Cryptography & Blockchain

Mariam Hersi
HER22555014
Submitted to The University of Roehampton
In partial fulfilment of the requirements for the degree of
BACHELOR OF SCIENCE IN COMPUTING

***Abstract*— This report analyzes Ethereum's security vulnerabilities, including The DAO Hack and 51% attacks, while examining cryptographic safeguards like public-key cryptography and hash functions. Finally, it provides recommendations to enhance blockchain security for users and developers.**

I. Introduction

Blockchain technology is a central part of cryptocurrency. A blockchain consists of data sets which are composed of a chain of data packages (blocks) where a block comprises multiple transactions [1]. It is extended by each block creating a record of transactions. A block can only be added if the majority of nodes in the network agree by a consensus mechanism on the validity of transactions in a block and on the validity of the block itself [1].

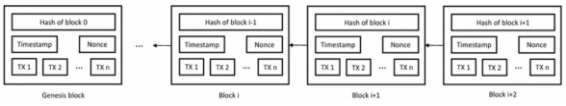

Fig. 1. Example of a blockchain. (*Zheng et al. 2016*)

This technology has revolutionised digital transactions by being decentralised [2]. Control and decision-making is transferred to a distributed network [2]. This ensures trust from the participants and deters those that intend harm.

However, despite this blockchain companies are not immune to security vulnerabilities. In this report I will be analysing those vulnerabilities and examine the security concerns in blockchain technology by evaluating Ethereum.

II. Security Incidents

Ethereum is the second largest cryptocurrency blockchain technology out there. It was announced in 2014 launched in 2015. Ethereum allows anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions [3]. Ethereum as a company has experienced attacks because of its vulnerabilities. Low it is innovative it has been susceptible two security threats such as:

A. Smart Contracts

One of the most noticeable vulnerabilities that Ethereum has dealt with is the smart contracts. Smart contracts combine computer protocols with user interfaces to execute the terms of a contract [1]. These contracts make applying block chains easier and may replace third parties like lawyers in the future. Ethereum is one of the biggest users of smart contracts and uses cryptography to replace these third parties. Blockchain might disrupt the entire transaction process by automatically executing contracts in a cost-effective, transparent and secure manner [1]. A smart contract generally contains some branch codes of *If* and *Else*, for describing the corresponding contract rules [4].

The DAO was an open-source project based on Ethereum application platform, and it is maintained by smart contracts [4]. On the 9th of June It was revealed that the was a recursive call vulnerability on the DAO project. Developers were waiting for the agreement of all on the methods for patching the vulnerabilities. On the 17th of June the DAO project was attacked by a hacker who was able to take 1/3 of the crowding ETH tokens ($50,000,000). Here we can see that smart contracts led to a vulnerability as the waiting on all members gave time for hackers to infiltrate.

B. PoW Consensus

Ethereum like Bitcoin relies on Proof of Work (PoW) consensus. This is where nodes compete to find a partial collision of a cryptographic hash function and produce the next block [3]. A consensus mechanism is a protocol which is in place to ensure that all the participants in the blockchain network are complying with the agreed rules [5]. This build trust between users and ensures there isn't one centralized control, instead everyone gets a say. A large quantity of electricity power is wasted for achieving consensus by Proof of Work (PoW); on the other hand, the increasing time for acknowledging a transaction is hard to endure, with the expansion of the whole system [4]. PoW consensus reliance makes it vulnerable to 51% attacks.

The 51% attack is a technique which intends to fork a blockchain in order to conduct double spending [5]. If a hacker can control more than half of the total hashing power of a network, they can perform this attack [5]. This is dangerous and once obtained a lot of money can be lost. Recent attacks proved that PoW is vulnerable to the 51% attack. Low hashing crypto coins utilizing PoW consensus are more vulnerable to 51% attack, as the required hash can be acquired easily [5].

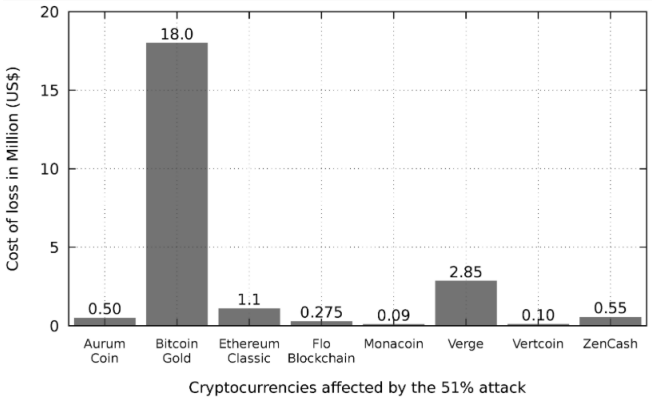

Fig. 2. Loss from 51% attack on eight cryptocurrencies. (*Zheng et al. 2016*)

III. Cryptographic Safeguards

Blockchain transactions rely on cryptographic mechanisms to ensure security, integrity, and authenticity. I will review below the cryptography algorithms that are used to protect assets:

A. Hashing Algorithms

Hash Functions are designed to generate a hash value from a piece of data [6]. It allows for verification that a message was not corrupted. The sender sends the hash value of the message together with it, and receiver can calculate the hash value of the received message and compare it to the one provided by the sender so any inconsistencies will mean corruption of the message during transfer [6].

Hashing is very essential to blockchains. The strength of the links between the blocks is dependant on it. It is ensured by writing the hash of the previous block into the new one [6]. If any sort of changes were made it would affect all the other blocks before it.

B. Assymetric Algorithms

Also known as public-key cryptography uses a pair of keys to create a secure communication channel between two peers - each peer has a key one being the public key and the other being the private key [6].

A type of public-key cryptography is public key encryption. It is used when a peer wants to send a secret message to another peer [6]. Between the two there is a private key. The recipient would use that private key to decrypt the message. They can then check the authenticity of that particular key using several ways. This would not be worth it for a adversary to try to infiltrate.

Public-Key Cryptography is extensively used in blockchain platforms, especially in crypto-currency ones, like Bitcoin. It also underpins such widely used technologies as Secure Shell (SSH) and Transport Layer Security (TLS) [6].

IV. Recommendations

To enhance blockchain security and mitigate potential vulnerabilities, it is essential to adopt proactive measures at both the protocol and user levels. The following recommendations focus on improving smart contract security, strengthening consensus mechanisms, encouraging best practices for users, and enhancing exchange security protocols.

A. Smart Contract Development

- Use formal verification tools: Static analysis tools such as MythX, Slither, and Oyente can identify vulnerabilities in smart contract code before deployment.
- Implement multi-signature authorization: Ensuring critical operations require multiple signatures reduces the risk of single-point failures.
- Follow best practices for contract design: Using design patterns like checks-effects-interactions can prevent reentrancy attacks.
- Regularly audit smart contracts: Independent security audits by third-party firms can uncover hidden vulnerabilities.

B. Delayed Proof of Work (dPoW)

Transition from PoW to dPoW for increased security against 51% attacks. To defend a 51% attack against the Komodo's blockchain, any existing copy of the Komodo chain permits the entire chain to take control of malicious activities [5].

C. User Best Practices

Individual users play a crucial role in maintaining security and protecting their assets.

- Use hardware wallets: Cold storage solutions like Ledger and Trezor provide the highest level of security for private key management.
- Employ privacy-enhancing techniques: Users concerned with privacy should leverage methods such as CoinJoin, shielded transactions (Zcash), and mixers (Wasabi Wallet).
- Beware of phishing and scams: Users should verify sources before signing transactions or entering credentials on websites.

V. Conclusion

Blockchain technology provides strong cryptographic security, yet vulnerabilities persist in its implementation. By analyzing security incidents, cryptographic safeguards, and privacy risks, we can better understand how to enhance blockchain security. Implementing robust security practices at both the protocol and user levels is crucial for mitigating risks and ensuring the long-term integrity of blockchain ecosystems.

References

[1] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Business & Information Systems Engineering*, vol. 59, no. 3, pp. 183–187, Mar. 2017, Available: https://link.springer.com/article/10.1007/s12599-017-0467-3

[2] AWS, "What is Blockchain Technology? - Blockchaining Explained - AWS," *Amazon Web Services, Inc.*, 2023. Available: https://aws.amazon.com/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc

[3] S. Tikhomirov, "Ethereum: State of Knowledge and Research Perspectives," *Foundations and Practice of Security*, vol. 10723, pp. 206–221, 2018, doi: https://doi.org/10.1007/978-3-319-75650-9_14

[4] X. Zhao, Z. Chen, X. Chen, Y. Wang, and C. Tang, "The DAO attack paradoxes in propositional logic," *IEEE Xplore*, Nov. 01, 2017. doi: https://doi.org/10.1109/ICSAI.2017.8248566. Available: https://ieeexplore.ieee.org/abstract/document/8248566. [Accessed: May 06, 2023

[5] S. Sayeed and H. Marco-Gisbert, "Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack," *Applied Sciences*, vol. 9, no. 9, p. 1788, Apr. 2019, doi: https://doi.org/10.3390/app9091788

[6] N. Storublevtcev, "Cryptography in Blockchain," *Computational Science and Its Applications – ICCSA 2019*, pp. 495–508, 2019, doi: https://doi.org/10.1007/978-3-030-24296-1_39