Cover Page

Blockchain Report

Danyil Tymchuk &
another two people

04.12.2023

Personal & Professional Development
Group Project

Table

Introduction (Not my Part)

Banking and Bitcoin (Not my Part)

Hacking (Danyil)

Introduction

(150 words)

Overview of Blockchain Technology

Blockchain is like a digital ledger, but instead of being kept in one place, it's spread out across a whole network of computers. Think of it as a record book that everyone can see, but no one owns. This setup is really cool because it means there's no central control - it's all about teamwork across many computers.

Importance of Security

Now, why is this security thing a big deal? Imagine you're using blockchain for something super important, like transferring money or keeping sensitive data. You don't want anyone messing with that, right? That's where blockchain's security shines. Each piece of data (or block) is tied to the previous one using complex cryptography. This makes it super tough for anyone to change anything without everyone else noticing. So, in a world where we're doing more and more online, having a safe and secure way to handle our digital stuff is super important, and that's exactly what blockchain offers.

The Nature of Blockchain Hacking

(200 words)

How Hacking Differs in Blockchain

Hacking in the blockchain world is a different beast compared to traditional hacking, mainly due to blockchain's unique structure. In traditional systems, hackers often target central points of control or vulnerabilities in a single system. But with blockchain, there's no central point to attack because the data is distributed across a network of computers, each holding a copy of the ledger. This means to hack a blockchain, a hacker would need to alter the majority of the copies simultaneously, a task that's not only incredibly difficult but also requires immense computational power.

Common Misconceptions

However, there's a common misconception that blockchain is totally invulnerable. While it's true that blockchain's design makes it tough to hack in the traditional sense, it's not foolproof. For instance, if someone gains control over more than half of the network's computing power, a scenario known as a 51% attack(I will talk about it later), they could potentially alter the blockchain. Even with blockchain's strong security, there are still some weak spots. Think about smart contracts or the software that runs the blockchain - if they're not set up perfectly, hackers could sneak in through those gaps. So, while blockchain is really secure, it's not completely unbeatable.

Types of Blockchain Hacks

(250 words)

51% Attacks

This happens in a blockchain network when a single person or group controls more than 50% of the network's mining power. In blockchain, "mining" involves validating transactions and creating new blocks. If someone has over half the network's power, they can potentially manipulate the blockchain. They could stop new transactions from getting confirmations, allowing them to halt payments. Even scarier, they could reverse transactions they made while they're in control, which could lead to double-spending. However, pulling off a 51% attack is tough, especially on larger networks like Bitcoin, because it requires immense computational resources.

Backdoor (Code Exploits and Smart Contract Vulnerabilities)

Code Exploits and Smart Contract Vulnerabilities: Imagine the blockchain as a complex machine running on code. Sometimes, there are hidden flaws in this code. Hackers love to find and use these flaws. It's like finding a secret door into a bank vault. Smart contracts are like automatic agreements on the blockchain. If they're not written carefully, they can have weaknesses too. Hackers can use these weak spots to do things like steal digital money.

Sybil Attacks

This is like one person pretending to be many people on the blockchain. They create a bunch of fake identities to gain more power or control in the network. It's like one person wearing lots of different masks to trick others. With all these fake identities, they can mess with the network by spreading false information or overwhelming it with fake transactions. It is somewhat similar to a 51% attack but much smaller, because sybil attacks can occupy a maximum of 1-2% of the network.

Notable Blockchain Hacks

(200 words)

Historical Examples

Blockchain technology, known for its security, has still faced some notable hacks over the years. A prime example is the DAO attack on Ethereum in 2016. The DAO (Decentralized Autonomous Organization) was a complex smart contract on the Ethereum blockchain, designed to function as a sort of investor-directed venture capital fund. However, due to a flaw in its code, a hacker managed to drain about a third of the DAO's funds, amounting to around $50 million in Ethereum.

Impact of These Hacks

When these big hacks happen, it's not just about losing money. People start to doubt how safe blockchain really is. Take the DAO attack on Ethereum as an example. It was a huge

deal because a lot of money was stolen. But the reaction to the hack was even more dramatic. The Ethereum community decided to essentially go back in time and create a new version of Ethereum where the hack never happened. This move was called a "hard fork". It's like taking a road and then splitting it into two different paths.

This decision caused a lot of arguments. Some people thought it was the right thing to do to fix the problem. Others thought it went against the whole idea of blockchain being unchangeable and secure. So, Ethereum split into two: Ethereum (ETH) and Ethereum Classic (ETC).

Mitigating Hacking Risks

(150 words)

Security Measures

To keep blockchain safe from hackers, a couple of smart moves are key. First, think of regular audits like a health check for blockchain. Experts look over the code, hunting for any sneaky bugs that hackers could use to cause trouble. It's all about catching issues early.

Then there's the cool idea of multi-signature systems. It's like needing several thumbs up instead of just one to make something happen. In blockchain land, this means more people need to say 'okay' before a transaction goes through. It's like having a bunch of people double-checking each other, making things a lot safer.

Role of the Community

The power of the people!
The blockchain community is super important. Everyone needs to keep their eyes peeled and report anything fishy. It's like having a neighborhood watch for the digital world. By everyone chipping in and staying sharp, the blockchain stays strong and secure. It's teamwork at its best!

Conclusion

(50 words)

Finally, I would like to say that no system is 100% secure, but blockchain technology wants to provide unlimited freedom and decentralization, as well as a large part of security. Don’t forget the importance of great security. because without it there will be no life for any project.

The main thesis

“No matter how advanced the system is, anything can be hacked”

References

Behanan, J. V. (n.d.). *OWASP Smart Contract Top 10*. OWASP Foundation. Retrieved December 4, 2023, from https://owasp.org/www-project-smart-contract-top-10/

Cobb, M. (2023, May 25). *9 smart contract vulnerabilities and how to mitigate them*. TechTarget. Retrieved December 4, 2023, from https://www.techtarget.com/searchsecurity/tip/Smart-contract-vulnerabilities-and-how-to-mitigate-them

51% Attack: The Concept, Risks & Prevention. (2023, June 29). Hacken.io. Retrieved December 4, 2023, from https://hacken.io/discover/51-percent-attack/

John, F., & Luciano, C. (2023, February 16). *Sybil Attack in Blockchain: Examples & Prevention*. Hacken.io. Retrieved December 4, 2023, from https://hacken.io/insights/sybil-attacks/

Seher, S. (2022, July 8). *Smart Contract Vulnerabilities & How to Prevent Them*. Hacken.io. Retrieved December 4, 2023, from https://hacken.io/discover/smart-contract-vulnerabilities/

Sergeenkov, A. (n.d.). *Sybil Attack Definition*. CoinMarketCap. Retrieved December 4, 2023, from https://coinmarketcap.com/alexandria/glossary/sybil-attack

7 Smart Contract Vulnerabilities & How to Prevent Them [2023]. (2022, December 15). PixelPlex. Retrieved December 4, 2023, from https://pixelplex.io/blog/smart-contract-vulnerabilities/

Sybil Attacks Explained. (2018, December 6). Binance Academy. Retrieved December 4, 2023, from https://academy.binance.com/en/articles/sybil-attacks-explained

What Is a 51% Attack? (2018, November 27). Binance Academy. Retrieved December 4, 2023, from https://academy.binance.com/en/articles/what-is-a-51-percent-attack

What is a 51% attack and how is it prevented? (n.d.). Bitpanda. Retrieved December 4, 2023, from https://www.bitpanda.com/academy/en/lessons/what-is-a-51-attack-and-how-is-it-prevented/

What is Sybil attack: How Blockchains Prevent Sybil Attacks. (2021, March 26). Phemex. Retrieved December 4, 2023, from https://phemex.com/academy/what-is-a-sybil-attack

Zykov, G. (2023, April 10). *51% Attacks on the Blockchain Explained: What Are the Dangers?* BeInCrypto. Retrieved December 4, 2023, from https://beincrypto.com/learn/51-attacks-explained

Copyright

All words in this text were formulated and written by us (indicated below), this work was not copied from any other works, all references we used in writing were indicated.

Part 1 – Introduction (Not my Part)
Part 2 – Banking and Bitcoin (Not my Part)
Part 3 – Hacking (Danyil) – Written by Danyil Tymchuk