International Journal of Internet, Broadcasting and Communication Vol.14 No.1 1-9 (2022)
http://dx.doi.org/10.7236/IJIBC.2022.14.1.1

IJIBC 22-1-1

Blockchain and Cryptocurrency Distributed Testing Methods

Taegyu Lee*

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

Abstract

Recently, a large number of cryptocurrencies and block chains have been continuously released. However, these cryptocurrencies and block chains are open to users without authorized verification and testing procedures, causing various reliability problems. Existing cryptocurrencies and blockchain test methods build a blockchain Testnet for a certain period of time by the developer without external verification by a third party, and after repeatedly self-testing and self-operating processes, commercialization is in progress by switching to the Mainnet. This self-verification method does not guarantee objectivity and publicness, and high reliability of customers cannot be realized. This study proposes a cryptocurrency and blockchain test interface and test control system as a third-party open test method.

Keywords: *Computer, Internet (Network), Software, Blockchain, Cryptocurrency, Testing, Certification.*

1. Introduction

Recently, as one of the next-generation information security and asset management technologies, blockchain and cryptocurrency technologies are heating up competition to secure leadership in various basic and applied technologies, centering on countries that lead technologies and standards related to blockchain. In particular, as interest in blockchain-based application services such as Metaverse and NFT (Non-Fungible Token) has recently increased, interest and demand for blockchain technology standards are growing. International standardization of blockchain is still in its infancy, and definitions of terms, reference structure, governance, smart legal contract standards and use cases are being developed in ISO TC307 (International Standardization Organization), and block chain platform based on reference structure standards, interworking, application, and identity management standards are ongoing activities in several standard groups [1, 2].

In addition, various patents are being applied for to lead the block chain standard technology in major countries such as China, the United States, Japan, and Europe. In particular, many patents are being applied for in China to secure the initiative in blockchain-based technology.

Recently, the number of blockchain patent applications applied to various fields in Korea is rapidly increasing. As the untack industry grows due to the spread of Covid 19, cyber-attacks targeting it are also

Manuscript Received: October. 15, 2021 / Revised: October. 18, 2021 / Accepted: October. 22, 2021
Corresponding Author: tglee@ptu.ac.kr
Tel: +82-31-659-8370, Fax: +82-31-659-8011
Assistant Professor, Smart Contents Major, Division of ICT Convergence, Pyeongtaek University, Gyeonggi, Korea

increasing, and accordingly, block chain technology with excellent security is attracting attention. The number of blockchain-related patent applications in Korea stood at 24 in 2015 but increased more than 50 times to 1301 in 2019.

Nevertheless, the safety of basic elements and functions of numerous blockchain software, quality testing and certification for blockchain networks and cryptocurrency services are not yet fully discussed. In Korea, the Korea Telecommunication Technology Association (TTA) is establishing standards related to distributed ledger technology and is developing the reliability evaluation standards for blockchain platforms [1]. Internationally, ISO has not yet fully developed standards related to blockchain platform performance measurement [2]. Research related to the security evaluation of the consensus algorithm related to this is in progress, and the basis for new project proposals related to performance measurement standards is being formed.

To improve blockchain performance and scalability, major blockchain platforms are applying various technologies such as on-off-chain solutions, cryptographic algorithms, and consensus algorithms improvement [3]. Domestic blockchain companies are also actively promoting technology development. Blockchain platform developers are developing performance measurement tools for their own platforms [4].

When testing the quality of blockchain and cryptocurrency, various test standards may be required depending on the type of blockchain software and service, such as cryptocurrency, NFT, and cryptocurrency exchange [5]. Evaluation indicators and regulations for various blockchain and cryptocurrency security functions, platforms, and interlocking technologies have been proposed, but there are insufficient or non-existent measures for blockchain test methods based on standard evaluation indicators.

This paper is described in the following order. Chapter 2 describes the research on blockchain test-related research, Chapter 3 describes the blockchain and cryptocurrency test system overview, and Chapter 4 describes the blockchain test interface method and examples. Finally, Section 5 describes the conclusion.

2. Related Works

So far, various blockchains and cryptocurrencies have been launched and operated [6-9]. These blockchain networks and cryptocurrencies are generally converted to Mainnet and released through a self-verification process called Testnet.

Recently, block chains and cryptocurrencies have had a tremendous impact on the global economic system, and despite negative views on real economy usability, the market value of cryptocurrencies is rapidly expanding, and its influence has grown rapidly to a point where it cannot be ignored. Nevertheless, existing blockchain networks and cryptocurrencies are being released and used without objective verification by external third parties. This is acting as a destabilizing factor for the growth of blockchain and cryptocurrencies, and it can act as a major obstacle for new cryptocurrencies to enter the market. For the blockchain and cryptocurrency market to be recognized as a recognized stabilization system for mankind, it does not depend on a privately operated and evaluated Testnet, but it is important to be verified through a publicly operated third-party test and certification institutions.

Most of the blockchain network and cryptocurrency services currently being launched have a demonstration and test process for a certain period through their own Testnet construction. And after a certain period has passed, the process of converting to Mainnet is carried out through self-disclosure without verification by an external third party. Until now, as cryptocurrencies operated based on blockchain networks, Bitcoin, Ethereum, Litecoin, Dogecoin, etc. developed blockchain technology and cryptocurrency functions based on the testnet built on the network by the development group itself. After a trial run, it was released. If the operation process of the Testnet proceeds smoothly and verification of various user functions such as

new functions is performed smoothly, it is converted to the Mainnet which is open to general users.

Testnet describes cases where the blockchain network is not yet running at full capacity. Testnet is a test blockchain network to verify that blockchain transactions are secure and ready to operate to transition to a Mainnet system for business that builds a blockchain independent ecosystem. It is primarily used by programmers and developers to test and solve all aspects and functions of blockchain networks. In other words, the Testnet exists only as a prototype of the blockchain project, while the Mainnet is a fully developed blockchain network that allows users to smoothly conduct cryptographic transactions (or digital data). It also operates a Testnet and tests whether it can establish itself as an independent blockchain network. This period can range from a few months to long several years. This is because stabilization tasks such as exchange connection problems and wallet creation are not easy. Developers can use open communities such as GitHub to share and modify how much development has been completed and proceed with development. After that, if the Testnet of the corresponding blockchain and cryptocurrency succeeds, it is converted to the Mainnet and released.

Mainnet is a self-contained blockchain network, including cryptocurrency exchanges and transactions between individual wallet transactions, as well as constructing blockchain and cryptocurrency ecosystems and creating coin wallets. Through this process, cryptocurrency coins and tokens can be converted into coins with Mainnet. Although these self-testing and verification methods support a certain degree of functional and quality stability, they are very insufficient in terms of objectivity to confirm the stability of service quality for block chains and cryptocurrencies released to subsequent users after being released as Mainnet. to be. Moreover, service insecurity and problems can cause great economic loss to both service providers and consumers. This series of blockchain and cryptocurrency development and launch processes are conducted through an informal process by self-determination centered on early developers and operators. This reveals a limitation in establishing objective reliability in terms of information stability, performance, and functionality of the service for subsequent users accessing the public blockchain network and service.

If new blockchains and cryptocurrencies as well as existing blockchains and cryptocurrencies undergo an open and objective testing and certification process by a third party, customer reliability and system safety for the released block chains and cryptocurrencies can be maximized.

This study proposes a method for measuring and testing the quality of blockchain and cryptocurrency services to overcome the limitations of existing blockchain and cryptocurrency services that are released without objective testing and evaluation.

3. Blockchain and Cryptocurrency Testing System

This study aims to build a blockchain evaluation platform for blockchain public evaluation authentication testing based on a blockchain network composed of a distributed system.

3.1 Organization of Testing System

In this paper, the blockchain network to which the test logic and interface are applied is divided into Normal mode and Test mode, which can be selectively operated by the blockchain test operator. And, according to the choice of blockchain network developers and operators, blockchain clients can be deployed by removing test logic and interfaces.

And according to the classification of major transactions and functions, blockchain and cryptocurrency tests can be conducted separately from the independent functional test of each participating node and the interaction (or two-way) transaction test between the participating nodes.

The evaluation and authentication test system of this study shows the overall configuration as shown in Figure 1 to apply various test scenarios (test cases) based on blockchain and cryptocurrency transactions.

And the configuration example of the test system can provide an overall blockchain test authentication integration interface layer for applying, monitoring, and controlling test events to the test blockchain and cryptocurrency transaction. Next, it is possible to provide a blockchain test distributed cluster layer that operates by applying a test input/output interface to the target blockchain and target cryptocurrency functions and transactions to be verified. In addition, this system can support a database that can systematically store and extract various test input and output data according to blockchain test case application, and a blockchain test data backup layer that stores various evidence data collected.

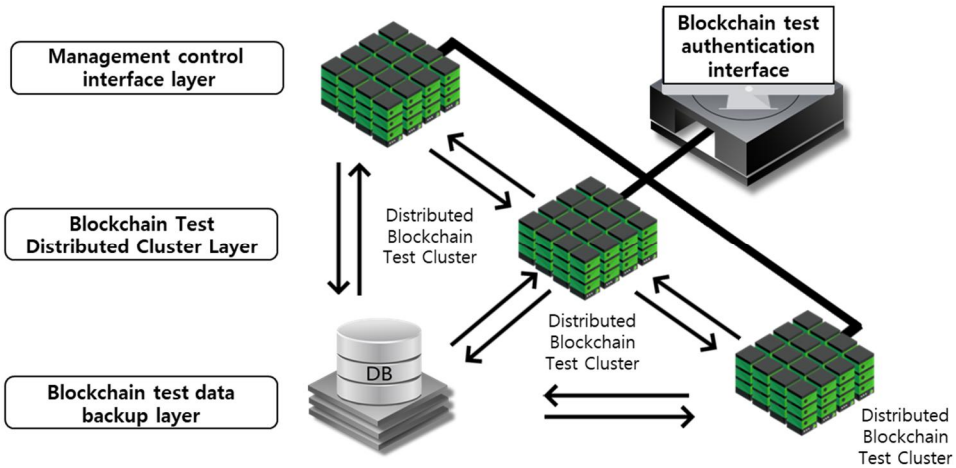

Figure 1. Block chain and cryptocurrency test system configuration

This hierarchical structure can be selectively operated in various ways according to the test operator and the scale and needs of the target blockchain. For example, it may be transformed into various hierarchical structures such as a single layer, a two layer, a three layer, and the like. Figure 2 shows the main components of a blockchain and cryptocurrency test system and their relationships.

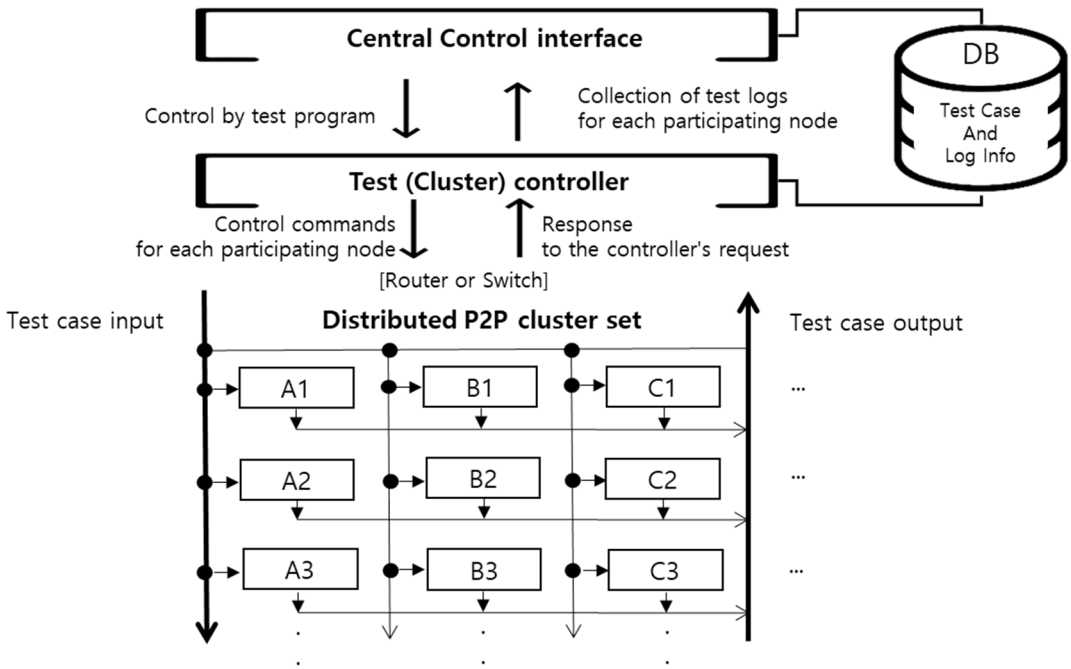

Figure 2. Main components of blockchain and cryptocurrency test system

First, the central control interface supports the test operator to monitor the test progress or its results. It sends control command messages such as test start, stop, participating node type selection, and test case (test code, test data, etc.) to the test (cluster) controller. Next, the test (cluster) controller receives commands from the central control interface and transmits control messages to each node participating in the test on the blockchain network (or distributed cluster set) such as the start and stop of testing, the selection of participating node type, and the input and output of test case (test code, test data, etc.). Next, each participating node that receives the test start command selects its participating node type (full node, miner node, lightweight node, reference node, etc.) according to the deterministic selection of operators and users, or random probability choose. Those choices determine what role the test node will play within the blockchain. In addition, when the type of each participating node is determined, its own type information is transmitted to the test controller or the central control interface. Next, the test (cluster) controller collects the roles of each participating node and delivers them to the central control interface. Then, each participating node repeatedly performs a test on each test case according to the test start command. The test results for each stage are transmitted to the central control interface through the test (cluster) controller. Finally, the central control interface feeds back the test results for each test case from the test (cluster) controller, collects them, and stores them in the database.

Here, the central interface can control each participating node through the test (cluster) controller, and each participating node distributed on the P2P blockchain network independently determines the type of participating node, test case, etc. and plays a role can do. In addition, the configuration of the central control interface and the test controller can be integrated and operated according to the developer and operator's choice.

3.2 Principal Testing Scenarios

This study can provide two methods to set the types of nodes participating in the test. In the first method, the client on the P2P blockchain network, that is, the participating node user manually selects his or her participating node type (full node, lightweight node, miner node, etc.) with deterministic or random probability, and report the results. The second method selects the node types (full node, lightweight node, miner node, etc.) of participating nodes with deterministic or random probability led by the test controller or central control interface, and the result is report. The following describes the test case application process according to the type change of each participating node.

First, the miner node test process. A miner node creates a block through the process of creating a new block by inputting a test transaction (Tx) of a certain size or more into the block and performing mining. In this case, validation of each test transaction Tx may be included or omitted in the process. The generated block is broadcast on the participating test blockchain network, and participating nodes verify that the block is a valid block. This test process continuously synchronizes the test block state information with the test controller and can transmit block data or transaction data upon request. In this test process, the test program counts the block generation cycle and transaction processing count of the test block chain. Through this, it is checked whether the block generation cycle and transaction processing speed (TPS) of the test blockchain satisfy the performance suggested by the test blockchain. For example, if the block generation cycle of the test block chain is 1 minute and the TPS is 3000, and the TPS is 1500 in the test process, it does not satisfy the suggested performance, so the test did not pass.

In addition, the degree of decentralization of the test blockchain is evaluated by counting the block generation cycle and transaction processing number of each miner node, respectively, and comparing the block generation cycle and transaction processing speed of the test blockchain. As a means to evaluate the decentralization of blockchain, the Gini coefficient and Nakamoto coefficient can be used. In addition, along

with the block generation period and number of transaction processing, the mining power of each node, that is, the hash rate and power consumption used for mining, is measured and recorded. This can measure whether the mining algorithm of the test blockchain is friendly to CPU, GPU, ASIC, etc., and it can measure the efficiency of power used to maintain the blockchain system.

The second is the full (blockchain) node test process. This test creates a large number of test transactions in full nodes and broadcasts them to the blockchain network. When a transaction is generated by a random full node, the sending address is randomly selected from among the wallet addresses of the test node and sent. At this time, the central test monitor should record information about which node sent how many transactions to which node. Here, the test controller intercepts the transaction packet, stores important information in the test database, and outputs it to the central test monitor. At the same time as the above process is running, the full node continuously synchronizes the test block state, and when there is a request, block data or transaction data can be transmitted to the requesting node. This process can be extended to test blockchain network overload testing. Any full node sends a transaction, and at the same time receives a block or transaction from another full node or miner node. The full node validates the test block and transaction, and the test program calculates and records the effectiveness of the validation. High verification efficiency may mean that a full node can operate smoothly even on a device with low performance.

Third, the lightweight wallet (or SPV: Simplified Payment Verification) node test process. The overall process of a lightweight wallet node is like that of a full node, but it performs simple block verification and transaction verification compared to a full node. That is, this test is a process of verifying the validity and transaction of lightweight blocks based on the test block header. It continuously synchronizes block headers, validates block headers, and validates and stores only those transactions that are related to one's own wallet address, rather than storing all transactions. This lightweight process increases transaction validation and storage efficiency. The lightweight wallet node testing process can be performed similarly to the full node testing. This test generates many test transactions and broadcasts them to the blockchain network, and, just like the full node test, the test controller stores important information in the test database through a snapshot of the transaction packet, and outputs it to the central test monitor. However, as described above, when receiving a transaction, only transactions related to one's own wallet are received, not all transactions.

4. Blockchain Network Based Test Case

4.1 Interface Structure of Applying Test Cases

Figure 3 is a two-dimensional model of a general blockchain network.

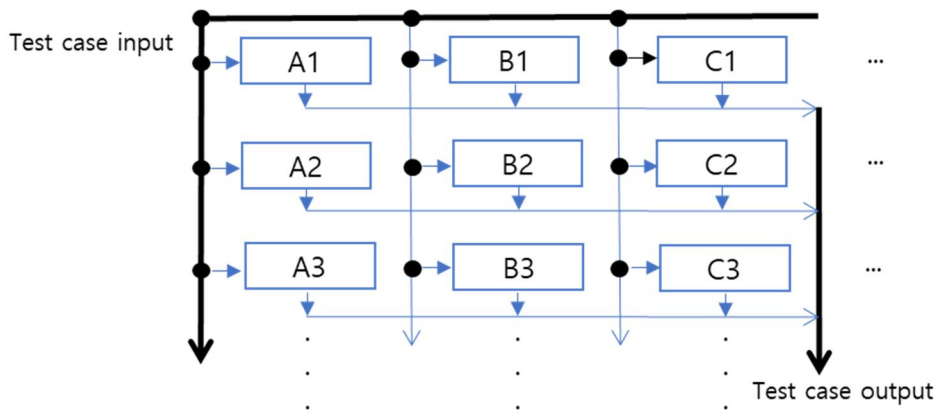

Figure 3. Block chain network and test case input/output interface structure

It consists of rows 1, 2, 3, etc., and columns A, B, C, etc. Each participating node A1, A2, A3, etc. participating in the blockchain network consists of a combination of the following main functions. First, it is a full blockchain function with a complete blockchain copy including the first block, the Genesis block, to the most recent block. Second, it is a wallet function that manages the user's private and public keys and generates addresses used for transactions. Third, there is a mining function which valid transactions are created in blocks at regular intervals (for example, for 10 minutes in Bitcoin) using block proof algorithms such as Proof of Work (PoW) and Proof of Stake (PoS) and connects the generated block to the main block chain. Finally, it is a network routing function that is responsible for the P2P network transmission function on the block chain.

By combining these major blockchain functions, participating nodes with various phases on the blockchain network are formed. For example, there are a reference client node, a full blockchain node, a solo miner node, a lightweight wallet (Simplified Payment Verification (SPV)) node, and the like.

First, the Reference Client node is in the form of a complete blockchain network including all functions. Bitcoin Core is one such example. Second, a full blockchain node is a form with network routing functions and all blockchain data. Third, a single miner node (Solo Miner) is a type of node specialized for mining except for the wallet function. Fourth, a Lightweight wallet (SPV: Simplified Payment Verification) node is a node that includes only a wallet function and a network routing function, and only transaction and validation are possible without the entire blockchain data. This is a wallet node installed mainly in a lightweight terminal with weak resources, such as a smartphone. This is because it may be impossible to install and operate full blockchain large-capacity data of tens to hundreds of gigabytes in smartphones and mobile devices, which have weak computing resources.

All participating nodes include a network routing function, and various test cases can be applied depending on the status of each participating node.

4.2 Characteristics of blockchain and cryptocurrency Test

The distributed test method of the blockchain network configures the event interface for test input/output of the test case unit of the main components and major transactions of the currently operating blockchain network. According to the selection and request of the test operator, it is possible to monitor the results according to various evaluation indicators such as the performance, functionality, and quality of the test module.

The following describes the advantages and characteristics of blockchain and cryptocurrency public testing strategies. First, by supporting an open test interface for each blockchain and cryptocurrency, it can support compatible modules of test snapshots and checkpoints. It is possible to strengthen test evaluation certification compatibility and objectivity by performing a test strategy based on a virtual test machine. Second, as a standardization and standardization model for blockchain and cryptocurrency tests, various test cases and test matrices can be provided. Third, by providing an open blockchain test bed and test environment, publicity can be strengthened by providing a blockchain and cryptocurrency accredited authentication service. Fourth, this study can provide the following various input/output interface configurations. These include a distributed transaction event sensing interface, a participating node transaction test case input interface, a participating node transaction test result output interface, test monitoring center configuration, test monitoring center interworking test case database construction, and test case alarm (alarm) event service.

4.3 Algorithm of blockchain and cryptocurrency Test

Figure 4 shows the blockchain network and cryptocurrency test algorithm.

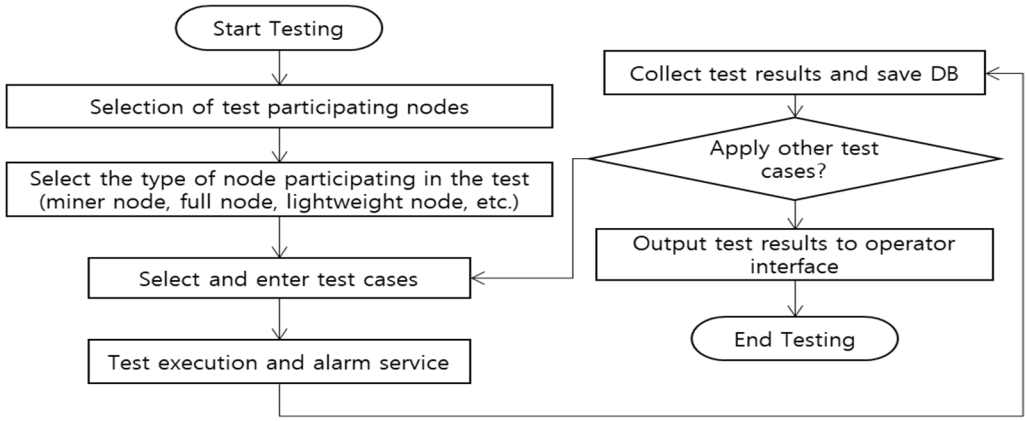

Figure 4. Blockchain and cryptocurrency test algorithm

First, the test operator can selectively operate the normal mode and test mode of the blockchain network. At this time, if the test mode is selected, the test process starts. Second, when the test mode starts, the nodes participating in the blockchain network recognize that they have entered the test mode. In addition, it may be selected whether to participate in the test process or may be selected according to a command of the test controller. In this case, the selection method may be determined manually by a user or an operator or may be arbitrarily selected by a random logic. Third, each test participating node can select its own node type (or topology). At the time, selectable types are miner node, full node, lightweight node, reference node, etc. In addition, the selection method may be determined manually by a user or an operator or may be arbitrarily selected by a random logic. Fourth, select or enter a test case (test code, test data, etc.).

Depending on the type of participating node, a preset test case is applied, or it depends on the external input of the test operator. Fifth, each test participating node executes a test, and when an emergency or exceptional situation occurs, an alarm message is sent to the test controller or operator. Sixth, when the unit test task is completed, the result is transmitted to the test controller and operator interface to be collected and stored in a specific database (DB). Seventh, it is determined whether the test is to be repeatedly performed on other test cases, and if so, return to the fourth step and continue the test. This series of step-by-step test procedures or results are displayed on the test operator interface. Finally, you can exit the test mode, or optionally switch to the normal mode.

5. Conclusion

The blockchain network distributed test method in this paper provides an event interface for input and output of test case unit tests of major components and major transactions of a normally operating blockchain network. According to the tester's selection and request, a method for monitoring the results according to various performance indicators such as function presence, performance and quality suitability was presented. This cryptocurrency and blockchain distributed test methods include blockchain transaction event-based test interface, transaction test case application input interface of participating nodes, transaction test result output interface of participating nodes, test status monitoring configuration, test monitoring center interworking test case database construction, test cases, alarm event services, and the like.

Therefore, this study can expect various effects as follows. First, the soundness of the blockchain and cryptocurrency market can be expanded by quantitatively and qualitatively comparing and evaluating the performance and quality of various blockchain and cryptocurrency services. Second, among the crowding block chain software, it is possible to strengthen the public interest by providing a transparent block chain test bed and test environment to determine the stability of block chain and virtual currency services and

provide an accredited authentication service that guarantees it. Third, when improving the performance or user convenience of blockchain software, various evaluation indicators are provided to enhance customer choice and objectivity. Fourth, it is possible to improve the reliability of traders and consumers by conducting tests based on the evaluation index and displaying and announcing the performance and quality grades. Finally, Metaverse and NFT content developers can provide stable and sustainable blockchain application services by considering the blockchain certified by the blockchain authentication system as reliable blockchain software and using it as a payment method for Metaverse and NFT content.

The results of this study can be expected to have the following utility. First, it can be used as a next generation blockchain software test standard. It can be proposed as a test standard for various blockchain software research results in the future. The developed block chain authentication service can be presented as an example of block chain test standard software, and improvement requests and suggestions from external experts can be reflected to establish it as a standard system. Next, the distributed cluster-based software test model of this study can be extended to other fields. For example, it can be a reference model when designing a test model of software with similar characteristics, such as a metaverse and distributed financial transaction system, based on the software test model established in the blockchain.

Acknowledgement

Following are results of a study on the "Leaders in INdustry-university Cooperation +" Project, supported by the Ministry of Education and National Research Foundation of Korea.

References

[1] K. C. Koo, D. J. Kim, K. Y. Oh, J. H. Ko, Y. C. Hwang, Y. H. Park, S. J. Jo, and Y. E. Lee, "*ICT Standardization Strategy Report Ver.2021*, "Telecommunications technology Association, Dec. 2020.

[2] 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, pp. 96-101, Sep 2016.

[3] K. S. Jang and O. Lee, "*The Design and Development of a Onchain Game for Scalability Verification of Blockchain Platform*," Journal of Digital Convergence, vol. 18, no. 10, pp. 253–263, Oct. 2020. DOI: https://doi.org/10.1109/icic50835.2020.9288610

[4] Y. A. Min, "*A Study on Performance Evaluation Factors of Permissioned Blockchain Consensus Algorithm*," Journal of Information and Security, Vol. 20, No. 1. Korea Convergence Security Association, pp. 3–8, Mar. 2020. DOI: https://doi.org/10.33778/kcsa.2020.20.1.003

[5] B. H. Oh, "*Method and apparatus for integrity check of software*," KR20130045759A20, Korean Intellectual Property Office, May 2013.

[6] T. S. Kang, M. I. Joo, B. S. Kim and T. G. Lee, "*Blockchain-based Lightweight Transaction Process Modeling and Development*," 2021 23rd International Conference on Advanced Communication Technology (ICACT), pp. 113-118, Feb. 2021. DOI: https://doi.org/10.23919/icact51234.2021.9370771

[7] T. S. Kang, J. W. Choi, and T. G. Lee, "*Development of a Smart Blockchain-based Cryptocurrency Payment Service Application*," 2021 Fall KIBME Conferences, The Korean Institute of Broadcast and Media Engineers, pp. 310-313, Nov. 27, 2021.

[8] K. C. H. Kim, "*The Impact of Blockchain Technology on the Music Industry,*" International Journal of Advanced Smart Convergence Vol.8 No.1 196-203, 2019. DOI: http://doi.org/10.7236/IJASC.2019.8.1.196

[9] C. Y. Song, and S. H. Hong, "*One way to solve the problem of presales of Ethereum: how to use public key cryptography*," International Journal of Advanced Science and Convergence, Vol.1, No.2, pp.27-31, 2019. DOI: https://doi.org/10.22662/IJASC.2019.1.2.027