KENNESAW STATE UNIVERSITY

COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING

CS 4850-01 | FALL 2023 | SP-24 RED | SECURITY IN BLOCKCHAIN

IMPROPER BLOCKCHAIN MAGIC VALIDATION

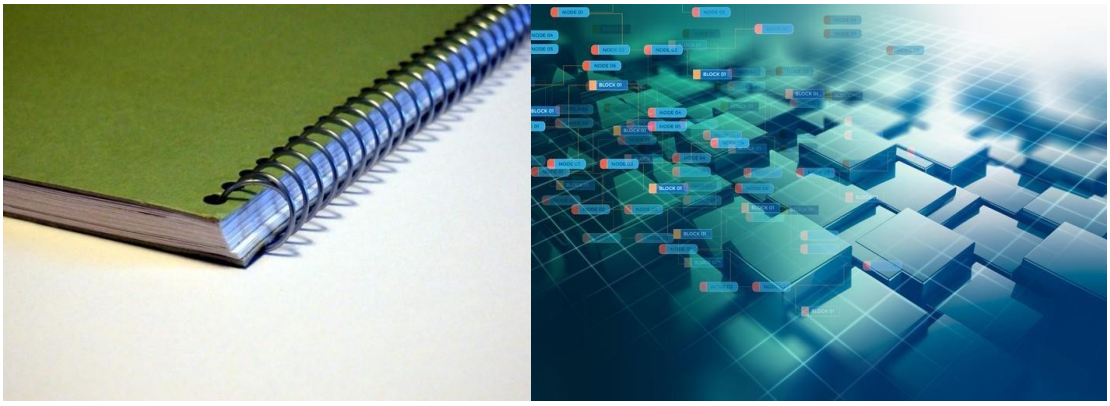
JALON BAILEY

INSTRUCTOR: SHARON PERRY

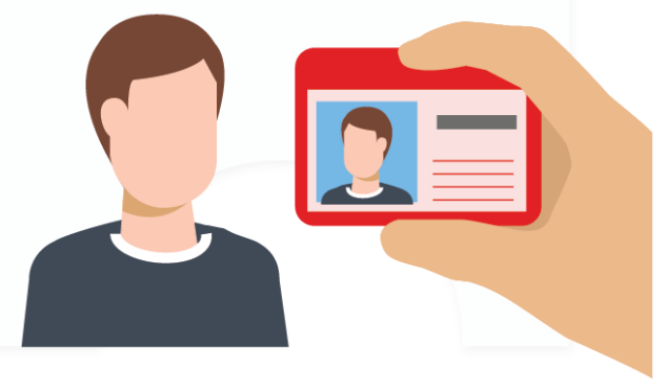
INTRODUCTION

What is blockchain validation?

Let's first define blockchain; Imagine a special notebook that everyone in your class can see, or even better a school board. No one can access the board or book by tearing pages out or cheating. The notebook is like a blockchain; it keeps track of who owns what without needing a teacher or a superior to step in. Relating back to the world of computers, there are digital notebooks shared by lots of computers all over the world. Any type of digital transaction, from crypto to bitcoin, being used to buy or sell something with digital money, everyone in the network has access to see it.



Now, how do we make sure that nobody cheats and everyone agrees on who owns what? This is where validation comes in. Validation in blockchain is like having a bunch of friends in your class who are really good at math. When you want to buy or sell something, they quickly solve a math problem related to your transaction. Once they all agree that your math is correct, the transaction is added to the notebook. This math problem is really hard to solve, but once your friends solve it, everyone knows they did the work properly. This is called validation. When using validation, the blockchain keeps everything good and secure. This is to make sure that nobody can trick the system and that everyone can trust the digital currency transaction.



IMPROPER USES?

The improper use of blockchain validation leads to unsafe and unwanted transactions. According to *Blockchain Vulnerabilities in Practice*, "If there is no such check, then an attacker can replay a transaction originally performed on another chain, thus creating transactions meant for another chain." Without the validation of the blockchain, an undesirable user can reuse the transaction for another. The original, "unique" transaction can be recycled a number of times until there is insufficient amount left, causing the transaction to be invalid for further use.

Cases of Improper Uses

To understand the difference between improper and proper, here are some valid cases:

- A notable case for blockchain validation is finance. Finance covers the source of money transactions between banking and consumers. There are contracts, digital currencies, compliance regulations, management, and simple payments.
- Another application can be rated to the healthcare system. Healthcare has an abundant amount of personal documentation and transactions, for both employees and patients. Documentation can include health records, clinical trial research, supply chain management, staff credentials, and patient monitoring.

Improper cases:

- Ethereum Classic (ETC) 51% Attack: In 2019, Ethereum Classic experienced a 51% attack, with the attackers reportedly double-spending approximately 219,500 ETC.
- Bitcoin Gold 51% Attack: In 2018, Bitcoin Gold, a fork of Bitcoin, suffered a 51% attack. The

attacker managed to defraud exchanges of over $18 million.

- False Smart Contracts: In some instances, vulnerabilities in a blockchain's smart contract code can be exploited. For instance, the DAO attack on Ethereum in 2016 resulted from a loophole in a smart contract, leading to a significant amount of Ether being drained from the DAO.

CONCLUSION

In conclusion, while blockchain validation provides a robust system for transaction verification, it's not impervious to attacks or misuse. Proper and continuous security measures, network monitoring, and updates are essential to maintaining the integrity and trust of a blockchain network.

REFERENCES

"Blockchain Vulnerabilities in Practice Blockchain Vulnerabilities in Practice." *Blockchain Vulnerabilities in Practice*, dl.acm.org/doi/fullHtml/10.1145/3407230. Accessed 17 Oct. 2023.

Orenes-Lerma, Linda. "What Is a Blockchain Validator?" *Ledger*, 21 July 2023, www.ledger.com/academy/what-is-a-blockchain-validator#:~:text=A%20validator%20is%20a%20participant,crypto%20to%20support%20the%20network.