Proof-of-concept for a reliable common data environment utilizing blockchain and smart contracts for supply-chain of public civil works

Fumiya Matsushita[1] and Kazumasa Ozawa[2]

[1]Institute of Engineering Innovation, School of Engineering, The University of Tokyo, Japan
[2]Institute of Engineering Innovation, School of Engineering, The University of Tokyo, Japan
matsushita@i-con.t.u-tokyo.ac.jp, ozawa@i-con.t.u-tokyo.ac.jp

Abstract –

To rationalize and automate public civil engineering works, it is crucial to directly utilize the information produced by the contractor for quality/ as-built inspection, and progress measurement. In this study, a highly reliable common data environment that utilizes blockchain and smart contracts to ensure tamper resistance and traceability of construction management information on quality and progress was developed and proved through verification tests in two project sites.

Keywords –

Blockchain; Smart contract; As-built inspection; Progress measurement; Common data environment

1 Introduction

With the introduction of information and communications technology (ICT) in construction, it has become possible to measure and verify construction progress using various devices and collecting the information necessary for construction management (hereinafter referred to as "construction management information") at the construction site. Among civil engineering works, in earthwork, many efforts that utilize building information modeling (BIM) and ICT for excavation, leveling, compaction, and as-built surveying are being promoted [1] and its productivity has been improved in recent years. However, on-site inspections which are confirmed by using various measurement methods, are still required by the client similar to the case in the past. Thus, to justify construction costs and efforts, including the number of inspections, it is required to develop a common data environment (CDE) that can detect falsification of measured data and ensure its credibility. Here, CDE means a mechanism for sharing information between involved players in a project defined by ISO19650.

To rationalize and automate public civil engineering works, it is crucial to directly utilize the information produced by the contractor for quality/ as-built inspection, and progress measurement. Productivity can be improved by directly using the data collected from the site by the contractor for inspection. On the other hand, if the data would be falsified to hide a defect in quality and as-built, safety and reliability of infrastructure as well as involved stakeholders might be damaged when revealed, and its social loss and impact would be enormous. For this purpose, the risk of falsification must be reduced. For payments, in addition to inspection results, a mechanism to appropriately manage and trace construction progress measurement according to conditions of contract must be developed.

In this paper, a reliable CDE that can realize these mechanisms utilizing with blockchain and smart contracts is proposed and its concept is proved.

2 Literature review

A blockchain is technically a chain of blocks of information. What makes it special is that the chain is copied across several devices and exists in many copies. Once "chained," the contents of the blocks cannot be modified, and despite data being copied on several devices, the blockchain algorithm ensures that there are no conflicts and that all copies are identical [2]. In contrast to a conventional centralized data management system, blockchain technology integrates data in a unique ledger while maintaining consistency where management is decentralized. Therefore, it is a trailblazing technology for implementing low-cost information management systems with tamper resistance and high availability that is expected to form the basis for next-generation ICT [3]. In addition, the blockchain has traceability of information [4].

In contrast, smart contracts refer to an ambiguous concept proposed by legal scholar and cryptographer Nick Szabo in the late 1990s [5]. Nick Szabo described smart contracts as "reducing transaction costs by signing

and fulfilling contracts over a network." In recent years, smart contracts have also been used to refer to computer programs implemented on a blockchain. In this sense, smart contracts are defined as computer codes that execute a contract partially or fully automatically and are stored on a blockchain platform [6]. In recent years, various smart contracts has been proposed and developed, and some of them can implement computer programs on blockchain. Ethereum [7] is an example of a blockchain with this function.

Blockchain technology is still relatively new but is widely regarded as having the potential to solve many business problems. Many organizations and governments are attempting to incorporate blockchain technology into their processes [8]. In particular, blockchain and smart contracts are expected to offer benefits to construction projects on key issues, such as timely payments [6]. For example, one study [9] introduced a semi-autonomous payment based on Hyperledger by the confirmation of qualified work quantities, though the confirmation process itself is manual. Another paper focuses on construction quality information management using blockchains [10]. By applying blockchain, it is possible to realize accurate recording of quality information in the construction process. This information can assist coordination among project participants and reduction of disputes caused by inaccurate documentation of nonconformances. However, because the original data of quality inspection results are not stored on the blockchain, the rationalization of the inspection process itself has not been achieved. For payments, the blockchain-based crypto assets to integrate the physical and financial supply-chains have been proposed [11]. This paper validated through a series of experiments in which crypto assets were used for processing payments. However, it does not include the inspection by the client, which is the target of this research. The CDE using blockchain at the design stage has been proposed [12].

This research focuses on the rationalization of the production process itself at the construction stage, such as quality/ as-built inspection, progress measurement and payment by clients. To achieve this rationalization, blockchain is used to ensure the credibility of information collected from the site by the contractor, and the contract information and contract performance information are managed using smart contracts. Furthermore, it is necessary to develop a smart contract that can connect the results of quality inspections to payment. In contrast to previous research, the proposed CDE with blockchain has advantage of rationalizing the production process itself by directly utilizing data collected from the site for quality/as-built inspection by eliminating the risk of falsification.

3 Requirements and scope of construction management information as input

A reliable CDE using blockchain and smart contracts has to meet the following requirements to ensure the credibility of collected information, rationalize inspections, and automate payments:

1. Information on quality and progress measurement can be stored on the premise of high availability in the blockchain.
2. Because the information collected from the site is directly used for quality/as-built inspection and progress measurement of the construction process, the tamper resistance of construction management information is guaranteed, and the presence or absence of tampering can be detected.
3. Contract information and contract performance information can be managed to make inspections and autonomous payments based on contracts possible.

In the supply-chain of construction projects, a multi-layered subcontracting structure is often formed by various companies, such as a subcontractor, and a material supply company, which makes a sales contract, starting from the main contractor (Figure 1). The construction object comprises a combination of specialized work types and materials carried out by many subcontractors. Hence, in addition to the main contractor, the information on civil engineering works, which is the input value to the as-built inspection system handled in the construction management system, includes the quality and as-built information of construction by a subcontractor and the quality certificate of the material supplied by the manufacturer. In the inspection by the client, the main contractor manages the suppliers, such as specialized construction companies and manufacturers, and the generated information is summarized in the inspection form included in the specifications by the main contractor. Therefore, in the system, the primary data generated by each supplier before the main contractor aggregates the information for inspection, and it is also used as the input value.

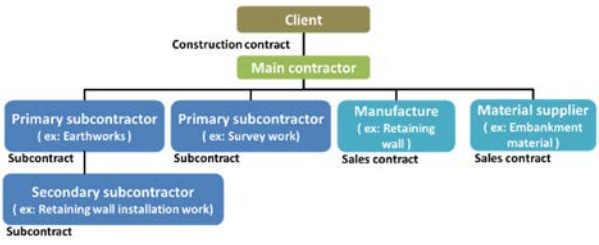

Figure 1. Example of a construction supply chain

4 System design

In order to realize a reliable CDE, it is necessary to consider the mechanism of tamper resistance in order to rationalize inspection. All inspections and payments are then carried out according to the contract. For this reason, smart contract functions are defined to realize inspection and payment workflows. Finally, the necessary system configuration is designed.

4.1 System design for tamper resistance of quality and progress information

Ensuring the tamper resistance of quality/ as-built and progress information is necessary to improve the credibility of the information saved by the contractor. The term "tampering" here refers to a situation wherein the main contractor or the subcontractor makes an intended revision during the inspection or assessment after the information is obtained. As shown in Figure 2, intended corrections have two types: falsification of input values and falsification of stored data. However, the act of redoing the construction and saving again the correction of information does not correspond to falsification.

Here, we assume situations of falsification that may occur and consider how to handle these situations. Specifically, falsification of stored data refers to the act of accessing the information stored in the data storage of the CDE and falsifying the information. For example, if the main contractor finds that some of the results from the surveying company do not meet the required level, some of the survey results stored in the data storage may be falsified by the main contractor. Falsification of input value refers to the act of falsifying and saving the false value by the contractor. Falsification of input values can be detected because true input values are obtained through devices and instruments directly connected to the data storage of the CDE through WebAPI. Therefore, here how to detect falsification of stored data is discussed.

The CDE uses a one-way hash function [13] to obtain the hash of the data when storing the data and stores this value in the blockchain. This makes it possible to be checked by reacquiring and collating the hash value of the file saved on the blockchain with the hash value of the file saved in the data storage at the time of inspection. If the stored data is tampered, it can be detected because the hash values will not match, as shown in Figure 3. In addition, the hash value stored on the blockchain cannot be tampered because of the characteristics of the data structure of the blockchain.

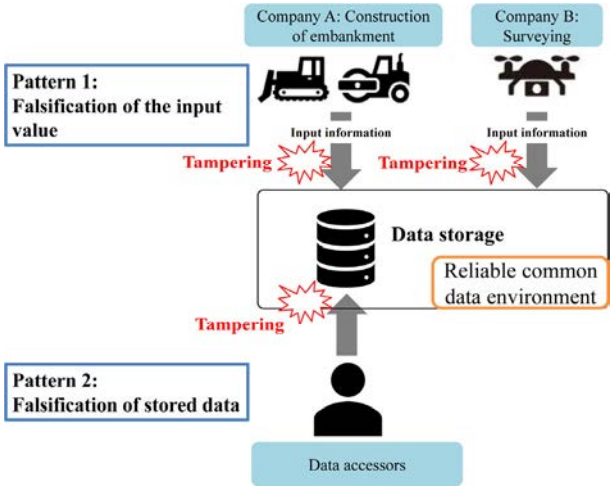

Figure 2. Tampering pattern

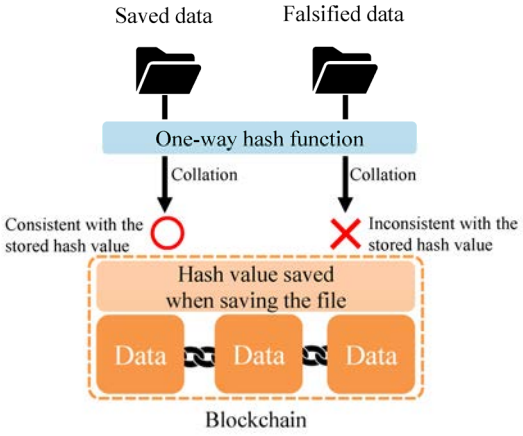

Figure 3. Falsification resistance of stored data

In addition, a company or a person suspected of falsifying data should be traced after the falsification is detected. To realize this, the system design requires an externally owned account [14] at the time of storage of the data to ensure the traceability of the company or the person. This design makes it possible to associate saver information with saved data and to describe it on the blockchain.

4.2 Definition of function for smart contract

When conducting inspections and payments based on smart contracts, the conditions of the contract and the performance of the contract based on those conditions should be managed. For that purpose, "non-tampering information" and "information to be traced at each stage" are needed to be defined appropriately as the functions of the smart contract using a program that implements the

smart contract.

The items of information that should not be tampered include conditions of contract and its performance. Here, conditions of contract cover the following:

- information on contractors (owners and contractors)
- contract amount (unit price and contract amount).

And contract performance includes the following:

- pass/fail of quality and as-built inspection
- construction progress rate by progress measurement
- determination of the payment amount
- management of paid amount on contractors (owners and contractors)

Regarding the conditions of contract, the contents agreed by both parties cannot be changed and tampered by a third party on the network unless both parties allow it. Regarding its performance, the information must not be tampered and updating of the information according to the construction progress should be performed through the joint measurement process. Furthermore, the person who can update the state transition needs to be limited to the client (i.e., project owner).

The information to be input and that to be traced at each stage are determined as shown in Figure 4. Stages 2–5 aim to trace the necessary information (i.e., site ID, contract number, and owner and contractor information) entered when making the contract. The site ID is an ID number assigned to the construction contract and is used to identify the project. The contract number is assigned to the unit price item and is used to identify the contract item. In addition, because inspections and payments are performed between the parties who have signed the contract, the information of the owner and the contractor is traced at stages 2–5. For stages 2 and 3, the obtained results are input from the as-built inspection system and construction progress measurement system. At stage 4, progress payment is made according to the construction progress measurement determined by stages 2 and 3. It is necessary to make the final inspection at completion for the final payment of stage 5, and the performance of construction period, required submissions, and results of the technical proposal, needs to be entered. The final payment is determined by inspection results based on the comparison between the conditions of contract and its performance. The contractor sometimes needs to pay penalty or to receive bonus according to the results based on the conditions of contract.

To handle the performance and its transition on the smart contract, the necessary information is described in the contract ID in strut. Strut is a data type in Solidity and is called a structure type [15], which is prepared by the user to categorize variables described in the contract ID. The categorized variables are shown in Figure 5.

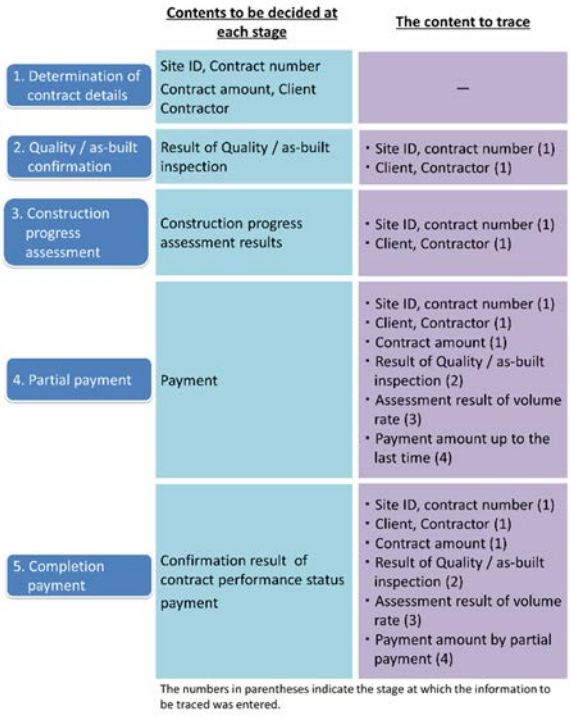

Figure 4. Input and traced information at each stage

In addition, the developed smart contract needs to be placed on the blockchain to execute its function. Several methods are available to place smart contracts on the blockchain; here, Ethereum was used as the blockchain using Truffle. Truffle [16] is a framework for arranging programs that implement smart contracts developed in Ethereum.

Contract performance status	
Item	**Variable name**
Contract ID	contractId
Client account	sender
Subcontractor account	receiver
Contract price	unitPrice
Contract quantity	unitVolume
Construction progress assessment rate that passed quality and as-built inspection	isPassedVolume
Construction progress rate determined by assessment	progress

Figure 5. Schematic diagram of variables categorized by contract ID

4.3 System configuration

To execute quality/as-built inspection, construction progress measurement, and payment, it is necessary to trace the data held by the CDE and to execute the processing according to the purpose. Figure 6 shows the overall picture of the system, including the system that executes these processes. As shown in this figure, the CDE consists of several sub-system.

System for tampering confirmation is the falsification confirmation system to ensures the reliability of the data. This system is used before carrying out the necessary inspections using the as-built inspection system and construction progress measurement system to utilize the information directly for inspection.

System for as-built inspection uses information that detects the presence or absence of falsification by the system of the CDE. It has a function to check whether the acquired information matches within the allowable range described in the standard required by the client, and input the inspection result to the smart contract of the CDE. The as-built inspection system must have this function to check whether the criteria are satisfied and to visualize its results.

The system for construction progress measurement includes functions to save the construction progress rate that the contractor applies for progress payment, to check the construction progress rate by the client, and to determine the construction progress rate. To confirm the applied construction progress rate, it has a function to calculate the construction amount for assessment using the value confirmed by the falsification detection system as an input value.

System for payment amount confirmation has the function to appropriately trace the information for each progress payment and completed payment via a program on the smart contract, and to determine the payment amount.

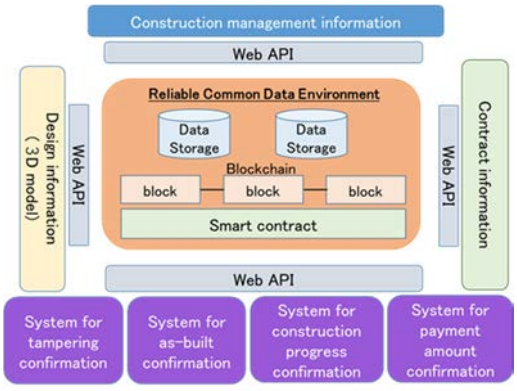

Figure 6. Input information and trace information at each stage

5 Proof-of-concept (PoC) using prototype

In the proof-of-concept, a prototype of a reliable CDE was developed to verify the following two items:

- It is possible to make quality and as-built inspection after confirming that the information produced by the supplier has not been tampered.
- The information of the contract performance status can be updated based on the result of the construction progress measurement conducted by the client or the owner. Furthermore, it is possible to calculate automatically the payment amount by tracing conditions of contract and its performance.

It was applied to the cut and embankment work, and a proof test was conducted. Verification item 1 is the content to be verified for the rationalization of the on-site inspection, and verification item 2 is the item to be verified for the rationalization of payment.

5.1 Outline of PoC

PoC is consisted of two verification tests in total for each verification item1 and item2. In conducting the verification test, the client and contractor participated in the verification test, and each of them played the necessary role. In the verification test, it was verified whether the falsified data and the companies involved in the falsification can be identified. If the falsified data cannot be detected, the product that should be rejected may pass its inspection, which will result in loss of safety and reliability of infrastructure. Therefore, verification is needed whether the falsified data can be detected. For this reason, we rewrote part of the information collected by the contractor from the site and created falsified data intentionally.

5.1.1 PoC for as-built inspection (verification item1)

The verification test related item1 was carried out at Higashi-Saitama Road in Okawado district improvement and other works (embarkment work) project under the jurisdiction of the Northern Capital National Highway Office, Kanto Regional Development Bureau, Ministry of Land, Infrastructure, Transport and Tourism. Figure 7 shows a standard cross-sectional view of the target construction. The inspection items that require on-site inspection include the rolling compaction frequency inspection and as-built inspection, and a verification test was conducted for these two inspections. Table 1 shows the design model and information for this inspection item as a list of input values. Regarding this PoC, a total of seven inspection patterns were prepared for vilification test (Table 3).

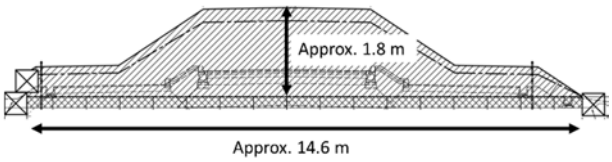

Figure 7. Cross section

Table 1. List of input values

Item	Input value
Design model data	3D design model (LandXML)
Position data for machinery	Coordinate values (x,y,z) and reception time (GNSS data)
Point cloud data	Coordinate values (x,y,z)

5.1.2 PoC for construction progress measurement and payment (verification item2)

The verification test related item2 was carried out using data from the 2018 Kamanashi River channel correction and other works project under the jurisdiction of the Kofu River National Highway Office, Kanto Regional Development Bureau, Ministry of Land, Infrastructure, Transport and Tourism. This project aims to straighten the river channel and excavate the coloured parts in Figure 8. The input values used in the verification tests are listed in Table 2. In this PoC, payment term was set as twice. Regarding this PoC, a total of 9 inspection patterns were prepared for vilification test (Table 4).

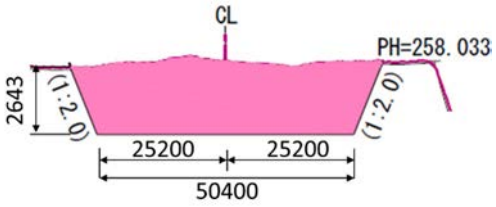

Figure 8. Cross section

Table 2. List of input values

Item	Input value
Design model data	3D design model (LandXML)
Position data for machinery	Coordinate values (x,y,z) and reception time (GNSS data)
Point cloud data	Coordinate values (x,y,z)

Table 3 Inspection pattern for PoC for as-built inspection

No.	Item	Confirmation of quality and as-built	Confirmation of falsification of input value	Judgment
1	Check the number of rolling compactions	Satisfied	Tampered	Failure
2	Check the number of rolling compactions	Satisfied	No tampering	Pass
3	Check the number of rolling compactions	Satisfied	—	Failure
4	Check the number of rolling compactions	Not satisfied	—	Failure
5	Confirmation of as-built	Satisfied	—	Failure
6	Confirmation of as-built	Satisfied	No tampering	Pass
7	Confirmation of as-built	Satisfied	There is tampering	Failure

Table 4 Inspection pattern for PoC for construction progress measurement and payment

No.	Contractor	Partial payment	Confirmation of falsification of saved data	Confirmation of construction progress measurement	Judgment
1	A company	First	Tampered	—	Fail
2	B company	First	—	—	Fail
3	C company	First	No tampering	OK	Pass
4	D company	Second	Tampered	—	Fail
5	E company	Second	No tampering	OK	Pass

5.2 Implementation of PoC

5.2.1 System flow

As shown in the inspection pattern of each verification test, checking the falsification of information is performed on the stored data in the as-built inspection, construction progress measurement, and payment. In addition, for each, the as-built is confirmed, the construction progress is confirmed, and the payment amount is confirmed. Figure 9 shows the overall flow of this system.

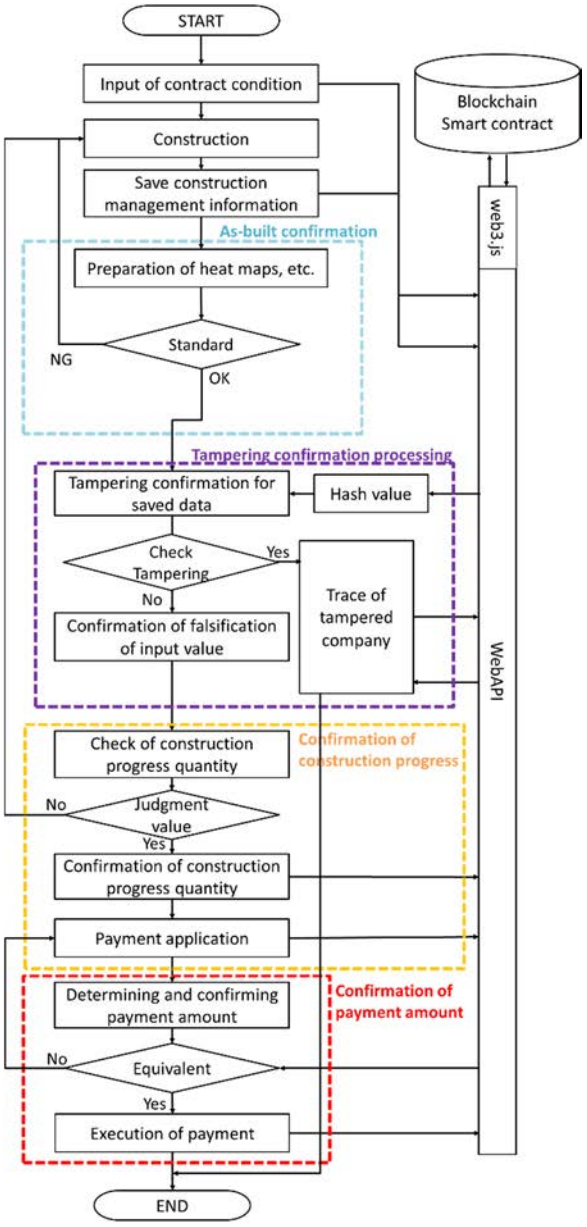

Figure 9. Overall system flow

5.2.2 As-built confirmation

The number of compactions can be checked using a heat map. The required level set by the test construction is six times, and if it is coloured, it indicates that the required level is satisfied. The as-built was also confirmed using a heat map from the design information and point cloud survey results.

5.2.3 Tampering detection process

To check the falsification of the saved data, the URL of the saved data was added to the body and the HTTP request was executed as shown in Figure 10. As a result, a true or false response is returned to check whether the data have been tampered. If true is returned, tampering does not occur; however, if false is returned, the data are tampered. For example, No. 1 (Table 3) returns true, whereas No. 3 returns false.

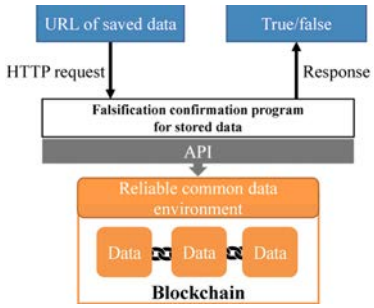

Figure 10. Detection of falsification of saved data

5.2.4 Progress calculation program

The construction amount (excavated soil volume) was calculated from the point cloud data, design model data, and bulldozer blade position information. For the test, an excavated soil model was generated using the extracted blade position information and point cloud data of the site.

5.2.5 Payment

The contractor makes a progress payment by inputting the construction amount using the contract information storage function of the construction progress measurement system. When making a payment, it is first checked whether the applied construction progress rate matches the value confirmed by the measurement stored on the blockchain using the payment confirmation system's functions. If they match, the value obtained by multiplying the contract amount and the construction progress rate is remitted between the owner and contractors. In addition, the amount paid at the time of the second and subsequent payments should be traced.

5.3 Result of PoC

In the verification test related to the as-built inspection, Nos. 1, 3, 4, 5, and 7 (Table 3) were identified as failures. In addition, in the verification test related to the construction progress measurement, Nos. 1, 2, and 4 (Table 4) were failed, and the expected amount of payment was also calculated. Thus, the proposed system was able to identify all instances of tampering, and it is valid to execute as-built inspection, construction progress measurement and payment.

6 Conclusion and future work

In this study, a reliable CDE was designed that utilizes blockchain and smart contracts to ensure the credibility of information, rationalize inspections, and automate payments. It was also confirmed by PoC to the reliable CDE works appropriately to identify falsification of data in quality and as-built, which will secure safety and reliability of infrastructure as well as improve efficiency for quality inspection and measurement. The conclusions are summarized as follows:

1. To detect the falsification of information, the stored data and the input value were assumed to be falsified and the hash value stored on the blockchain was compared with the inspection data.
2. To manage contract information and its performance and to realize inspection and payment based on the contract, “non-tampering information” and “information traced at each stage” were stored in the smart contract. In addition, a system was proposed in which each site ID and contract ID was assigned in a tree structure to handle this information on a smart contract and to update and trace the information appropriately.
3. After checking the falsification of the information, it was confirmed that the quality and as-built form inspection can be successfully carried out.
4. Based on the results of the construction progress measurement conducted by the client, it was confirmed that the smart contract information can be updated as the contract performance status.
5. It was confirmed that the payment amount can be calculated automatically by tracing the contract conditions and contract performance status.

Based on the above, a proof-of-concept for a reliable CDE utilizing blockchain and smart contracts was successful.

In this study, a prototype for an ICT earthwork was developed. Regarding falsification detection of input values, it was possible to directly save the data acquired by the device through WebAPI and to confirm the input values. As a result, the risk of tampering can be reduced.

References

[1] Tateyama K. A new stage of construction in Japan – i-Construction, *IPA News Letter*, Volume 2, 2017.

[2] Turk Ž. and Klinc R. Potentials of blockchain technology for construction management, *Creative Construction Conference 2017*, pp. 638–645 2017.

[3] Kogure J., Kamakura K., Shima T. and Kudo T. Blockchain technology for next generation ICT, *FUJITUS Sci. Tech. J.*, Vol. 53, 2017.

[4] Oinghua L. and Xiwei X. Adaptable blockchain based systems, *IEEE Software*, Voume34, 2017.

[5] Szabo N. Formalizing and securing relationships on public networks, *First Monday 9* , 1997.

[6] Atlay H. and Motawa I. An investigation on the applicability of smart contracts in the construction industry, *ARCOM Doctoral Workshop*, March 2020

[7] Ethereum. On-line: https://ethereum.org, Accessed: 8/January/2023.

[8] Yang R., Wakefield R., Lyu S., Jayasuriya S., Han F., Yi X., Yang X., Amarasinghe G. and Chen S. Public and private blockchain in construction business process and information integration, *Automation in Construction*, Volume 118, 2020.

[9] Luo H., Das M., Wang J. and Cheng J., Construction payment automation through smart contract-based blockchain framework, *ISARC*, 2019.

[10] Sheng D., Ding L., Zhong B., Love P.E., Luo H., and Chen J. Construction quality information management with blockchains, *Automation in Construction*, Volume 120, 2020.

[11] Hesam H. and Martin F. The application of blockchain-based crypto assets for integrating the physical and financial supply chains in the construction & engineering industry, *Automation in Construction*, Volume 127, 2021.

[12] Xingyu T., Moumita D., Yuhan L. and Jack C. Distributed common data environment using blockchain and Interplanetary File System for secure BIM-based collaborative design, *Automation in Construction*, Volume 130, 2021.

[13] Naik R.P. Optimising the SHA256 hashing algorithm for faster and more efficient Bitcoin mining, *MSc Information Security, Department of Computer Science, UCL*, 2013.

[14] Bahg A. and Madisetti V.K. Blockchain platform for industrial internet of things, *J. Soft. Eng. Appl.*, 533-546, 2016.

[15] Andreas M. and Antonopoulos G.W., *Mastering Ethereum*, O’Reilly, 2018.

[16] Truffle. On-line https://www.trufflesuite.com/, Accessed: 8/January/2023.