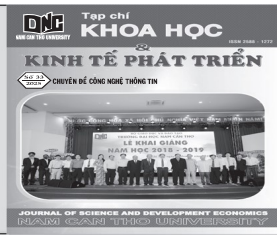
Journal of Science and Development Economics
Nam Can Tho University

Website: jsde.nctu.edu.vn



Cybersecurity in blockchain technology: Analysis of cyber-attacks on decentralized financial platforms

Dang Manh Huy[1*], Phan Thị Xuân Trang[1], Trương Thanh Thảo[1]

[1]*Faculty of Information Technology, Nam Can Tho University*

[*]*Corresponding author: Dang Manh Huy (email: manhhuydang@gmail.com)*

Received: 30/12/2024
Revised: 20/1/2025
Accepted: 10/2/2025

Keywords: *blockchain, consensus algorithm, decentralized, distributed, network security, security*

Từ khóa: *an ninh mạng, blockchain, phân tán, phi tập trung, thuật toán đồng thuận*

ABSTRACT

The rise of decentralized applications has propelled blockchain technology to prominence in recent years due to its decentralized, secure nature and ability to facilitate peer-to-peer transactions. Coupled with smart contracts, blockchain has found applications in various sectors, including finance, healthcare, and IoT. The DeFi sector, in particular, has garnered significant attention and investment. As blockchain adoption grows, so do concerns about the cybersecurity of decentralized systems built on this technology. This study delves into the security vulnerabilities of blockchain consensus mechanisms and the source code, providing insights into the cybersecurity challenges facing the DeFi sector.

TÓM TẮT

Sự phát triển của các ứng dụng phi tập trung đã đưa công nghệ blockchain trở nên nổi bật trong những năm gần đây nhờ vào tính chất phi tập trung, bảo mật và khả năng hỗ trợ giao dịch ngang hàng. Kết hợp với các hợp đồng thông minh, blockchain đã tìm thấy ứng dụng trong nhiều lĩnh vực, bao gồm tài chính, y tế và IoT. Đặc biệt, lĩnh vực tài chính phi tập trung (DeFi) đã thu hút được sự chú ý và đầu tư đáng kể. Khi việc ứng dụng blockchain ngày càng gia tăng, các mối lo ngại về an ninh mạng đối với các hệ thống phi tập trung được xây dựng trên công nghệ này cũng ngày càng nhiều. Nghiên cứu của tôi tập trung vào các lỗ hổng bảo mật trong cơ chế đồng thuận blockchain và mã nguồn, cung cấp những hiểu biết về các thách thức an ninh mạng mà lĩnh vực DeFi đang phải đối mặt.

1. INTRODUCTION

The concept of blockchain was first proposed in 1991 by Stuart Haber and W. Scott Stornetta, who developed a method to timestamp digital documents to prevent tampering [1]. Satoshi Nakamoto further popularized the idea in 2009 as the underlying technology for Bitcoin, a decentralized cryptocurrency [2]. Blockchain is a distributed database that records transactions across many computers. Each block contains a timestamp and a link to the previous block, forming an unchangeable chain of data. The technology ensures security and transparency through cryptographic hashing, creating a unique identifier for each record. Trust, accountability, and security are fundamental to blockchain.

The combined market capitalization of all cryptocurrencies currently stands at approximately $804 billion, with Bitcoin accounting for around $320 billion (as of January 3, 2023), according to CoinMarketCap.com. The global online payment market is valued at $6.75 trillion (Research and Markets). Beyond cryptocurrencies, blockchain technology is employed in various sectors including finance, IoT, and public services. Consequently, the amount of capital invested in blockchain systems is substantial. This makes these systems attractive targets for hackers, who can gain significant financial rewards from even small-scale attacks.

Essentially, blockchain is a distributed ledger technology, a continuously growing list of records, each recorded as a block. The data in each block is encrypted and secured using a cryptographic hash. Blocks are chained together sequentially, with each new block containing a hash of the previous block. These blockchains are distributed across a network of nodes. Nodes authenticate transactions and communicate with each other via a peer-to-peer network.

2. RESEARCH METHODS

This research employs a combination of qualitative and quantitative methods to analyze blockchain security vulnerabilities and attack trends. The study is structured into three main phases: data collection, data analysis, and case study evaluation.

2.1 Data collection

The data utilized in this study is sourced from multiple reputable databases, including:

- Blockchain security reports from organizations such as Chainalysis, CipherTrace, and SlowMist.
- Academic literature published in journals and conferences related to blockchain and cybersecurity.
- Publicly available incident reports from affected companies and security firms detailing blockchain-related attacks.
- Cryptocurrency market data from sources like CoinMarketCap and Messari to assess financial impacts.

Additionally, real-time blockchain transaction data and security alerts from platforms such as Etherscan and BTCExplorer were used to track attack patterns.

2.2 Data analysis

The collected data was processed using statistical and analytical techniques, including:

- Trend analysis: Examining the frequency and evolution of blockchain attacks over time [5].
- Comparative analysis: Evaluating different attack techniques and their effectiveness [4].
- Risk assessment frameworks: Applying models such as the STRIDE framework

(Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) to classify vulnerabilities.

- Network analysis: Mapping relationships between malicious actors, compromised smart contracts, and affected entities.

2.3 Case study evaluation

To provide a deeper understanding of blockchain security challenges, this study examines three major case studies:

1. Euler Finance Flash Loan Attack (March 2023) – Analysis of the vulnerability exploitation and its financial consequences [3].

2. Ronin Network Hack (March 2022) – Evaluation of security weaknesses in blockchain governance mechanisms [6].

3. Wormhole Bridge Exploit (February 2022) – Examination of smart contract vulnerabilities in cross-chain bridges.

Each case study includes an in-depth review of:

- The attack mechanism: How the attackers executed their plan.
- The exploited vulnerabilities: System weaknesses that were targeted.
- The financial and operational impact: The extent of damage caused by the attack.
- Mitigation measures: Strategies employed post-attack to prevent recurrence.

This multi-faceted approach ensures a comprehensive understanding of blockchain security threats and helps identify critical areas for strengthening blockchain-based systems.

3. RESULTS AND DISCUSSION

3.1 Representative attacks

Blockchain theory offers a robust framework for cybersecurity. Once data is recorded in a block, it becomes immutable, preventing any subsequent alterations. This ensures data integrity and provides a secure, decentralized method for verifying transactions and preserving privacy. Any attempt to modify even a single bit of data will invalidate the entire blockchain, making it easily detectable. Additionally, blockchain incorporates inherent security features such as encryption, smart contracts, and identity management.

Blockchain's unique properties make it an ideal technology for highly secure systems. Nevertheless, attacks targeting blockchain-based systems are on the rise [4].

Figure 1. Number of attacks and value of cryptocurrency stolen

(Source: Tsihitas, 2023)

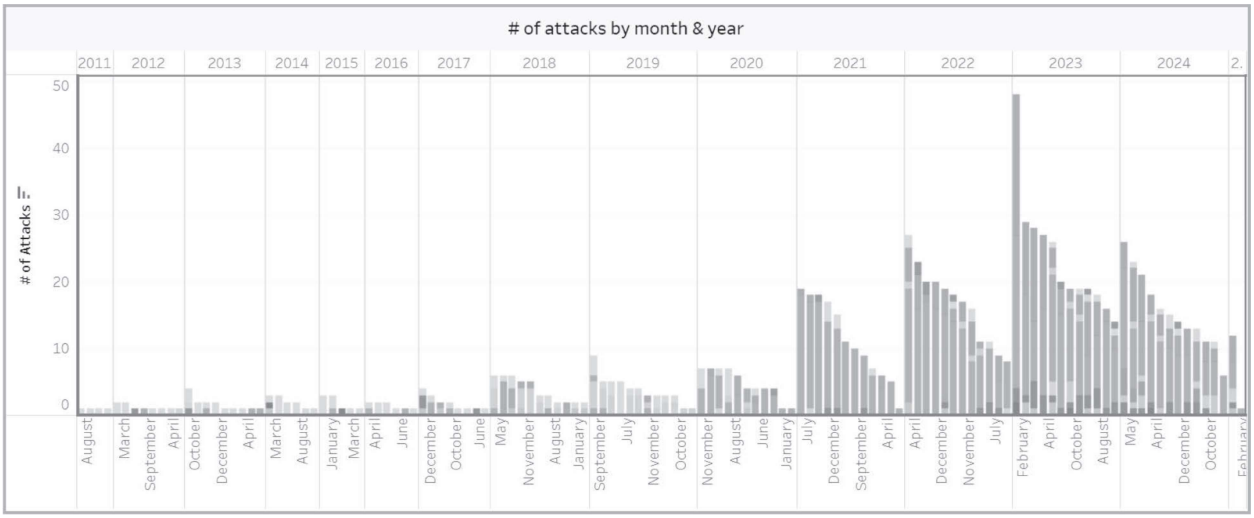


Figure 2. Number of attacks and attack methods by year

(Source: Tsihitas, 2023)

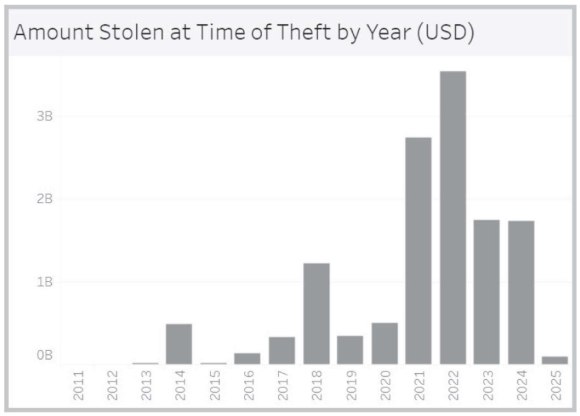


Figure 3. Annual amount of money stolen

(Source: Tsihitas, 2023)

Type of Attack	
51% Attack	16
Accidental	7
Exploit	404
Flash Loan	229
Governance Attack	1
Hack	277
Insider	15
Malware	1
Price Oracle/Price Ma..	39
Reetrancy Attack	18
Third Party	24
Unknown	1

Figure 4. Attack techniques

(Source: Tsihitas, 2023)

The data indicates a significant rise in both the frequency and diversity of attacks. While in 2011, hacking was the primary concern, by 2022, we faced a much broader spectrum of threats, including governance attacks, exploits, accidental losses, and flash loans. The total value of stolen funds surged from a mere 2.3 million USD in 2011 to over 3.5 billion USD in 2022. Notably, exploits, flash loans, and traditional hacking remained the most prevalent attack vectors [5].

3.1.1 Flash loan

A flash loan is an instant loan where borrowing and repayment occur in a single transaction. These loans have gained traction in the DeFi space, providing businesses and individuals with access to substantial funds without collateral requirements. The primary goal is to capitalize on price discrepancies.

Flash loan attacks capitalize on the temporary liquidity provided by loans to manipulate cryptocurrency prices, exploit DeFi smart contract vulnerabilities, or steal funds [3]. These attacks typically involve three steps

- Borrowing: The attacker will take out a large flash loan of cryptocurrency from a DeFi platform.

- Manipulation: The attacker leverages the borrowed funds to manipulate the target

cryptocurrency's price or exploit a DeFi smart contract vulnerability.

- Repayment: The attacker returns the borrowed funds to the lending platform, pocketing the profits.

In March 2023, one of the most recent and largest flash loan attacks was executed against Euler Finance. The hackers exploited a flaw in the ratio calculation within the platform itself. Euler Finance users interact with two primary token types: eTokens (representing collateral) and dTokens (representing debt). The attackers took advantage of a vulnerability in Euler's eToken mechanism, causing an inaccurate conversion of borrowed assets into collateral.

The hackers flash loaned approximately $30 million worth of DAI from the DeFi protocol Aave. They deposited $20 million DAI into the Euler platform and received an equivalent amount in eDAI. By leveraging Euler's borrowing capabilities, the attackers were able to borrow ten times the amount of their initial deposit. They used the remaining $10 million DAI to partially repay the borrowed debt and continued to borrow until the flash loan was completed.

As a result of the attack, Euler lost approximately $197 million worth of cryptocurrencies, including DAI, wBTC, stETH, and USDC. Additionally, Euler's native token, EUL, experienced a more than 45% decline in value.

3.1.2 Hack

Consensus algorithms are the backbone of blockchains, ensuring the decentralized nature of the network. They guarantee the validity, honesty, and transparency of transactions and ensure all nodes agree on the ledger's accuracy [6].

In March 2022, Sky Mavis, the developer behind Axie Infinity, reported a massive hack on the Ronin Network. Hackers stole approximately $624 million worth of cryptocurrency. The attack went unnoticed until a group of users reported being unable to withdraw funds from the Ronin bridge. This incident marked one of the largest DeFi hacks to date.

The Ronin Network hack was executed by compromising private keys. The Ronin Network employs a set of nine validator nodes to approve transactions on its bridge, requiring a majority of five to authorize deposits or withdrawals. The attackers stole four of these from Sky Mavis's systems and one more from the blockchain operated by Axie DAO. Subsequently, the attackers used these five nodes to conduct a transaction sending 173,600 Ethereum to a private wallet, a sum that escalated to approximately $615 million. In November 2021, Axie DAO temporarily allowed Sky Mavis to sign transactions on their behalf as part of an effort to help Sky Mavis cope with a myriad of free transactions (3). While the program expired the following month, the permission list was never revoked, meaning Sky Mavis could still generate signatures for Axie DAO. When the hackers stole Sky Mavis's keys, they subsequently gained access to the Axie network and used it to obtain the Axie DAO validator node key using a gas-free RPC.

The attack exploited the fact that only five out of nine validator nodes were needed to approve transactions. This is akin to a 51% attack, but instead of controlling the majority of the

network's hashing power, the attackers merely needed to compromise a specific set of nodes.

3.1.3 Exploit

The Wormhole Bridge hack in February 2022 is a prime example of exploiting vulnerabilities. This cross-chain bridge, facilitating asset transfers between different blockchains, suffered a significant breach, leading to the theft of over 325 million USD worth of 120,000 wETH. The incident was attributed to a flaw in the account verification process.

The attackers circumvented the verification process by injecting a fraudulent sysvar account, crafting a malicious "message" that authorized the minting of 120,000 wETH. By executing the "complete wrapped" function with this malicious "message", the attackers successfully minted the specified amount. Within two minutes, 10,000 ETH was bridged to the Ethereum blockchain, followed by another 80,000 ETH transaction approximately 20 minutes later.

The exploit leveraged a deprecated function that relied on a sysvar account for instructions. The vulnerability arose from the function's failure to verify the data within the sysvar account before processing. This allowed attackers to manipulate the instructions, enabling them to illicitly mint $320 million worth of tokens.

3.2 Analysis of attacks

Exploits, flash loans, and hacks accounted for 584 out of 676 attacks on cryptocurrency systems as of June 2023. Attack methods have diversified significantly, from a single form of hacking in 2011 to over 11 different types today. Concurrently, the number of attacks has surged from 4 in 2011 to 198 in 2022. Attacks can be as simple as exploiting a logical flaw in a system, such as the ratio calculation in the Euler Finance flash loan attack, or as complex as the Ronin Network attack. Additionally, minor oversights can be the primary cause of attacks, such as the failure to revoke a permission list in the Ronin attack or the Wormhole Bridge attack, which could have been prevented if a discovered function call error had been deployed earlier. Laxities in consensus algorithms can lead to the easy takeover of validators, as demonstrated by the simple requirement of only five out of nine validator nodes to approve transactions on the Ronin Network. Currently, the Ronin Network has increased the required number of validator nodes for consensus to eight.

4. CONCLUSION

Blockchain technology powers decentralized finance, offering decentralization, transparency, and trustlessness. This gives users complete control of their assets. With over $78 billion locked in DeFi protocols, as reported by DeFi Pulse, it’s a prime target for hackers. Tracking attacks becomes extremely difficult when large sums of cryptocurrency are sent to wallets identified by hashed strings. Given the nascent nature of blockchain technology, there are no universal regulations. Companies have the flexibility to innovate and implement solutions they deem fit, such as consensus mechanisms that are only updated in response to exploits. Blockchain attacks will persist, and it's impossible to anticipate all the tactics hackers will employ. Nevertheless, lessons learned from previous incidents allow us to audit our systems and identify vulnerabilities in the underlying algorithms and codebase.

REFERENCES

[1] Haber, S., & Stornetta, W. S. (1991). How to timestamp a digital document. *Journal of*

Cryptology, 3(2), 99–111. https://doi.org/10.1007/BF00196791

[2] Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.* Bitcoin. Retrieved from https://bitcoin.org/bitcoin.pdf

[3] Palamarchuk, R. (2022). *Flash loan attacks.* Hacken. Retrieved July 4, 2023, from https://hacken.io/discover/flash-loan-attacks/

[4] Palamarchuk, R. (2023). *Biggest cryptocurrency heists.* Comparitech. Retrieved July 4, 2023, from https://www.comparitech.com/crypto/biggest-cryptocurrency-heists/

[5] Tsihitas, T. (2023). *Biggest cryptocurrency heists.* Comparitech. Retrieved July 4, 2023, from https://www.comparitech.com/crypto/biggest-cryptocurrency-heists/

[6] Behnke, R. (2022). *Explained: The Ronin hack - March 2022.* Halborn. Retrieved July 5, 2023, from https://www.halborn.com/blog/post/explained-the-ronin-hack-march-2022