELFOR), 2018, pp. 1–4. doi:10.1109/TELFOR.2018.8612034.
6. Saad, M.; Spaulding, J.; Njilla, L.; Kamhoua, C.; Shetty, S.; Nyang, D.; Mohaisen, A. Exploring the attack surface of blockchain: A systematic overview. *arXiv preprint arXiv:1904.03487* **2019**.
7. Courtois, N.T.; Bahack, L. On subversive miner strategies and block withholding attack in bitcoin digital currency. *arXiv preprint arXiv:1402.1718* **2014**.
8. Bonneau, J.; Felten, E.W.; Goldfeder, S.; Kroll, J.A.; Narayanan, A. Why buy when you can rent? bribery attacks on bitcoin consensus **2016**.
9. Tschorsch, F.; Scheuermann, B. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communications Surveys Tutorials* **2016**, *18*, 2084–2123. doi:10.1109/COMST.2016.2535718.
10. Conti, M.; Sandeep Kumar, E.; Lal, C.; Ruj, S. A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys Tutorials* **2018**, *20*, 3416–3452. doi:10.1109/COMST.2018.2842460.
11. Atzei, N.; Bartoletti, M.; Cimoli, T. A Survey of Attacks on Ethereum Smart Contracts (SoK). Principles of Security and Trust; Maffei, M.; Ryan, M., Eds.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2017; pp. 164–186.