

A Test Method for the Convergence of the Metaverse and Blockchain

Tae-gyu Lee*

*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 combining blockchain and metaverse technologies. This research analyses the interaction between blockchain networks and virtual reality worlds, developing a secure and efficient testing process. The paper evaluates the interaction between metaverse and blockchain in various scenarios, offering insights to enhance reliability and security. This study makes a significant contribution to strengthening safety in the digital environment through the fusion of metaverse and blockchain technologies. This study proposes key evaluation factors and formulas to objectively assess the integration of blockchain and the metaverse services. These evaluation metrics can be valuable in the development of assessment tools and simulation instruments.

Keywords— Blockchain, Metaverse, Cryptocurrency, Testing, Evaluation

I. INTRODUCTION

In recent times, despite the ongoing economic and social issues and concerns associated with cryptocurrencies and cryptocurrency exchanges, the role of cryptocurrencies as a digital economy and an alternative means of currency continues to expand steadily [1, 2]. Especially, following Blockchain 2.0, various emerging technologies like smart contracts, NFTs, and metaverse platforms have extended their reach, forming new markets and enhancing utility and stability [3, 4]. Nevertheless, there remain limitations in ensuring mutual trust among stakeholders, including developers, operators, and users, within the cryptocurrency and exchange ecosystems, and the fundamental security and reliability of virtual trading systems are under threat [5, 6, 7].

Currently, the convergence of metaverse and blockchain technologies is presenting new possibilities in the digital domain [8]. Metaverse is realized through virtual reality, while blockchain offers security, transparency, and reliability in a distributed manner. This convergence provides opportunities and challenges in terms of testing and ensuring the reliability of system operations within a dynamic ecosystem.

A robust testing process tailored to metaverse-supported blockchain applications becomes essential. Conventional testing methodologies may often fail to address the complexities arising from the immersive and interconnected virtual environments of the metaverse. Addressing these

challenges necessitates new approaches to guarantee uninterrupted functionality and security of blockchain networks in such environments.

This paper proposes a comprehensive framework for designing a testing process for metaverse-supported blockchain applications. Our research aims to provide a framework that allows thorough testing of blockchain-based metaverse applications, taking into consideration the unique features and challenges resulting from this convergence. By conducting 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 growth of both metaverse and blockchain technologies.

This paper is described as follows: Section 2 presents the related works, while Section 3 proposes the metaverse and blockchain interaction and convergence testing process. In Section 4, we analyse key issues related to the proposed testing process. Finally, Section 5 provides conclusions.

II. RELATED WORKS

Previous studies in this context have primarily focused on the security and safety of blockchain and cryptocurrencies. Additionally, research on the combination of the metaverse and blockchain is increasing, but there is still a lack of focus on the testing process [5, 9, 10]. These studies emphasize the need for the development of effective testing tools and methodologies in the context of metaverse and blockchain environments [11, 12].

The fusion of the metaverse and blockchain is reshaping the digital economy, fostering novel business models and value creation. However, ensuring success requires a robust testing process to safeguard stability and security, enabling trust and unlocking opportunities in finance, gaming, art, and beyond.

Existing research has shown the absence of new methodologies and testing processes for the convergence of the metaverse and blockchain [10, 13, 14]. Effective testing methods that consider the immersive and interconnected virtual environments of the metaverse and the distributed nature of blockchain are lacking, potentially leading to security and stability issues. Therefore, this study aims to propose a new testing process that considers the characteristics of the metaverse and blockchain.

Through this, 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 the metaverse and blockchain. This model is proposed to concretize the testing and authentication procedures while enhancing practicality [15].

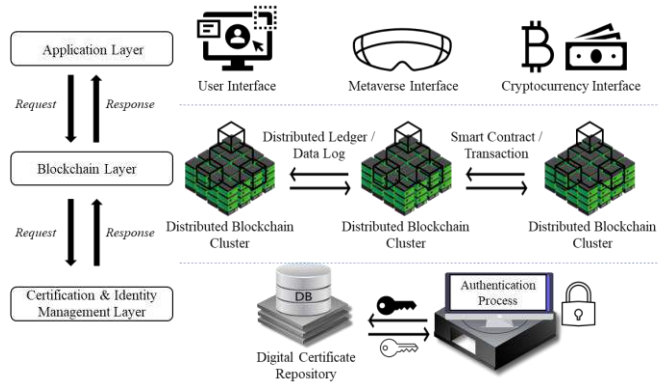


Figure 1. Metaverse and Blockchain Convergence Testing Operating Environment

For conducting metaverse and blockchain integration tests, a hierarchical structure of converged application services can be organized into three layers. First, the top-tier Application Layer encompasses applications and smart contracts running in the metaverse environment. It operates user interfaces, virtual environments, and services. Second, the Blockchain Layer is based on blockchain technology and houses the distributed ledger and smart contract platform. Transaction processing and data recording occur within the blockchain. Nodes of the blockchain network and the smart contract execution environment belong to this layer. Third, the Certification & Identity Management Layer is a core component of the certified structure, responsible for identity verification and digital certificate management. It manages user identities and provides authentication and permissions needed by smart contracts and applications. This layer includes digital certificate repositories and secure authentication processes.

Through this layered model, when conducting blockchain integration tests in a metaverse distributed environment, smart contracts and applications running 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 enables effective testing and security verification.

Furthermore, the metaverse and blockchain integration testing process model is used to identify the key components and issues in each testing phase and establish input and output elements. This research aims to provide solutions for testing issues related to stable smart contract service expansion for the integration of metaverse services and blockchain networks.

III. METAVERSE AND BLOCKCHAIN INTEGRATION TESTING PROCESS

In this section, we aim to propose an integrated testing process to effectively test this interaction. It outlines the proposed testing process, taking into consideration the intricate interaction between the metaverse and blockchain. This process offers a step-by-step approach to effectively test metaverse-supported blockchain applications, accommodating various testing scenarios and interactions. The testing process, designed to address the complex interplay between the metaverse and blockchain, provides a systematic framework for testing metaverse-supported blockchain applications. Figure 2 illustrates the stepwise approach of this testing process, which can be utilized effectively.

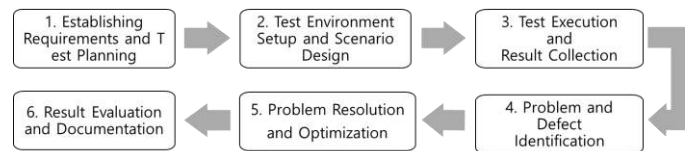


Figure 2. Convergence Testing Process

A. Requirement Definition and Test Planning

The initial phase of the testing process involves defining the requirements for the metaverse and blockchain application and establishing test objectives.

- **Define Test Objectives and Scope:** Clearly define the objectives for testing the metaverse-supported blockchain application and specify the aspects to be tested.
- **Set Up Test Environment:** Establish the test environment by integrating the metaverse and blockchain, and configuring the necessary hardware and software.
- **Allocate Test Resources:** Assign resources, including the testing team, testers, developers, etc., and define their roles.
- **Develop Test Plans:** Document comprehensive test plans, including schedules, task allocation, test case design, execution plans, and risk management.
- **Design Test Cases:** Create test cases based on the defined objectives and scope, specifying the expected behavior under different scenarios.
- **Generate Test Data:** Generate or import the required test data to simulate real-world situations.
- **Prepare Test Environment and Data:** Configure the test environment, load test data, initialize metaverse and blockchain networks, and apply necessary settings.
- **Review, Approve, and Execute Tests:** Review and gain approval for the test plans from the testing team and stakeholders, then execute the tests according to the established schedule and process.

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 the comprehensive testing of the interaction between the metaverse and blockchain, as well as the identification and improvement of any issues.

B. Test Environment Setup and Scenario Design

In this phase, the test environment for the metaverse and blockchain integration testing is set up, and various test scenarios are designed. The environment encompasses the integration of the metaverse environment and the blockchain network.

- **Environment Setup:** Construct and configure the testing environment, which includes integrating the metaverse and blockchain, along with setting up necessary hardware and software components. Ensure that the environment aligns with testing objectives.
- **Scenario Definition:** Define various test scenarios representing specific situations or use cases. Each scenario is intended to test the interaction between the metaverse and blockchain.
- **Test Data Preparation:** Prepare the required test data for the defined scenarios, simulating specific states and events in each scenario.
- **Test Case Design:** Design test cases based on the defined scenarios, specifying in detail the behavior to be verified.
- **Environment Validation:** Verify that the configured test environment functions as expected, addressing any issues that arise, and loading and preparing the test data.
- **Test Execution and Result Analysis:** Execute tests based on defined scenarios, record the results, identify and document any problems or errors, and analyze the results. Summarize the findings in a report, which may include proposed solutions for addressing issues and improvements.

Through the setup of the test environment and scenario design, various situations are created to test the metaverse-supported blockchain application.

C. Test Execution and Result Collection

In this phase, tests are executed in 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 data related to performance is collected.

- **Test Execution:** Execute tests based on predefined scenarios, simulating interactions between the metaverse and blockchain.
- **Real-time Monitoring:** Continuously monitor the test environment and scenarios during testing, checking for operational issues.
- **Result Collection and Performance Measurement:** Collect results after each scenario, document state changes, and measure system performance, including latency, response time, and throughput.
- **Error Documentation and Log Analysis:** Document errors and issues encountered during testing, including error types, timestamps, and their impact. Analyze log files to identify root causes.
- **Evaluation and Reporting:** Evaluate collected results against test objectives, identify issues, and document

test outcomes in a report, including test success/failure, identified problems, and proposed solutions. Complete testing and clean up the test environment and resources once all tests are finished.

Through these steps, the metaverse and blockchain integration application can be effectively tested, and results can be collected to address and improve identified issues.

D. Identifying Issues and Defects

This process involves identifying and analysing issues and defects that occurred during test execution. During this stage, all errors and unexpected situations related to metaverse and blockchain interactions are recorded, and the root causes of issues are determined.

- **Error Identification:** Identify errors and deviations from expected system behavior during test execution.
- **Defect Classification and Severity Assessment:** Categorize and evaluate defects by type and severity, considering their impact on system functionality.
- **Root Cause Analysis and Issue Reporting:** Analyze the causes of defects, document them in a report, including descriptions, root causes, and proposed fixes.
- **Priority Assignment and Issue Tracking:** Prioritize defects for resolution, track their status, and manage them until they are addressed.
- **Test Re-execution:** After fixing defects, re-run relevant test cases to confirm issue resolution.

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

E. Issue Resolution and Optimization

In this phase, identified issues and defects are addressed, and the system is optimized. This involves fixing errors and implementing measures to enhance stability and reliability.

- **Issue Resolution:** Address identified issues and defects, including root cause analysis and corrective actions.
- **Re-Testing and System Testing:** Verify the modifications and assess their impact on system behavior, ensuring that previously identified problems are resolved without introducing new defects.
- **Performance and Security Enhancement:** Optimize system performance and strengthen security measures as needed, including improvements in latency, response times, scalability, and security features.
- **Performance Evaluation:** Evaluate the performance of the optimized system to confirm improvements are effective.
- **Issue Tracking and Documentation:** Manage and track resolved issues and defects to prevent recurrence, and update issue reports to reflect the status and outcomes of 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.

F. Evaluation and Documentation of Results

In this final phase, the test process's results are evaluated and documented. The aim 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 used for future quality management and reporting.

- **Result Evaluation and Performance Measurement:** Evaluate the resolution of identified issues and measure performance improvements achieved through testing.
- **Result Report and Sharing:** Prepare a comprehensive result report that includes testing objectives, executed test cases, issues, resolution methods, optimization outcomes, and performance measurements. Share this report with stakeholders and teams involved in testing, gathering feedback.
- **Documentation and Quality Assurance:** Archive the result report in project records and archives for future reference. Assess overall system quality based on the results and develop strategies for improvement, aiming to prevent similar issues in future phases.
- **Process Improvement:** Evaluate the test process and identify areas for enhancement to ensure more efficient testing in future projects.

Through these evaluation and documentation activities, the testing outcomes and conclusions for metaverse-integrated blockchain applications are clearly summarized. They provide information for future improvement and maintenance tasks.

IV. ANALYSIS OF KEY ISSUES IN THE PROPOSED TESTING PROCESS

In this section, we analyse the strengths and limitations of the proposed testing process and aim to enhance our understanding of the interaction between the metaverse and blockchain.

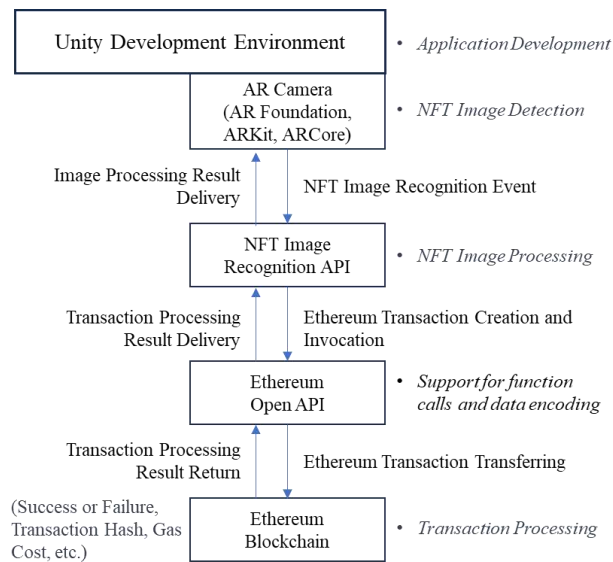


Figure 3. Metaverse and Blockchain Convergence Development Environment and Routines

The following issues can be considered as key evaluation factors 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.	relative scores
Smart Contract Score	It is an evaluation metric for assessing smart contracts within the metaverse.	relative scores
Security and Safety Score	It is a function used to evaluate security and safety in the metaverse and blockchain integration testing.	relative scores
Improvement Score	It is a function used to evaluate the improvement and optimization of the testing process.	relative scores

A. Interaction Issues Between the Metaverse and Blockchain

The interaction between the metaverse and blockchain presents various complexities and challenges. This section analyses the key issues that can arise due to the interaction between these two technologies. For instance, difficulties in reconciling blockchain transaction processing with real-time interactions within the metaverse and concerns related to security and personal data protection are addressed. To analyse the interaction between the metaverse and blockchain, we define an evaluation function based on various weighted factors, including interoperability weight ($W_{interoperability}$), security level weight ($W_{security}$), performance and processing speed weight ($W_{performance}$), cost efficiency weight ($W_{cost_efficiency}$), and community and developer support weight ($W_{community_support}$) as seen in Equation (1).

$$\begin{aligned}
 \text{Interaction_Score} = & W_{interoperability} * \text{Interoperability} \\
 & + W_{security} * \text{Security_Level} \\
 & + W_{performance} * \text{Performance} \\
 & + W_{cost_efficiency} * \text{Cost_Efficiency} \\
 & + W_{community_support} * \text{Community_and_Developer_Support}
 \end{aligned} \quad (1)$$

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

B. Smart Contract Issues Within the Metaverse

The execution of smart contracts within the metaverse environment can pose complex issues. Errors or vulnerabilities in smart contracts can have a significant impact on interactions within the metaverse and integration with blockchain. Key variables related to smart contracts, such as metaverse integration weight ($W_{metaverse_integration}$), smart contract security weight ($W_{security}$), smart contract functionality weight ($W_{functionality}$), smart contract efficiency weight ($W_{efficiency}$), and smart contract scalability weight ($W_{scalability}$), can be considered in the metaverse. The evaluation function

for analysing smart contracts within the metaverse, taking these weight variables into account, is as seen in Equation (2).

$$\begin{aligned} \text{Smart_Contract_Score} = & W_{\text{metaverse_integration}} * \text{Metaverse Integration} \\ & + W_{\text{security}} * \text{Security} + W_{\text{functionality}} * \text{Functionality} \\ & + W_{\text{efficiency}} * \text{Efficiency} + W_{\text{scalability}} * \text{Scalability} \end{aligned} \quad (2)$$

This formula allows for the evaluation of various aspects of smart contracts, with each weight representing the relative importance of the respective aspect.

C. Security and Safety Issues

The combination of the metaverse and blockchain introduces new considerations in terms of security and safety. Key concerns include user data protection, vulnerabilities in smart contracts, the application of encryption technologies, and more. As variables for analysing security and safety in metaverse and blockchain integration testing, key weights can be considered, such as metaverse security weight ($W_{\text{metaverse_security}}$), blockchain security weight ($W_{\text{blockchain_security}}$), data privacy weight ($W_{\text{data_privacy}}$), and compliance weight ($W_{\text{compliance}}$). The security and safety evaluation function can be defined as seen in Equation (3).

$$\begin{aligned} \text{Security_and_Safety_Score} = & W_{\text{metaverse_security}} * \text{Metaverse_Security} \\ & + W_{\text{blockchain_security}} * \text{Blockchain Security} \\ & + W_{\text{data_privacy}} * \text{Data Privacy} \\ & + W_{\text{compliance}} * \text{Compliance} \end{aligned} \quad (3)$$

To calculate the security and safety evaluation score (security_safety_score) for the Metaverse convergence application service, the following steps are taken: Firstly, assign weights to key components: $W_{\text{metaverse_security}} = 0.3$, $W_{\text{blockchain_security}} = 0.3$, $W_{\text{data_privacy}} = 0.2$, $W_{\text{compliance}} = 0.2$. Secondly, consider actual measurement values: $\text{Metaverse_security} = 8.5$, $\text{Blockchain_security} = 9.0$, $\text{Data_privacy} = 7.5$, $\text{Compliance} = 8.8$. 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 of the Metaverse convergence application service.

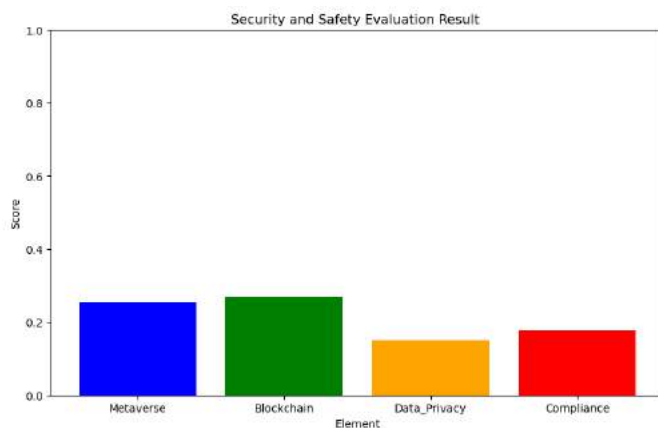


Figure 4. Security and Safety Evaluation Result on Metaverse and Blockchain Convergence Applications

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 data privacy and compliance are relatively more vulnerable compared to Metaverse and blockchain security.

D. Test Process Improvement and Optimization

After analysing the key issues, research is conducted on how to improve and optimize the test process. Consideration is given to improvements in error and defect handling, enhancing safety, performance optimization, and efficient test scenario design. The evaluation function for improving and optimizing the fusion test process for blockchain and the metaverse is as seen in Equation (4).

$$\begin{aligned} \text{Evaluation_Score} = & (W1 * (1 - \text{Test Duration} / 100)) \\ & + (W2 * (\text{Resource Utilization} / 10)) \\ & + (W3 * (\text{Test Coverage} / 100)) \\ & + (W4 * (\text{Error Handling} / 10)) \end{aligned} \quad (4)$$

Each weight variable, $W1$ represents the weight for *Test Duration*, $W2$ represents the weight for *Resource Utilization*, $W3$ represents the weight for *Test Coverage*, and $W4$ represents the weight for *Error Handling*. These weights can be adjusted based on the project's characteristics, and they may vary depending on the project's goals and priorities for improving the testing process.

V. CONCLUSION

In conclusion, this paper has presented a comprehensive framework for testing the fusion of the metaverse and blockchain. It highlights the significance of a testing process that considers the intricate interactions between these technologies and underscores the advantages and outcomes it can yield. In Section 4, various evaluation function models applicable to the metaverse and blockchain integration testing process were presented. Based on these diverse evaluation models, improved simulations can be conducted to obtain accurate prediction data. In this study, the development and application of the testing process are expected to play a crucial role in the reliability and security of metaverse and blockchain applications.

In terms of future research directions, there is a need for the development of improved testing methodologies and tools to adapt to these changes. 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.

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] 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>
- [10] C. Lal and D. Marijan, "Blockchain Testing: Challenges, Techniques, and Research Directions," Mar. 2021, DOI: <https://doi.org/10.48550/arXiv.2103.10074>
- [11] 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>
- [12] Z. Zheng, S. Xie, H.N. Dai, W. Chen, X. Chen, J. Weng and M. Imran, "An Overview on Smart Contracts: Challenges, Advances and Platforms," Future Generation Computer Systems, Vol.105, Apr. 2020, 475-491, DOI: <https://doi.org/10.1016/j.future.2019.12.019>
- [13] 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>
- [14] 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.
- [15] 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>

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.