International Journal of Advanced Smart Convergence Vol.12 No.3 40-50 (2023)
http://dx.doi.org/10.7236/IJASC.2023.12.3.40

IJASC 23-9-6

Analysis of Blockchain Network and Cryptocurrency Safety Issues

Taegyu Lee*

**Assistant Professor, Dept. of Smart Contents, Division of ICT Convergence, Pyeongtaek University, Gyeonggi, Korea*
E-mail : tglee@ptu.ac.kr

Abstract

Blockchain is a technology designed to prevent tampering with digital documents or information, safeguarding transaction data and managing it in a structured manner. This proves beneficial in addressing issues of trust and data protection in B2B, B2C, and C2B transactions. Blockchain finds utility not only in financial transactions but also across diverse industrial sectors. This study outlines significant cases and responses that jeopardize the security of blockchain networks and cryptocurrency technology. Additionally, it analyzes safety and risk factors related to blockchain and proposes effective testing methods to preemptively counter these challenges. Furthermore, this study presents key security evaluation metrics for blockchain to ensure a balanced assessment. Additionally, it provides evaluation methods and various test case models for validating the security of blockchain and cryptocurrency transaction services, making them easily applicable to the testing process.

Keywords: *Blockchain Network, Cryptocurrency, Safety, Testing, Test Case.*

1. Introduction

Blockchain is a cutting-edge cryptographic technology that employs timestamping to prevent tampering or backdating of digital documents, ensuring their integrity. This technology or platform uses a distributed and encrypted format to protect, store, and manage transaction data. It addresses trust and data violation issues among Business-to-Business (B2B), Business-to-Consumer (B2C), and Consumer-to-Business (C2B) transaction entities. Particularly, it offers reliability in transactions among parties who do not inherently trust each other. Blockchain serves as an incorruptible digital ledger for economic transactions that can be programmed to record nearly all forms of value, extending beyond just financial transactions. In 2009, Satoshi Nakamoto adopted blockchain technology to create the digital cryptocurrency Bitcoin. Subsequently, blockchain technology has revolutionized business practices and become a fundamental element of mainstream digital currencies and utility tokens [1, 2].

The types of blockchain networks are categorized as follows: Public Blockchain, Consortium Blockchain,

Manuscript Received: June. 22, 2023 / Revised: June. 29, 2023 / Accepted: July. 4, 2023
Corresponding Author: tglee@ptu.ac.kr
Tel: +82-31-659-8370, Fax: +82-31-659-8011
Assistant Professor, Dept. of Smart Contents, Division of ICT Convergence, Pyeongtaek University, Gyeonggi, Korea

Private Blockchain, and Hybrid Blockchain, as depicted in Figure 1 [2, 3]. Public Blockchain operates openly for general users, allowing the network to expand continuously without constraints, thereby enhancing the safety and scope of transactions among participants. In contrast, Private Blockchain is limited to specific user groups and corporate entities, restricting network scalability and transaction safety to a narrower range. Hybrid Blockchain is controlled by a single organization; however, it necessitates a level of oversight comparable to that provided by public blockchains to validate certain transactions.

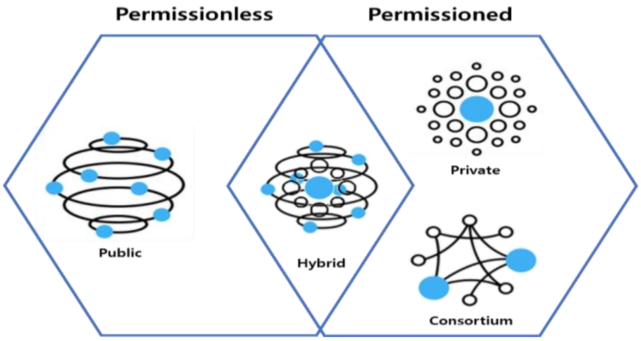

Figure 1. Type of Blockchain

The key components of a blockchain network are as follows [4, 5]. First, the Node Application: Each participating node installs and operates a computer application suitable for the ecosystem aiming to join the blockchain network. Second, the Shared Ledger: The data structure (or ledger) is managed within the node application. While the node application is in an operational state, it can view the ecosystem's content. Third, the Consensus Algorithm: This algorithm, implemented as part of the node application, provides the "rules of the game" for how the ecosystem reaches a single view of the ledger. Fourth, the Virtual Machine: It abstracts a machine that operates according to instructions and is implemented as part of the node application executed by all participants in the ecosystem.

Blockchain's characteristics lie in its ability to provide enhanced transaction security due to multiple nodes participating in the authentication and validation of transactions. Additionally, blockchain and cryptocurrencies form decentralized systems, leading to convergence applications across various industries such as finance, real estate, insurance, healthcare, manufacturing supply chains, distribution, media, entertainment, and communications, as illustrated in Figure 2 [2, 3, 6]. Furthermore, the continuous and stable increase in transaction capacity and traffic of the entire blockchain network is achieved by avoiding centralization.

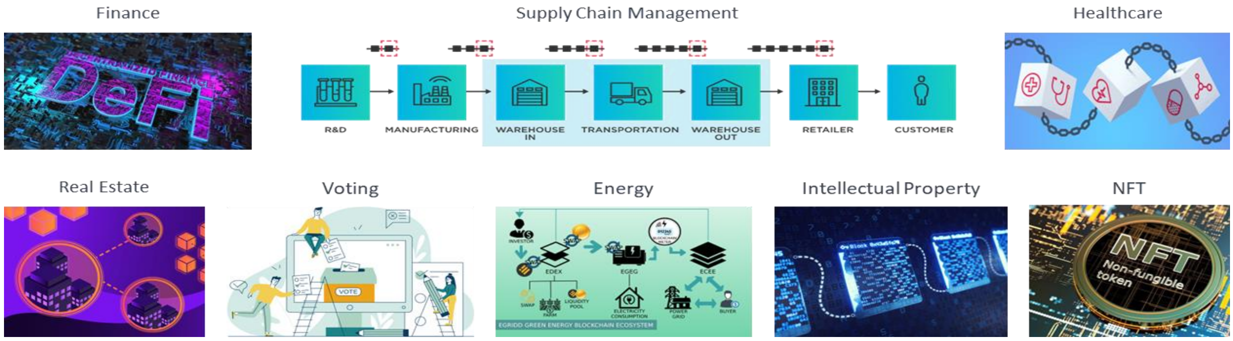

Figure 2. Potential Use Cases of Blockchain across Various Industries

Recent trends show a significant surge in interest in blockchain-based applications such as the Metaverse and Non-Fungible Tokens (NFTs). This trend is driving increased interest and demand for blockchain technology standards. International standardization of blockchain is still lacking, and there is a need for active standard proposal activities from various standard groups based on established reference structure standards.

The increasing number of risks and hacking incidents threatening the security of blockchain, and cryptocurrencies has prompted a strong demand for enhanced security measures and improved testing methods for blockchain security.

This paper aims to analyze the major risk factors associated with blockchain networks and cryptocurrencies and proposes testing methods to prevent these risks.

This paper is described as follows. Chapter 2 describes the research on blockchain safety and hacking related works, Chapter 3 describes the analysis of blockchain network safety, and Chapter 4 describes the blockchain test method and examples. Finally, Section 5 describes the conclusion.

2. Related Works: Security Threats in Blockchain Networks and Cryptocurrencies

Blockchain technology is an innovative approach that combines distributed ledgers with cryptographic techniques to enable secure and reliable transactions. However, blockchain networks and cryptocurrency systems are also vulnerable to various security threats and attack scenarios. This chapter outlines the key cases that jeopardize the security of blockchain networks and cryptocurrencies. Here, as illustrated in Figure 3, we examine the operational principles of a typical blockchain process and the associated risk factors.

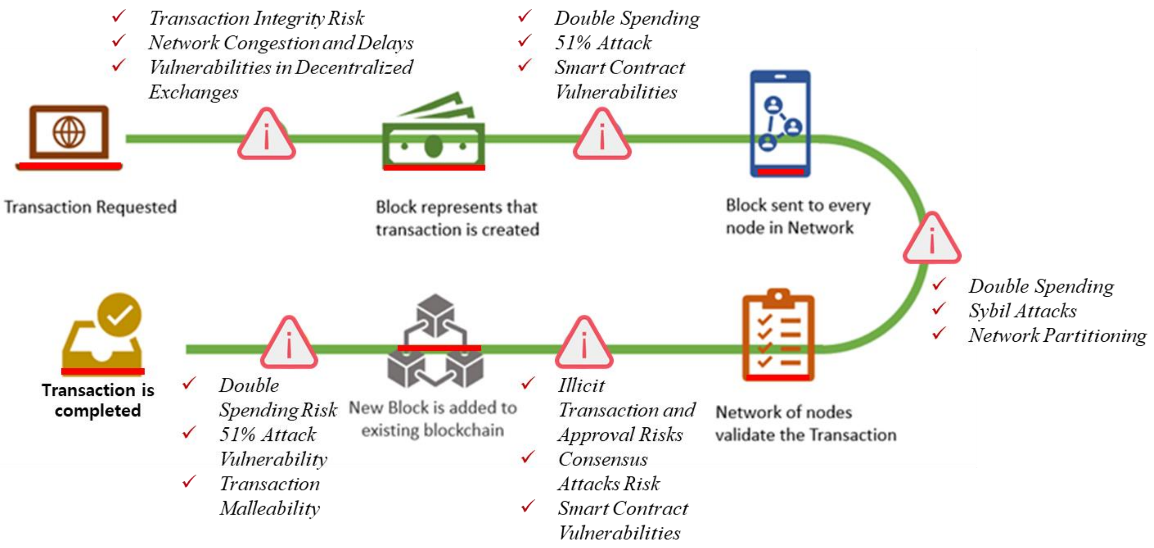
✓ Transaction Integrity Risk
✓ Network Congestion and Delays
✓ Vulnerabilities in Decentralized Exchanges
✓ Double Spending
✓ 51% Attack
✓ Smart Contract Vulnerabilities
Transaction Requested
Block represents that transaction is created
Block sent to every node in Network
✓ Double Spending
✓ Sybil Attacks
✓ Network Partitioning
Transaction is completed
✓ Double Spending Risk
✓ 51% Attack Vulnerability
✓ Transaction Malleability
New Block is added to existing blockchain
✓ Illicit Transaction and Approval Risks
✓ Consensus Attacks Risk
✓ Smart Contract Vulnerabilities
Network of nodes validate the Transaction

Figure 3. Transaction Process and Safety Crisis Point in Blockchain

The blockchain-based transaction process unfolds as follows: (1) Transaction Initiation and Authentication: Initially, a transaction is requested and then verified. (2) Representation as a Block: The generated transactions are represented as a single block. (3) Broadcasting to the Network: This block is then transmitted to all participating nodes within the network. (4) Transaction Verification by Participating Nodes:

Participating nodes verify the transactions. As a typical practice, nodes receive rewards for proof of work, often in the form of cryptocurrencies. (5) Addition to the Existing Blockchain: The created block is added to the existing blockchain, and any modifications to the blockchain are distributed across the network. (6) Completion of the Transaction: Finally, the transaction is considered complete. Each step in this process is designed to ensure the security, integrity, and consensus of the transactions within the blockchain network.

2.1 Blockchain Network Attack Cases

2.1.1 51% Attack

In a blockchain network, a 51% attack refers to an attack where a specific group or individual secures over half of the total hash power of the network to manipulate ledger records [6]. This can lead to data tampering or double-spending attacks. Several cryptocurrencies such as Bitcoin Gold, Monacoin, Zencash, and Litecoin Cash have fallen victim to such attacks [7]. Notably, Bitcoin Gold suffered a 51% attack resulting in double-spending damages. Approximately 388,200 Bitcoin Gold were transferred to a hacker's wallet address, leading to the delisting of the cryptocurrency from exchanges. In the case of Zencash, it suffered three instances of 51% attacks, resulting in the theft of 21,000 Zencash tokens (worth 40 million KRW).

2.1.2 Smart Contract Vulnerabilities

Bugs or vulnerabilities discovered within smart contracts due to blockchain code attacks can pose a more significant threat than actual cryptographic algorithms. An example of an attack exploiting such vulnerabilities is the Decentralized Autonomous Organization (DAO) infinite refund attack. DAO is structured around token ownership, where token holders exercise voting rights, distribute dividends, and approve projects with over 20% token approval for proposals. The DAO infinite refund attack exploited a recursive calling bug, allowing a hacker to request infinite refunds, leading to a damage of approximately 5.8 billion JPY [8].

2.2. Cryptocurrency Wallet and Exchange Hacking

2.2.1 Cryptocurrency Wallet Hacking

Cryptocurrency wallets represent a vulnerable point where hackers can gain unauthorized access by bypassing personal computers or smartphones. As a result, cases of individuals' cryptocurrency holdings being stolen have arisen. Among notable hacking incidents, the virtual currency wallet service 'Kaikas' provided by the Kakao subsidiary, Klip, was affected [9]. While the wallet service itself boasts high-security measures against hacking, vulnerabilities in insecure personal PCs or smartphones were exploited, leading to the associated damages.

2.2.2 Exchange Hacking

Virtual currency exchanges have also experienced multiple hacking incidents [10]. In such cases, malicious actors (including operators) exploit vulnerabilities within exchanges to steal assets from members. For instance, in the virtual currency information-sharing cafe 'Bitman,' approximately 52,000 members suffered a loss of around 2.21 trillion KRW. Hot wallet attacks typically involve hackers stealing the private key of an electronic wallet, granting them permission to transfer cryptocurrencies, which are then moved to other wallets. One instance is the Bithumb exchange, where a hot wallet hack in June 2018 resulted in the theft of cryptocurrencies worth 35 billion KRW. One of the most severe exchange hacking cases is the Coincheck incident in Japan, where on January 26, 2018, a hacking attack led to the theft of approximately 57 billion JPY (about 570 billion KRW) worth of virtual currency. This incident affected 260,000 victims, with 99% of the damage being stolen within a mere 19 minutes. The main cause of this incident was storing the private key in an internet-connected "hot wallet" without implementing a "Multi-Signature" system for key distribution to enhance security.

2.3. Blockchain Testing and Security Enhancement Issues

Due to the complexity of distributed systems, blockchain technology poses challenges in testing and security enhancement. Currently, standards for verifying the safety of blockchain networks and cryptocurrencies are lacking, necessitating diverse testing criteria based on their respective types. Blockchain integrated quality testing must consider unique aspects distinct from traditional software testing, and suitable testing methods should be adopted based on the type of blockchain software.

Given the inherent nature and complexity of security threats and attack cases within blockchain networks and cryptocurrencies, protection requires essential security reinforcement and testing of blockchain technology and systems. This study aims to examine components threatening the safety of blockchain networks and describe various testing approaches to address security vulnerabilities.

3. Analysis of Blockchain Network Component Safety

In this chapter, we conduct a safety analysis of various components within the blockchain network, focusing on different types of hacking attacks and corresponding countermeasures. The main objective is to establish a comprehensive assessment platform that can be utilized for public evaluation, certification, and testing of blockchain networks.

3.1 Hacking Attack Types and Responses for Blockchain Network Elements

Even blockchain networks built upon distributed system architectures are not immune to hacking attacks. This section outlines various types of hacking attacks and strategies to mitigate their impacts.

3.1.1 Use of Hardware Wallets

An essential element of blockchain security is the use of hardware wallets, such as hot wallets and cold wallets. Hot wallets are accessible via smartphone apps or PCs and are connected to the internet. In contrast, cold wallets, like Ledger Nano S, Trezor, KeepKey, and paper-based solutions, protect private keys offline. Cold wallets enhance security by generating private keys in a secure offline environment. Operational principles include creating backup keys and storing them in separate locations. In the event of hardware wallet theft, wallet encryption is recommended to prevent cryptocurrency theft.

3.1.2 Software-Based Key Management

To enhance blockchain network security, various software-based key management methods can be employed. Multi-factor authentication combines additional authentication technologies with private keys, such as One-Time Password (OTP) tokens, biometric authentication (iris, fingerprint, signature), and SMS-based verification. Multi-signature methods involve using a multi-signature scheme that requires multiple private keys. For example, BitGo requires 2 out of 3 private keys for transaction approval, enhancing protection against unauthorized transactions.

3.1.3 Ensuring Availability Through Transaction Fees

Some blockchain networks require strategies to counter network availability degradation attacks like Distributed Denial of Service (DDoS). Limitations can be imposed based on the amount of executed code to prevent unlimited transactions. This approach safeguards blockchain network availability by preventing hackers from executing unlimited transactions. Ethereum, for example, uses Gas consumption during code execution to defend against DDoS attacks.

3.1.4 Strengthening Consensus Algorithms

Various solutions are being proposed to mitigate 51% attacks on cryptocurrency exchanges [6]. One method is delaying transaction confirmation until dual-spending confirmation is achieved by increasing the number of confirmations required for deposits. While effective, this method extends transaction times, reducing user convenience. Examples include Bitcoin, Bitcoin Cash, Ethereum Classic, and Litecoin, which increase confirmation counts to mitigate security risks. To address inherent vulnerabilities in blockchain, technical verification and implementation of new consensus algorithms, such as Proof of Stake, Delegated Proof-of-Stake, Proof of Importance, and Zero-Knowledge Proof, are necessary.

3.1.5 Enhancing Exchange Security

Security of cryptocurrency exchanges is crucial to protect user assets. Measures to enhance security include installing access control mechanisms and employing technical defense mechanisms such as encryption for personal data protection. For high-volume exchanges, adopting Information Security Management System (ISMS) certification is mandated to improve information protection levels.

3.1.6 Strengthening Cryptocurrency and NFT Security

Recent hacking cases related to cryptocurrencies and NFTs have revealed vulnerabilities within the blockchain ecosystem. Axie Infinity suffered a breach on its sidechain network 'Ronin,' resulting in the theft of over $600 million worth of cryptocurrencies [11]. This incident involved a breach on the sidechain network 'Ronin,' which connects Ethereum and the platform's utility tokens. The breach exploited the verification process, allowing the attacker to take control of five out of nine nodes, resulting in losses. To address such sidechain vulnerabilities, required signatures were increased to eight. Particularly, OpenSea, a major NFT marketplace, experienced cases of unauthorized NFT trades due to a system bug [12]. Attackers manipulated NFTs registered at lower prices in the past, reselling them at significantly higher prices for profit. As an off-chain response, enhancing security features such as regional restrictions or two-factor authentication during exchange logins, advanced monitoring and strengthening of Fraud Detection Systems (FDS), and the introduction of blockchain and dark web intelligence (OSINT) can be utilized to detect and trace threats such as account information leaks or asset breaches, enhancing customer asset protection.

3.2 Safety Challenges in Blockchain Testing

Enhancing the security of blockchain applications through testing presents various challenges as follows:

- Technical Understanding: Adequate comprehension of blockchain technology and its application domains is necessary.

- Lack of Best Practices: Absence of best practices for blockchain application development can complicate the testing process.
- Absence of Blockchain Testing Tools: The lack of suitable tools for testing blockchain applications can hinder effective testing.
- Lack of Standardization: The absence of standardized testing approaches can complicate the testing process.
- Defining Testing Strategies: Designing effective testing strategies requires a deep understanding of the technology.
- Blockchain Size: Testing block and chain sizes is crucial for successful implementation.
- Absence of Optimal Testing Strategies: Lack of specialized knowledge in blockchain testing often results in suboptimal strategies.
- Performance and Load: Confirming appropriate performance and load handling is essential for reliable blockchain applications.
- Transaction Irreversibility: Due to the irreversible nature of blockchain transactions, careful implementation is needed to prevent duplication.
- Consistency/Availability: Maintaining a balance between consistency and availability in blockchain applications is a challenge.
- Trustworthiness: Rigorous testing and verification should be conducted at different levels to foster user trust in blockchain and cryptocurrencies.
- Objectivity: Third-party or certified authorities often conduct blockchain and cryptocurrency testing, ensuring objectivity.
- Safety: The foundational system of the blockchain and cryptocurrencies used by users should be securely established, safeguarding services against arbitrary attacks.
- Persistence: Blockchain and cryptocurrency services conducted openly on the internet persist until customers themselves discontinue them.

In conclusion, testing blockchain and cryptocurrency applications involves a complex process considering various factors and challenges. Addressing these challenges and implementing robust testing methodologies are crucial to ensure the security, stability, and trustworthiness of blockchain and cryptocurrency systems.

4. Proposal for Security Testing of Blockchain and Cryptocurrency

Blockchain and cryptocurrency play innovative roles in modern finance and technology, with their safety and reliability being significant concerns. Therefore, this chapter presents effective testing strategies for enhancing security.

4.1 Testing Methods of Blockchain and Cryptocurrency

The term 'test model' refers to a model that experiments with and simulates the operation principles, technologies, scenarios, etc., of blockchain and cryptocurrency. A test model for blockchain can simulate the functioning of blockchain and evaluate performance in various scenarios. Such testing models contribute to the development and enhancement of new blockchain technologies. Similarly, test models for dealing with cryptocurrencies simulate various cryptocurrency transactions and exchange functions, allowing the evaluation and improvement of stability and performance in cryptocurrency networks.

These test models play a crucial role in evaluating and optimizing the functionalities, security aspects, and performance of blockchain and cryptocurrency. Importantly, these test models can be utilized for simulation before applying changes to the actual network, enabling the discovery and rectification of unforeseen issues in advance.

4.1.1 Limited Self-Testing

Due to the constrained user participation, limited nodes, restricted cryptocurrency issuance, confined test cases, and the limitations of time and space in which the test network and cryptocurrency testing system operate, the testing comprehensiveness is restricted. Furthermore, the constrained testing model must be thoughtfully downsized to create a representative sampling model that adequately reflects the entire blockchain system. Currently, blockchain testing might suffer from a deficiency of quantitative or qualitative test cases and could exhibit bias toward one side.

4.1.2 Test User Interface

This model facilitates users to test various test cases, including fundamental functionalities, transaction generation, broadcasting performance, block size, presence of mining, mining intervals, etc., by configuring input-output interfaces for test cases. In order to alleviate issues of insufficient or biased sample test data, there is a need for balanced composition of sample test data.

4.1.3 Types of Blockchain Testing

To comprehensively assess blockchain network services, diverse types of testing are essential, as outlined below:

- Unit (Functional) Testing: Tests basic functionalities, system configuration, and settings.
- Integration Testing: Tests interactions, consistency, and coherence among different components.
- Security Testing: Validates security protocols and detects bugs in blockchain applications.
- Performance Testing: Evaluates processing speed and throughput of blockchain applications.
- Node Testing: Validates consensus protocols and proper execution of transaction storage.
- Smart Contract Testing: Tests the execution of automatically run transactions.
- API Testing: Confirms interactions between the blockchain and external applications.

4.1.4 Evaluation Elements of Blockchain Testing

- Block Size: Tests operations exceeding the maximum block size of 1MB.
- Chain Size: There's no limit to chain size, and testing focuses on performance and functionality.
- Smart Contract Testing: Tests software modules in the blockchain with specific conditions and business logic.
- Security: Essential for blockchain applications, security assurance entails testing transaction safety and susceptibility to malicious attacks.
- Load: A key parameter of blockchain applications, load testing assesses maximum throughput to evaluate performance.
- Data Transmission: Given global data transmission in blockchains, testing ensuring data integrity is necessary.
- Block Addition: Tests the process of adding new blocks to the chain, verifying smooth block addition and flow.

- Encrypted Data: Tests encryption and decryption processes to verify data security.

4.2 Characteristics of Blockchain and Cryptocurrency Test Cases

Testing of cryptocurrency applications must consider various testing aspects. First, from a successful scenario testing perspective, it evaluates the successful operation of blockchain components, encompassing mining tests, transaction tests, halving period, and total issuance tests. Moving on, from a failure scenario testing viewpoint, deliberate failure situations are simulated to verify blockchain forks and exception handling. Additionally, in terms of performance and quality testing, performance metrics such as transaction processing speed, blockchain confirmation time, and network load handling can be measured.

4.2.1 Test Case for Success Testing

Attempt test cases and examples that must succeed for the proper functioning of the blockchain. Successful completion of these tests is considered successful mining, whereas failure indicates unsuccessful mining. For instance, in mining tests, evaluate if blocks are being generated as per the specified numerical values. Is the average block creation time (e.g., 10 minutes for Bitcoin) functioning correctly? Does the average block creation time exhibit an exponential distribution as shown in Figure 21? Are blocks being generated with values lower than the defined Bits value? Does the mining difficulty change appropriately after a defined number of blocks and do blocks get generated accordingly?

Furthermore, test cases for blockchain transactions include the following: Transaction testing – Do transactions created in a legitimate manner process correctly? Create transactions with randomized internal values (amounts, fees, etc.). Do nodes correctly recognize legitimately created transactions as valid transactions? Are valid transactions properly registered in the mempool? Are transactions in the mempool successfully registered in the blockchain?

Additional success test cases include halving period and total issuance testing – Are the halving period and total issuance functioning correctly? After the set halving period, does the mining output decrease as expected and eventually converge to zero? Does continuous mining result in issuance equal to the total issuance?

4.2.2 Test Case for Failure Testing

Introduce deliberate failures within the blockchain and test if failures are handled properly. Examples include:

First, test block branching and merging to evaluate the network's ability to recover from branches in a distributed network. This is relevant to evaluating consensus algorithm performance and stability. Simulate a temporary blockchain fork by simultaneously generating blocks from different nodes. Does the blockchain converge to the longest chain without continuous branching? (Criteria: within 6 blocks after the fork) If it succeeds, the test is considered successful; if not, it fails.

Second, exception handling I/O testing covers handling of exceptions that should be processed. Test ranges like transfer amounts (above 0 and within the current balance), fee imposition range, etc. If it succeeds, the test is considered successful; otherwise, it fails.

Third, forged block and transaction handling tests involve generating a set of intentionally forged blocks and transactions in a specific node and broadcasting them to the blockchain network. Check if other nodes successfully detect these forged blocks and transactions. Verify if other nodes recognize and if countermeasures against malicious nodes operate properly. If it succeeds, the test is considered successful; if not, it fails.

4.2.3 Test Case for Performance and Quality Testing

Instead of using a simple True/False approach to assess blockchain performance and quality, numerical indicators are used to represent performance and quality metrics for different areas. Examples of tests for blockchain network quality and performance include:

First, measure transaction processing speed, where average transaction processing speed, block creation time, and other metrics are evaluated comprehensively. Transaction per Second (TPS) is used to denote the number of transactions processed per second by the blockchain network. Block creation time measures the average time to create a new block and affects the average transaction waiting time. Blockchain confirmation time measures the time taken for a transaction included in a block to be included in the long-term consensus chain. These metrics can be graphically represented by measuring the number of blocks created in the blockchain network per unit transaction until processing.

Second, distributed network load testing generates many transactions and blocks to test the maximum transaction processing rate. This tests if blockchain integrity is maintained under network load. Availability and service stability during high-load situations for normal service users are also tested. Recovery tests evaluate how effectively and quickly unexpected errors, such as block and transaction losses from load testing, can be restored.

5. Conclusion and Future Works

The purpose of this study was to comprehensively analyze the safety issues of blockchain networks and cryptocurrencies from various perspectives, and to propose effective countermeasures and testing methods. Blockchain technology is designed to prevent manipulation of digital documents and information, ensuring the security and systematic management of transaction data. It plays a crucial role in addressing issues of trust and data protection.

This study analyzed the security threats of blockchain networks and cryptocurrencies, as well as the stability components of blockchain network. Additionally, it proposed effective testing models and test cases to address these security and safety issues. Particularly, through methods like constrained self-testing, test user interfaces, and various types of blockchain testing, it presented a way to evaluate and optimize the safety of blockchain and cryptocurrencies. The use of these testing models and test cases is expected to assist in the proactive evaluation and enhancement of the safety of blockchain and cryptocurrencies.

As a result of this study, by presenting a systematic approach to recognizing and addressing safety issues in blockchain networks and cryptocurrencies, it is expected to contribute to preparing for security threats that may arise in the modern finance and technology sectors. Furthermore, it emphasizes the importance of safety testing for the advancement of blockchain and cryptocurrencies, aiming to contribute to the establishment of a secure and reliable blockchain ecosystem.

References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Oct. 2008, Accessed 2023. https://bitcoin.org/bitcoin.pdf

[2] D. H. Shin, "Report on the Future of Blockchain based on the 2018 Technology Impact Assessment Results," Ministry of Science, ICT, and Future Planning · Korea Institute of Science and Technology Evaluation and Planning (KISTEP).

[3] K. S. Min, "Domestic and International Trends and Status of Blockchain Technology," BioINpro, Vol.49, 2018.

[4] True Tamplin, “Components of Blockchain Network,” Aug. 2023, Accessed 2023. https://www.financestrategists.com/

[5] R. Lenz, “Managing Distributed Ledgers: Blockchain and Beyond,” Mar. 2019. Available at SSRN: https://ssrn.com/abstract=3360655, DOI: http://dx.doi.org/10.2139/ssrn.3360655

[6] E. Lee, J. Moon, C. Han, Il-Gu Lee, "Analysis of Trends in Blockchain Network Security Threat Detection Technologies," Korea Institute of Information Security and Cryptology, Review of KIISC, Vol. 31, Issue 3, pp. 61-71, 2021.

[7] Hashnet, "51% Attack," Available at http://wiki.hash.kr/

[8] Infosec, "Security Threats Possible in Blockchain," EQST insight, Nov. 2019. Available at https://m.blog.naver.com/skinfosec2000/.

[9] J. Y. Lee, "Hacking Damage to Users of Cryptocurrency Wallet KaiKas... Police Launch Investigation," Nov. 12, 2021, Asia Economy. Available at https://www.asiae.co.kr/

[10] J. H. Song, "Are Bitcoin Exchanges Safe from Hackers and Thieves?" Jul. 2017 issue, Monthly SW Centered Society, Software Policy & Research Institute.

[11] J. H. Park, "Axi Infinity Sidechain Hack, Over $600 Million in Damages," Block Media, Mar. 30, 2022.

[12] K. S. Min, G. Y. Kim, J. S. Park, J. H. Baek, H. Kwon, J. D. Jang, "Prospects and Analysis of Cyber Security Threats in Metaverse and NFT," KISA Insight Vol.04, 2022.