

Design of metaverse-supported blockchain test process

Taegyu Lee *

* Associate Professor, Department of Smart Contents, Division of ICT Convergence, Pyeongtaek University, 3825 Sedong-daero Pyeongtaek-si, Gyeonggi, 17869, Korea

tglee@ptu.ac.kr

Abstract— This paper proposes an effective testing method that combines blockchain and metaverse technologies. It analyzes the interaction between blockchain networks and virtual reality worlds, leading to the development of a secure and efficient testing process. The paper evaluates this interaction in various scenarios, offering insights to enhance both reliability and security. By integrating metaverse and blockchain technologies, this study makes a significant contribution to improving safety in the digital environment. Additionally, it proposes key evaluation factors and formulas to objectively assess the integration of blockchain and metaverse services. These evaluation metrics can be valuable in developing assessment tools and simulation instruments.

Keyword—Blockchain, Metaverse, Virtual Reality, Cryptocurrency, Testing Methodologies, Security Evaluation, Integration Assessment, Digital Environment Safety

I. INTRODUCTION

DESPITE ongoing economic and social concerns associated with cryptocurrencies and exchanges, the role of cryptocurrencies as a key component of the digital economy and as an alternative currency continues to expand steadily [1][2]. Following the advent of Blockchain 2.0, emerging technologies such as smart contracts, NFTs, and metaverse platforms have significantly extended their reach, creating new markets and enhancing both utility and stability [3][4]. However, challenges remain in ensuring mutual trust among stakeholders—developers, operators, and users—within the cryptocurrency and exchange ecosystems, while the fundamental security and reliability of virtual trading systems are increasingly under threat [5][6][7].

The convergence of metaverse and blockchain technologies is currently opening new possibilities in the digital domain [8]. The metaverse, realized through virtual reality, combined with blockchain's security, transparency, and reliability, offers both opportunities and challenges, particularly in terms of testing and ensuring the reliability of system operations within such dynamic ecosystems.

A robust testing process tailored specifically to metaverse-supported blockchain applications is therefore

essential. Conventional testing methodologies often fall short in addressing the complexities that arise from the immersive and interconnected virtual environments of the metaverse. New approaches are needed to ensure the uninterrupted functionality and security of blockchain networks within these environments.

This paper proposes a comprehensive framework for designing a testing process tailored to metaverse-supported blockchain applications. Our research aims to establish a framework that facilitates thorough testing of blockchain-based metaverse applications, taking into account the unique features and challenges of this convergence. Through a systematic investigation into metaverse interactions, blockchain integration, and security considerations, we contribute to the development of a reliable testing methodology. Our goal is to support the continued growth and integration of both metaverse and blockchain technologies.

This paper is organized as follows: Chapter 2 presents the research background and related studies. Chapter 3 proposes a testing process for the interaction and convergence of the metaverse and blockchain. In Chapter 4, we analyze key issues related to the proposed testing process. Finally, Chapter 5 offers conclusions and outlines directions for future research.

II. RESEARCH BACKGROUND AND RELATED STUDIES

A. Research Background

In recent years, metaverse and blockchain technologies have experienced rapid growth, establishing themselves as key components of the digital economy and virtual worlds [9][18]. The metaverse serves as a platform for creating virtual reality environments, allowing users to interact and communicate within these digital spaces. Concurrently, blockchain technology, as a distributed ledger, facilitates secure and transparent transactions while eliminating the need for centralized control.

The convergence of metaverse and blockchain technologies fosters the creation of more innovative digital experiences. This fusion, which includes features such as smart contracts, NFTs (Non-Fungible Tokens), and digital asset ownership management, gives rise to new application models and business opportunities [10]. This integration plays a significant role in blurring the lines between the digital economy and virtual worlds.

However, while the fusion of the metaverse and blockchain introduces new opportunities, it also presents

Manuscript received August 00, 2024. This paper was supported by the Research Fund, 2023, Pyeongtaek University in Korea.

T. L. Author is with the Division of ICT Convergence, Pyeongtaek University, Pyeongtaek, Gyeonggi 17869 Korea (corresponding author to provide phone: +82-31-659-8370; fax: +82-31-659-8011; e-mail: tglee@ptu.ac.kr).

challenges in terms of testing and security. Effective testing methods are crucial to ensuring the reliability and security of these combined environments. Current testing methodologies often fail to fully account for the unique characteristics of the metaverse and blockchain, potentially leading to reliability and security issues.

B. Related Studies

Previous studies in this field have primarily focused on the security and safety of blockchain and cryptocurrencies. While research on the combination of the metaverse and blockchain is increasing, there remains a lack of emphasis on the testing process [5][11][12]. These studies highlight the need for developing effective testing tools and methodologies within the context of metaverse and blockchain environments [13][14].

The primary objective of this research is to develop and propose an effective testing process for the convergence of metaverse and blockchain technologies, ensuring the stability, reliability, and security of metaverse-supported blockchain applications.

The integration of metaverse and blockchain technologies is driving innovative changes in the modern digital economy, enabling the creation of new business models and value generation opportunities. Although this convergence holds the potential to radically transform the digital economy and virtual environments, the successful implementation of an effective testing process is crucial. By ensuring the stability and security of both blockchain and the metaverse, trust in the provided services can be maintained, opening new opportunities in fields such as finance, gaming, art, and more.

Existing research indicates a significant gap in the development of new methodologies and testing processes for the convergence of metaverse and blockchain technologies [12][15][16]. The lack of effective testing methods that account for the immersive and interconnected virtual environments of the metaverse, along with the distributed nature of blockchain, can lead to potential security and stability issues. Therefore, this study aims to propose a new testing process that addresses the unique characteristics of both the metaverse and blockchain.

To this end, we aim to design and propose an effective testing process for the metaverse and blockchain convergence environment. Figure 1 illustrates the design model for testing the integration of these technologies, with the goal of concretizing the testing and authentication procedures while enhancing practicality [17].

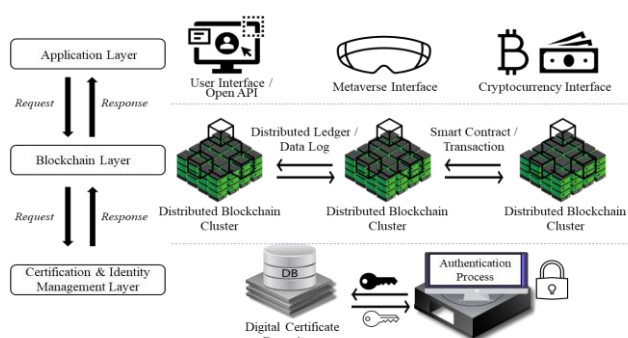


Fig. 1. Metaverse and Blockchain Convergence Testing Operating Environment [23]

For conducting integration tests between metaverse and blockchain technologies, a hierarchical structure of converged application services can be organized into three layers.

First, the top-tier **Application Layer** includes applications and smart contracts operating within the metaverse environment. This layer manages user interfaces, virtual environments, and services. Examples include smart contract-based parking management systems within metaverse virtual cities and digital asset trading platforms.

Second, the **Blockchain Layer** is based on blockchain technology and contains the distributed ledger and smart contract platform. It is responsible for transaction processing and data recording within the blockchain. This layer includes nodes of the blockchain network and the smart contract execution environment. Examples of applications in this layer include blockchain platforms like Ethereum, Cardano, and Solana.

Third, the **Certification & Identity Management Layer** is a critical component of the certified structure, responsible for identity verification and digital certificate management. It handles user identities and provides the necessary authentication and permissions for smart contracts and applications. This layer includes digital certificate repositories and secure authentication processes. Examples include blockchain-based identity verification services and digital certificate repositories.

Through this layered model, when conducting blockchain integration tests in a distributed metaverse environment, smart contracts and applications operating within the metaverse environment are implemented in the **Application Layer**. Transaction processing and data storage occur in the **Blockchain Layer**, and user identities are managed and protected in the **Certification & Identity Management Layer**. This layered structure facilitates effective testing and security verification.

Moreover, the **Metaverse and Blockchain Integration Testing Process Model** is employed to identify key components and issues at each phase of testing and to establish the input and output elements. This research aims to provide solutions for testing challenges related to the stable expansion of smart contract services within the integrated metaverse and blockchain networks.

III. METAVERSE AND BLOCKCHAIN INTEGRATION TESTING PROCESS

In this chapter, we explore the interaction between the metaverse and blockchain and propose an integrated testing process to effectively evaluate this interaction.

Figure 2 illustrates a step-by-step process related to NFTs (Non-Fungible Tokens) within the integrated environment of the metaverse and blockchain. Below is an explanation of each step:

Application Development:

The first step involves the development of the application. In this stage, an application is created that will be used within the metaverse and blockchain environment. This application enables users to create and manage NFTs

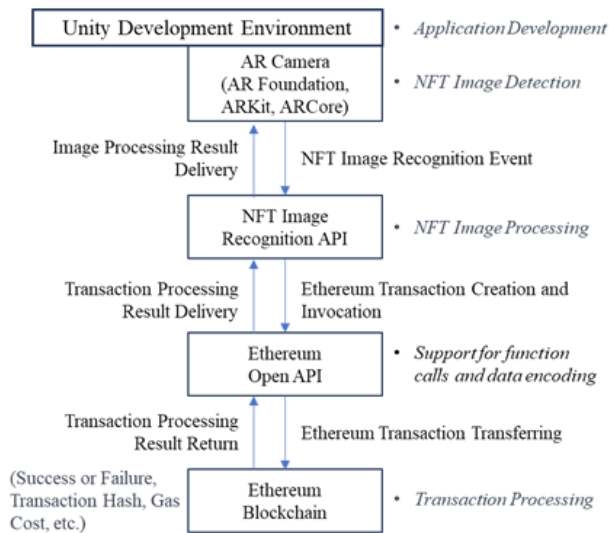


Fig. 2. Metaverse and Blockchain Convergence Development Environment and Routines [23]

NFT Image Detection:

The next step is NFT image detection. In this stage, the developed application detects images that users upload or create, preparing them for conversion into NFTs. This step involves reviewing the images and generating appropriate metadata to verify their suitability as NFTs.

NFT Image Processing:

Once the image detection is complete, the process moves to the NFT image processing stage. This step involves processing the detected images to generate NFTs. Tasks in this stage include creating a hash of the image and preparing the data that will be recorded on the blockchain.

Transaction Processing:

After NFT image processing is completed, the transaction processing step begins, where the information is recorded on the blockchain. This stage involves creating a transaction to record the NFT on the blockchain and submitting this transaction to the blockchain network.

Result Feedback:

The final step is the result output. Once the transaction is recorded on the blockchain, the outcome, including success or failure, transaction hash, gas cost, etc., is returned to the user. This result confirms the completion of the NFT creation process.

This process represents the overall flow of creating and managing NFTs within a combined environment of the metaverse and blockchain. Each step includes a series of tasks aimed at securely recording and managing NFTs on the blockchain.

A. Interaction between the Metaverse and Blockchain

The metaverse and blockchain are each built upon unique technologies and concepts, making it essential to understand how these two technologies interact. This section describes how blockchain technology is utilized within the metaverse and how the presence of blockchain influences the metaverse environment.

NFT and Digital Asset Management:

Within the metaverse, users can own and trade digital assets using Non-Fungible Tokens (NFTs). These NFTs are based on blockchain technology, which securely records ownership rights for each asset on the blockchain. This allows metaverse users to own unique digital assets, trade with other users, and securely document ownership on the blockchain.

Execution of Smart Contracts:

Smart contracts play a crucial role in the metaverse environment. Blockchain smart contracts facilitate automated transactions and interactions within the metaverse, securely executing these operations by leveraging the immutability and security of the blockchain. For example, in metaverse games, smart contracts can be used for item transactions and enforcing game rules.

Security and Trustworthiness:

Blockchain ensures the security and trustworthiness of transactions. Activities such as transactions and economic interactions within the metaverse are recorded on the blockchain, ensuring transparency and immutability. This increases user trust and prevents fraud or malicious activities.

Digital Identity and Ownership Management:

Blockchain simplifies and secures the management of digital identity and ownership. In the metaverse, user digital identities and asset ownership are stored on the blockchain, allowing for verification and sharing as needed.

Distributed Economic Ecosystem:

The metaverse forms a distributed economic ecosystem through blockchain. Users can own and manage assets via blockchain and participate in various economic activities within the metaverse, enabling direct economic interactions without centralized intermediaries.

In this way, the metaverse and blockchain complement each other, creating innovative opportunities within the digital economy and virtual worlds.

B. Proposed Testing Process

This section outlines the proposed testing process, which considers the intricate interactions between metaverse and blockchain technologies. The process provides a step-by-step approach to effectively test metaverse-supported blockchain applications, accommodating a variety of testing scenarios and interactions. Designed to address the complex interplay between the metaverse and blockchain, this testing process offers a systematic framework for ensuring the reliability and security of metaverse-supported blockchain applications.

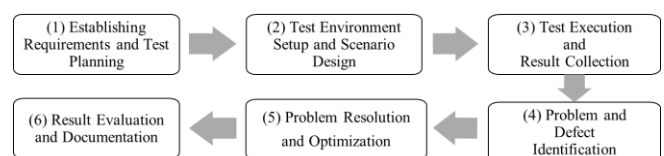


Fig. 3. Convergence Testing Process [23]

Figure 3 illustrates the step-by-step approach of this testing process, demonstrating how it can be effectively utilized.

1) Requirement Definition and Test Planning

The initial phase of the testing process involves defining

the requirements for the metaverse and blockchain application and establishing clear test objectives. Based on an understanding of the interaction between the metaverse and blockchain, various test scenarios are developed, and a comprehensive plan is formulated.

- a) **Definition of Test Objectives:** First, the test objectives for the metaverse-supported blockchain application are clearly defined, specifying the aspects to be tested and validated.
- b) **Determination of Test Scope:** The test scope is determined, indicating the specific aspects to be tested. This step focuses on the interaction between the metaverse and blockchain, specifying which parts will be emphasized.
- c) **Establishment of Test Environment:** A test environment is set up to conduct the tests, including the integration of the metaverse and blockchain, and the configuration of necessary hardware and software.
- d) **Allocation of Test Resources:** Resources, including the testing team, testers, developers, and others, are allocated for the testing process, with their roles clearly defined.
- e) **Writing Test Plans:** Test plans are documented, covering test schedules, task allocation, test case design and execution plans, risk management plans, and other relevant details.
- f) **Designing Test Cases:** Test cases are designed based on the defined test objectives and scope. Each test case specifies the behavior to be verified in each scenario.
- g) **Generating Test Data:** Necessary test data is generated or imported to simulate various real-world scenarios that may occur during the testing.
- h) **Preparing the Test Environment:** The test environment is configured, and the test data is loaded. The metaverse and blockchain networks are initialized, and required settings are applied.
- i) **Review and Approval of Test Plans:** The written test plans are reviewed and approved by the testing team and stakeholders to ensure the efficiency and accuracy of the tests.
- j) **Verification of the Test Environment:** The configured test environment is verified to ensure correct operation. Any issues identified are addressed and corrected as needed.
- k) **Validation of Test Data:** The test data is verified to ensure it has been appropriately generated, with any necessary additions or modifications made.
- l) **Establishment of Test Execution Plan:** The schedule and process for conducting the tests are planned and executed.

These steps allow for the clear definition of requirements for metaverse-supported blockchain applications and the establishment of efficient test plans. This systematic approach enables comprehensive testing of the interaction between the metaverse and blockchain, as well as the identification and resolution of any issues.

2) Test Environment Setup and Scenario Design

In this phase, the test environment for metaverse and blockchain integration is set up, and various test scenarios are designed. This environment includes the integration of the metaverse environment with the blockchain network. Additionally, it involves the development of various test cases and scenarios that consider user interactions within the metaverse and blockchain transaction processing. The key activities carried out in this phase include:

- a) **Test Environment Setup:** Construct and configure the testing environment, which involves integrating the metaverse and blockchain, as well as setting up the necessary hardware and software components. Ensure that the environment aligns with the testing objectives.
- b) **Definition of Test Scenarios:** Define various test scenarios that represent specific situations or use cases. Each scenario is

designed to test the interaction between the metaverse and blockchain.

- c) **Preparation of Test Data:** Prepare the necessary test data required for the defined test scenarios. This data simulates specific states and events in each scenario.
- d) **Design of Test Cases:** Design test cases based on the defined test scenarios. Each test case specifies in detail the behavior to be verified.
- e) **Validation of Test Environment:** Verify that the configured test environment functions as expected. Address and rectify any issues that arise. Also, load and prepare the test data.
- f) **Establishment of Test Execution Plan:** Plan and execute the testing by defining the order and priority of executing the test scenarios.
- g) **Interaction Testing:** Execute tests that verify the interaction between the metaverse and blockchain. Conduct various tests according to the scenarios and record the results.
- h) **Issue Identification and Recording:** Identify and record any problems or errors that occur during testing, including analyzing logs and error reports.
- i) **Analysis of Test Results:** Analyze the results of the executed tests to identify issues or performance concerns that have arisen from the interaction between the metaverse and blockchain.
- j) **Report Writing:** Summarize the test results and create a report. This report may include proposed solutions for addressing issues and recommendations for improvements.

Through the setup of the test environment and the design of scenarios, various situations are simulated to test the metaverse-supported blockchain application. This allows for the identification of problems and areas for improvement across different contexts.

3) Test Execution and Result Collection

In this phase, tests are executed within the previously established environment, and results are collected. This stage involves simulating actions such as transactions within the metaverse, smart contract execution, NFT issuance, and trading. The success or failure of the executed test cases is recorded, and performance-related data is collected. The key activities in this phase include:

Test Execution: Execute tests according to the predefined test scenarios. Simulate the interaction between the metaverse and blockchain and perform the test cases as planned.

- a) **Monitoring of Executed Tests:** Monitor the test environment and scenarios in real-time while tests are being conducted. Continuously check the system's operational status and identify any issues immediately.
- b) **Result Collection:** After each test scenario is completed, collect the corresponding results. Document the events and state changes that occurred during the execution of the test cases.
- c) **Performance Measurement:** Measure the system's performance during testing. Monitor metrics such as latency, response time, throughput, and other relevant performance indicators to detect any performance issues.
- d) **Recording of Errors and Issues:** It is essential to document errors and issues in detail. Record the types of errors, timestamps, and the scope of impact for each issue encountered.
- e) **Log Analysis:** Analyze the log files generated during test execution to extract information related to system behavior. This analysis can help identify the root causes of problems.
- f) **Evaluation of Test Results:** Evaluate the collected results against the test objectives. Verify whether the test cases passed successfully and identify any issues that need to be addressed.
- g) **Result Documentation:** Document the test results in a report. The report should include records of the success and failure of test executions, identified problems, and proposed solutions.

*h) **Test Completion and Cleanup:** After all tests are completed, clean up the test environment and release any test resources.*

These steps ensure that the metaverse and blockchain integration application is effectively tested, and results are collected to address and improve identified issues. Examples of testing types that can be applied to metaverse-integrated blockchain testing include API Testing, Block Testing, Functional Testing, Performance Testing, Security Testing, Integration Testing, and Smart Contract Testing.

4) Identifying Issues and Defects

This phase involves identifying and analyzing issues and defects that arise during test execution. In this stage, all errors and unexpected situations related to metaverse and blockchain interactions are recorded, and the root causes of these issues are determined. Security and safety vulnerabilities are also identified and addressed. The key activities in this phase include:

- a) **Error Identification:** Identify errors that occurred during test execution. These errors represent behaviors or exceptional situations that deviate from the system's expected behavior.*
- b) **Defect Classification:** Categorize the identified errors and defects by type. For example, classify defects as functional defects, performance issues, security vulnerabilities, etc.*
- c) **Severity Assessment:** Evaluate the severity of each issue or defect. Severe defects may impact critical system functionalities, while minor defects may have a less significant impact.*
- d) **Root Cause Analysis:** Analyze the causes of discovered issues and defects. Investigate why the issues occurred and determine their underlying causes.*
- e) **Issue Reporting:** Document the issues and defects in a report. This report should include descriptions of the issues, their severity, root causes, reproduction steps, and proposed fixes or improvements.*
- f) **Priority Assignment:** Prioritize the discovered issues. Determine which defects should be addressed first, assigning higher priority to severe defects and lower priority to less critical ones.*
- g) **Issue Tracking:** Track and manage the identified issues and defects. Continue tracking them until they are resolved, and update the status of each issue.*
- h) **Test Re-execution:** After fixing the identified defects, re-run the corresponding test cases to confirm whether the issues have been resolved.*

Through these processes, issues and defects in metaverse-integrated blockchain applications can be effectively identified, and appropriate corrective actions can be taken to address them.

5) Issue Resolution and Optimization

In this phase, identified issues and defects are addressed, and the system is optimized. This includes fixing errors and implementing measures to enhance stability and reliability. It may also involve modifications and security enhancements to the blockchain smart contract code. The key activities in this phase include:

- a) **Issue Resolution:** Implement corrective or improvement actions for identified issues and defects. Developers or system administrators work to address the root causes of problems and re-test the system.*
- b) **Re-Testing:** Re-test the modified system or application to confirm that the changes have resolved the issues and to assess their impact on system behavior.*
- c) **Performance Optimization:** If performance issues were identified, optimize the system to improve its performance. This*

may involve reducing latency, enhancing response times, and increasing scalability.

- d) **Security Strengthening:** If security vulnerabilities were found, reinforce security measures to make the system more secure. This may include improvements in encryption, authentication, access control, and other security features.*
- e) **System Testing:** Re-test the modified and optimized system to ensure that previously identified problems have been resolved and that no new issues or defects have emerged.*
- f) **Performance Evaluation:** Assess the performance of the optimized system and confirm that performance improvements are functioning as expected.*
- g) **Issue Tracking and Management:** Track and manage the resolved issues and defects to prevent their recurrence. This ongoing management helps to continuously improve quality.*
- h) **Issue Report Updates:** Update the issue and defect reports to reflect the current status. Document the outcomes of issue resolution and optimization efforts.*

Through these activities, metaverse-integrated blockchain applications can be maintained in a stable and optimized state, with issues continually addressed and improvements made over time.

6) Evaluation and Documentation of Results

In this final phase, the results of the test process are evaluated and documented. The goal is to summarize the outcomes of the testing process, confirm the reliability and safety of the metaverse and blockchain application, and document the scenarios and procedures for future quality management and reporting. The key activities in this phase include:

- a) **Result Evaluation:** Assess whether all issues and defects identified during testing have been successfully resolved. Ensure that previously identified problems have been properly addressed.*
- b) **Performance Measurement:** Measure and evaluate the outcomes and performance improvements achieved through the testing process. This confirms the success and effectiveness of the testing.*
- c) **Result Report Writing:** Prepare a detailed report that documents the testing objectives, executed test cases, identified issues and defects, resolution methods, optimization outcomes, performance measurements, and other relevant details.*
- d) **Result Sharing:** Share the prepared report with stakeholders or teams involved in the testing. Communicate the testing outcomes and problem resolution details, and gather feedback and opinions.*
- e) **Documentation and Archiving:** Store the result report in project records and archives. This ensures that information related to the results can be retrieved or verified in the future as needed.*
- f) **Quality Assurance and Improvement:** Assess the overall system quality based on the testing results and develop improvement strategies. Establish measures to prevent similar issues in future project phases.*
- g) **Process Improvement:** Evaluate the executed testing process and identify areas for improvement. Work on enhancing the process to conduct testing more efficiently in future projects.*

Through these evaluation and documentation activities, the testing outcomes and conclusions for metaverse-integrated blockchain applications are clearly summarized. These activities provide valuable information for future improvement and maintenance tasks. This proposed testing process serves as an essential tool for effective testing, considering the interaction between the metaverse and blockchain, and supports the development and operation of metaverse-supported blockchain applications.

IV. ANALYSIS OF KEY ISSUES IN THE PROPOSED TESTING PROCESS

In this chapter, we analyze the strengths and limitations of the proposed testing process, with the goal of deepening our understanding of the interaction between the metaverse and blockchain. Specifically, this chapter reviews the testing process outlined in Chapter 3 and analyzes key issues as follows. As illustrated in Table 1, the following factors can be considered key evaluation criteria for conducting tests on the integration of blockchain and the metaverse.

TABLE 1. EVALUATION METRICS FOR CONVERGENCE TEST PROCESS

Metric for Element	Explanation	Unit
Interaction Score	This metric can assign a high score when smooth data and asset transfer between blockchain and metaverse technologies is possible. This evaluation factor takes into consideration smooth data and asset migration, data security and privacy, performance optimization capabilities and scalability, establishment and maintenance costs, as well as the vibrancy of the community and developer ecosystem.	relative scores
NFT_complexity	It is an evaluation metric for assessing the complexity of NFT issuance and transactions. This evaluation metric considers factors such as the expected costs associated with NFT issuance and transactions, NFT security levels, user experience, scalability, and more.	relative scores
Smart Contract Score	It is an evaluation metric for assessing smart contracts within the metaverse. This evaluation metric considers factors such as metaverse integration, smart contract security levels, smart contract functionality, smart contract efficiency, smart contract scalability, and more.	relative scores
Security and Safety Score	It is a function used to evaluate security and safety in the metaverse and blockchain integration testing. This evaluation metric considers factors such as the security level of the metaverse, the security level of the blockchain, data privacy protection, compliance with regulations, and more.	relative scores
Improvement Score	It is a function used to evaluate the improvement and optimization of the testing process. This evaluation metric considers factors such as the testing duration, resource utilization, test coverage, error handling, and more.	relative scores

A. Issues Related to the Interaction Between the Metaverse and Blockchain

The interaction between the metaverse and blockchain presents various complexities and challenges [22]. This section analyzes the key issues that can arise from the interaction between these two technologies. For example, challenges in reconciling blockchain transaction processing with real-time interactions within the metaverse and concerns related to security and personal data protection are addressed.

To analyze the interaction between the metaverse and

blockchain, we define an evaluation function based on various weighted factors, including interoperability weight (W_{inter}), security level weight (W_{sec}), performance and processing speed weight (W_{perf}), cost efficiency weight (W_{eff}), and community and developer support weight (W_{supp}).

$$\text{Interaction Score} = W_{inter} * \text{Interoperability} + W_{sec} * \text{Security Level} + W_{perf} * \text{Performance} + W_{eff} * \text{Cost Efficiency} + W_{supp} * \text{Community and Developer Support} \quad (1)$$

Using this evaluation formula (1), we can assess the interaction between the metaverse and blockchain from various perspectives, with each weight adjusting the importance of its respective aspect.

To calculate the interaction evaluation score (**Interaction Score**) for the metaverse convergence application service, the following steps are taken: Firstly, assign weights to key components: $W_{inter} = 0.2$, $W_{sec} = 0.2$, $W_{perf} = 0.2$, $W_{eff} = 0.2$, $W_{supp} = 0.2$. Secondly, consider actual measurement values: *Interoperability* = 8.0, *Security Level* = 9.0, *Performance* = 7.0, *Cost Efficiency* = 3.0, *Community and Developer Support* = 8.0. Thirdly, multiply each component's measurement value by its weight, then sum the results. Finally, calculate the weighted average to obtain the interaction service evaluation score. The calculated score is 0.78, representing the interaction of the metaverse convergence application service. Each weight represents the relative importance of the factors in various projects or situations.

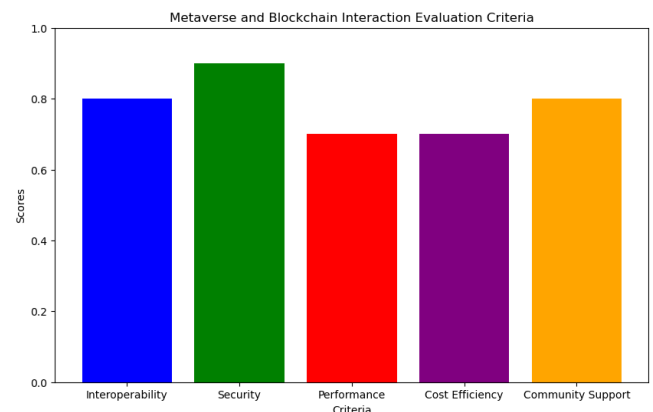


Fig. 4. Interaction Service Evaluation Result on Metaverse and Blockchain Convergence Applications

Figure 4 illustrates the relative evaluation results, normalized to a range from 0 to 1, considering the weighting variables for each element. This indicates that performance and cost efficiency are relatively more vulnerable compared to interoperability, security, and community support.

B. Smart Contract Issues Within the Metaverse

The execution of smart contracts within the metaverse environment can present complex challenges. Errors or vulnerabilities in smart contracts can significantly impact interactions within the metaverse and the integration with blockchain. Key variables related to smart contracts, such as metaverse integration weight (W_{inte}), smart contract security weight (W_{sec}), smart contract functionality weight (W_{func}), smart contract efficiency weight (W_{eff}), and smart contract scalability weight (W_{scal}), should be considered when

evaluating smart contracts in the metaverse. The evaluation function for analyzing smart contracts within the metaverse, accounting for these weight variables, is as follows:

$$\text{Smart Contract Score} = W_{\text{inte}} * \text{Metaverse Integration} + W_{\text{sec}} * \text{Security} + W_{\text{func}} * \text{Functionality} + W_{\text{eff}} * \text{Efficiency} + W_{\text{scal}} * \text{Scalability} \quad (2)$$

This formula (2) allows for the evaluation of various aspects of smart contracts, with each weight representing the relative importance of the respective aspect. By adjusting these weights, evaluations can be tailored to meet the specific requirements of a project.

To calculate the smart contract evaluation score (**Smart Contract Score**) for the metaverse convergence smart contract application service, the following steps are taken: Firstly, assign weights to key components: $W_{\text{inte}} = 0.2$, $W_{\text{sec}} = 0.2$, $W_{\text{func}} = 0.2$, $W_{\text{eff}} = 0.2$, $W_{\text{scal}} = 0.2$. Secondly, consider actual measurement values: *Metaverse Integration* = 8.0, *Security* = 9.0, *Functionality* = 7.0, *Efficiency* = 8.0, *Scalability* = 6.0. Thirdly, multiply each component's measurement value by its weight, then sum the results. Finally, calculate the weighted average to obtain the security and safety evaluation score. The calculated score is 0.76, representing the smart contract performance of the metaverse convergence application service. Each weight reflects the relative importance of the factors in various projects or situations.

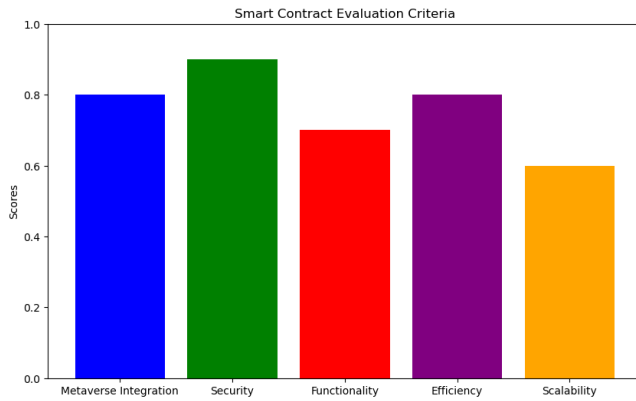


Fig. 5. Smart Contract Evaluation Result on Metaverse and Blockchain Convergence Applications

Figure 5 illustrates the relative evaluation results, normalized to a range from 0 to 1, considering the weighting variables for each element. This indicates that functionality and scalability are relatively more vulnerable compared to metaverse integration, security, and efficiency.

C. The Complexity of NFT Minting and Trading

NFTs (Non-Fungible Tokens) play a crucial role in the integration of the metaverse and blockchain. However, the issuance and trading of NFTs involve various complexities that require effective testing and validation [20]. To assess the complexity of NFT minting and trading, a quantitative evaluation can be conducted, considering factors such as *transaction cost* (W_{tran}), *security level* (W_{sec}), *user experience* (W_{ux}), and *scalability* (W_{scal}).

$$\text{NFT Complexity Score} = W_{\text{tran}} * \text{Transaction Cost} + W_{\text{sec}} *$$

$$\frac{\text{Security Level} + W_{\text{ux}} * \text{User Experience} + W_{\text{scal}} * \text{Scalability}}{\quad} \quad (3)$$

The weight variables adjust the relative importance of each aspect, allowing the complexity of NFT minting and trading to be assessed and compared from various perspectives using this evaluation equation.

To calculate the NFT complexity evaluation score (**NFT Complexity Score**) for the metaverse convergence NFT minting and trading application service, the following steps are taken: Firstly, assign weights to key components: $W_{\text{tran}} = 0.3$, $W_{\text{sec}} = 0.2$, $W_{\text{ux}} = 0.2$, $W_{\text{scal}} = 0.3$. Secondly, consider actual measurement values: *Transaction Cost* = 7.0, *Security Level* = 8.0, *User Experience* = 5.0, *Scalability* = 7.0. Thirdly, multiply each component's measurement value by its weight, then sum the results. Finally, calculate the weighted average to obtain the NFT complexity evaluation score. The calculated score is 0.56, representing the NFT complexity of the metaverse convergence NFT minting and trading application service. Each weight reflects the relative importance of the factors in various projects or situations.

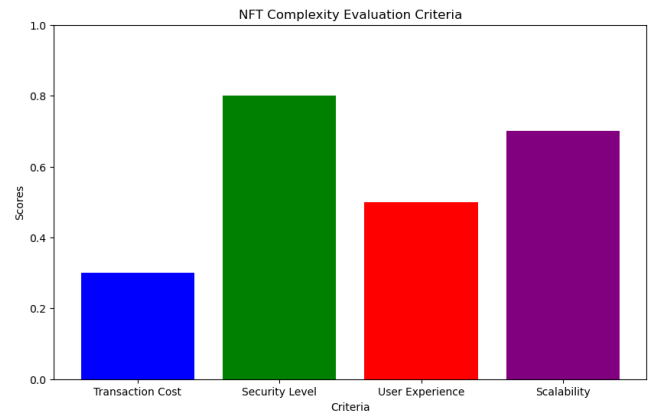


Fig. 6. NFT Complexity Evaluation Result on Metaverse and NFT Convergence Applications

Figure 6 illustrates the relative evaluation results, normalized to a range from 0 to 1, considering the weighting variables for each element. This indicates that transaction cost and user experience are relatively more vulnerable compared to security level and scalability.

D. Security and Safety Issues

The integration of the metaverse and blockchain introduces new challenges regarding security and safety [19]. Key concerns include user data protection, vulnerabilities in smart contracts, the application of encryption technologies, and more [21].

To analyze security and safety in metaverse and blockchain integration testing, key weights such as metaverse security weight (W_{mse}), blockchain security weight (W_{bsec}), data privacy weight (W_{pri}), and compliance weight (W_{com}) can be considered. The security and safety evaluation function can be defined as follows:

$$\text{Security and Safety Score} = W_{\text{mse}} * \text{Metaverse Security} + W_{\text{bsec}} * \text{Blockchain Security} + W_{\text{pri}} * \text{Data Privacy} + W_{\text{com}} * \text{Compliance} \quad (4)$$

To calculate the security and safety evaluation score (**Security and Safety Score**) for the metaverse convergence application service, the following steps are taken: Firstly, assign weights to key components: $W_{msec} = 0.3$, $W_{bsec} = 0.3$, $W_{pri} = 0.2$, $W_{com} = 0.2$. Secondly, consider actual measurement values: *Metaverse security* = 8.5, *Blockchain security* = 9.0, *Data privacy* = 7.5, *Compliance* = 8.8. Thirdly, multiply each component's measurement value by its weight, then sum the results. Finally, calculate the weighted average to obtain the security and safety evaluation score. The calculated score is 0.851, representing the security and safety level of the metaverse convergence application service. Each weight reflects the relative importance of the factors in various projects or situations.

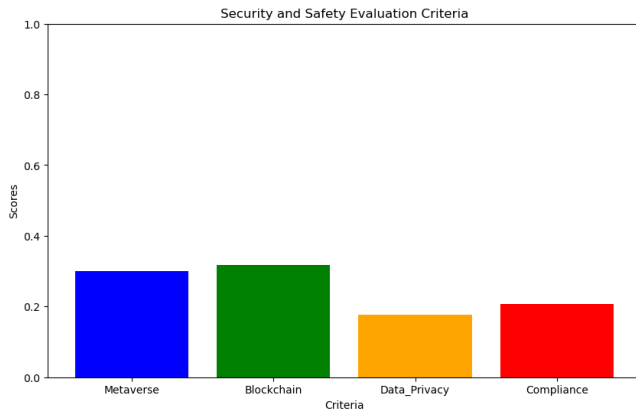


Fig. 7. Security and Safety Evaluation Result on Metaverse and Blockchain Convergence Applications

Figure 7 illustrates the relative evaluation results, normalized to a range from 0 to 1, considering the weighting variables for each element. This indicates that data privacy and compliance are relatively more vulnerable compared to metaverse and blockchain security.

E. Test Process Improvement and Optimization

After analyzing the key issues, research is conducted on how to improve and optimize the test process. This involves considering improvements in error and defect handling, enhancing safety, optimizing performance, and designing efficient test scenarios. The evaluation function for improving and optimizing the convergence test process for blockchain and the metaverse includes factors such as *test duration*, *resource utilization*, *test coverage*, and *error handling*. The function is defined as follows:

$$\text{Test Process Score} = (W_1 * (1 - \text{Test Duration} / 100)) + (W_2 * (\text{Resource Utilization} / 10)) + (W_3 * (\text{Test Coverage} / 100)) + (W_4 * (\text{Error Handling} / 10)) \quad (5)$$

Each weight variable is assigned as follows: W_1 represents the weight for *Test Duration* (0.3), W_2 represents the weight for *Resource Utilization* (0.2), W_3 represents the weight for *Test Coverage* (0.3), and W_4 represents the weight for *Error Handling* (0.2). These weights can be adjusted based on the project's characteristics, goals, and priorities for improving the testing process.

You can assign specific values to W_1 , W_2 , W_3 , and W_4 based on your desired weightage for each metric. Consider actual measurement values: *Test Duration* = 10, *Resource*

Utilization = 80, *Test Coverage* = 95, *Error Handling* = 90. Finally, calculate the weighted average to obtain the test process evaluation score. The calculated score is 0.895, representing the test process performance of the metaverse convergence application service.

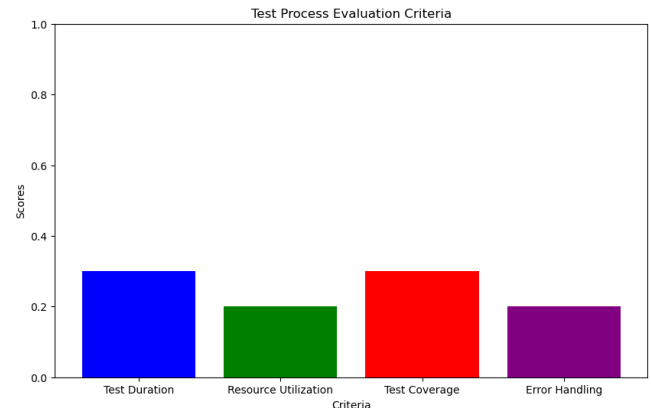


Fig. 8. Test Process Evaluation Result on Metaverse and Blockchain Convergence Applications

Figure 8 illustrates the relative evaluation results, normalized to a range from 0 to 1, considering the weighting variables for each element.

V. CONCLUSION AND FUTURE DIRECTIONS

In conclusion, this paper has presented a comprehensive framework for testing the integration of the metaverse and blockchain. It highlights the importance of a testing process that accounts for the intricate interactions between these technologies and emphasizes the benefits and outcomes it can produce. This research anticipates that the development and application of the proposed testing process will play a pivotal role in ensuring the reliability and security of metaverse and blockchain applications. As the integration of the metaverse with blockchain becomes increasingly prevalent across diverse sectors, including finance, entertainment, and education, the need for a reliable testing methodology is critical.

Chapter 4 introduced various evaluation function models applicable to the metaverse and blockchain integration testing process. These diverse evaluation models enable improved simulations, which can generate accurate predictive data. The development and application of the proposed testing process are expected to significantly contribute to the reliability and security of metaverse and blockchain applications. The interaction between the metaverse and blockchain is being utilized across multiple domains, making a dependable testing methodology essential.

Looking ahead, as metaverse and blockchain technologies continue to evolve, there is a need to develop enhanced testing methodologies and tools that can adapt to these changes. For instance, future research should explore the development of testing methodologies for emerging technologies and protocols beyond Blockchain 3.0. Based on the evaluation factors proposed in this study, it is possible to develop assessment tools and simulation instruments. Furthermore, by analyzing the evaluation results, the objectivity of the assessment method can be validated.

ACKNOWLEDGMENT

This paper was supported by the Research Fund, 2023, Pyeongtaek University in Korea.

REFERENCES

- [1] M. Fauzi and N. Paiman, "Bitcoin and Cryptocurrency: Challenges, Opportunities and Future Works," *Journal of Asian Finance Economics and Business*, Vol.7 695-704, 2020. DOI: <http://doi.org/10.13106/jafeb.2020.vol7.no8.695>.
- [2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Available: <https://git.dhimmel.com/bitcoinwhitepaper/>, 2008.
- [3] Vitalik Buterin, "A Next Generation Smart Contract & Decentralized Application Platform," *Ethereum White Paper*, Vol.3 Issue37, 2-1, 2014.
- [4] Andrea Bonaceto, "Non-Fungible Tokens (NFTs)-The New Paradigm," *Eterna Capital*, Mar. 30, 2021, <https://eternacapital.medium.com/non-fungible-tokens-nfts-the-new-paradigm-6da78a85e73f>
- [5] J. Leng, M. Zhou, L.J. Zhao, Y. Huang and Y. Bian, "Blockchain Security: A Survey of Techniques and Research Directions," *IEEE Transactions on Services Computing*, 2020. DOI: <http://doi.org/10.1109/TSC.2020.3038641>
- [6] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Krol, E. W. Felten, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," 2015 IEEE Symposium on Security and Privacy, 104-121, 2015, DOI: <http://doi.org/10.1109/SP.2015.14>
- [7] Z. Chen, J. Wu, W. Gan and Z. Qi, "Metaverse Security and Privacy: An Overview," *IEEE BigData*, Nov. 2022, DOI: <https://doi.org/10.48550/arXiv.2211.14948>
- [8] Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang and Z. Zheng, "Fusing Blockchain and AI With Metaverse: A Survey," *IEEE Open Journal of the Computer Society*, Vol.3, 122-136, 2022, DOI: <http://doi.org/10.1109/OJCS.2022.3188249>
- [9] Reddspark out, "What is metaverse in blockchain? A beginner's guide on an internet-enabled virtual world," *Cointelegraph* 2022, Available: <https://cointelegraph.com/learn/what-is-metaverse-in-blockchain>
- [10] G. Weston, "The Role of NFTs in the Metaverse," *101blockchains*, Dec. 24, 2021, Available: <https://101blockchains.com/nfts-and-metaverse/>
- [11] T.T. Huynh, T.D. Nguyen, and H. Tan, "A Survey on Security and Privacy Issues of Blockchain Technology," 2019 International Conference on System Science and Engineering (ICSSE), 362-367, 2019, DOI: <https://doi.org/10.1109/ICSSE.2019.8823094>
- [12] C. Lal and D. Marijan, "Blockchain Testing: Challenges, Techniques, and Research Directions," *Mar. 2021*, DOI: <https://doi.org/10.48550/arXiv.2103.10074>
- [13] T. H. The, T. R. Gadekallu, W. Wang, G. Yenduri, P. Ranaweera, Q.V. Pham, D.B. Costa and M. Liyanage, "Blockchain for the metaverse: A Review," *Future Generation Computer Systems*, Vol.143, 2023, 401-419, DOI: <https://doi.org/10.1016/j.future.2023.02.008>.
- [14] Z. Zheng, S. Xie, H.N. Dai, W. Chen, X. Chen, J. Weng and M. Imran, "An Overview on Smart Contracts: Blockchain ensures, Advances and Platforms," *Future Generation Computer Systems*, Vol.105, Apr. 2020, 475-491, DOI: <https://doi.org/10.1016/j.future.2019.12.019>
- [15] M. Krichen, M. Ammi, A. Mihoub and M. Almutiq, "Blockchain for Modern Applications: A Survey," *Sensors* 2022, 22, 5274, DOI: <https://doi.org/10.3390/s22145274>
- [16] T. H. Im, "Trends in Standards and Testing and Certification Technology - Current Status of International Standards for Software Testing (ISO/IEC/IEEE 29119)," *TTA Journal*, No. 167, Telecommunications technology Association, 96-101, Sep 2016.
- [17] T. Lee, "Blockchain and Cryptocurrency Distributed Testing Methods," *International Journal of Internet, Broadcasting and Communication*, Vol.14 No.1, Feb 2022, 1-9, Available: <https://www.earticle.net/Article/A409169>
- [18] Lee, L.-H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., Kumar, A., Bermejo, C., & Hui, P. (2021). All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda. *arXiv preprint arXiv:2110.05352*. DOI: 10.48550/arXiv.2110.05352.
- [19] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 2017, pp. 557-564, DOI: 10.1109/BigDataCongress.2017.85.
- [20] Ritterbusch, Georg & Teichmann, Malte. (2023). Defining the Metaverse: A Systematic Literature Review. *IEEE Access*. PP. 10.1109/ACCESS.2023.3241809.

- [21] Archana Prashanth Joshi, Meng Han, Yan Wang. (2018). A survey on security and privacy issues of blockchain technology. *Mathematical Foundations of Computing*, 1(2): 121-147. DOI: 10.3934/mfc.2018007.
- [22] Minghui Xu, Yihao Guo, Qin Hu, Zehui Xiong, Dongxiao Yu, Xiuzhen Cheng, (2023). A trustless architecture of blockchain-enabled metaverse. *High-Confidence Computing*, Vol. 3, Issue 1. DOI: 10.1016/j.hcc.2022.100088.
- [23] T. -G. Lee, "A Test Method for the Convergence of the Metaverse and Blockchain," 2024 26th International Conference on Advanced Communications Technology (ICACT), Pyeong Chang, Korea, Republic of, 2024, pp. 321-326, DOI: 10.23919/ICACT60172.2024.10472002.



Tae-Gyu Lee (BSc'92–MSc'96–PhD'06) received the B.Sc. degree from Kunsan National University, Kunsan, Korea in 1992, the M.Sc. degree from Soongsil University, Seoul, Korea in 1996, and the Ph.D. degree from Korea University in 2006. He is currently a Professor in the Dept. of Smart Contents, Division of ICT Convergence, Pyeongtaek University, Gyeonggi, Korea from 2018. He has been a Professor in the Support center for Field Practice Education, WonKwang University, Jeonbuk, Korea for 2014-2018. He has been a Professional Researcher in Advanced Convergent Technology R&D Group, Korea Institute of Industrial Technology (KITECH), Ansan, Korea for 2009-2013. He has also been a President in the JIGUNET Corporation, Seoul, Korea, from 1999. His research interests are in distributed systems, ubiquitous computing, middleware, networks, wearable and robot computing. Prof. Lee is an honorary member of the Korea Information Processing Society and actively serves as a reviewer for ICACT. Furthermore, he has fulfilled the role of a judge at the 10th International Abilympics.