Reducing information asymmetry and building trust in projects using blockchain technology

Author:

Prof. **Anita Cerić**, PhD. CE
University of Zagreb
Faculty of Civil Engineering
Department of Construction Management
anita.ceric@grad.unizg.hr
Corresponding author

Original scientific paper

Anita Cerić

Reducing information asymmetry and building trust in projects using blockchain technology

The success of every construction project is highly dependent on effective communication and trust between key project participants. It is assumed that all participants in the project will work smoothly together to complete the project. Nevertheless, according to the principal-agent theory, there is information asymmetry between project participants because they also have their own self-interests. Information asymmetry is the situation in which one of the two parties is better informed than the other. Due to complexity of construction projects and the number of participants involved, implementation of blockchain technology would reduce information asymmetry. This paper provides a framework for implementation of *blockchain* technology in construction projects so as to reduce information asymmetry and enhance trust between project participants. Blockchain technology ensures that all project participants have access to all the information exchanged between them over the duration of the project, and thus helps in developing a more trustful relationship between them.

Izvorni znanstveni rad

Anita Cerić

Smanjenje informacijske asimetrije i izgradnja povjerenja u projektima primjenom *blockchain* tehnologije

Uspjeh svakog građevinskog projekta uvelike ovisi o učinkovitoj komunikaciji i povjerenju između ključnih sudionika projekta. Pretpostavlja se da će svi sudionici u projektu nesmetano zajedno raditi na dovršetku projekta. Ipak, prema agencijskoj teoriji (engl. principal-agent theory), postoji informacijska asimetrija među sudionicima projekta jer svaki od njih ima svoje vlastite interese. Informacijska asimetrija je situacija u kojoj je jedna od dviju strana bolje informirana od druge. Zbog složenosti građevinskih projekata i broja uključenih sudionika, implementacija blockchain tehnologije smanjila bi asimetriju informacija. Ovaj rad pruža okvir za primjenu *blockchain* tehnologije u građevinskim projektima kako bi se smanjila asimetrija informacija i povećalo povjerenje među sudionicima projekta. Blockchain tehnologija osigurava da svi sudionici projekta imaju pristup svim informacijama koje se razmjenjuju tijekom trajanja projekta, te na taj način pomaže u razvoju povjerenja među njima.

1. Introduction

Ineffective communication is a common risk that can be encountered in all phases of construction projects. Effective communication among project participants is crucial for project success. The Project Management Institute [1] reports that ineffective communication represents 56 % of the total risk in any project. The main objective of this paper is to develop a framework for the implementation of decentralized, permissioned, consortium-type blockchain, for use in communication protocols on construction projects.

Information asymmetry is one of the main sources of communication risk. This asymmetry is a situation between two parties in which one is better informed than the other, and they do not have common interests [2]. According to a survey of project managers [3], the main strategy for minimising communication risk is to build trust between project participants. On projects, regarded as time-dependent organisations, a special emphasis must be placed on the development and maintenance of trust between the parties involved. Furthermore, a survey of project managers suggests that communication protocols should be developed for each construction project. In order to implement such communication protocols, project managers need to have appropriate tools as these will greatly assist in successful realisation of construction projects. Communication protocols can involve the use of blockchain technology as the latter will guarantee to project participants a proper access to all the information they exchange during realisation of the project.

For their work on information asymmetry conducted in the 1970s, George Akerlof, Michael Spence, and Joseph Stiglitz received a Nobel Prize in economics in 2001. One of widely known examples of adverse selection effects, in which used cars of different levels of quality are traded between buyers and sellers [5, 6] is presented in paper *Market for Lemons* written by Akerlof [4]. It provides one of the best-known uses of information asymmetry in economics based on the *principal–agent theory*.

Construction project management deals with trust-related issues in almost every sphere of regular activities. Using blockchain, two parties are likely to trust each other without a third-party enforcer [7]. Casey and Vigna [8] consider that blockchain does not eliminate the need for trust between individuals, i.e. it actually serves as its enabler. Blockchain can be described as a peer-to-peer distributed ledger technology in the scope of which transactions, agreements, contracts, and sales are recorded [9]. Blockchain is therefore presented in this paper as a tool for minimising information asymmetry and as an enabler and enhancer of trust between project participants.

The concepts of information asymmetry and blockchain are introduced in the following section. After introduction of these concepts, the principal-agent relationship and information asymmetry in construction projects are described. This is followed by presentation of a framework for implementing blockchain technology on construction projects. At that, a special emphasis is placed on communication risk related to asymmetric information by giving examples of blockchain algorithms for single and multiple file transactions.

2. Principal-agent relationship and information asymmetry in construction projects

In their paper, Turner and Müller [10] state that the key relationship on construction projects is the one that is established between the project owner and contractor. A *principal–agent relationship* between the project owner and contractor involves delegation of tasks, where the principal (project owner) relies on the agent (contractor) to perform a task on behalf of the principal [11]. It could be assumed that agents will try to maximize their own benefit even when it could prove detrimental to the client [12]. This problem is normally characterized by three issues of risk regarding the principal–agent relationship: *adverse selection*, *moral hazard*, and *hold-up*. *Adverse selection* is the case when the principal does not have the exact qualifications of the agent before contract signing. *Moral hazard* involves the situation in which the principal cannot be certain that the agent will fully protect principal's interests after the contract is signed. As to *Hold-up*, this situation occurs when the principal has invested some resources trusting that the agent will behave in an appropriate way, but the agent breaks this trust by acting opportunistically after the contract comes into force [12, 13]. In this paper, the relation between the project owner and contractor is extended so as to cover project managers, as illustrated in Figure 1. The project owner has the status of the overall principal and all other persons are agents directly or indirectly employed by the project owner. On the other hand, the contractor is considered as principal in relation to his project manager. These four stakeholders are considered to be of key significance on every construction project.

It should nevertheless be noted that no contract is signed between the two project managers; the project owner's project manager watches over the performance of the contractor's project manager, and the latter is required to inform the former about the matters relating to the contract. Although their actions are guided by two contracts, it should be emphasized that their direct relationship with each other remains non-contractual. It can be based at best on the guidelines that have been issued by professional organizations dealing with project management and related fields. It is important to add that all key players in a contract are additionally guided by self-interest. In that respect, it can be stated that there are twelve relationships in total. Six of these relationships are contractual, while the remaining six are non-contractual. The key non-contractual relationships are the relationships between the two project managers. As proposed in this paper, these relationships gain in importance as projects grow in extent and complexity.

The relationships in a three-party project is shown in Figure 2. In addition to the contractor, a designer is hired by the project owner. The other two project managers are monitored by the project owner's project manager, but there is no contractual relationship between them. There are ten contractual relationships in total, and they are regulated by five contracts. However, the contractual relationship does not exist between the designer and contractor and the same is true for the project managers forming the core of the project team. Therefore, the projects involving three parties are characterized by fourteen non-contractual relationships.
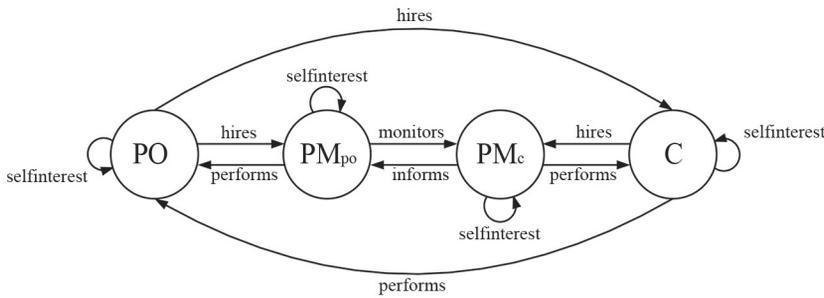
Figure 1. Principal–agent theory framework for construction projects (PO - Project owner, C: Contractor, PM_{po} - Project owner's project manager and PM_c - Contractor's project manager) [3, 14]
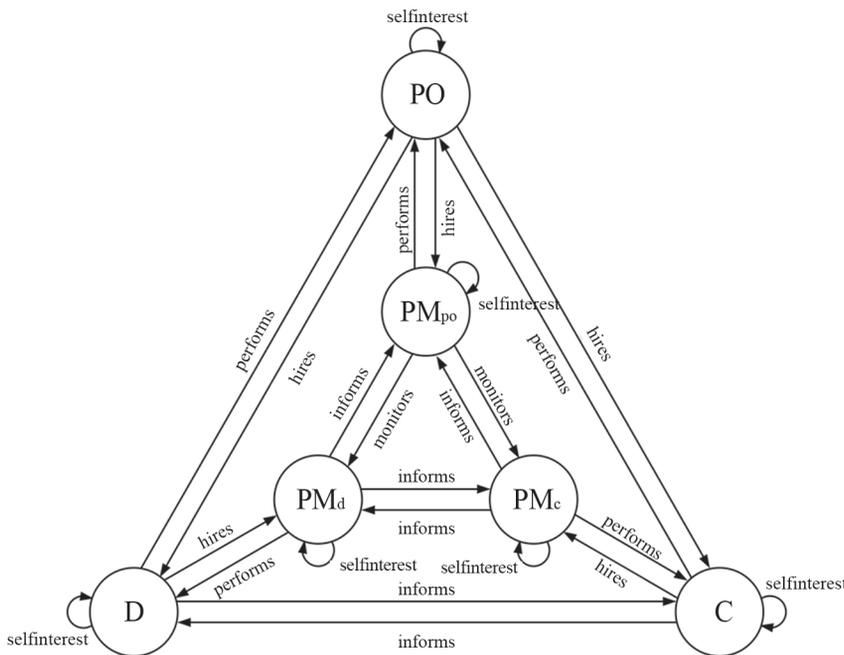

Figure 2. Principal–agent theory framework for construction projects involving three parties (PO - Project owner, C - Contractor, D - Designer, PM_{po} - Project owner's project manager, PM_d - Designer's project manager and PM_c - Contractor's project manager) [3, 15]
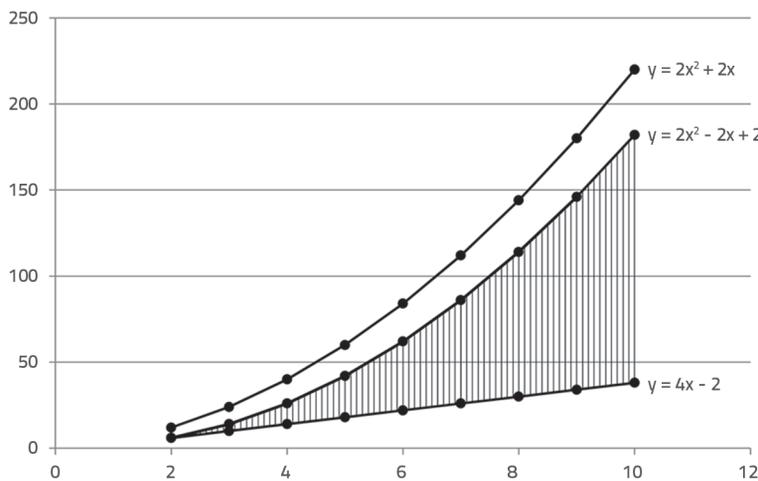

Figure 3. Project parties and relationships for up to ten parties, with shaded area representing non-contractual gap [3, 15]

The number of participants increases with the size and complexity of construction projects. The results for up to ten project parties, based on the network structure presented in Figure 1, are shown in Figure 3. These networks involve the project team of project managers surrounded by the principal and all the agents. The topological network structure remains the same for all cases.

As shown in the figures, contractual relationships start to be dominated by non-contractual relationships even in cases when there are no more than three project parties. On large and complex projects that are realized over larger periods of time, the project team becomes increasingly autonomous from the project owner, as well as the contractor, designer, and consultants as agents. Although contracts will undoubtedly always play an important role in construction projects, the need for trust-based relationship between project parties increases exponentially with the size of projects.

Relationships between project participants are generally regulated by contract [16]. The intentions of the two parties are expressed in the contract, which is why the rights and responsibilities of both parties are quite clear in the case of dispute [17]. In any case, if trust is missing, the final outcome of any construction project may be uncertain, even when stringent control systems, such as contractual documents, are available [18].

According to Zaghloul and Hartman [18], it can be quite costly to manage mistrust: "With the absence of trust in business relationships, there is a significant need for a good and powerful control system to manage and administrate the contracting process. However, even with the existence of this powerful control system (the contract documents), the success of any project or business relationship is always questionable in the absence of trust." Kadefors [19] states that trust also involves costs, because the former requires both time and effort to build and maintain. Wicks *et al.* [20] argue that in each situation there is an optimum level of trust, and that trust increases with an increase of interdependence between the parties. Furthermore, Lui and Ngo [21] argue that contractual documents that are excessively detailed are usually insufficiently flexible, making it difficult, or even impossible, to check implementation of their provisions.

3. Minimizing information asymmetry in construction projects using blockchain

The issue of trust is the first challenge faced by construction corporations. Partnering is very important in construction industry because of presence of various methods of project delivery. Gad and Shane [22] argue that trustful relationships in partnering make the project environment less adverse, contribute to successful cooperation, and reduce the level of inefficiency on construction projects. At the time of increasing spread of virtual projects, trust is also considered as being one of crucial tactical variables for an effective delivery of results [23]. In project teams, it influences the quality of relationships between the parties [24]. On the other hand, a breakdown of trust can be a consequence of opportunistic behavior of project participants [25]. It has been established that dependence between the uncertainty, opportunism and trust is particularly evident on very large projects [26]. This can be a threat to a successful project delivery because trust is often associated with project success [27, 28].

An imprecise dependency has been established by investigating the link between trust and contract in relations between the project owner and contractor [29]: sometimes trust is preceded by contract and sometimes contract is preceded by trust. Therefore, different trust increase strategies have often been researched [25, 30, 31] especially as it is highly challenging to develop and keep trust relations on construction projects [32]. Research carried out recently on this issue places a high emphasis on the significance of replacing the relational trust with technological trust on construction projects. It is precisely here that blockchain technology can be highly useful. In fact, this technology offers a method for avoiding information asymmetries while promoting trustful relationships between project participants. The methodology also has the potential to develop inter-firm trust at the front-end, during contract negotiations, and in the construction phase [33].

The increasing complexities of buildings and structures, and complex nature of information flow within supply chains, are often diverse and lead to communication gaps and sometimes to litigation [34]. Blockchain can be used on construction projects to avoid information asymmetries between key project participants: project owner, contractor, and their respective project managers. Blockchain technology can help decrease information asymmetry that arises from the complexity of construction projects and large number of participants involved on such projects.

Considered from a technical perspective, blockchain can be described as a distributed, transparent, immutable, validated, secure, and pseudo-anonymous database [35], i.e. it is a distributed file/database that has a specific data structure and is not governed by a central system or server. Blockchain networks can be created by companies or groups of individuals by means of a dedicated software, and identical copies of the blockchain can be distributed over hundreds and even thousands of computers, which can be viewed as nodes [36]. In addition, these networks can be public, which means open to everybody for reading and writing, or private, i.e. destined to well trusted participants such as various industry groups [34]. Decentralization, autonomy, peer-to-peer relationship,

immutable record, and time stamping, are the most significant features of the blockchain technology when applied on construction projects [37]. The possibility of one company or party controlling the data is eliminated by decentralisation, and so the possibility of information asymmetry is reduced to minimum. Another feature, i.e. time stamping, enables, at any given moment, provision of a digital or digitalized proof-of-existence of an asset. In other words, when the blockchain application is used in construction business or in construction activities, the trust relationship does not have to be established between participants simply because their trust is placed in the automated system [7].

The implementation of blockchain technology in construction industry involves the use of smart contracts implying fewer administrative hurdles, improved flow of the project, improvements in materials and service delivery, and higher security of Building Information Modelling (BIM) or project documents [38]. The use of blockchain in the realisation of contracts can be described as follows: "the Blockchain properties, guaranteeing the unchangeability of the data and the presence of a widespread control of every single step of the procedure, are, therefore, well disposed to face the waste of time and cost due to the lack of trust and the absence of a transparent sharing of information between the participants in the different process stages" [39]. Blockchain may be also applicable to building and rebuilding trust when it is lost or diminished [40]. It has broad prospects, such as distributed consensus, smart contract execution, encryption algorithms, and distributed ledgers, which can enhance trust, transparency, efficiency, and equity in construction industry [40]. The technology can also be used in supply chain management for data tracking, contracting and transferring resources [41], asset management, construction management integration - with BIM as a procurement solution, in building maintenance systems, and in many other areas [42].

Blockchain database applications can be divided into three categories: public, consortium, and private. In the case of a public blockchain database, transactions can be read and submitted by anyone, and so everyone can take part in the consensus process. A preselected set of nodes and rules for achieving consensus are used to control a consortium blockchain database. The right to read the blockchain can be given to everyone or can be restricted to some specific participants that are known in advance. For instance, in the case of a ten banks consortium, a block can be considered a valid representation of the truth if a previously agreed majority of these banks (e.g. seven banks) have given their approval for the said block. A private blockchain database is a database maintained by a single organization or by a part of that organisation [35].

On the other hand, the lack of transparency has implications beyond those of pure technological functionality in markets with asymmetric information, which can lead to hidden information at the pre-contractual stage, and to hidden action problems at the post-contractual stage [4, 43]. In such case, the crucial objective is to minimise information asymmetry through development of trust between project participants. According to a survey of project managers with considerable experience, communication protocols are the ones that should increase and maintain trust among project parties and this from the earliest conceptualisation to final

completion of a construction project [3]. It was established in the scope of the same survey involving project managers that these managers give a very high ranking to information systems as a strategy through which information asymmetry can be reduced to minimum [3, 44]. Communication protocols involving the use of blockchain technology can be applied to ensure that project participants can access all information and data that are exchanged between such participants throughout the realisation of the project. It can be applied either in a particular stage or throughout the project lifecycle, and can serve all or a specific set of stakeholders (e.g., clients, contractors, or suppliers) [40]. The efficiency of processes within the construction industry can greatly be increased through implementation of the blockchain technology, which can also aid in elimination of current issues surrounding trust, transparency and verification [45]. Blockchain is therefore presented in this paper as a tool that enables minimisation of information asymmetry, while also increasing trust between participants on the project.

4. Framework for implementation of blockchain technology in construction projects

An appropriate framework for implementation of blockchain technology in the management of construction projects is proposed in this section. Figure 4 shows relationships between the key participants on construction projects. In this particular setting, there are eight project participants during the construction phase of the project: project owner, contractor, construction supervisor, material supplier, designer, structural engineer, and two subcontractors. Project managers are omitted for simplicity of graphical representation. Arrows depicting self-interests are also omitted. Relationships between project participants, illustrated in Figure 4, are listed in Table 1. For instance, the project owner hires the contractor and designer, the contractor hires subcontractors and material suppliers and the designer informs the site manager and contractor. When one participant *hires x* participants including the project managers, there are $2x + 1$ *hire*, $2x + 1$ *perform*, $2x^2 - x$ *inform*, and *x monitor* relationships. The number of contractual relationships is the sum of the number of *hire* relationships and that of *perform*

relationships. This number is $4x+2$. The number of non-contractual relationships is the sum of the number of *inform* relationships and that of *monitor* relationships. This number is $2x^2$.
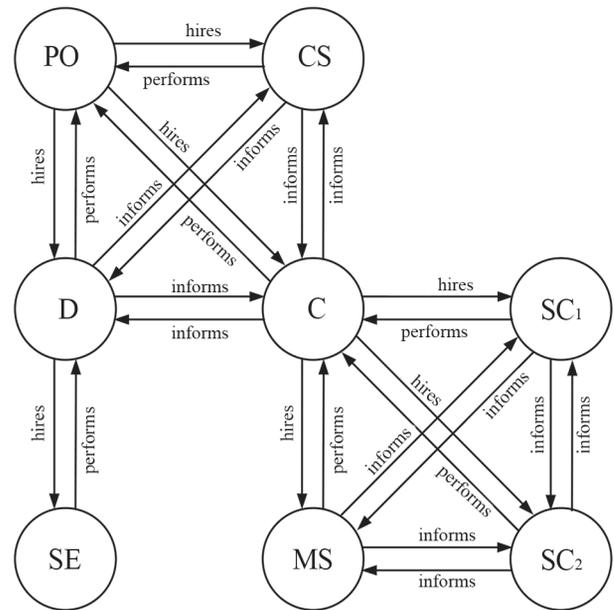

Figure 4. Framework for blockchain implementation: Relationships between key participants on construction projects: PO - project owner, D - designer, C - contractor, SE - structural engineer, CS - construction supervisor, MS - material supplier, SC$_1$ - subcontractor$_1$ and SC$_2$ - subcontractor$_2$ [44]

Here, there are eight project participants and eight project managers. Three participants are hired by the project owner (contractor, designer, and construction supervisor), three participants are hired by the contractor (material supplier, subcontractor$_1$, and subcontractor$_2$), and one participant is hired by the designer (structural engineer). Therefore, contractual relationships can be defined as follows: $(4\cdot3+2) + (4\cdot3+2) + (4\cdot1+2)$. According to previous calculation, four contractual relationships must be excluded (contractor–contractor's

Table 1. Relationships between project participants

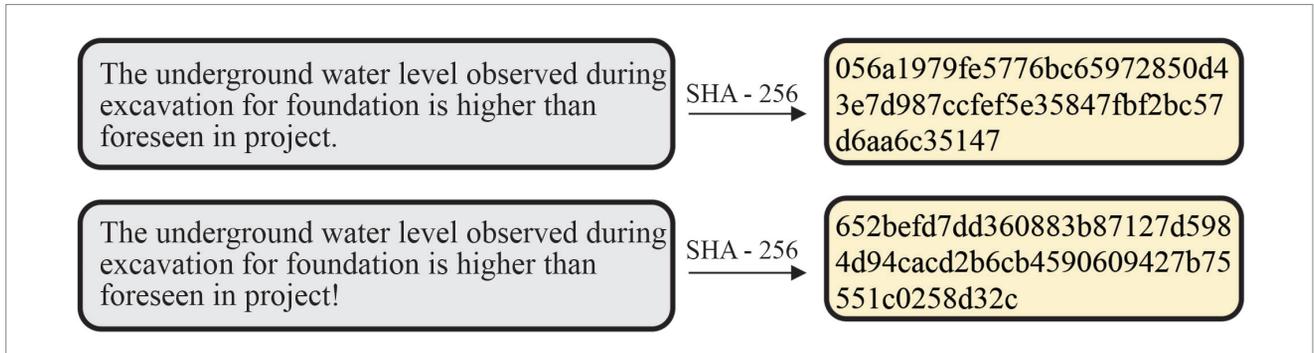|	PO	CS	D	SE	C	SC$_1$	SC$_2$	MS
PO	–	H	H		H			
CS	P	–	I		I			
D	P	I	–	H	I			
SE			P	–				
C	P	I	I		–	H	H	H
SC$_1$					P	–	I	I
SC$_2$					P	I	–	I
MS					P	I	I	–
PO - project owner, D - designer, C - contractor, SE - structural engineer, CS - construction supervisor, MS - material supplier, SC$_1$ - subcontractor$_1$ and SC$_2$ - subcontractor$_2$, H-hire, P-perform								

Figure 5. Calculating hash value of the contractor's slightly different messages

project manager, and designer–designer's project manager) because these have been calculated twice. The number of contractual relationships is 30. The number of non-contractual relationships is $(2·3^2) + (2·3^2) + (2·1^2) = 38$. In addition, there are 16 self-interest relationships. Thus, there are 30 contractual and 54 non-contractual relationships in total. According to the principal–agent theory, contractual relationships can also be guided by opportunistic behaviour between project parties.

The number of *Perform* relationships is $(2·3+1) + (2·3+1) + (2·1+1)$. According to previous calculation, two *perform* relationships have to be excluded (contractor–contractor's project manager, and designer–designer's project manager) as they have been calculated twice. The final number of *perform* relationships is 15. The number of *inform* relationships is $(2·3^2–3) + (2·3^2–3) + (2·1^2–1) = 31$. There are $15+31 = 46$ *perform* and *inform* relationships that can deliver asymmetric information for 18 project parties. Taking into account such high level of complexity, the main goal of the framework proposed for implementing the blockchain technology on construction projects is to lower information asymmetry, and to provide information that is distributed, transparent, immutable, validated and secure.

Blockchain is a distributed database or ledger that is related to a specific data structure. In the proposed area of activity, the data can be any digital document or file related to construction phase of the project, including delivery notes, periodic reports, quality control, health and safety issues, resource control, daily logs, tests and inspections, meeting records, work schedules, drawings, technical specifications, daily forecasts, construction diary, photographs, and videos. To enable file sharing between project parties, the blockchain is organized as a distributed system without any central point of coordination or control, and hence it does not have a single point of failure. The peer-to-peer network is a special type of distributed system. It consists of individual computers of its users, who are called nodes and communicate through a network. In this particular case, the project parties (eight participants and eight managers) are the nodes sharing a distributed database. The Internet is used by the peer-to-peer system as a network to connect individual nodes and send files. Each node can disconnect from and reconnect with the system at any time, and can be identified by a unique address, while also having the ability to independently maintain a list of all other nodes it communicates with. Each node has an identical copy of the ledger.

4.1. Blockchain algorithm for single file transaction

The distributed ledger is updated by using blockchain whenever one of the parties to the projects wishes to inform another party about his activities related to the construction phase of the project. We could mention as an example the case when the contractor wishes to inform the designer that the ground water level, registered during excavation for foundations, is higher than that initially foreseen for this particular project. The message (transaction data) is first converted by the blockchain algorithm on the contractor's computer into a 256-bit long string represented by 64 hexadecimal digits comprising digits from "0" to "9" and letters from "a" to "f." This is executed by computer by using the SHA-256 cryptographic hash function. This function, being a one-way noninvertible function, takes an input of any size and produces an output of a fixed size regardless of the size of the input data. Hash function cannot be used to obtain the original data, and hash values do not disclose anything about the content of the input data. Small changes in the input data result in large changes in output [47]. The hash value of the transaction data is referred to as hash reference in blockchain terminology because it is related to the transaction data. The way in which the hash value dramatically changes when the full stop is replaced with an exclamation mark at the end of the message is shown in Figure 5.

The contractor's transaction is authorized in the next step by creating a digital signature. This is executed by the algorithm by means of asymmetric cryptography, which is also known as the public-private-key cryptography. This protect the data from being used by unauthorized parties. Two complementary keys are used by asymmetric encryption algorithms to encrypt and decrypt transaction data. One key, shared with all nodes in the system, is called the public key. The other is the private key, and it remains confidential. If the private key is used for encryption, the public key is used for decryption, and vice versa. The term ciphertext is used to denote the encrypted transaction data. A digital signature is created by the contractor's computer by using its private key to encrypt the hash reference to the transaction data using the Base64 Encoder/Decoder [48]. As shown in Figure 6, the digital signature and transaction data are put together and submitted to all nodes in the system.

When transaction data are received by all the nodes, including the digitally signed hash reference to the transaction data, the decision is made by the blockchain algorithm about which node will create a
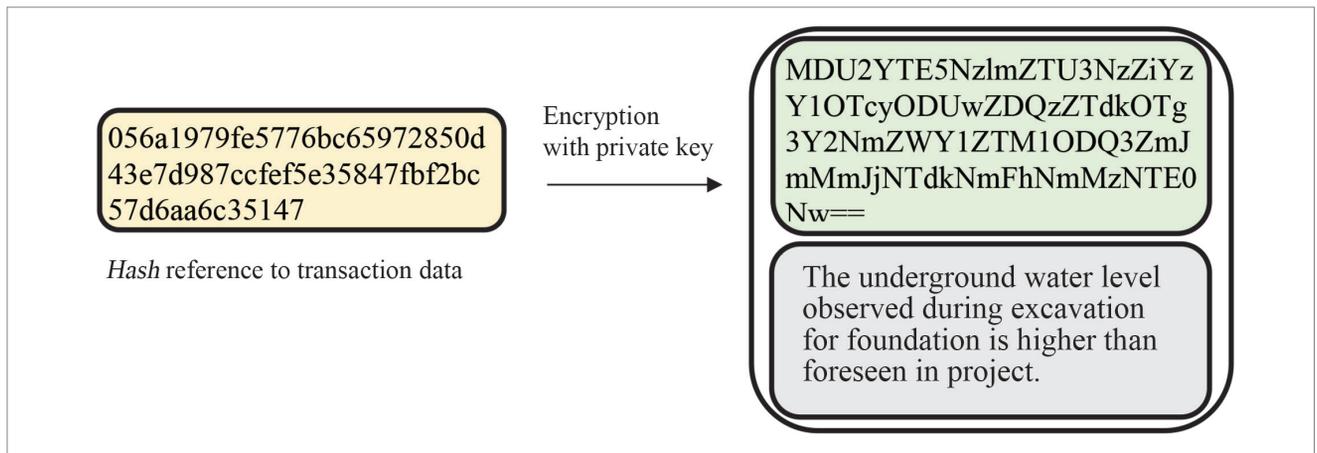
056a1979fe5776bc65972850d43e7d987ccfef5e35847fbf2bc57d6aa6c35147

Hash reference to transaction data

Encryption with private key

MDU2YTE5NzlmZTU3NzZiYzY1OTcyODUwZDQzZTdkOTg3Y2NmZWY1ZTM1ODQ3ZmJmMmJjNTdkNmFhNmMzNTE0Nw==

The underground water level observed during excavation for foundation is higher than foreseen in project.

Figure 6. Creation of digital signature of transaction data

MDU2YTE5NzlmZTU3NzZiYzY1OTcyODUwZDQzZTdkOTg3Y2NmZWY1ZTM1ODQ3ZmJmMmJjNTdkNmFhNmMzNTE0Nw==

Decryption with public key

056a1979fe5776bc65972850d43e7d987ccfef5e35847fbf2bc57d6aa6c35147

The underground water level observed during excavation for foundation is *higher* than foreseen in project.

Identical

SHA- 256

056a1979fe5776bc65972850d43e7d987ccfef5e35847fbf2bc57d6aa6c35147

Figure 7. Use of digital signature to verify transaction data

new block and append it to the chain or distributed ledger. A proof-of-stake consensus algorithm is applied in this blockchain [49, 50]. The node that is allowed to append a new block to the blockchain is chosen at random. In other words, the more stakes a node owns, the more chance it has to append a new block. The number of blockchain tokens (stakes) each node (project party) receives before the start of the construction phase of the project is defined by the project owner. The chance of node X acquiring the right to create a new block is M/N if there are a total of N tokens for all nodes, and node X has M tokens. The lucky node is selected every 30 min. According to the proof-of-stake consensus algorithm, an attacker has to own at least 51 % of the total number of stakes in the network to perform an attack, and this percentage is very difficult to obtain.

When a node gets the chance to create a new block, it first identifies the sender, and then verifies the transaction data. As it knows the public keys of all nodes, this particular node will attempt to use them to decrypt digital signature. The sender is identified by a public key that successfully decrypts the digital signature. The decrypted ciphertext is the hash reference to the transaction data. Digital signature is used to verify transaction data. The hash value of the transaction data is first calculated by the selected node. The node then compares that hash value with the hash reference to the

transaction data. If both hash values are identical, the authorization is confirmed and the transaction is verified (Figure 7). If this is not the case, the transaction and the data are rejected. The situation in which a hacker or any node in the system replaces the word "higher" with the word "lower," thus completely changing the meaning of the message, is shown in Figure 8. Comparison of two hash values reveals that they are not identical, and the transaction is not verified. Once the sender is identified and the data transaction verified, a new block consisting of the block header and transaction data is created by the selected node. The block header is made of the hash reference to the transaction data, current time (timestamp), and hash reference to the previous block. The hash value of the block header is then calculated to obtain the hash reference to the new block (Figure 9). This reference is also called the head of the chain because it refers to the most recently created block in the chain of data. Finally, it digitally signs the hash reference to the new block and submits it together with the new block to all the nodes in the system. The sender is then identified by each node, which verifies the entire ledger in the reverse direction from the head of the chain to the transaction data contained in the first block. In case of successful verification, the distributed ledger on each computer in the system is updated and all the copies are identical. Should the verification fail, the distributed
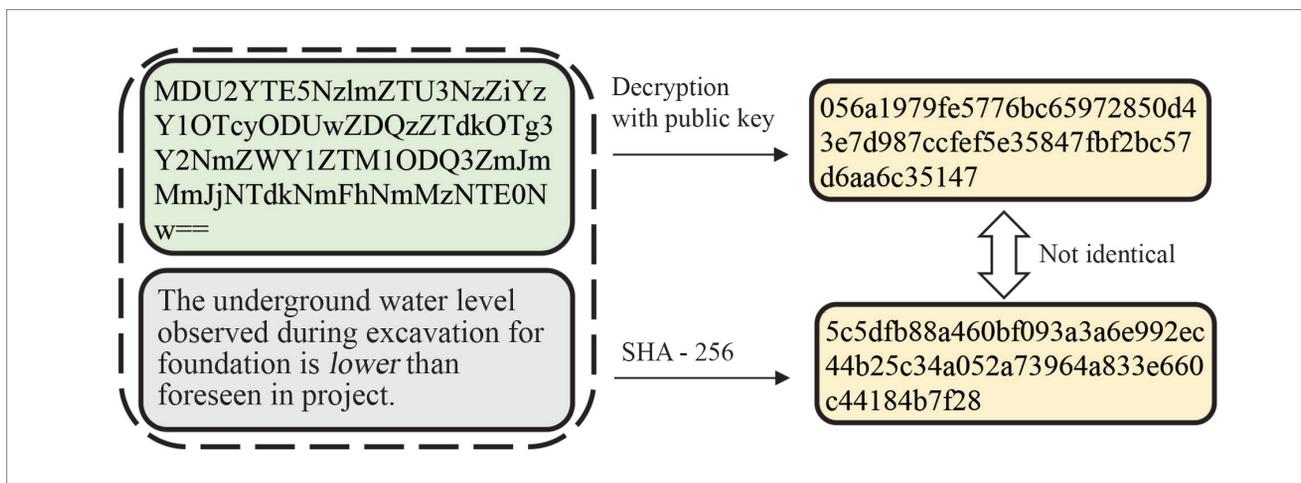
Figure 8. Use of digital signature to reject transaction data
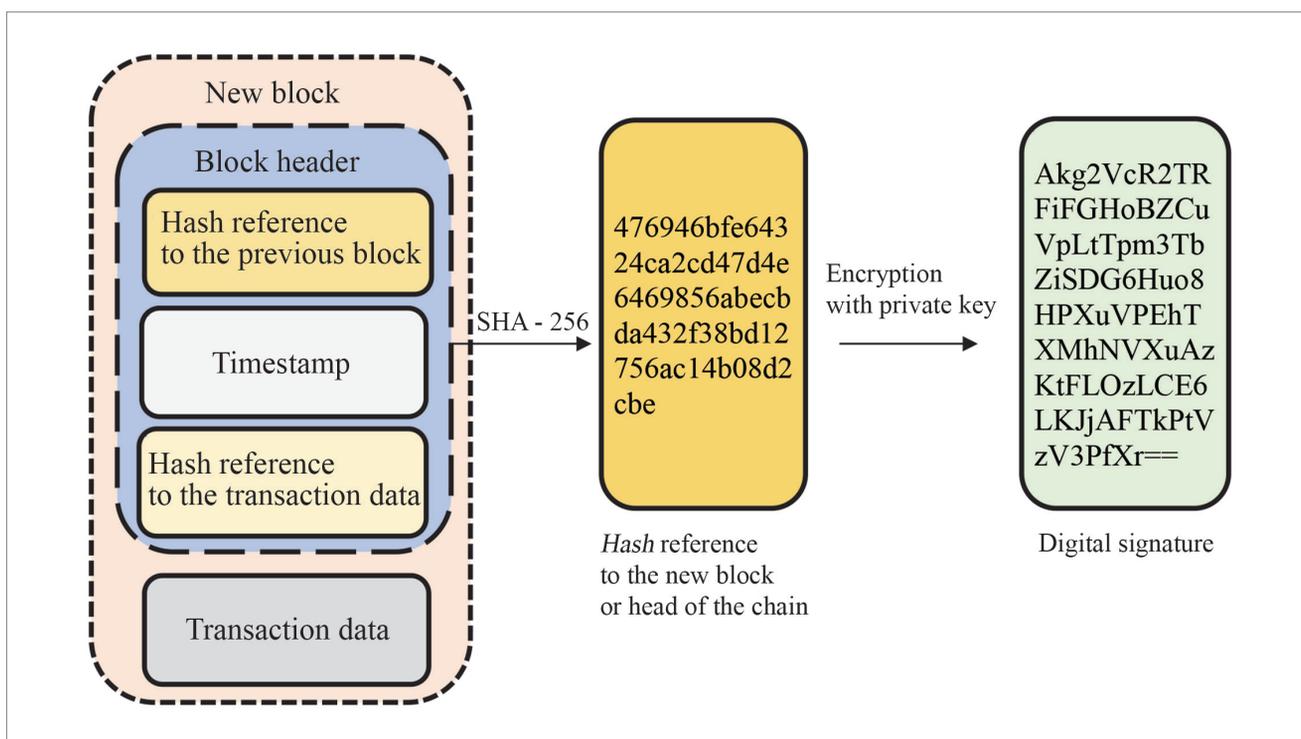

Figure 9. Creation of new block for single file transaction

ledger is not updated by the nodes. The entire process starts again when one of the project parties wishes to inform another about their new activities related to the construction phase of the project.

4.2. Blockchain algorithm for multiple file transaction

Other than the information that the groundwater level observed during the excavation for the foundations is higher than that foreseen for the project, the contractor might wish to send to the designer at the same time appropriate drawings, technical specifications and recommendations for the foundations. Different blockchain data structure, capable of managing transactions with any number of files, should in such cases be used. This structure,

invented by Ralph Merkle, is called a Merkle tree because it looks like a tree turned upside down [51]. This structure is very useful for storing data accurately and securely, and can be used in distributed ledger for efficient data verification [52]. In the framework proposed in this paper, the Merkle tree is implemented as a binary hash tree, and has two children per node (Figure 10).

Four transaction data files are contained in the transaction list given in Figure 10. SHA-256 cryptographic hash function is used to individually hash these transactions to obtain their corresponding hash reference. Thus HR2 is the hash reference to the transaction data 2. The hash references to the transaction data files, always representing child nodes in the Merkle tree, are referred to as "leaves". The two adjacent hash references of child nodes are
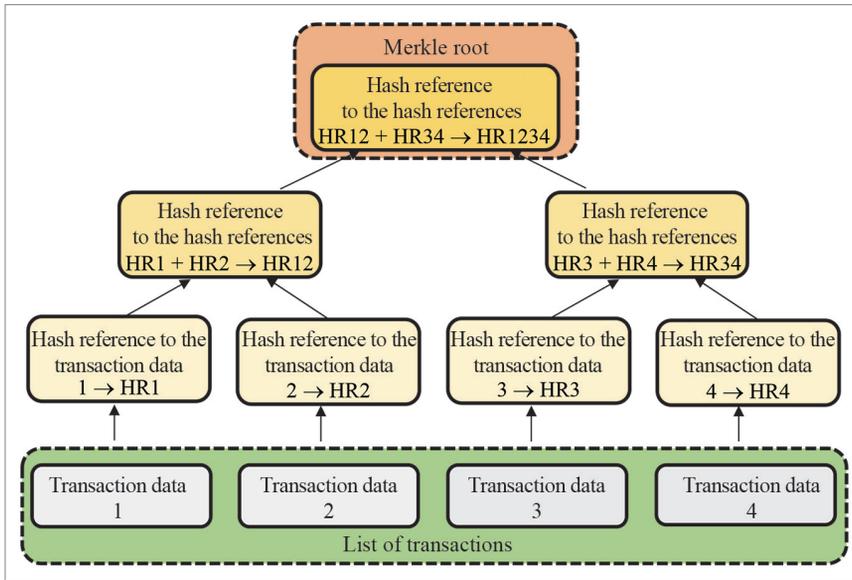
Figure 10. Creation of Merkle tree for multiple file transaction

A Merkle tree that contains all the transactions and corresponding hash references is first created by the blockchain algorithm for multiple file transaction on the contractor's computer. This is followed by authorisation of the contractor's transaction list by creating a digital signature by means of the public-private-key cryptography. A digital signature is created by the contractor's computer by using its private key to encrypt the Merle Root to the transaction list by means of the Base64 Encoder/Decoder. The digital signature and transaction list are put together and submitted to all the nodes in the system. When all the nodes receive the transaction list and the digitally signed Merkle Root to the transaction data, the blockchain algorithm decides which randomly chosen node will create a new block and append it to the chain. The proof-of-stake consensus algorithm explained in previous section is used to this effect.

merged into a string. If the transaction list contains an odd number of files, the hash reference to the last file is paired with itself. Then the hash reference of the resulting string is calculated. For example, HR12 is the hash reference to the merged hash references (HR1 + HR2). The hash references to the merged hash references are known as "branches". They can represent child and parent nodes in the Merkle tree. This process is repeated until the last hash value has been calculated. The hash reference at the top, the so called Merkle Root, always represents the parent node. For example, HR1234 is the hash reference to the merged hash references (HR12 + HR34).

A node that gets an opportunity to create a new block first identifies the sender by using a public key through which the digital signature is successfully decrypted. The decrypted ciphertext is the Merkle Root reference to the transaction list. Then it verifies all the transactions in the transaction list. Otherwise, the transaction list is rejected. For example, if the transaction data 2 is replaced or modified by a hacker or any node in the system, then its corresponding hash reference HR2a will not be identical to HR2. The hash reference to the merged hash references (HR1 + HR2a
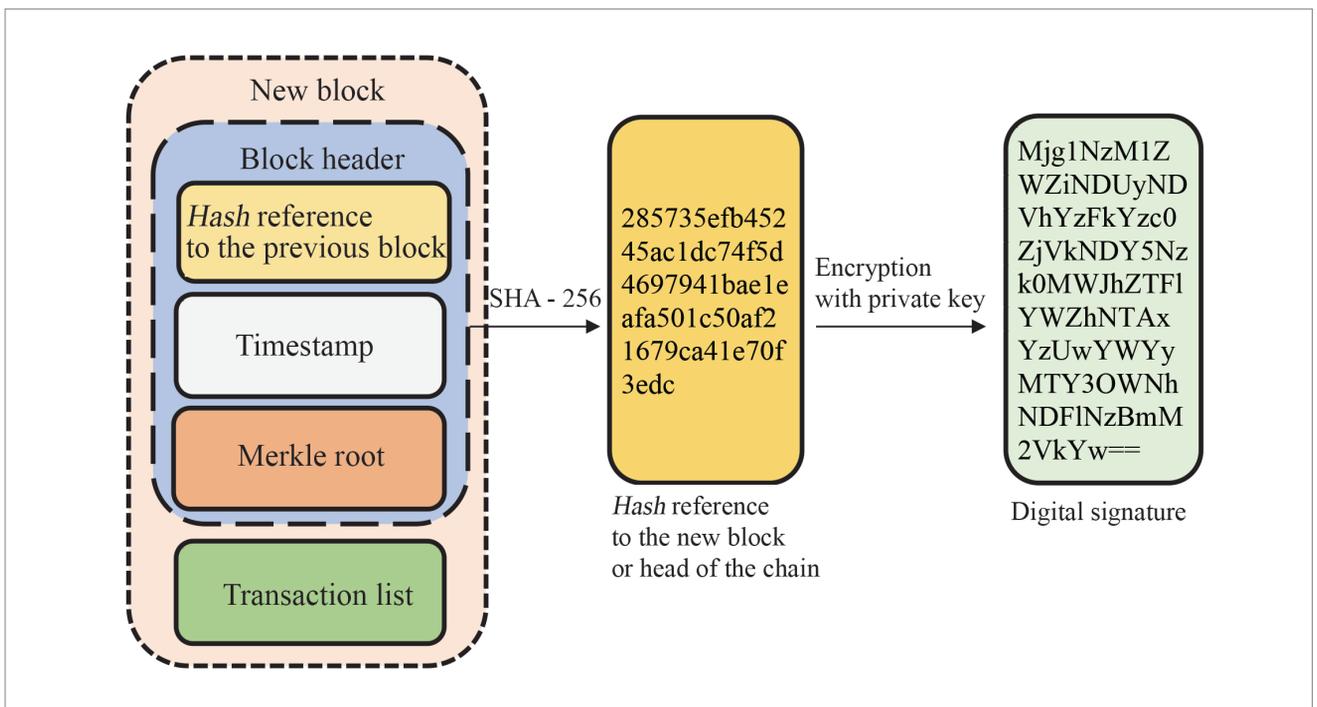

Figure 11. Creation of new block for multiple file transaction

→ HR12a) will not be identical to HR12, and the hash reference to the merged hash references (HR12a + HR34 → HR1234a) will not be identical to HR1234. The block header includes the Merkle Root, current time (timestamp), and hash reference to the previous block. As shown in Figure 11, the hash reference to the new block is then calculated, digitally signed and submitted together with the new block to all the nodes in the system. Each node identifies the sender, verifies the entire ledger, and updates the distributed ledger on its computer. If the verification fails, the distributed ledger is not updated by the nodes.

The framework presented in this paper is an example of how the blockchain technology can be implemented at the construction phase of project. The flow of transaction, *i.e.* information, between project participants is shown. Of course, in construction projects, the whole process of implementation of blockchain technology is more complicated and requires more time than in other types of projects, which is mainly due to their complexity, uniqueness and many changes during the construction phase. It has been shown in recent research [53] that there is real potential for digital ledger technology to support digitalisation in the construction industry and to enable finding solutions to many of its challenges. However, the implementation of blockchain technology at the construction phase is of great importance and provides transparency and proper information sharing between all participants on the construction project. The blockchain technology can be used in communication protocols to mitigate information asymmetry and enhance trust between all the project participants over the duration of the project.

5. Conclusions

Communication risk is considered to be one of the most important types of risk that can occur on construction projects, and trust is one of the most effective ways of minimising such risk. Information asymmetry is one of the main causes of communication risk. In effect, information asymmetry is a situation between two parties in which one is better informed than the other, and they do not have common interests. The use of blockchain technology can significantly decrease information asymmetry because of the complexity of construction projects and the number of participants involved. Furthermore, the establishment of communication protocols using blockchain technology ensures that all project participants can get all the information exchanged between them during the project. Blockchain thus helps in the development of a more trustful relationships between project participants.

The main objective of this paper is to develop a framework for the implementation of decentralized, permissioned, consortium-type blockchain, for use in communication protocols on construction projects. The proposed framework provides a distributed, secure, and transparent database that maintains the entire history of any digital document or file exchanged during the construction phase of the project. The framework utilizes all relevant blockchain elements, such as proof-of-stake consensus, asymmetric cryptography for identification, authentication of users, and authorization of transaction data.

The framework would be a useful tool for managing and recording changes to the Building Information Model during all the phases of the construction project. Most importantly, the framework proposed in this paper offers the backbone of communication protocols that need to be developed for every construction project regardless of its size and complexity [3]. Such communication protocols would ensure trustful relationships between all project parties and thus help project managers to ensure successful completion of construction projects.

Acknowledgments

REFERENCES

[1] Project Management Institute, PMI's Pulse of the Profession In-Depth Report: The High Cost of Low Performance: The Essential Role of Communications, May 2013, https://www.pmi.org/-/media/pmi/documents/public/pdf/learning/thought-leadership/pulse/pulse-of-the-profession-2013.pdf (accessed 30 May 2019).

[2] Jensen, M.C.: The Theory of the Firm: Governance, Residual Claims, and Organizational Forms, Harvard University Press, Cambridge, Massachusetts, 2000 https://ssrn.com/abstract=1791761.

[3] Cerić, A.: Trust in Construction Projects, Routledge, London, 2016 (ISBN: 978-1-138-81416-5).

[4] Akerlof, G.: The market for lemons: quality, uncertainty, and the market mechanism, Q. J. Econ., 84 (1970) 3, pp. 488-500, https://www.jstor.org/stable/1879431.

[5] Notheisen, B., Cholewa, J.B., Shanmugam, A.P.: Trading real-world assets on blockchain, Bus. Inform. Syst. Eng., 59 (2017) 6, pp. 425–440 https://doi.org/10.1007/s12599-017-0499-8.

[6] Notheisen, B., Weinhardt, C.: The blockchain, plums, and lemons - information asymmetries & transparency in decentralized markets, in: KIT Working Paper Series in Economics, Karlsruher Institut für Technologie (KIT), Karlsruhe, 130 (2018), http://dx.doi.org/10.2139/ssrn.3202667.

[7] Wang, J., Wu, P., Wang, X., Shou, W.: The outlook of blockchain technology for construction engineering management, Front. Eng. Manag., 4 (2017) 1, pp. 67-75, https://doi.org/10.15302/J-FEM-2017006.

[8] Casey, M.J., Vigna, P.: The Truth Machine: The Blockchain and the Future of Everything, St. Martin's Press, New York, 2019, (ISBN: 1250114578).

[9] Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the Internet of Things, IEEE Access, 4 (2016), pp. 2292–2303, https://doi.org/10.1109/ACCESS.2016.2566339.

[10] Turner, J.R., Müller, R.: Communication and cooperation on projects between the project owner as principal and the project manager as agent, Eur. Manag. J., 22 (2004) 3, pp. 327-336, https://doi.org/10.1016/j.emj.2004.04.010.

[11] Müller, R., Turner, J.R.: The impact of principal-agent relationship and contract type on communication between project owner and manager, Int. J. Proj. Manag., 23 (2005) 5, pp. 398-403, https://doi.org/10.1016/j.ijproman.2005.03.001.

[12] Schieg, M.: Strategies for avoiding asymmetric information in construction project management, J. Bus. Econ. Manag., 9 (2008) 1, pp. 47-51, https://doi.org/10.3846/1611-1699.2008.9.47-51.

[13] Jäger, C.: The Principal-Agent—Theory within the Context of Economic Sciences, Books on Demand GmbH, Norderstadt, 2008, (ISBN: 3837055205).

[14] Cerić, A.: Communication risk in construction projects: application of principal-agent theory, Organization, Technology & Management in Construction: An international Journal, 4 (2012) 2, pp. 522-533, https://doi.org/10.5592/otmcj.2012.2.8.

[15] Cerić, A.: The nemesis of project management: the gaping non-contractual gap, in: 27th International Project Management Association (IPMA) World Congress, Elsevier Procedia – Social and Behavioral Sciences, 119 (2014), pp. 931-938, https://doi.org/10.1016/j.sbspro.2014.03.104.

[16] Bower, D., Skountzos, F.: Partnering, benchmarking and incentive contracts, in: R. Turner (Ed.), Contracting for Project Management, Gower Publishing Limited, Hampshire, 2003, pp. 81-104 (ISBN: 9781315259352).

[17] Simister, S., Turner, R.: Standard form of contract, in: R. Turner (Ed.), Contracting for Project Management, Gower Publishing Limited, Hampshire, 2003, pp. 59-63 (ISBN: 9781315259352).

[18] Zaghloul, R., Hartman, F.: Construction contracts: The cost of mistrust, Int. J. Proj. Manag., 21 (2003), pp. 419-424 https://doi.org/10.1016/S0263-7863(02)00082-0.

[19] Kadefors, A.: Trust in project relationship-inside the black box, Int. J. Proj. Manag., 22 (2004), pp. 175-182, https://doi.org/10.1016/S0263-7863(03)00031-0.

[20] Wicks, A.C., Berman, S.L., Jones, T.M.: The structure of optimal trust: Moral and strategic implications, Acad. Manage. Rev. ,24 (1999) 1, pp. 99-116, https://www.jstor.org/stable/259039.

[21] Lui, S.S., Ngo, H.Y.: The role of trust and contractual safeguards on cooperation in non-equity alliances, J. Manag., 30 (2004) 4, pp. 471-485, https://doi.org/10.1016/j.jm.2004.02.002.

[22] Gad, G.M., Shane, J.S.: Trust in the Construction Industry: A Literature Review, in: Construction Research Congress 2014, May 19-21, Atlanta, Georgia, 2014, pp. 2136–2145, https://doi.org/10.1061/9780784413517.217.

[23] Barima, O.K.B.: Crucial tactical variables for value delivery in virtual projects, Autom. Constr., 18 (2009) 7, pp. 875-880, https://doi.org/10.1016/j.autcon.2009.03.014.

[24] Ling, F.Y.Y., Ning, Y., Ke, Y., Kumaraswamy, M.M.: Modeling relational transaction and relationship quality among team members in public projects in Hong Kong, Autom. Constr., 36 (2013), pp. 16-24, https://doi.org/10.1016/j.autcon.2013.08.006.

[25] Zheng, X., Zhang, S., Wang, C.: Trust repair after opportunistic behaviors in the chinese construction projects, Sustainability, 10 (2018) 7, pp. 23-39, https://doi.org/10.3390/su10072339.

[26] Wang, D., Fu, H., Fang, S.: The efficacy of trust for the governance of uncertainty and opportunism in megaprojects: The moderating role of contractual control, Eng. Construct. Architect. Manag., 27 (2019) 1, pp. 150-167, https://doi.org/10.1108/ECAM-09-2018-0409.

[27] Love, P.E.D., Mistry, D., Davis, P.R.: Price competitive alliance projects: identification of success factors for public clients, J. Constr. Eng. Manag., 136 (2010) 9, pp. 947–956, https://doi.org/10.1061/(ASCE)CO.1943-7862.0000208.

[28] Wang, D., Fang, S., Fu, H.: Impact of control and trust on megaproject success: the mediating role of social exchange norms, Adv. Civ. Eng., (2019), pp. 4850921, https://doi.org/10.1155/2019/4850921.

[29] Khan, S., Gul, S., Shah, A.: A review of literature on the role of trust and partnering in success of construction projects, African J. Bus. Manag., 5 (2011) 35, pp. 13541–13549 https://doi.org/10.5897/AJBMX11.024.

[30] Xu, J.: In the shadow of a negative past: repairing and developing trust in construction projects, Proceedings of the Institution of Civil Engineers - Management, Procurement and Law, 173 (2020) 1, pp. 5-13 https://doi.org/10.1680/jmapl.19.00030.

[31] Zheng, X., Song, X., Zhang, S., Gao, Y.: Identification of trust-repair strategies and their effectiveness in the Chinese construction industry, J. Manage. Eng., 33 (2017) 6, pp. 04017032, https://doi.org/10.1061/(ASCE)ME.1943-5479.0000557.

[32] Xu, J.: Understanding trust in construction supply chain relationships, in: S. Pryke (Ed.), Successful Construction Supply Chain Management: Concepts and Case Studies, second ed., Wiley-Blackwell, 2020, pp. 307-333, https://doi.org/10.1002/9781119450535.ch15.

[33] De La Peña, J., Papadonikolaki, E.: From relational to technological trust: How do the Internet of Things and Blockchain technology fit in?, in: Proceedings of the 2019 European Conference for Computing in Construction, July 10-12, Chania, Crete, Greece, 2019, pp. 415-424, https://doi.org/10.35490/EC3.2019.153.

[34] Heiskanen, A.: The technology of trust: How the Internet of Things and blockchain could usher in a new era of construction productivity, Constr. Res. Innov., 8 (2017) 2, pp. 66-70, https://doi.org/10.1080/20450249.2017.1337349.

[35] Bambara, J.J., Allen, P.A.: A Practical Guide to Developing Business, Law, and Technology Solutions, McGraw-Hill Education, New York, 2018 (ISBN: 1260115879).

[36] Gupta, M.: Blockchain For Dummies®, IBM Limited Edition, John Wiley & Sons, Inc., New York, 2017 (ISBN: 978-1-119-37123-6 (pbk); ISBN: 978-1-119-37139-7 (ebk)).

[37] San, K.M., Choy, C.F., Fung, W.P.: The potentials and impacts of blockchain technology in construction industry: a literature review, IOP Conference Series: Materials Science and Engineering, 495 (2019), pp. 012005, https://doi.org/10.1088/1757-899X/495/1/012005.

[38] Shojaei, A.: Implementation of blockchain technology in the construction industry, in: D. Ozevin, H. Ataei, M. Modares, A. Gurgun, S. Yazdani, A. Singh (Eds.), Proceedings of International Structural Engineering and Construction, ISEC Press, Chicago, 2019, pp. 31-1-31-6 (ISBN: 978-0-9960437-6-2).

[39] Di Giuda, G.M., Pattini, G., Seghezzi, E., Schievano, M., Paleari, F.: The construction contract execution through the integration of blockchain technology, in: B. Daniotti, M. Gianinetto, S. Della Torre (Eds.) Digital Transformation of the Design, Construction and Management Processes of the Built Environment, Springer Open, 2020, pp. 27-35, https://doi.org/10.1007/978-3-030-33570-0_3.

[40] Lu, W., Wu, L., Zhao, R.: Rebuilding trust in the construction industry: a blockchain-based deployment framework, Int. J. Constr. Manag., (in print) (2021), https://doi.org/10.1080/15623599.2021.1974683.

[41] Qian, X.A., Papadonikolaki, E.: Shifting trust in construction supply chains through blockchain technology, Eng. Constr. Archit., 28 (2021) 2, pp. 584-602, https://doi.org/10.1108/ECAM-12-2019-0676.

[42] Perera, S., Nanayakkara, S., Rodrigo, M.N.N., Senaratne, S., Weinand, R.: Blockchain technology: is it hype or real in the construction industry?, J. Ind. Inf. Integr., 17 (2020), pp. 100-125, https://doi.org/10.1016/j.jii.2020.100125.

[43] Hellman, T., Stieglitz, J.: Credit and equity rationing in markets with adverse selection, Eur. Econ. Rev., 44 (2000) 2, pp. 281-304, https://doi.org/10.1016/S0014-2921(98)00076-2.

[44] Cerić, A.: Minimising communication risk in construction: a Delphi study of the key role of project managers, J. Civ. Eng. Manag., 20 (2014) 6, pp. 829-838, https://doi.org/10.3846/13923730.2013.802739.

[45] Hargaden, V., Papakostas, N., Newell, A., Khavia, A., Scanlon, A.: The role of blockchain technologies in construction engineering project management, in: 2019 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), IEEE, New York, 2019, https://doi.org/10.1109/ICE.2019.8792582.

[46] Cerić, A.: Blockchain Strategy for Minimizing Information Asymmetry in Construction Projects, in: I. Završki, Cerić, A.: M. Vukomanović, M. Huemann, D. Ronggui (Eds.), 14th International Conference Organization, Technology and Management in Construction and 7th International Project Management Association Research Conference, Proceedings of the Croatian Association for Construction Management and University of Zagreb, Faculty of Civil Engineering, September 4-7, Zagreb, Croatia, 2019, pp. 494-556, (ISBN: 978-953-7686-08-6).

[47] Carter, J.L., Wegman, M.N.: Universal classes of hash functions, J. Comput. Syst. Sci., 18 (1979), pp. 143–154, https://doi.org/10.1016/0022-0000(79)90044-8.

[48] Abas, A., Yusof, Y., Ahmad, F.K.: Expanding the data capacity of QR codes using multiple compression algorithms and base64 encode/decode, J. Telecommun. Electron. Comput. Eng., 9 (2017) 2-2, pp. 41-47, https://journal.utem.edu.my/index.php/jtec/article/view/2217.

[49] Wenting, L., Sébastien, A., Jens-Matthias, B., Ghassan, K.: Securing proof-of-stake blockchain protocols, in J. Garcia-Alfaro, G. Navarro-Arribas, H. Hartenstein, J. Herrera-Joancomartí (Eds.), Data Privacy Management, Cryptocurrencies and Blockchain Technology, Springer, Cham, 2017, pp. 297–315, https://doi.org/10.1007/978-3-319-67816-0_17.

[50] Nguyen, T., Kim, K.: A survey about consensus algorithms used in Blockchain, J. Inf. Process. Syst., 14 (2018), pp. 101–128, https://doi.org/10.3745/JIPS.01.0024.

[51] Merkle, R.C.: Secrecy, Authentication, and Public Key Systems, PhD thesis, Stanford University, Stanford, CA, USA, 1979, https://www.merkle.com/papers/Thesis1979.pdf.

[52] Merkle, R.C.: Protocols for public key cryptosystems, in: Proceedings of the 1980 IEEE Symposium on Security and Privacy, IEEE, Oakland, CA, USA, 14–16 April, 1980, pp. 122-134, https://doi.org/10.1109/SP.1980.10006.

[53] Li, J., Greenwood, D., Kassem, M.: Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases, Autom. Constr. 102 (2019), pp. 288–307, https://doi.org/10.1016/j.autcon.2019.02.005.