Construction Payment Automation through Smart Contract-based Blockchain Framework

H. Luo[a], M. Das[a], J. Wang[b], and J.C.P. Cheng[a]

[a]Department of Civil and Environmental Engineering, the Hong Kong University of Science and Technology, Hong Kong
[b]Australasian Joint Research Centre for Building Information Modeling, Curtin University, Australia
E-mail: hluoaf@connect.ust.hk, moumitadas@ust.hk, Jun.Wang1@curtin.edu.au, cejcheng@ust.hk

Abstract –

A construction contract facilitates payments through the supply chain by integrating people, activities, and events throughout the project period through obligations, permissions, and prohibitions in its terms and conditions. The management of payments is a manual process and is more difficult in the case of construction projects as different stakeholders at different levels of the project organizational structure are bound by different contracts. Moreover, payments are strongly affected by the lack of clarity in the definitions of the obligations, responsibilities, and liabilities of various stakeholders in construction contracts. This intensifies disputes and causes delays in construction payments leading to additional expenditure, cash flow problems, and lack of trust. Therefore, to address these problems, we propose a methodology to automate construction payments by formalizing them into smart contracts and executing on a decentralized blockchain based framework. We formalize the payment logic that binds the prohibitions and liabilities associated with financial commitments, such as interim payments on completion of tasks in a construction project, and convert it into a computer-executable code. A framework based on blockchain is used to host this smart contract and to automate actions such as the triggering of payments after achieving consensus among the relevant project stakeholders. This framework also address the conditions required for the security of information in construction projects, such as confidentiality and information integrity in a multi-party environment. The proposed framework is demonstrated through a case-based scenario.

Keywords – Blockchain; Smart Contracts; Construction Projects; Interim Payments

1 Introduction

Construction projects often suffer from payment problems. Due to the adversarial working relationships of different stakeholders, and the complexity and uncertainty of the construction environment in Hong Kong construction projects, the outstanding payment amount was reported to be over HK$20 billion in 2015[1]. The solution to payment problems in construction projects greatly depend on the execution of construction contracts, which regulates the behaviour of the stakeholders by holding them accountable through commitments, prohibitions, obligations, and liabilities. It is the foundation for information management, claims, and payments, and therefore is a key to successful project completion. However, the execution of construction contracts is a complex process and faces many challenges, such as delays in payment [2]. A contract is said to have been breached or halted in cases such as defaulting on payment due to lack of funds or disputes on unsatisfactory quality of work. These problems escalate due to the ambiguity of language in the identifying responsibility, authority, and prohibitions described in the contracts. Moreover, the process of contract management is slow due to the fact that consensus among stakeholders is required for decision making. Achievement of consensus is preceded by several levels of approval from the stakeholders from various organizations, and therefore an immutable audit trail must be kept in order to prevent any disputes in the future. Previous research proposed measures to improve construction contract management. For example, standard construction contracts have been proposed by many countries and regions as references for contract formalization for specific types of construction projects, such as the FIDIC contract [3]. However, standard construction contracts focus on the improvement of the contract structure and are still difficult to interpret by individuals who are not lawyers by profession. To simplify contract management, e-contracts have been proposed. E-contracts are created by analysing relationships between the contract participants and contractual information, followed by modelling traditional textual contract in xml format [4]. However,

current applications of e-contracts are mainly found in electronics trade, where the complexity of relationships between parties, obligations, and activities is simpler compared to that in construction contracts. Therefore, a framework that improves the current state of construction contract management by addressing the challenges due to complexities and inherent nature of the construction industry is required. In this paper, we propose a blockchain based framework to facilitate semi-automatic contract execution and consensus achievement for the construction industry. Blockchain was selected for the proposed framework because it possesses the following characteristics: (1) information sharing among multiple parties; (2) information updating among multiple parties; (3) verification/approval at several levels [5].

The general architecture of blockchain is comprised essentially of a shared ledger. Every participant in a blockchain stores a local copy of this ledger in his/her database. The integrity of information in each local copy is maintained as they can be altered only upon achieving consensus by the majority of the participants. Information security and integrity is ensured through cryptographic techniques and consensus mechanisms. In general, there are three types of blockchain - public blockchain, private blockchain, and permissioned blockchain. A public blockchain network is open for anyone to join and host information. The BOPTI project utilized Ethereum, a well-known public blockchain platform, to issue their cryptocurrency, attracting customers through the reward mechanism [6]. Unlike public blockchains, private blockchains have a closed network and is owned by one controller. For example, it is especially useful for a closed network of banks. The private blockchain system has been used to store construction-related transactions by SiteSense software [7]. However, the construction industry may require access control mechanisms to allow or reject participants joining certain transactions. Therefore, a permissioned blockchain is most suitable for construction projects. In a permissioned blockchain, participants can join by invitation and require access rights to read or write from the blockchain, therefore adapting to the intrinsic feature of decentralization in the construction industry and the complexity of construction contracts. Thus, we propose a permissioned blockchain based framework to formalize and execute smart contracts. Our methodology includes contract formalization and a framework for automated contract execution. The methodology is supported by a case-based scenario that demonstrates its key features and advantages, such as information integrity, security, and transparency.

2 Methodology

In this study, a framework is proposed to automate payments in construction projects by formalizing construction contracts into smart contracts. The contract is executed on a blockchain based decentralized framework which supports the achievement of consensus for decision making based on the conditions of the smart contract. The methodology is divided into two parts - (1) contract formalization and (2) contract execution.

2.1 Contract Formalization

In this section, we describe our methodology for converting construction contracts into smart contracts for automatic interim payment. Construction contracts (such as HKGCC [9]) were studied to identify the general concepts of construction contracts, such as parties and activities and the logic relating them. Based on this study, data representation for smart construction contracts and the formalization of logic was done. The methodology for contract formalization as follows:

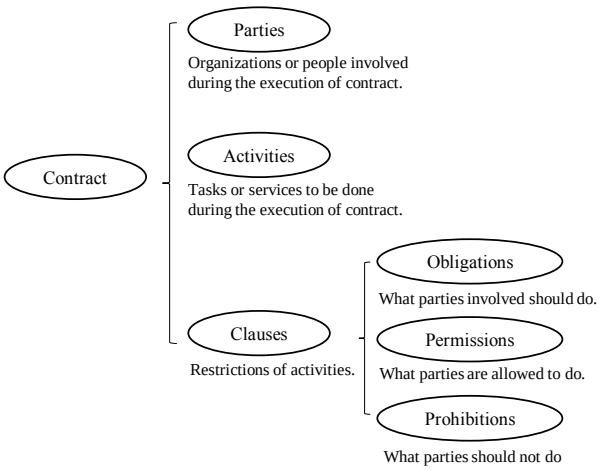

Figure 1. General structure of a construction contract

1) As shown in Figure 1, data representation for smart construction contracts was developed. Contract clauses were analyzed and key concepts were extracted, such as parties, activities, triggering events, conditions, actions, and resultant events.
2) Construction contracts were studied to identify and formalize the logic for executing smart contracts. For example, the relationship among parties and the sequence in which they are supposed to execute their responsibilities were identified. The parties involved in a construction contract for interim payment are

the contractor, inspector, quantity surveyor, engineer, and employer.

During the payment process, the obligation of a contractor is to submit an application with supplementary documents and to the initiate interim payment procedure. The inspector is supposed to check the correctness of all quantities claimed by the contractor followed by the quantity surveyor who is responsible for checking the correctness of the valuation in the payment claim and so on as shown in Figure 2.

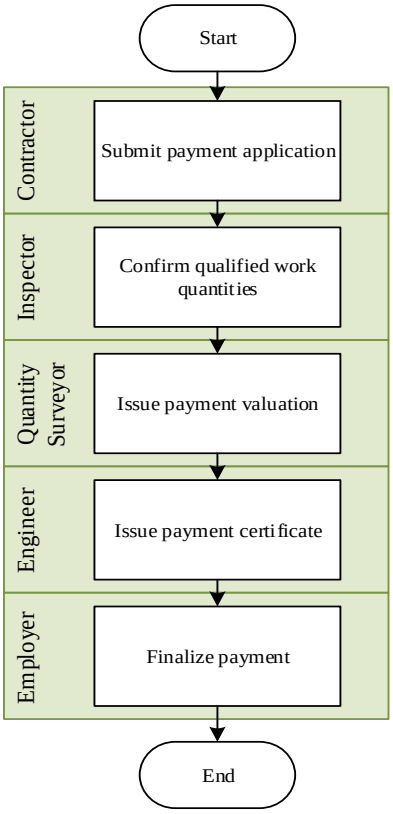

Figure 2. The sequence of activities and participants for interim payment

At the end of this process, interim payment should be triggered. This logic was converted into pseudocode and then into executable code using JavaScript. The conversion process is illustrated with an example scenario in Section 4.

2.2 Automated Contract Execution

The execution of the smart contract is done through a permissioned blockchain based framework and has two parts – (1) A automated consensus process based on pre-defined conditions of the smart contract and (2) a manual process which requires an input from the authorized stakeholder. In a blockchain based framework, information is stored in the two data models – one is for recording transactions which represents the action done by the authorized stakeholder, called the ledger, and another data model, called the asset model, is for checking and recording current values of construction data assets such as tasks and payments. All the project participants store the same construction information in their local asset data models and ledgers. The asset model is based on the transactions recorded in the ledger. The ledger is the actual backbone of blockchain which is an unmodifiable cryptographically linked storage structure, and therefore is a trusted source of information.

At the beginning of the contract execution process, a project participant, for example a contractor in this case, submits a request for payment. When the transaction of payment application is received by the following project participant which is the inspector in this case, the process of automatically achieving consensus begins. The incoming data is stored locally with every participant in a pre-defined data model, from where it is evaluated by the smart contract. Smart contracts are executed automatically to check pre-defined conditions of standard prohibitions and obligations (as discussed in Section 2.1). These pre-defined conditions check the validity of the incoming request by assessing information such as price, quantity of material, and other construction information against information such as historical records of payment and variations, stored in their local asset model. Consensus is achieved when all participants either approve or disapprove the proposed request according to the results of executing the smart contract on their local systems. After consensus on the correctness of a transaction is achieved, the transaction is added to the blockchain. This transaction contains information on who approved what (for example, who approved the payment application, quantity checking, and quality inspection results and so on), along with a timestamp, and is digitally signed by all the participants. Meanwhile, the asset model is be updated according to the transaction, which becomes the reference for validating later transactions. After this, the control is passed for manual input to the next project participant (which is quantity surveyor, as shown in Figure 3). It is to be noted that there is manual and automated consensus at each level of approval. During the manual approval part, the authorized participant has the right of approval or refusal based on existing information from the local asset model. The approver may also check other information manually, such as through on-site inspection, and may use his/her professional judgement to make a decision. After that, the decision is manually inputted by approver. The execution progresses through a series of manual inputs and automatic consensuses till the end of the approval process is reached. At every

stage, actions on construction data are recorded by transaction models in the blockchain ledger, which is unalterable. Therefore, at a later stage such information can be used for audit trail for identifying a defaulting participant or the responsible person for a project delay.

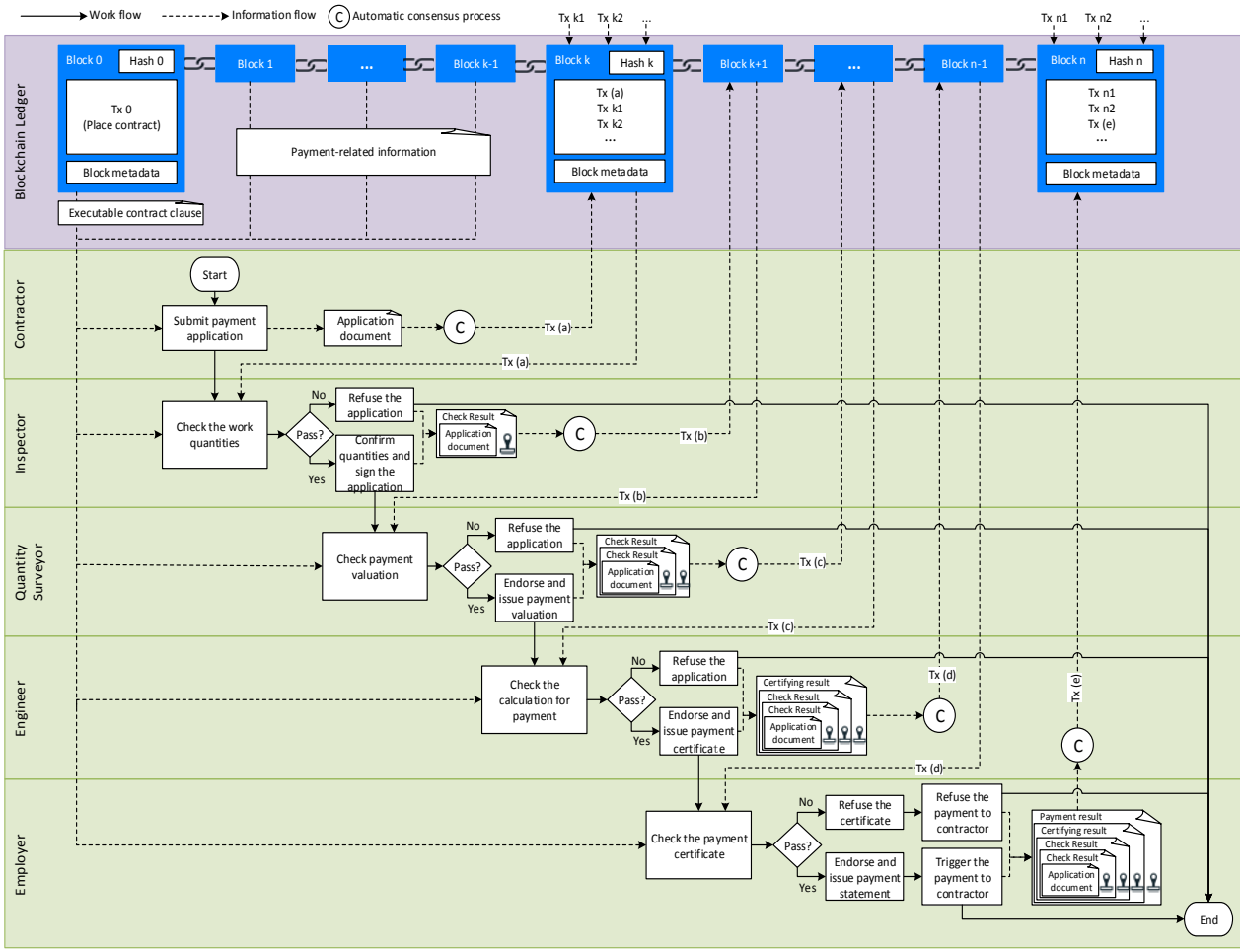

Figure 3. The semi-automatic blockchain based framework for interim payment

3 Contract Security Protection

In this section, we discuss the security related features of the proposed framework, which allows participants to come to a common consensus with verified endorsement in a secure fashion, without having to meet face-to-face. To do this, the framework implements blockchain based cryptographic protocols for the authenticity of participants and authenticity of data during transfer, and data confidentiality. This means that it ensures that only authorized participants are allowed to exchange information, that data is not altered during transmission between two participants, and sensitive project information is kept private. The proposed cryptographic protocol and hash functions ensure authenticity of the participants and authenticity of data during transfer. The private-key public-key is a type of asymmetric encryption where plain data is encrypted with a key, but is decrypted with its respective key pair. Hashing

however facilitates robust one-way encryption of plain text into encrypted text. Hash functions are collision free, which means that for a particular plain text, there a unique corresponding encrypted text. In our framework, in order to securely achieve endorsement and consensus, a participant, say A calculates the hash value of a message to be exchanged. After that, A signs (encrypts) the hash value of the message with a private key that is only known to him, as shown below.

$$signature_A = \mathrm{Pr}_{\mathrm{k_A}}(hash(message)) \quad (1)$$

The participant A, then broadcasts the concatenation of the original message and signature in the format, "$Encrypted(message \,||\, signature_A)$" to

every other participant on the blockchain framework. The participants at the receiving end can confirm that the message has been sent by A only if they can decrypt the signature with the corresponding publicly available key of A. Furthermore, the message is be confirmed to be unaltered during transfer, if calculation of the $hash(message)$ performed at the receiver's end is the same as that sent as a part of $signature_A$ by the sender, A. It is to be noted that this is done only to ensure the authenticity of the participants and data during transfer having nothing to do with data confidentiality. Data confidentially is implemented by separately encrypting the message itself in the first place with a different key available only to the project participants. Thus, only the parties within the permissioned blockchain network have the key to decrypt the message after they have ensured the authenticity of the users and data during transfer.

4 Example Scenario

In this section, an example scenario is demonstrated for describing the feasibility and key properties of the proposed methodology. Hyperledger [10] is used to set up the permissioned blockchain network for the involved parties in a construction project. The example scenario is based on the clauses related to interim payment from the General Conditions of Contract for Term Contracts for Civil Engineering Works in Hong Kong (HKGCC) [9]. Different parties have different obligations and responsibilities in the interim payment process (shown in Figure 2). These responsibilities and obligations are guided by clauses of HKGCC (as shown in step 1 of Figure 4) which have been transformed into machine executable logic to realize interim payments.

Contract execution is demonstrated in Figure 5. The contractor initiates the payment process with a manual input comprising information such as payment application ID, total payable amount, tasks and material quantity and passes control to the automatic consensus process (designated by "C" in Figure 5). The first consensus process checks the condition such as whether the claim is submitted or not. If successful, a transaction (as shown by Tx(a)) is written to the blockchain ledger. As can be seen from the data representation of the transaction, information such as price and quantity of materials, submission time and the record of associated parties are recorded and are immutable. Therefore, in a subsequent transaction at any time in the future, information from this transaction can be drawn by the smart contract. For example, as shown in Figure 5, checking the quantity of material is one of the checks for achieving consensus at a particular stage of approval. This check is designed (in the smart contract) to pull quantity data from the transactions (Tx(a) in this case) stored in the blockchain ledger. Since this framework allows standards checks to be performed against the data stored in the blockchain, it can be assured that these checks are always evaluated against authentic data. There is no scope for altering this data even by hacking into the system. If such attempts are made, a trail of the same will be left in the blockchain (due to use of cryptographic protocols such as Merkle Tree in the inherent design of blockchain).

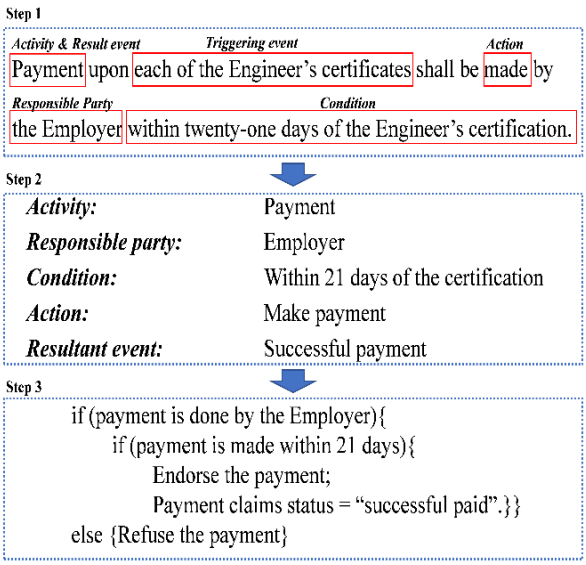

Figure 4. An example illustrating formalization and representation of smart contracts

5 Conclusion

Construction contracts regulate the behavior of the stakeholders in a construction project. Effective construction contract management protects the interests of all stakeholders, decreases the possibility of construction delay, and ensures smooth construction progress. In this research, a blockchain-based smart construction contract framework is proposed for semi-automatic execution of construction contracts for interim payments. A data representation for a smart contract is developed based on traditional textual contracts. This representation models contractual conditions into obligations, prohibitions, and actions, which can be read and executed automatically. By leveraging blockchain technology, a framework for executing this smart contract is developed which caters to the requirements of sequential approval process in a decentralized environment, such as that of the construction industry. A customized semi-automatic consensus mechanism is developed to facilitate interim payments through the blockchain framework. This mechanism regulates the sequence and conditions of

approval by stakeholders such as engineer, architect, and owner by automatically providing them with necessary information at the time of approval. It furthermore removes the scope of fraudulent approval by individual stakeholders as the consensus mechanism sends the result of individual approval to all the stakeholders on the platform.

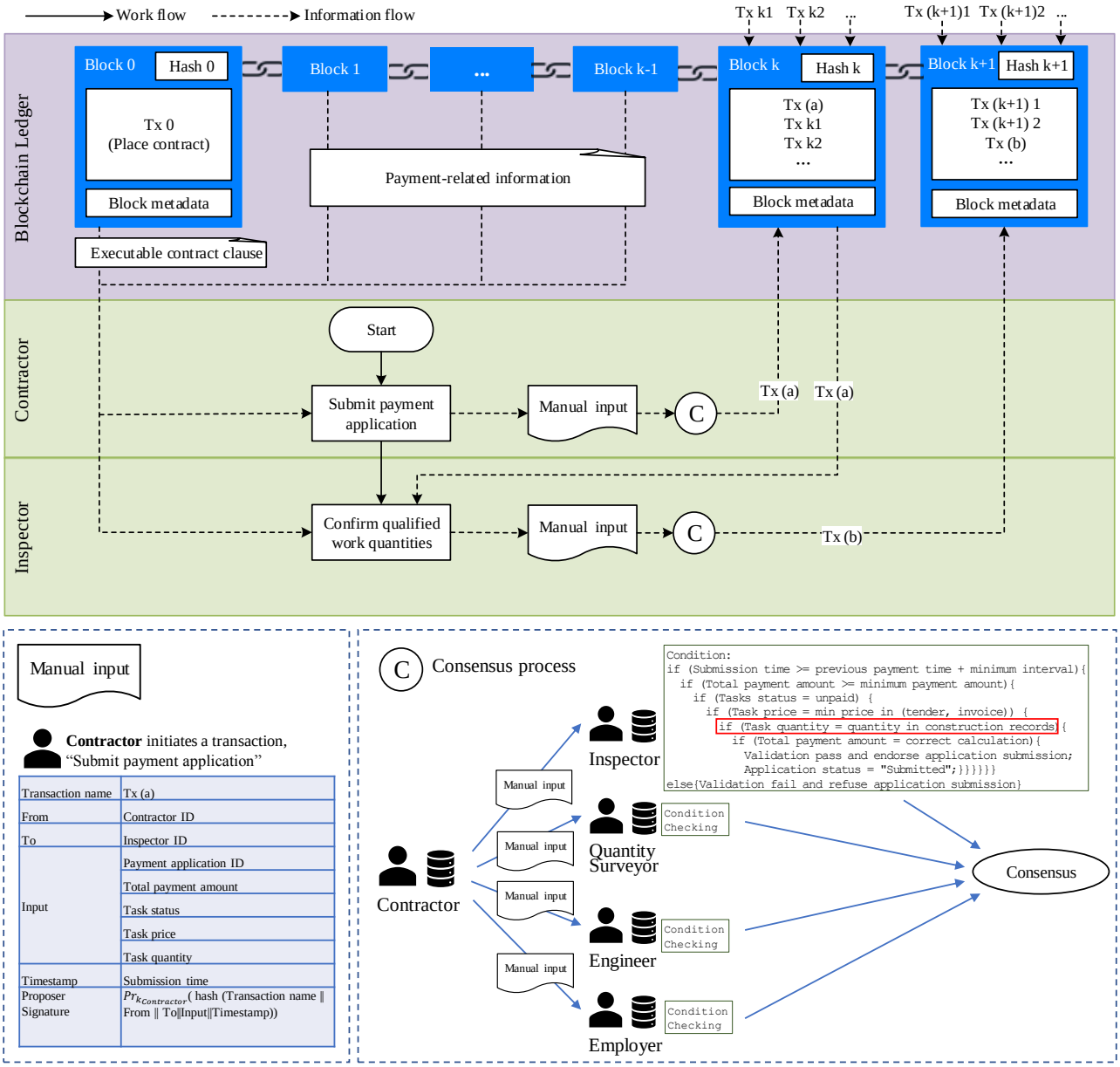

Figure 5. The example scenario illustrating blockchain-based smart contract for interim payments

All these stakeholders thereupon automatically check that result against certain pre-set rules, on their individual machines and communicate back their decisions across the group. Therefore, an approval is legitimized only when it has the collective endorsement from all the stakeholders. The record of this approval is thereupon stored on the blockchain ledger, which is inherently immutable, and therefore is secure against malicious alteration. Along with this, the proposed framework implicitly deploys cybersecurity measures to authenticate users through

public-private key encryption protocol. Presently in this research, the conditions of traditional contracts have been manually modelled into that of a smart contract by following a procedural approach. In

future, automatic development of smart construction contracts will be explored through technologies such as Natural Language Processing and Machine Learning. The scope of data representation will also be extended from interim payments to other technically feasible areas of construction contracts. The construct of the smart contract code in this paper is similar to that of e-contracts, but deployed on a secure distributed framework and regulated by a customized consensus. However, it has further potential to function as a fully enforceable contract management system through integration with resources such as BIM, which will be explored in the future. The performance of such smart contracts will also be studied in more complex scenarios such as that with various levels of project organizational structure spread across a construction supply chain.

References

[1] Development Bureau of Hong Kong SAR. Proposed Security of Payment Legislation for the Construction Industry - Consultation Document. , 2015.

[2] Davison B. and Sebastian R. J. The relationship between contract administration problems and contract type. *Journal of Public Procurement*, 9(2):261–285, 2009.

[3] Bunni N. G. The FIDIC forms of contract. Blackwell Pub, 2005.

[4] Cardoso H. L. and Oliveira E. A contract model for electronic institutions. In *Coordination, Organizations, Institutions, and Norms in Agent Systems III.*, pages 27–40, 2008.

[5] Davis, S., Arslanian, H., Fong, D., Watkins, A., Gee, W., and Cheung, C.Y. PwC's Global Blockchain Survey 2018, 2018.

[6] BOPTI – The first crypto currency dedicated to construction industry. On-line: https://bopti.io/,

[7] Intelliware Technologies Inc. How SiteSense® uses Blockchain for Construction Transactions. , 2017.

[8] Indukuri K. V. and Krishna P. R. Mining E-contract Documents to Classify Clauses. In *Proceedings of the Third Annual ACM Bangalore Conference*, 2010.

[9] The Government of The Hong Kong SAR. General Conditions of Contract for Term Contracts for Civil Engineering Works. , 2002.

[10] Androulaki E., Barger A., Bortnikov V., Cachin C., Christidis K., Caro A. De, Enyeart D., Ferris C., Laventman G., Manevich Y., Muralidharan S., Murthy C., Nguyen B., Sethi M., Singh G., Smith K., Sorniotti A., Stathakopoulou C., Vukolić M., Cocco S. W., and Yellick J. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In *Proceedings of the Thirteenth EuroSys Conference*, pages 30:1-3:15, 2018.