DOI: https://doi.org/10.13161/kibim.2021.11.1.001

블록체인 기반의 스마트 건설계약 프레임워크

Construction Contract Management Framework Using the Blockchain Technology

추이 진뤼이[1)], 문성우[2)]
Chui, Jinrui[1)] · Moon, Sungwoo[2)]

Received May 12, 2020; Received January 20, 2021 / Accepted January 29, 2021

ABSTRACT: Blockchain is a secure technology that enables transactions between parties without risking data corruption. Besides cryptocurrencies, blockchain technology is being widely adopted in various forms by diverse industries. One promising application is construction contracts. Given that construction projects are executed under strict contractual requirements, blockchain technology–based contracts can ensure that contractual requirements are executed among parties to the contract. The objective of this study is to apply blockchain technology to smart construction contracts and determine their potential feasibility in construction management. In this study, a prototype smart construction contract is presented and its applicability is explored. We conclude that smart construction contracts can be effective as a contractual tool to enhance payment flows in the construction process.

KEYWORDS: Blockchain, Smart Construction Contract, Contractual Parties, Contractual Requirement, Payment

키 워 드: 블록체인, 스마트 건설계약, 계약 참여자, 계약의무사항, 기성지급

1. Introduction

1.1 Background

As a basic concept, a blockchain is an open, distributed ledger that can record transactions between two parties in a verifiable and permanent way. Blockchain technology creates an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but exchanges of virtually anything of value (Tapscott and Tapscott 2016).

More specifically, a blockchain is a list of blocks connected in a series of links. It is time–stamped and interconnected to record transaction data and is managed by a network of computers, sometimes called a miner. Each block of data is secured safely using cryptographic hash values.

Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks in the blockchain, which requires majority consensus within the network. This no–alteration security is the most characteristic aspect of blockchain technology.

Blockchains are decentralized networks, meaning that there is no centralized control organizer. All participants in a blockchain may be required to approve transactions, although depending on management policy, the approval rate may differ. Therefore, blockchain technology enables transactions between parties without risking data corruption.

Due to these unique characteristics, blockchain technology is growing ever more popular among various industries. Besides cryptocurrencies, blockchain has been widely adopted in various industrial applications, including smart contracts (Kim, 2019), distributed ledgers (World Bank, 2018), video games (Curran, 2019), logistics (Heutager, 2018), and voting systems (CoinBundle Team, 2019), among others.

1) 학생회원, 부산대학교 석사과정 (cuijinrui@pusan.ac.kr)
2) 정회원, 부산대학교 토목공학과 교수 (sngwmoon@pusan.ac.kr) (교신저자)

Considering the scale and diversity of construction management, blockchain technology has an excellent chance of being adopted for project management in the construction industry. In this respect, Penzes (2018) argues that blockchain can integrate often-fragmented construction processes, making them more efficient, transparent, and accountable for all project participants. Penzes also states that blockchain can be applied in payment and project management; procurement and supply chains; and smart asset management.

Hughes (2017) also argues that, since construction projects bring together large teams to design and shape the built environment, blockchain can be used to streamline the construction management process. Hughes identifies four potential areas for blockchain application: 1) recording exchanges of value; 2) administering smart contracts; 3) combining smart contracts to form a decentralized autonomous organization; and 4) certifying proof of existence for certain types of data.

Blockchain technology has promising applicability for smart construction contracts. Since construction projects are executed under strict contractual requirements, a blockchain technology-based contract can ensure these requirements are met between the contractual parties.

This study presents a prototype smart construction contract and aims to identify its benefits in improving the effectiveness of the construction management process.

1.2 Research Objective and Procedure

The objective of this study is to apply blockchain technology to smart construction contracts and thus to determine its potential applicability in the construction process. In this study, a prototype smart construction contract has been developed in order to understand its potential benefits. Our conclusion is that smart construction contracts can be an effective contractual tool to enhance the flow of supply chain management.

Figure 1 illustrates the research procedure. As the figure shows, this study is organized in five steps. First, current construction contract practice is analyzed to determine requirements for a smart construction contract. Second, technical aspects of blockchain technology are studied. An overview of the technical terms used in this study is presented in Section 3, "Blockchain Overview." Third, a smart construction contract framework is designed to provide an environment in which contractual parties can execute a secure payment process. Fourth, the smart construction contract is prototyped and applied to a hypothetical example. Finally, the findings of the study are evaluated and implementation of the smart construction contract framework in the construction sector is recommended.

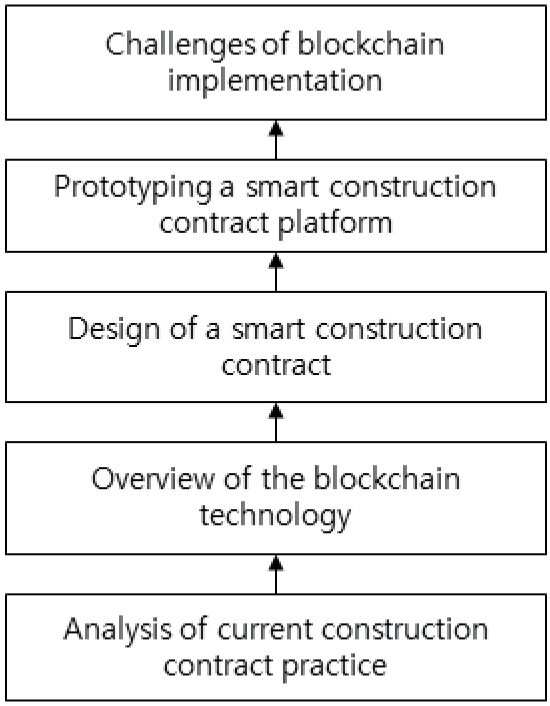


Figure 1. Research procedure

2. Literature Review

Blockchain technology creates profound challenges and opportunities in industrial development. Li et al. (2018) discuss the operational theory of blockchain and its application in financial and nonfinancial fields. For example, in the financial field, blockchain technology can be used for digital asset records, while nonfinancial applications include authenticity verification, decentralized storage, and decentralized compound networking.

Li et al. also argue that blockchain can facilitate large-scale collaboration in a decentralized and untrustworthy way. As such, many contexts are appropriate for blockchain applications, not only in finance but also in a wide range of contexts such as the Internet of things, renting, and others.

However, blockchain technology is currently in its infancy. Although blockchain-based applications can be found in social media and business processes, the full range of application is yet to come. The innovative use of blockchain also faces certain risks, including blockchain oversize, high barriers to entry, and criminal behavior (Tapscott et al. 2018)

Zhu (2018) defines the concept and characteristics of blockchain technology as applied in China, and provides three use cases in the Chinese construction industry. The first is auxiliary verification of engineering bidding. The tamper-proof nature of blockchain technology is capable of assuring authenticity and can make the bidding process more transparent and reliable, effectively reducing transaction costs.

The second use case involves improving engineering quality and accident traceability. The traceability of blockchain technology is useful in quality and safety investigations for construction projects, and can quickly and clearly verify any steps not performed in accordance with quality and safety standards.

The third use case combines blockchain technology with building information modeling (BIM) technology in collaborative BIM modeling and sharing. When BIM is applied to construction, all parties involved in the process contribute to BIM management. Blockchain can be used to track the project management process.

Li et al. (2018) believe that existing studies addressing UK-based blockchain applications within construction and the built environment have ignored the interrelation of social and technological dimensions. To address this gap, they propose a multi-dimensional emergent framework for distributed ledger technology (DLT) adoption within the construction sector. This framework was developed following a focus group discussion and took a socio-technical systems approach encompassing three dimensions: political, social, and technical. The framework was overlaid with an extensive set of construction-related challenges and opportunities and identified a number of associated agents across the dimensions. The structuring of interconnected dimensions provided by the framework can be used by field researchers as a point of departure for investigating a range of research questions from political, social, and/or technical perspectives.

In Korea, Lee et al. (2018) have investigated the problem of personal information leakage and invasion of construction workers' privacy in sensor networks used for safety management on construction sites, and they examine the applicability of blockchain technology as a solution to this problem. In this research, Lee et al. construct a framework for sensor networks that secures workers' privacy, and propose enhanced personal information security through utilizing blockchain characteristics such as decentralization, security, anonymity, speed, and scalability.

Choi et al. (2018) state that although blockchain is a core technology of the fourth industrial revolution, there is no remarkable service, and for the most part remains in the design and planning stage. In order to implement blockchain technology, it is necessary to develop various relevant use cases, export appropriate business models, and establish the direction of technological development.

Kang (2018) untangles the relationships among blockchain, BIM, and smart contracts in the construction sector. The possibility of applying a smart contract framework to the content and mode of building-infrastructure services is under study. In the field of overseas construction, plans are being developed for introducing smart contracts at contract signing.

In addition, in order to verify the batch chain operation mechanism that forms the basis of smart contracts, Kang investigates an Ethereum platform-based approach to smart contract approach. Finally, Kang describes necessary preconditions and for applying blockchain in smart city or construction contracts and the results of doing so.

3. Blockchain Overview

3.1 Sequence Diagram

A blockchain is made up of a series of blocks and is created with the use of hash functions. Besides these functions, the blockchain comprises many other technical features that are involved in realizing a decentralized and distributed environment in which stored data cannot be altered without the consent of participants.

Descriptions of blockchain characteristics can be found in many references (e.g. Crosby et al., 2016; Ammous et al., 2016). This section gives a technical overview of the aspects of blockchain technology needed for building a smart construction contract.

The first block of a blockchain is the genesis block (Figure 2). The main chain consists of the longest series of blocks from the genesis block to the current block. Orphan blocks exist outside of the main chain. A new block is typically added every ten minutes.

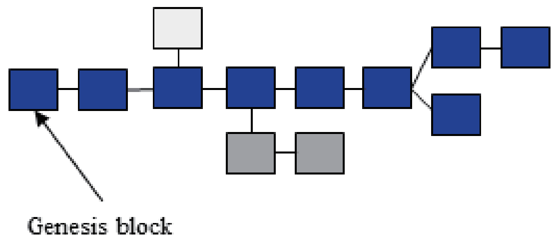


Figure 2. **Blockchain structure**

Each block in a blockchain is connected in sequence using the previous block header. Each block is connected to every previous block via that block's hash. Since all these blocks are connected to each other, blockchain forms an immutable connection.

A block header comprises the following information: version, previous block hash, merkle hash tree, time stamp, difficulty bits, and nonce. Each leaf tree of the merkle hash tree is converted into hash values, two of which are merged into the upper level of parent hash values. The top hash value is included as one of the header files. The time stamp is the time at which the block was generated.

Proof of work is a computational piece of work used to find a number that can be converted into the block's hash number. Proof of work creates effort in finding the nonce value that can produce hash values lower than a certain hash value. Miners, which try to find the number, compete with each other to find the nonce value fastest, and are rewarded with cryptocurrencies.

A hash function converts data into an output of fixed length. A cryptographic hash function cannot be computed in the reverse direction. SHA-256 (SHA-2) is the most widely used hash in blockchain (SHA stands for secure hash algorithm), and converts all data into a 256-bit output.

Distributed ledgers are groups of nodes in a network that share the same database information regardless of location and affiliation. Each node holds the same copy of the ledger, and changes in the ledger are synchronized to all copies of the ledger within a very brief time interval. Blockchain is a representative technology for distributed ledgers. Its key innovation is that not only is it a database but it can also be used to specify business rules. Traditional databases usually specify rules for the database as a whole or for the application layer, but blockchain can design rules directly for transactions.

The first characteristic of distributed ledgers is decentralization. The rights of all nodes are equal and the data is jointly maintained by the nodes using system maintenance functions. The second is that the ledger information cannot be tampered with. Once information has been verified and added to the ledger, it will be stored permanently. So the data stability and reliability of distributed ledgers are extremely high.

Blockchain 1.0 denotes the first generation of blockchain technology, used for decentralization of money and payments. Bitcoin is a representative example, a cryptocurrency that is traceable and can be transacted directly between two individuals over the Internet.

3.2 Categories of Blockchain

There are two types of blockchain: public and private. In a public blockchain, anyone can participate in the network, executing the consensus protocol and maintaining the shared ledger. Thus, anyone can join the blockchain and read and write to it (Zheng et al., 2017). Therefore, no transactions are private: every participant can see each transaction. No one party has control over the blockchain. The most representative examples of public blockchains are cryptocurrencies (Kosba et al., 2016), in which every cryptographic currency user can see trading transactions shown in the ledger blocks.

Private blockchains only allow those who are invited to participate in a permissioned network (Pongnumkul et al., 2017). Depending on policies, blockchain participants may or may not be able to read and/or write. An individual party can have control over the blockchain. The most representative private blockchain is Hyperledger, a multi-project open source collaborative effort hosted by private companies (Cachin, 2016).

Since a smart construction contract involves only those contractual parties involved in the construction process, the contract framework is implemented using a private blockchain.

3.3 Smart Contracts

A smart contract is a set of blockchain rules by which the contract participants agree to be bound in their interactions with each other (Blockchain Hub, 2019). Blockchain Hub states that smart contracts can facilitate, verify, and enforce the negotiation or fulfillment of an agreement or transaction.

In this context, a smart contract is a protocol that performs various contractual functions, using blockchain technology to build self-executing components and express terms in logical statements (Swan, 2015).

When implemented in the construction sector, smart contracts offer three major benefits (Wang et al., 2017):

1) Elimination of payment and cash flow problems: Cryptocurrencies are stored in the smart contract to prevent late payments and protect contractors during the construction process. These smart contracts can be connected to each other to create payment networks. For example, when a construction project reaches a payment milestone, the smart contract automatically pays the general contractor on behalf of the owner.

2) Efficiency gains in the contract management process: In contrast to traditional contracts, smart contracts can automate the construction process and save significant contract registration, monitoring, and update time.

3) Reconstruction of trust behavior from human to coded trust: The smart contract can replace lawyers and enforce business rules through blockchain-based contracts and litigation. Blockchain makes it easier for contractual parties to trust each other without the expense of relying on lawyers.

4. Prototyping a Smart Construction Contract Framework

4.1 Current Construction Contract Practice

The construction industry is based on orders: the construction process starts when contractual parties initiate an order by signing a contract that specifies certain contractual requirements (Figure 3). When the contract is signed, the contractual parties are bound by the contractual requirements, forming a temporary team with the common goal of completing the construction project. Therefore, the contract plays a critical role in project success.

Besides being written into the contract at the start of a project, contractual requirements should be reviewed throughout the construction process. One example is the owner's responsibility to make progress payments. During construction, the owner should pay the contractor in installments for work that has been done on schedule. Equally, the contractor should also meet technical requirements for specifications.

Traditionally, there is a likelihood that contractual parties will ignore contractual requirements, leading to legal disputes. Such lack of awareness around contractual requirement may be the main cause of construction claims.

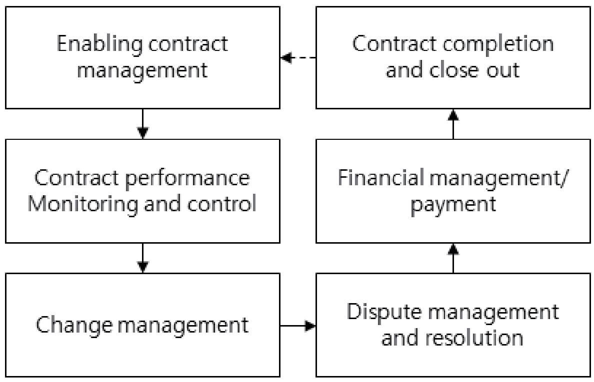


Figure 3. Construction contract procedure

4.2 Example Scenario for a Smart Construction Contract

A smart construction contract would be implemented at many points in the construction process, such as bidding, procurement, supervising, inspection, payment, installation, and authorization. Blockchain, being tamper-proof and non-editable, ensures the credibility of contractual requirements.

All contractual parties need to agree if any contractual change is made in the contract. Since contractual requirements are automatically executed, the construction process can become faster and more productive.

Since a smart construction contract would involve only the contractual parties to the construction process, the contract framework should be implemented using a private blockchain. Depending on policy guidelines, participants may or may not have read and/or write permission.

Figure 4 shows the sequential flow of data or actions of entities for a smart construction contract in a simulated environment. The elements of this sequential diagram include each contractual party: 1) owner, 2) construction manager, 3) contractor, 4) subcontractor, 5) materials supplier, and 6) equipment supplier. These parties participate in the smart construction contract to ensure secure, reliable transfer of all assets.

The diagram also shows the smart construction contract as being executed using blockchain technology. Contracts are made at each step and are saved in revocable blockchain contractual forms. Each node in the blockchain network will automatically supervise each step of the smart contract. In case of problems with subsequent transactions, such as claim applications or an accident investigation, the accountability clauses of the smart contract will automatically take effect and oblige each party to perform their contractual obligations as agreed.

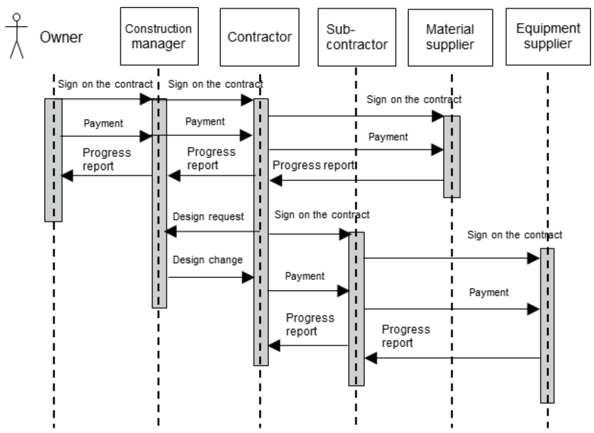
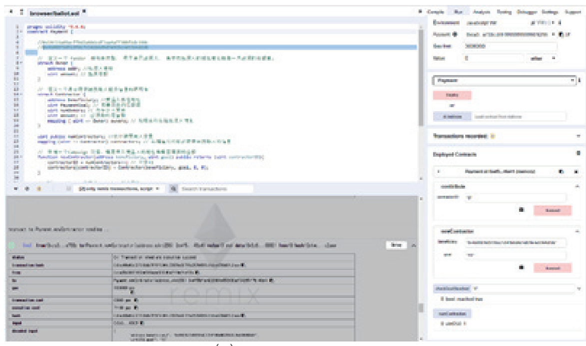


Figure 4. Sequential diagram for a smart construction contract

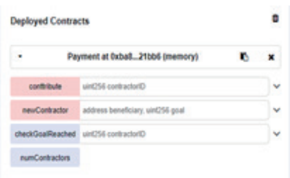
4.3 Program Development

In blockchain technology, a distributed accounting function is used to write program code for the authentication system, whose role is to protect contractual information through encryption and remove the risk of legal disputes. This system uses private and public keys to prevent data tampering and protect the security of contractual participants' job progress records and any other related information.

Figure 5 shows an example of a smart payment contract developed using Remix, an integrated development environment for the intelligent contract programming language Solidity. An object-oriented language, Solidity can be used for implementing smart contracts (Dannen, 2017). Remix generates as a private chain a JSVM (Joint Scalable Video Model) environment for developers to test smart contracts.



(a) Remix interface

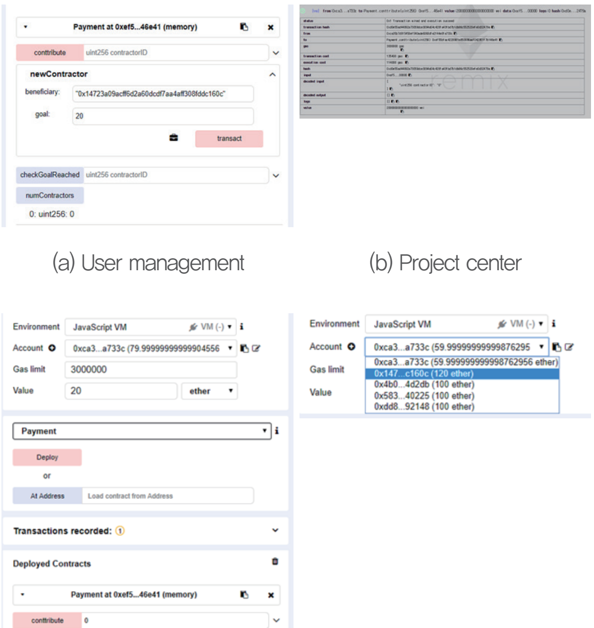


(b) Coding example for payment (c) Smart payment contract

Figure 5. Prototype Remix program for smart construction contract

This smart payment contract enables the owner to send money to the contractor using a contractor ID in a simple and secure manner. The owner can check that the payment amount is transacted as intended. A smart payment contract of this kind could also be applied to a contracted payment between the contractor and the supplier.

This case assumes that the contractor needs to be paid 20 Ether coins (1 Ether = $210.19 at the time of writing). In this contract environment, the owner can add a new address for the contractor to the contract and select the option that the contractor needs to receive 20 Ethercoins (Figure6(a)). The contractor is assigned a contractor ID of “0” from the system (Figure 6(b)).



(a) User management (b) Project center

(c) Smart contract (d) Settlement

Figure 6. User interface for smart construction contract platform

Figure 6(c) shows the user interface through which the owner pays 20 Ether coins to the contractor with ID “0”. The balance of this contractor’s account will be increased by 20 Ether coins as shown in Figure 6(d). The owner can then check that the amount received is up to contractual standard by entering the contractor’s iD. If so, the interface will display “true”; otherwise it will display “false”.

4.4 Payment Platform Modules

The payment platform prototyped in this study can be used to verify the integrity and authenticity of the project and the information in the transaction process. Information queries are limited to transaction information and also user information as to whether either the owner or the contractor is hidden from public view. Only the project participants can see each others’ details, through a private key.

As Table 1 shows, the payment platform is divided into the following four modules:

(1) The user management module is dedicated to login and registration. When the participant logs in for first time, data is submitted to the blockchain platform during registration. Participants are thus identified and can be assigned different levels of authority for system access.

(2) The project center module retains project information, participant information, individual contracts, contractual requirements, general and technical specifications, and other related information. In this platform, project progress and schedule are updated as prompted by contractual requirements on the construction progress timeline.

(3) The smart contract module is where actual contractual activities are recorded and activated for execution. These activities may involve adding accounts to contracts, sending money, verifying compliance, and so on. The contractual parties are obliged to conform to contractual requirements according to the agreed conditions.

(4) The settlement module handles earnings and dynamic funds, and completes monetary transactions. That is, this settlement module checks job progress and proceed with construction payment. The process in this module is important to verify the work that has been done and remove future contractual disputes. For example, in construction payment, the contractor should meet the contractual requirements in quality and assure the work amount that has been finished. If the two-way consensus is reached in this process, the contractor can be paid for the construction payment.

Table 1. Payment platform modules

Project	1st Level (Module)	2nd Level
Case study project	User management	Registration management
		Key management
		User management
		Role attribute
	Project center	Key management
		User management
		Role attribute
	Smart contract	User management
		Role attribute
	Settlement module	User management
		Role attribute

4.5 Application to the Transactional Process

Figure 7 shows, in five steps, the transactional process as implemented through the payment platform.

(1) Project initiation: The smart payment contract is set up by the owner to start the project. The owner adds contractor address(es) to the contract. The contractor's account is registered, and the contractor is assigned a private key. After private key has been generated, all the information is saved in the project center. That is, the construction contract system can generate a private key for the contractor. Then, the contractor can use the private key to open the information that is saved in the project center.

(2) Successful linking: The owner and contractor are connected if their private keys match correctly. Also, the private and public keys are used to verify construction documents and maintain authenticity. When the owner and the contract both verifies the authenticity of the payment documents, the system transfers the payment to the contractor.

(3) Contract signing: The contract agreed by the owner and the contractor is coded onto the blockchain to form a smart payment contract. When a contractually agreed portion of the project reaches completion, the owner can have the payment directly transferred to the contractor's account. These direct monetary transactions tend to improve operational efficiency and help to avoid or deter illegal foul play between owner and contractor.

(4) Execution: Smart payments are automatically executed according to the contract. If the contractor does not receive the payment stipulated in the contract within the time specified, the smart payment contract will enforce transfer of this payment to the contractor's account. Such strict control of contractual requirements not only ensures reliability of payment but also enhances the contract's binding force as a deterrent to intentional default.

(5) Project execution settlement: Finally, when the contract ends, a completion report is transferred to the user and project center for record keeping.

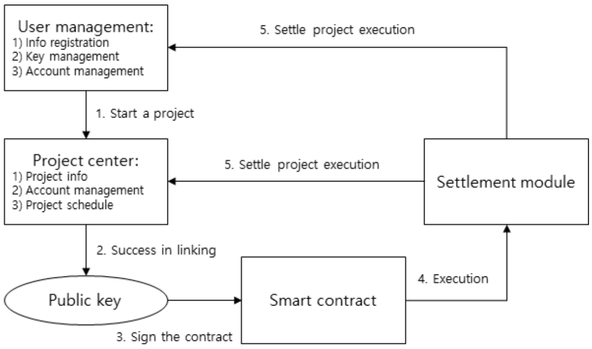


Figure 7. Payment transaction process

5. Conclusion

This paper discusses the application of blockchain technology in smart construction contracts, which are studied as a way to promote automatic procurement and payment in construction projects. This new contract approach is expected to improve transparency and traceability along the construction supply chain.

The prototype smart construction contract developed in this paper demonstrates the potential application of blockchain technology to the construction industry. Although the prototype focuses on transactions between the owner and the contractor, such payment transactions can be applied to each aspect of a construction project.

When applied to actual construction contracts, more contractual details can be built into the smart construction contract framework to realize the construction process fully. For example, smart construction contracts can stipulate that the owner pays the contractor for completion of each construction activity. Blockchain-based smart contracts enable the project participants to understand the procedural sequence and track the implementation of the construction contract. This kind of coordinated effort fosters team work, and could ultimately remove any future disputes and claims.

There are many issues that need to be addressed in applying the blockchain technology to construction contract. In this sense, this study has limitations that should be further studied in future. First, the contractor can pay the construction payment using bitcoins. However, the bitcoin value has a high volatility which makes it difficult to predict future value. In this context, bitcoin might not be a feasible means for construction payment. However, the bitcoin value can be recalculated with regard to the current currency value to overcome the volatility. A conversion model can be also built to interlock the difference between the bitcoin and the monetary values when the construction payment is paid. Second, construction documents should be stored in the smart construction contract system using hash functions and linked to the payment function when developing an actual smart construction contract system.

Blockchain technology is now flourishing in every industrial sector, and the smart construction contract has a good chance of adoption by the construction industry. Although smart construction contracts could initially be disorienting for users and could therefore face barriers to adoption, there are great benefits available to construction project participants from its application to the construction sector. Looking ahead, additional case studies are expected to explore various contractual scenarios in construction projects so as to assess the effectiveness of smart construction contracts.

Acknowledgments

이 논문은 부산대학교 기본연구지원사업(2년)에 의하여 연구되었습니다.

References

Ammous, S. (2016). Blockchain technology: What is it good for? Lebanese American University, SSRN, F30(O31).

Blockchain Hub (n.d.). Smart contracts. Retrieved from https://blockchainhub.net/smart-contracts/

Cachin, C. (2016). Architecture of the hyperledger blockchain fabric. IBM Research, CH-8803.

Choi, S. I., Sim, S. B., Jeon, C. J., Kim, C. Y. (2018). Development of international trade system using blockchain technology and validation of utilization in construction industry. Korea Institute of Construction Technology, pp. 1183-1184.

CoinBundle Team (n.d.). Using blockchain for: Voting. Retrieved from https://medium.com/coinbundle/using-blockchain-for-voting-3287817291dc

Crosby, M., Pattanayak, P., Verma, S., Kaly, V., Nachiappan. (2016). Blockchain technology: Beyond Bitcoin. Applied Innovation Review, 2.

Curran, B. (n.d.). Blockchain games: The current state of blockchain gaming technology. Retrieved from https://blockonomi.com/blockchain-games/

Dannen, C. (2017). Introducing Etherium and Solidity. New York, NY: Springer Science + Business Media. pp. 89-110.

Heutger, M. (2018). Blockchain in logistics. DHL Trend Research, DHL CSI, 53844.

Kang, T. W. (2018). Blockchain-based BIM, smart contract concepts and trends. Information Science Institute, 36(5).

Kim, E. B. (2019). Patent trend analysis of block chain Technology: Focus on smart contract field. Korea University Graduate School of Management and Technology. I804:11009-000000082601.

Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C. (2016). The blockchain model of cryptography and privacy-preserving smart contracts. Sixth IEEE International Congress on Big Data, 55.

Lee, H. R., Song, S. H., Yoon, H. S., Hwang, S.J. (2018). Construction of a sensor network framework based on the blockchain technology with enhanced safety and privacy security for construction workers. Proceedings of the Autumn Conference of the Architectural Institute, 38(2) (Korea).

Li, J., Greenwood, D., Kassem, M. (2018). Blockchain in the construction sector: a socio-technical systems framework for the construction industry. Northumbria University, UK, Conference paper.

Pongnumkul, S., Siripanpornchana, C., Thajchayapong, S. (2017). Performance analysis of private blockchain platforms in varying workloads. Sixth IEEE International Congress on Big Data, 17.

Reiff, N. (2020). Why Bitcoin Has a Volatile Value. Investopia. Retrieved from https://www.investopedia.com/articles/investing/052014/why-bitcoins-value-so-volatile.asp

Tapscott, D., Tapscott, A. (2018). Blockchain revolution: How the technology behind Bitcoin and other cryptocurrencies Is changing the world. New York: Penguin Random House LLC. pp. 96-130.

Wang, J., Wu, P., Wang, X., Shou, W. (2017). The outlook of blockchain technology for construction engineering management. Higher Education, 4(1), pp. 67-75.

World Bank (2018). Blockchain and distributed ledger technology. Retrieved from https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt

Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H. (2017). An overview of blockchain technology: Architecture, consensus and future trends, Sixth IEEE International Congress on Big Data, 85.

Zhu, Y. (2018). Application scene prospect of block chain technology in the construction industry. Engineering Economy, 28(6).