Towards Secure Layer-2 Blockchain Solutions Using TEEs

Vitor Ribeiro
Advisor: Sandro Pinto PhD
Co-Advisor: David Cerdeira

CENTROALGORITMI

UNIVERSIDADE DO MINHO

Universidade do Minho

Nov, 2021

Contextualization

Blockchain

- Technology that allows recording digital information that can't be changed, hacked or cheated.

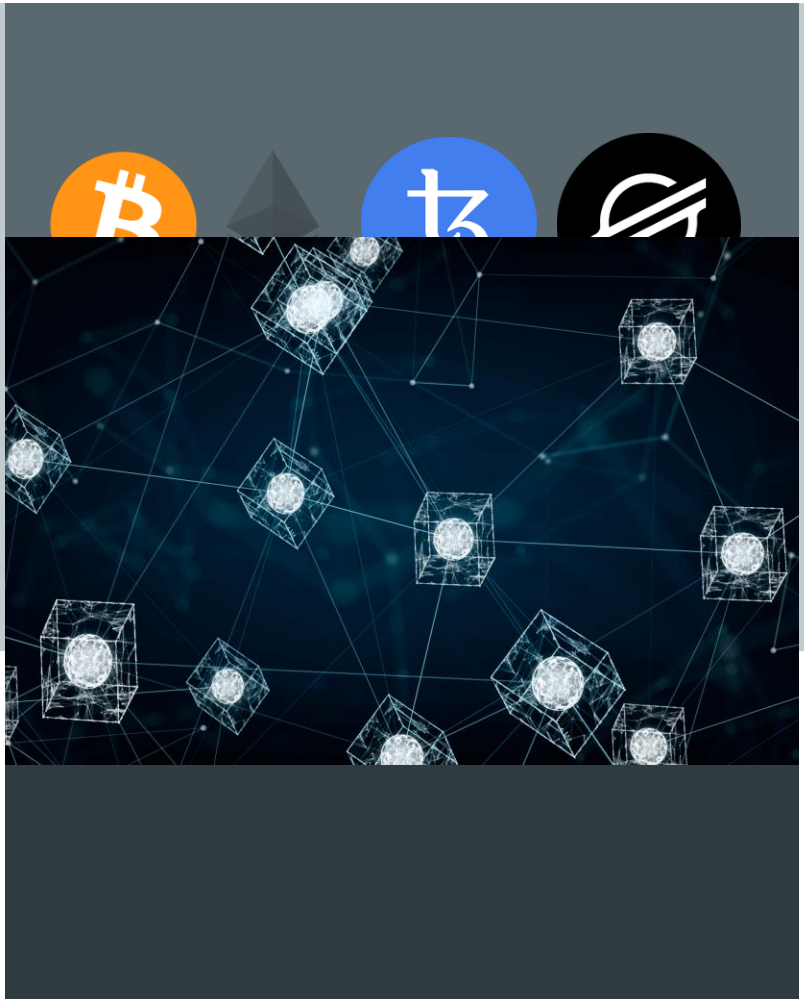
Blockchain

- Technology that allows recording digital information that can't be changed, hacked or cheated.
- Transactions are duplicated and distributed across the entire network of computers on the blockchain.

Blockchain

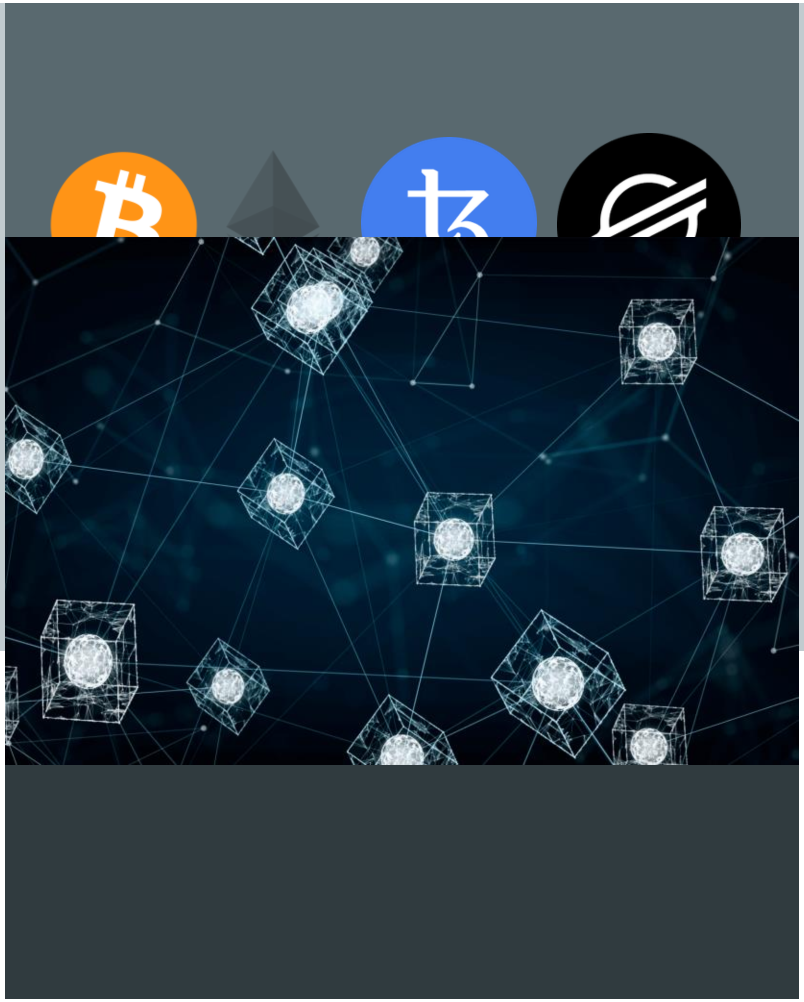
- Technology that allows recording digital information that can't be changed, hacked or cheated.
- Transactions are duplicated and distributed across the entire network of computers on the blockchain.
- Nowadays, Blockchain is often associated to cryptocurrency, because is the core technology behind, Bitcoin and Ethereum.

Blockchain – Vulnerabilities



Blockchain industry is not very mature when it comes to **vulnerabilities** and **weaknesses**.

Blockchain – Vulnerabilities



Blockchain industry is not very mature when it comes to **vulnerabilities** and **weaknesses**.

Weaknesses are introduced into software (web services, smart contracts,DApps,...) →

Blockchain – Vulnerabilities

Blockchain industry is not very mature when it comes to **vulnerabilities** and **weaknesses**.

Weaknesses are introduced into software (web services, smart contracts,DApps,...)

Results in vulnerabilities:

- Logic bugs
- Integer overflows
- Reentrancy issues

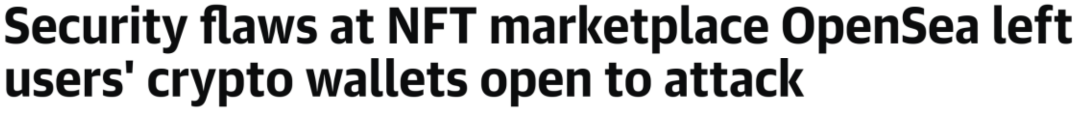
Blockchain – Vulnerabilities

Blockchain industry is not very mature when it comes to **vulnerabilities** and **weaknesses**.

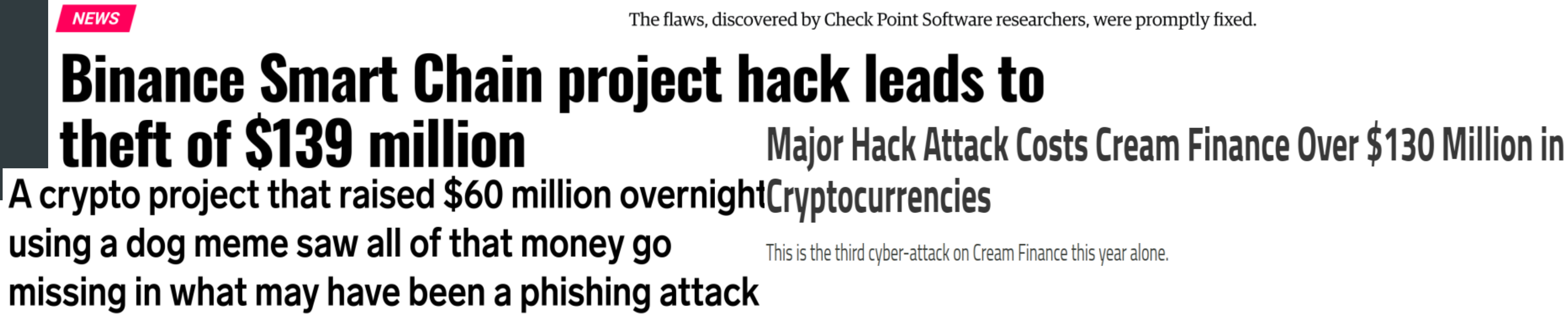
Weaknesses are introduced into software (web services, smart contracts,DApps,...)

→

Results in vulnerabilities:
- Logic bugs
- Integer overflows
- Reentrancy issues



Security flaws at NFT marketplace OpenSea left users' crypto wallets open to attack



The flaws, discovered by Check Point Software researchers, were promptly fixed.

NEWS

Binance Smart Chain project hack leads to theft of $139 million

Major Hack Attack Costs Cream Finance Over $130 Million in Cryptocurrencies

This is the third cyber-attack on Cream Finance this year alone.

A crypto project that raised $60 million overnight using a dog meme saw all of that money go missing in what may have been a phishing attack

Trusted Execution Environment (TEE)

- Isolated environment for executing code, in which those executing the code can have high levels of trust

Trusted Execution Environment (TEE)

- Isolated environment for executing code, in which those executing the code can have high levels of trust
- Guarantees the authenticity and confidentiality of the code

Trusted Execution Environment (TEE)

- Isolated environment for executing code, in which those executing the code can have high levels of trust
- Guarantees the authenticity and confidentiality of the code
- Resists software attacks

Trusted Execution Environment (TEE)

- Isolated environment for executing code, in which those executing the code can have high levels of trust
- Guarantees the authenticity and confidentiality of the code
- Resists software attacks
- We will study how TEE can improve Blockchain security problems

Motivation

Motivation

Work in upcoming platforms
- RISC-V Architecture -

Work in Security Analysis

Work with TEEs

Work with Linux

Work in open-source projects

Work with Blockchain Technology

Goals

Goals

- Create a threat model for a Blockchain solution (Cartesi)

Goals

- Create a threat model for a Blockchain solution (Cartesi)
- Threat Analysis

Goals

- Create a threat model for a Blockchain solution (Cartesi)
- Threat Analysis
- Threat mitigation using TEEs

Technical & Scientific Relevance

Technical & Scientific Relevance

Blockchain is a recent and disruptive technology, gaining a lot of adoption

- Immutability
- Transparency
- Security

Technical & Scientific Relevance

Blockchain is a recent and disruptive technology, gaining a lot of adoption

- Immutability
- Transparency
- Security

Blockchain Technology are not yet adopting TEEs as security method

Although it is secure, transparency brings some problems

"Simplicity is the ultimate sophistication" - Leonardo da Vinci

THANK YOU!

| Vitor Ribeiro a86619 |