Front. Eng. Manag. 2020, 7(4): 564–577
https://doi.org/10.1007/s42524-020-0129-x

RESEARCH ARTICLE

Gjorgji SHEMOV, Borja GARCIA de SOTO, Hoda ALKHZAIMI

Blockchain applied to the construction supply chain: A case study with threat model

Abstract The construction industry has long faced the challenge of introducing collaborative systems among multiple stakeholders. This challenge creates a high level of rigidity in terms of processing shared information related to different processes, robust holistic regulations, payment actualizations, and resource utilization across different nodes. The need for a digital platform to cross-connect all stakeholders is necessary. A blockchain-based platform is a prime candidate to improve the industry in general and the construction supply chain (CSC) in particular. In this paper, a literature review is presented to establish the main challenges that CSC faces in terms of its effects on productivity and efficiency. In addition, the effect of applying blockchain platforms on a case study is presented and analyzed from performance and security level. The analysis aims to emphasize that blockchain, as presented in this paper, is a viable solution to the challenges in the CSC regardless of the risks associated with the security and robustness of the flow of information and data protection. Moreover, a threat analysis of applying a blockchain model on the CSC industry is introduced. This model indicates potential attacks and possible countermeasures to prevent the attacks. Future work is needed to expand, quantify, and optimize the threat model and conduct simulations considering proposed countermeasures for the different blockchain attacks outlined in this study.

Keywords blockchain taxonomy, construction supply chain, threat model analysis, security level analysis, cybersecurity, vulnerability, smart contract, cyber-attack

Received December 1, 2019; accepted June 5, 2020

Gjorgji SHEMOV, Borja GARCIA de SOTO (✉), Hoda ALKHZAIMI
Division of Engineering, New York University Abu Dhabi (NYUAD), Saadiyat Island, Abu Dhabi 129188, United Arab Emirates
E-mail: garcia.de.soto@nyu.edu

1 Introduction

The construction industry is one of the main drivers of economic growth worldwide, with annual revenues of approximately USD 10 trillion, or equivalent to 6% of the global GDP (Gerbet et al., 2016). However, recent reports indicate that the industry is stagnant, mainly due to resistance by construction firms to invest in the integration of technological advancements (Marks, 2017) to address issues of material flow synchronization and information transparency (Vrijhoef and Koskela, 2000), in addition to poor collaboration and data interoperability (Garcia de Soto et al., 2018). To point out the issues of productivity with construction management processes, Penzes (2018) used the Burj Khalifa project in the United Arab Emirates as an example, in which 12000 workers from more than 100 countries participated on-site at the peak of construction. In large-scale construction projects like the Burj Khalifa, the supply chain represents a multi-organizational process because it involves consultants, contractors and subcontractors, suppliers, and clients. The connections between the different parties are constantly linking and disconnecting based on the required function for execution (Behera et al., 2015).

A way to increase productivity and transparency in construction projects is through the integration of technical elements such as cross-functional teams, emphasizing the rapid deployment of the latest technologies (Streule et al., 2016; Barbosa et al., 2017). Some of these technologies are building information modeling (BIM), blockchain, and the Internet of Things (IoT). Among these technologies, blockchain is one of the fastest emerging technologies that can be applied to address construction project challenges to ensure an efficient and transparent supply chain process with a certain claim of robustness and security. Blockchain is a decentralized distributed ledger database using a peer-to-peer (P2P) network. The data on the blockchain are maintained by every node on the network, such that all users have the right to access all transactions made (Ye et al., 2018). According to

Viriyasitavat et al. (2018) and Mendling et al. (2018), other than efficiency and transparency, the main advantage of applying blockchain in any business activity is cost reductions through disintermediation, trust, and faster transactions. The study by Turk and Klinc (2017) is one of the first to address the potentials of blockchain for the different phases of construction projects and, in particular, to address some of the confidentiality issues raised by BIM. Blockchain technology can be applied across the different phases of a project, from design to end of life. Blockchain can be used as a connection among the different project participants to improve management and tracking during the progress of a project or reduce cash flow issues often experienced by contractors, subcontractors, and suppliers (Maciel, 2020).

The lack of trust, limited collaboration between parties, issues related to documentation, delayed payments, and transactions in the construction projects could also be addressed with blockchain (Wang et al., 2019). Li et al. (2018) indicated that increased collaboration and trust between parties is going to be established at a higher level because data will be shared more freely, mostly due to the increase in data transparency. With increased reputation ratings, blockchain is becoming a potential booster for increasing collaboration throughout the supply chain. For example, cross-border trade can be simplified, removing international exchange rates and border controls (Li et al., 2018). With its distributed nature, blockchain technology removes the requirement for intermediaries, thereby providing a guarantee of execution of transactions (Li et al., 2018). As a result of the decentralization property of blockchain and the fact that data are immutable (i.e., existing data cannot be changed, and new data cannot be added without prior confirmation and verification), increased security and transparency can be achieved (Ye et al., 2018). Also, given the property of decentralization, a third party (i.e., a centralized party that controls the chain) does not need to be involved.

New technologies have many benefits to construction projects, including increasing productivity and reducing project delays (Sepasgozar et al., 2015). However, the integration of new technology, coupled with the digitalization of the construction sector, are believed to raise issues with trust and data protection (Mantha and Garcia de Soto, 2019). Examining the cybersecurity aspect of a blockchain application to construction projects is of great importance to understand the potential risks associated with the application and how to prevent attacks (Pärn and Garcia de Soto, 2020; Mantha et al., 2020). Notably, efforts have been accelerated globally to integrate blockchains in the construction industry to serve as a means of integrated and transparent service developments across the supply chain within construction and other industries (Li et al., 2019).

The remainder of this paper is organized as follows. Sections 2 and 3 present a literature review focusing on two areas: The core issues associated with the construction supply chain (CSC), and an overview of blockchain technology and its applications to improve the CSC. Section 4 provides a threat-model analysis of a hypothetical CSC scenario, focusing on the issues in the early stage of a construction project and pointing out the use of blockchain to reduce the issues from propagating to later stages of the project. As part of the example, a pseudocode for the actions taken by different participants in the network is provided, and a preliminary threat model is presented to highlight the potential risks of blockchain attacks and to provide measures for prevention and counterattacks as well as adding a severity analysis to the attacks, which is essential to estimate risks. Finally, conclusions and outlook for future work are provided.

2 Construction supply chain

In the construction sector, the supply chain represents a network of multiple organizational units and relationships (Xue et al., 2007), including information flow, material flow, flow of services and products as well as cash flow between the client, designer, provider, contractor, and consultant. The origins of current CSC frameworks are attributed to O'Brien and Fischer (1993), who developed it to help construction companies reduce waste, improve quality, and create accurate and reliable project schedules (Feng et al., 2018). Vrijhoef and Koskela (2000) emphasized two main characteristics of the structure and functions of CSCs as follows:

- CSC is a converging supply chain that directs all materials to the construction site, the point where the main object is assembled from the incoming materials;
- Most of the time, CSC is a temporary supply chain that produces one-off construction projects through constant organizational changes based on 1) project changes (mainly design-wise), and 2) constrained timeline for project completion.

Figure 1 shows an overview of a typical CSC, indicating the different types of flow associated with the different participating parties in the chain.

Materials flow from left to right with the raw material supplier as the starting point. Depending on the type of information exchanged, this flow has a two-way direction, which includes, but is not limited to, datasheets, standards, and quality of materials. Unlike materials, cash flows from right to left. The starting point is the project owner who pays the main- and sub-contractors, and the main contractor pays the parties that provide them the required materials and information for project execution and completion. Constant communication must exist between the main contractor, project owner, and all other participants in the chain to ensure an efficient flow of materials and information and on-time cash transactions.

Given the complexity involved in material and information flow during multiple interactions in the chain, issues

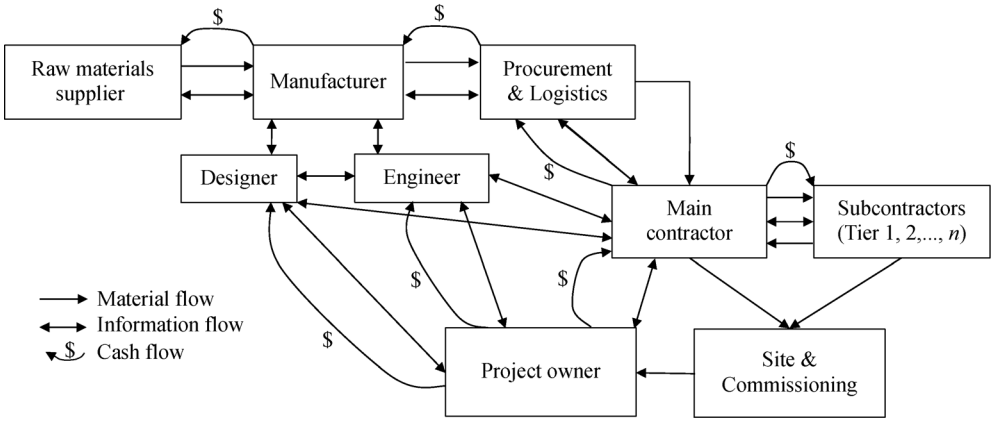

Fig. 1 Overview of a typical CSC.

have been raised on the efficiency of these flow types at all stages. These issues are mainly the result of the set buyer–supplier relationship and a high level of fragmentation between the parties involved, making the CSC a complex and dynamic network in which high-risk chances are present (Aloini et al., 2012).

Many of the problems in a construction project occur in the early stage and then are propagated, resulting in delayed project completion date, negatively affecting all parties involved. Most of the time, inefficient communication between the multiple parties in one part of the chain leads to sharing incorrect and undated documents. Such communication includes, but is not limited to, constant design changes and errors in the engineering drawings, prolonged processes of error detection and correction, and inabilities to meet quality specifications in manufacturing and delivering a specific product. Even though these problems were emphasized by Papadopoulos et al. (2016), the root cause is in the concept of a converging supply chain, limiting the amount of transparency, flexibility, and multi-level communication between the different parties involved. Kopczak and Johnson (2003) indicated that the ultimate goal of the supply chain management is to achieve a seamless and agile supply chain such that costs are minimized, and the needs of the project owner are satisfied. Wang et al. (2017) claimed that achieving this goal in the traditional supply chain is almost impossible due to conflicting interests between the parties involved in the chain.

Trust is a considerable challenge in the CSC. According to the study by Johnston et al. (2004), in the buyer–supplier relationship, the level of trust of the supplier is directly linked to inter-organizational cooperative behaviors, including but not limited to shared planning and flexibility. To successfully execute the project and deliver it on time, the participants in the chain must establish trust because this is the most critical factor leading to success (Wong and Cheung, 2005). However, the main issue with building trust in the traditional CSC is the use of a lump-sum contract and selecting the lowest bidder. The project owner would eventually spend more because many of the building components will not necessarily be accounted for very accurately, resulting in potential project completion delays and added cost (Wang et al., 2017). Many issues in the CSC are related to the information flow, referring to the constant change of requirements in the project that might prevent the establishment of a trust system (Kadefors, 2004), which hinges on the fact that the level of trust required for successful project completion is difficult to determine and even more difficult to achieve (Wang et al., 2017).

However, at present, the vision of Industry 4.0 will transform supply chain management through digitization. Schrauf and Berttram (2016) explained that the digital supply chain would provide integrated planning and execution, as well as increased transparency that allows a higher-level view of the supply chain and a real-time response on planning and execution level across all parties involved. The benefit of digitizing the supply chain in construction is that all node-to-node connections would be tracked and traced, allowing efficient communication with information available to all the members simultaneously. The result would minimize the number of problems associated with information flow, and consequently, material and cash flows.

According to Bhargava et al. (2019), the digital supply chain would benefit in multiple dimensions: 1) improved productivity, 2) reduced downtime, 3) lower costs, 4) reduced waste, and 5) improved utilization of resources. An IBM study in 2019 indicated that 54% of the construction and engineering companies believe that cloud computing can be used to run supply-chain applications and store data, followed by 37% that consider the integration of IoT would enable connectivity between sensors and devices in the networks such that materials, equipment, and supplies can be tracked and monitored. Mobile technologies and predictive analysis follow with a percentage rank of 34% and 29%, respectively. The move toward digitizing the CSC would lead to a reduced level of fragmentation present in construction projects, improved

efficiency, and enhanced transparency. IoT and cloud computing belong to the category of distributed ledger technologies (DLTs) or blockchain. The next Section focuses on providing an overview of blockchain technology and the benefits and challenges of applying blockchain to the CSC.

3 Blockchain architecture and applications to construction

In theory, blockchain is a DLT, in which data are the representation of transactions. Transactions represent the events that drive the blockchain application, and on DLT, these events are processed and stored across many different computers, known as nodes (Li et al., 2018). These nodes are decentralized; that is, no single organization stores and keeps track of all the transactions. DLT transactions replace trust with proof. According to Li et al. (2018), trust is built into the technology through its decentralized nature and basis of consensus representing a paradigm shift from a trust to a "trustless" society where third parties become redundant. Wang et al. (2019) investigated the way that blockchain can influence the practice and policies of the supply chain. Their study focused on how blockchain technology allows organizations and individuals to make and verify transactions without needing a central controlling authority to deal with the pressing issue of trust, which is particularly relevant in the construction industry. A comprehensive review of the application of blockchain use cases proposed by the research community, including those in the built environment, may be found in Shen and Pena-Mora (2018). Detailed information about the potential to transform the built environment may be found in Nguyen et al. (2019).

The different applications of blockchain use various consensus algorithms for trust among the P2P network over the state of the ledger, ensuring an increased level of transparency and consistent view of the blockchain (Saad et al., 2019). The blockchain is immutable once chained and has an algorithm ensuring that all nodes have the same version of the blockchain. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions (Nomura Research Institute, 2015). Fundamentally, the cryptographic construction of blockchains is the same across all different applications, regardless of the consensus algorithms (Garay and Kiayias, 2020). A fundamental property of blockchain is the hash, which is a unique public but pseudonymous key in the form of an alphanumeric string, usually containing 27 to 32 characters (Li et al., 2018). Owing to the asymmetric property of the blockchain, the relation between hashes is in the form of one-way and collision-resistant hash functions, making the blockchain immutable and tamper-proof (Konashevych and Poblet, 2018). Hence, if an attempt to attack a block to make changes in the data of the block occurs, the attacker would be required to change data in all subsequent blocks and, at the same time, to execute the consensus protocol correctly for all blocks individually. This process is an indication of the difficulty of achieving malicious attacks on blockchains.

Given all the nodes in the blockchain are connected in the P2P network, a "gossip protocol" is used for the nodes to exchange information. Ideally, every block would possess a copy of the blockchain. However, a set space constraint is placed on the node due to the append-only model and the growing size of the blockchain, as explained by Saad et al. (2019). This issue is addressed with the breakdown of nodes into full and lightweight nodes, such that the full nodes have a full copy of the blockchain and take part in the transaction propagation process while the lightweight ones keep the block header to verify the newly published block.

3.1 Benefits of blockchain to the CSC

The potential of blockchain applications in the CSC is high. The technology can facilitate the main targets of cost, transparency, security, trust, speed, dependability, risk reduction, sustainability, and flexibility (Kshetri, 2017). Different studies have been conducted on the classification of blockchain applications to the CSC. According to Saberi et al. (2019), the technology is capable of highlighting at least the following five key product dimensions: 1) nature, or what it represents; 2) quality, or how it is; 3) quantity, or how much there is; 4) location, or where it is; and 5) ownership, or who owns it. However, the framework is mainly a conceptual one rather than applied methodology in real-life applications. According to Queiroz et al. (2019), it is limited to application in the supply chain of the electric power industry.

Tezel et al. (2020) provided a review on how blockchain can digitally integrate supply chains, including the CSC. In blockchain-based supply chains, four major entities are emphasized (Project Provenance Ltd., 2015; Saberi et al., 2019): 1) the registrar provides identities to the nodes in the network (the parties involved), 2) standard organizations are responsible for the blockchain policies and technological requirements, 3) certifiers provide certification to the parties taking part in the network, and 4) actors are the parties involved, such as manufacturers, contractors, retailers, customers, consultants, and project owners, who require registration by a certifier to maintain system trust. Wang et al. (2017) classified the different types of applications across the CSC into three categories: 1) notarization-related applications are used to reduce the time required for verifying a document's authenticity, 2) transaction-related applications are used for facilitating automated procurement and payment, and 3) provenance-related applications are used to improve the transparency and traceability of the CSC.

Regarding notarization-related applications, Wang et al.

(2017) stated that with the use of blockchain, every document is stored in the distributed ledger such that a notarization exists for each creation, deletion, and any updates across the system. The system interprets the information stored on the transactions and enables the authentication. Many large construction companies can benefit if they integrate blockchain technology into recording construction quality data, project updates, and resource-consuming data for on-site operations.

Regarding transaction-related applications, smart contracts can be used for facilitating automated procurement and payment (Omohundro, 2014). In the CSC, late and missed payments are a case most of the time, especially in obtaining materials and matching them with engineering drawings and design. Issues experienced, as previously outlined, are specification quality of materials, ISO (International Standardization Organization) standards, and fabrication specification. In this part of the chain, the project owner does not play a major role because the two partners are independently working on the project. Thus, a higher level of traceability is required. Smart contracts can embed funds into the contract to protect the contractors, subcontractors, external partners, and providers from insolvency (Li et al., 2018). Once a smart contract is coded and embedded into the blockchain, it then becomes permanent, irrevocable, and unchangeable. If errors are detected, including improper data, information, and payment, the smart contract can be canceled and replaced with a new one once it has been uploaded to the blockchain (Li et al., 2018). Even though smart contracts can be considered efficient, longevity is a potential issue associated with them. Cryptocurrencies are volatile for value and exchange rates against fiat currencies, making them slightly challenging to rely on or implement (Li et al., 2018).

Owing to the inherent provenance nature of the architecture of blockchain technology, the supply of each product or service can be traced backward with authenticity from a compliance or quality assurance perspective (Wang et al., 2017). Such tracing alone provides a solution to the transparency and traceability concerns associated with the CSC. Many times during the construction phase, products are found to be defective. The responsible party for this product can easily trace its origins on the system because the history of all transactions is stored, making the product exchanging process easy and efficient.

Given that the construction industry is moving toward digitization, in the long run, it can benefit from the use of smart contracts not only for facilitating payment and procurement but also for forming a decentralized autonomous organization (DAO). Hughes (2020) defined DAO as an organization run through rules encoded as computer programs using smart contracts. He further explained that DAO can be used for the early stages of the project, the construction phase, and during the in-use and maintenance phase. In the construction phase, the different work orders would be integrated into the system, such as light fitting, wall color selection, or temperature and humidity range in occupied areas. As Hughes (2020) emphasized, the requirements and decisions generate a series of "if/then" statements using interrelated smart contracts exchanged between the project owner, main contractor and subcontractor, manufacturer, and material supplier. Although these parties are mainly involved until the hand-over phase, a group of large construction companies (project owners) continues to maintain their buildings after the hand-over. A building management system (BMS) is used for facility management of buildings, and the integration of blockchain and BMS could potentially lead to creating a building's DAO such that work orders can be placed, monitored, and easily resolved. Li et al. (2019) indicated that BIM can also benefit from the integration of smart contracts, blockchain, and IoT, with significant effects on construction activities and facility management. Blockchain can provide solutions to multiple issues when BIM is used, such as limited collaboration and information sharing (Mathews et al., 2017). Kinnaird and Geipel (2017) indicated that ownership and rights can be emphasized and made transparent to all parties involved in the blockchain, such that legal issues and those of shared-access BIM models will be eliminated. Furthermore, Mason (2017) identified BIM as a precursor to intelligent contracts where blockchain serves as the operating platform. Given the early-stage development of blockchain technology and the need for human intervention in construction projects, Mason and Escott (2018) stated that semi-automation is a better approach than full automation.

3.2 Limitations of blockchain to the CSC

Although studies indicate that the construction industry can improve efficiency, transparency, and traceability from the use of blockchain applications, many of the applications mentioned above remain theoretical and require time to be implemented in real-life projects. Although technology promises many advantages and benefits to the construction sector, some limitations must be accounted for (Zheng et al., 2018). The first main challenge is the high cost of implementing blockchain because all building systems or components would require IoT-enabled devices. The second challenge is the wide-spread time lag because blockchain developers have not provided yet 100% industry-tested blockchain applications for the construction industry (Heiskanen, 2017). Technical limitations also exist (Swan, 2016). Throughput is the first limitation. At present, the maximum number of transactions per second is seven. Latency is the second major limitation. In general, each block takes about 10 min to process. Thus, a period of 10 min is required for a transaction to be confirmed. Size and bandwidth comprise the third major technical limitation. A long time is needed to download the entire blockchain.

Business-related and operational challenges also exist (Nowiński and Kozma, 2017). Although 40%–50% of construction companies are willing to move toward the digital supply chain and apply blockchain, the construction industry is still very slow in adopting new technologies. Marks (2017) emphasized that the industry is highly stagnant due to resistance by construction companies to invest in the adoption and integration of technological advancement. Thus, even if construction companies are willing to move toward digitization, they are not necessarily willing to invest in integrating new technologies. Companies are used to the traditional supply chain, and as previously indicated, the required level of trust for successful project completion is difficult to determine and even harder to achieve (Li et al., 2019). These difficulties represent one more reason why construction companies are resistant to investment in new and not yet 100% proven-to-be effective technologies.

Even though one of the main advantages of using blockchain is enhanced security, blockchain vulnerability attacks are a form of cyber-security limitations. Blockchain applications have authentication and integrity associated with confidential data. Blockchain systems and applications are prone to various security threats. Multiple types of attacks are associated with specific applications and additional layers of the blockchain systems, including transaction verification, consensus algorithms, network, protocols, and smart contracts. Table 1 provides a summary of the most common types of attacks, and their root causes and severity based on the effect of the attack. The taxonomy of the attacks discussed in Table 1 is described in the following sections. The attacks in this paper are categorized into architecture, network, and application-level attacks for supporting analysis simplicity and clarity.

3.2.1 P2P architecture attacks (Double-spending attacks)

These attacks are also known as double-spending attacks, in which one peer attempts to use the same cryptocurrency in more than one transaction (Mosakheil, 2018). Double-spending attacks are related to the cash flow of the blockchain and could be applied to various blockchain systems depending on the type of transaction that is transferred. The main objective of these attacks is to capitalize on transactional or fundamental elements of algorithms to conduct the attacks, disturbing the nature or goal of each transaction. Although many types of double-spending attacks exist, Majority and Race attacks are the most widely known and tried on the Bitcoin network and consensus protocols. Thus, these two types of attacks are explained in detail below.

Majority Attack (51% Attack): This attack is a type of double-spending attack. It can be exploited when either 1) a single attacker, 2) a group of Sybil nodes, or 3) a mining (verifying) pool in the network gets access to the majority of the hash rate in the network to manipulate the blockchain (Saad et al., 2019). Given the blockchain works

Table 1 Blockchain vulnerability attacks

Attack type	Attack name	Root cause	Severity
P2P architecture attacks (Double-spending attacks)	Majority Attack (51% Attack)	Transaction verification /Consensus mechanism	High: System transactional disruption and denial of service (DoS) is possible
	Race Attack	Transaction verification	Medium: Transactional fraud will be possible if the system did not detect the duplicate transaction. Mitigations are possible
	Vector76 Attack	Transaction verification	Low: Can be blocked by a central verification system
	Finney Attack	Transaction verification	High: Can cause a DoS on the resources assigned. Mitigation is possible, but if not well implemented, it can be difficult to detect
Network attacks	Domain Name System (DNS) Attack	Consensus mechanism	Low: Can be mitigated and detected
	Eclipse Attacks	Routing manipulations	High: Can cause significant disruption and DoS to the network. If botnets are utilized, it can be hard to control and mitigate
	Distributed Denial of Service (DDoS) Attack	External resources	High: Several attacks can lead to this result, blocking network resources. If no proper mitigation and recovery plan exists, this would have a critical effect on the system
Smart contracts attacks	Vulnerabilities in blockchain	Program design flaws	Low: Mitigation techniques are available. This attack is subject to vulnerabilities under evaluation
	Vulnerabilities in contracts source code	Program design flaws	Low: Mitigation techniques and verification mechanisms are available. This attack is subject to vulnerabilities under evaluation

under the consensus protocol that 51% of the nodes need to approve a transaction, a 51% vulnerability exists for attackers to take part in the network and manipulate the blockchain (Mosakheil, 2018). Under the three types of attacking mechanisms used by the attacker(s), the attacker(s) can completely turn the network unstable. With the possession of the majority of the hash rate of the network, according to Saad et al. (2019), the attacker can:

- Prevent transactions or blocks from being verified; however, they do not have the power to prevent the transactions from being sent;
- Allow double-spending, by which they are capable of reversing transactions during the time they have control over the hash;
- Isolate the participants in the network to prevent them from verifying and finding any other blocks for a short period;
- Access the main blockchain and split the network, hence being able to make it fully unstable.

This attack is the worst-case double-spending attack that could happen to a blockchain. However, according to data presented by Mosakheil (2018), such an attack has not been successful until this point because of the difficulty of taking over more than 51% of the power of the network.

Race Attack: This attack occurs when an attacker is sending two conflicting transactions one after the other into the network (Mosakheil, 2018). The target of this attack is the node with status 0-unconfirmed. In this case, the transaction sent has not yet been added to the system but is visible (Dasgupta et al., 2019). The attack is known to be successful in consensus mechanisms that follow the Proof of Work consensus algorithm. Race attacks can be more applicable to organizations that rely on cryptocurrencies for payment systems for product purchasing. To avoid this type of attack, nodes should not consider a transaction valid before a few nodes have confirmed the transaction (Dasgupta et al., 2019). In any service industry, including the CSC, these attacks can be achieved successfully.

3.2.2 Network attacks

Multiple types of attacks are associated with blockchain networks and their elemental building blocks, among which the most widely known are the domain name system (DNS), Block Withholding, distributed denial of service (DDoS), and Eclipse attacks. In these attacks, the main goal of the attacker is to isolate users and miners from the real P2P network, limit their access to the resources available in the network, and then create a partition in the network, as well as to enforce conflicting rules among peers (Saad et al., 2019). The objective of these attacks is to minimize access to network resources to lead the entire system operation into halting.

DNS Attack: For a new node in the system to find out who the other nodes are, a bootstrapping mechanism is required, and DNS is used as one such mechanism. According to Saad et al. (2019), "DNS seeds are queried by nodes upon joining the network to obtain further information about other active peers". The command "addr" is used by the new node to initiate a connection with the new nodes, only once it has been added to the system. DNS is mainly used in the Bitcoin network. However, it can be applied to various blockchain applications. DNS is vulnerable to cache poisoning, resolver attacks, or stale records (Saad et al., 2019). In general, for this type of attack, the attacker can feed the user with fake blocks and transactions because the attacker can poison the DNS cache and partially or fully modify the data. The attacker can reallocate the user to another network by sending wrong information, and in the meantime, the attacker can take control over the network. A blockchain software client possesses a specific list of seeders with the right to provide others the chance to discover the network. When an attacker is feeding false information, they can instantly inject a fake list of seeders, such that the user will be completely compromised. DNS attacks can be used for money transferring, meaning to steal money by breaking the confidentiality of the network given money transactions are private and occur between two parties only. To a certain extent, DNS attacks could be used for injecting wrong information as regards product specification, quality assurance, and fabrication specifications for the service industry blockchain applications. The attacker can easily take over the network because these types of documents are part of public blockchains most of the time, such that the attacker can ruin the brand image of a specific company for that, according to wrong documentation, it might seem like they do not operate following rules and regulations.

Eclipse Attack: In this attack, a few nodes grouped try to isolate some of the neighboring nodes using IP addresses to compromise any flow of incoming and outgoing information (Saad et al., 2019). The view of honest nodes can be fully compromised by the attacker, feeding them with the wrong data (the name Eclipse originates from the formation of honest and dishonest nodes). The requirement to remain the true state of the network is having two adjacent honest nodes to exchange information, so both can receive correct data. However, if these nodes are surrounded by attackers, then they can be compromised. When the information of the honest nodes is changed, and the nodes are compromised, the attackers can change the blockchain and divert the honest nodes to a wrong view of the blockchain.

DDoS Attack: These attacks are highly common in blockchain applications because the technology is prone to such attacks. The attacker's primary goal is to disable one network's ability to service legitimate traffic because the attacker is trying to take advantage of the network and injecting excessive and wrong information and the number of requests to the network (Dasgupta et al., 2019). DDoS can be individually applied to all three categories of blockchains (i.e., private, public, and

consortium blockchain). In a private blockchain, DDoS can be launched if the adversary controls approximately 33% replicas, and the adversary can estimate the number of Sybil nodes needed for the attack to be executed (Saad et al., 2019). In a public network, the attack can be executed with the adversary possessing more than 50% of the network peers, but it is not very frequently tried in such networks because it is costly (Saad et al., 2019).

Given that construction projects have a large pool of participants in all phases, as discussed earlier, in such blockchain applications, the nodes are segmented into full and lightweight nodes. Given that lightweight nodes can draw their view of the blockchain from the full nodes, in the case of a full node being compromised, all of its associated lightweight nodes will also be compromised (Saad et al., 2019). For example, in the process of multiple contractors delivering products to the site, some contractors will be the full nodes alongside the project owner who oversees the site, while subcontractors would represent the lightweight nodes.

3.2.3 Smart contracts attacks

This section emphasizes application-level attacks. Arguably, the most current and common application of blockchain is smart contracts, and these can also be attacked (Atzei et al., 2017). The attacks associated with smart contracts use vulnerabilities in blockchain as well as in contracts source code (Groce et al., 2019).

Vulnerabilities in the blockchain: One such vulnerability is the Unpredictable State, and the leading cause is the actual state of the contract, which is changed before invoking applicable rules (Mosakheil, 2018). This vulnerability occurs because the transaction sender does not know whether the state and time of sending the transaction will match that of the contract when the transaction was sent (Mosakheil, 2018). Other types of blockchain vulnerabilities related to smart contracts include Time Dependency and Generating Randomness.

Vulnerabilities in contracts source code: These attacks are at the solidity level. Some attacks are related to errors in the functions written within the code, the transfer of transactions, and different disorders in the code (Mosakheil, 2018). Sometimes, if a non-existent function is called to execute a specific action, a malicious fallback function might be executed such that attackers can exploit this vulnerability to call their fallback functions to attack the code and cause issues with the execution of the smart contract. Other vulnerabilities at the solidity level are related to type errors, sometimes causing the wrong code to be executed, and the person calling the function might be unaware of the error (Mosakheil, 2018).

4 Case study: A blockchain application to CSC

An emergent framework design is presented for the use of smart contracts in the initial stages of the CSC. The block-diagram representation in Fig. 2 illustrates the two main participants involved (raw material supplier and manufacturer) and the three types of flows in the system (information, material, and cash flow). The designers and engineers related to the manufacturer would be participants as lightweight nodes because they are minor parties involved in this portion of the supply chain.

Information flows both ways because the two parties need to either send or receive. This information includes invoices (both sides send and receive), quality specification of materials (supplier sends to manufacturer), material specifications/ISO (supplier sends to manufacturer), material standards (supplier sends to manufacturer), fabrication specifications (manufacturer sends to supplier), storing and shipping specifications (supplier sends to manufacturer), rules and regulations for fabrication (manufacturer sends to supplier), and order due dates (manufacturer sends to supplier). Cash (payment transaction) flows from right to left, i.e., from the manufacturer to the supplier. Cash also flows from the manufacturer to the designer and engineer. Material flows from left to right, which means the supplier is shipping it to the manufacturer. In this flow, any means of organizing transportation are the responsibility of the supplier, and the respective payments are included in the cash flow. The types of materials that could be sent include supplies, services, components, and products.

Notably, this blockchain application would fall under the

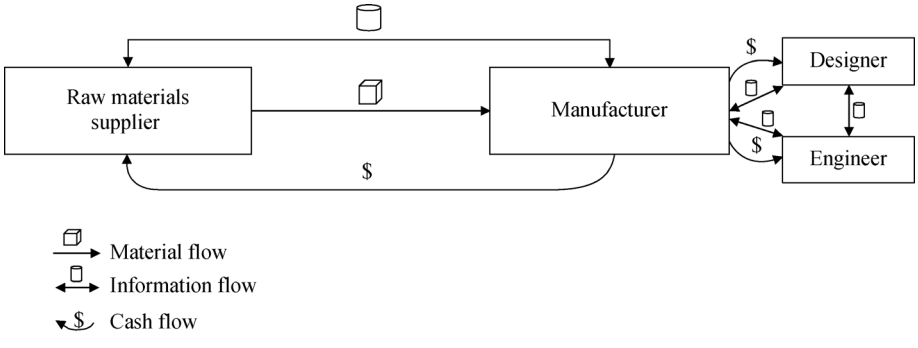

Fig. 2 Blockchain framework for the early stage of the CSC.

consortium (or semi-private) blockchain category because some of the data need to be open to multiple parties (that is, to be transparent) like rules and regulations, material quality standards, shipping information and time, while some data need to be kept safe and confidential (payments between the parties). This balance allows for a higher level of transparency and efficiency. However, as previously discussed, blockchain applications can be attacked. In this section, a threat model is presented for a specific case scenario for the initial stage of a CSC to outline potential attacks and how to prevent them.

Example: Manufacturing of prefab concrete pads

The case scenario for the framework is based on the example of producing concrete pads for the needs of a construction project for building a facility requested by the owner. This blockchain involves four participants, and they are represented in Fig. 3.

For purposes of this study, no connection is assumed between the three suppliers because their products are independently shipped to the manufacturer. For simplicity, the manufacturer is assumed to internally control the design and engineering of the prefabricated concrete pads, such that those two minor parties (designer and engineer) are excluded from the framework. The visual representation shows that the processes of sending information, receiving materials, and making payments are conducted individually between the manufacturer and suppliers.

4.1 Case logic implementation

To design this scenario and its specific application, the use of the concept from the Hyperledger Fabric[1)] open blockchain platform is considered (Cachin, 2016). In the distributed network, every participant has an ID, name, and location. Variables are represented through a string. An example of the code for defining a participant is shown below:

```
participant Manufacturer identified by manufacturerId {
String manufacturerId
String name
String location
}
```

The asset is used to define the type of action done by the participants. For all three products (cement, sand, and gravel), an asset with specific actions will be used. An example of the code for the cement asset is shown below:

```
asset CementProduct identified by CementProductId {
String CementProductId
String ProductName
DateTime Creation
Integer Quantity
Boolean FakeProduct
Boolean QualityAssurance
Boolean MaterialISO
Boolean Completed
Boolean PaymentCheck
Double Longitude
Double Latitude
String Status
⇒ Supplier cement_supplier
⇒ Manufacturer
}
```

The asset function has some key points. The lines with "String" take the name and ID of the product from the strings as well as the status of the product point in the delivery process. The role of "DateTime" provides information on when the product was made. The role of "Boolean" is to check if the material delivered is fake (counterfeit), its quality, whether the material ISO standards are met, and if the delivery of the product has been completed on time. The role of "Integer" is to check the quantity of material ordered by the manufacturer.

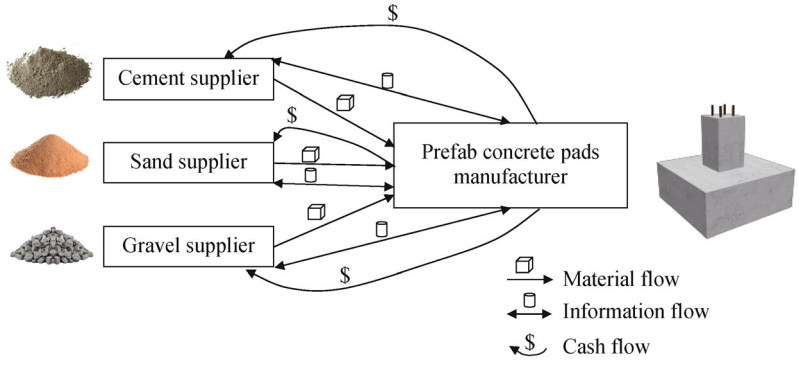

Fig. 3 Parties and transactions involved in the manufacturing of prefab concrete pads for a construction project.

1) Hyperledger Fabric is an enterprise-grade permissioned distributed ledger framework for developing solutions and applications (for more information please refer to github.com/hyperledger/fabric).

"Double" is used for longitude and latitude to check the location of the product in the delivery process. The last two lines indicate the participants for the exchange of information concerning the given asset. In the case of cement, the participants are the manufacturer and cement supplier.

The "transaction" is used to indicate the action executed through the specific transaction. Transactions used in this example would be to check if the material is fake (counterfeit), the quality of the material, material ISO, and the status of the material in the delivery process. Payment transactions are used in this part to execute the payment between the two participants. The example code illustrated below is part of the code used for checking if the quality of the product matches the expected quality:

```
transaction QualityAssurance {
⇒ ConcreteProduct asset
Boolean QualityAssuranceNewVal
}
```

In defining the network, some of the transactions will be private. In this example, it is the payment transaction, because the payment is relevant only to those parties that participate in the payment. The transactions used for aspects such as checking the quality of materials, the ISO standards, as well as location, are supposed to be public because non-participants can have access to them, meaning the transparency and efficiency of the project will be enhanced through more transparent and easily traceable process. The participants that have access to the network and specific transactions are explicitly defined in the blockchain before executing any transactions.

4.2 Threat model

A threat model is used to determine the security risks (i.e., possible attacks) to a given process, product, or network with the ultimate goal to define which threats require mitigation and decide on possible countermeasures. A general process for a threat model is shown in Fig. 4. This section describes a fundamental threat model analysis for the case presented. The analysis is essential to identify potential vulnerabilities (unutilized weakness), threats (activated weaknesses), and risks (the effect of threat) that the model will impose. Additionally, it will help in identifying mitigation and protection mechanisms.

The blockchain considered in this example (system) is a combination of private and public elements. Thus, different attacks can occur when analyzing threats, vulnerabilities, and risks. Table 2 summarizes the possible attacks identified for this case. Attacks within this model are actualized threats. To provide a general view, the detailed vulnerabilities and threat analysis will not be provided. The following text gives an overview of when each of the four identified attacks can occur and how they can be prevented (possible countermeasures).

Race Attack: This attack can occur when the attacker

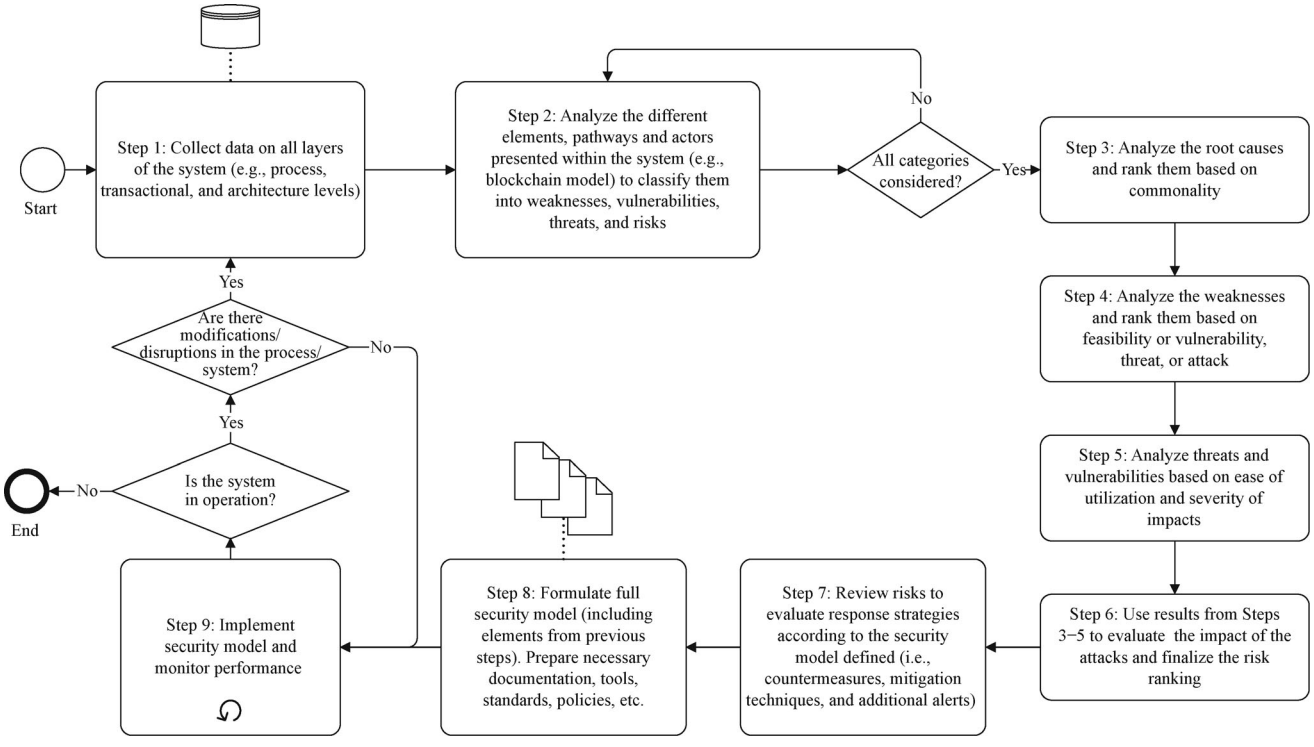

Fig. 4 Overview of the main steps to conduct a threat model.

Table 2 Potential attacks

Attack type	Attack name	Root cause	Severity
P2P architecture attack	Race Attack	Transaction verification	High: It can cause DoS ultimately
Network attack	DNS Attack	Consensus mechanism	Medium to Low: Especially if no central check and controls are applied
	DDoS Attack	External resources	Medium to High: Depends on the vulnerability that is utilized. This can affect the whole network
Smart contracts attack	Vulnerabilities in contracts source code	Program design flaws	Medium to Low: It can be mitigated through introducing frequent application-level checks

sends two conflicting transactions one after the other into the network. Transactions, including tracking material and checking quality assurance and quantity of material purchased, can be attacked with a Race Attack. The attacker targets transactions that have been sent but not yet added to the system and, at the same time, are visible (Dasgupta et al., 2019). In other words, the cement supplier has sent the documents related to the quality of the material. However, the manufacturer is the node in the chain that has not verified the transaction yet. The manufacturer would be the node with 0-unconfirmed status, and the attacker can then send the manufacturer documents with the wrong information. Given that this is a double-spending attack, the payment transaction can be targeted most of the time, such that the attacker wants to take advantage of the intermediate time between the initiation and confirmation of transactions to launch a double-spending attack (Mosakheil, 2018). In this case, the attacker injects wrong information regarding payments, possibly resulting in obtaining more money from the manufacturer.

Countermeasures: A few studies have been conducted on how to countermeasure the double-spending attacks, and in particular, the Race Attack. Many of these studies are based on the Bitcoin network. However, they can be adapted to the transactions in this case study. A proposal for an attack model that enables the detection of double-spending attacks in fast transactions has been written by Karame et al. (2012). One effective technique that is analyzed in their study is known as "forwarding double-spending attempts". The participants "propagate alerts whenever they receive two more transactions that share common inputs and different outputs" (Mosakheil, 2018), which is a double-spending attempt. With propagated alerts, the participants can easily detect if an attack is attempted on the network.

DNS Attack: The attacker attempts to send wrong information to the network to reallocate the participants to another network, and in the meantime, to take control over the network. The attacker can inject a fake list of seeders, and the participants will be compromised. When delivering materials to the manufacturer, the attacker can inject wrong data into the transaction regarding the material's location. Such an event can cause delays in the process, increased costs, and reduced trust between the two participants exchanging information (in this case, the manufacturer and supplier). The attacker can also send wrong information regarding the product manufacturing specifications and ISO standards. Given the DNS has been attempted successfully on the Bitcoin network, it can also be attempted on the payment transactions for breaking the confidentiality of the network and stealing money from the participants.

Countermeasures: High-security measures should be adopted in the process when the network and its participants are defined. For a specific construction project, most participants are defined at the beginning of the project such that the network can be closed for adding new participants or at least adding new full nodes (primary participants). This process would reduce the chance of a DNS Attack because a new full node would not be able to access the network and establish a communication with the active participants. Given the consortium nature of the blockchain, the read permission could be public. However, it can be restricted if the participants detect that an attack on the network has been attempted. The immutability of the blockchain could also be tampered using DNS. If the read permission is restricted, the immutability would be nearly impossible.

DDoS Attack: The costs are high for attempting execution of the DDoS Attack on a public platform. However, it can be launched in private blockchain only if the adversary controls around 33% of the replicas (Saad et al., 2019). For the case in this study, the blockchain is federated or a blockchain consortium and the likelihood for DDoS Attack to occur is moderate. The attacker needs to possess more than 50% of the network peers to execute the attack. Given the increased risks of higher costs for the attacker with an unsuccessful attempt, it is less likely for them to attempt this attack.

Countermeasures: Given that DDoS is less likely to occur if central controls are in place, countermeasures might not be necessary. If this is not the case, then meticulous resources allocation, access control, and authentication mechanisms to the network nodes should be applied to prevent malicious nodes activities that can lead to resource disruptions, especially in the cases that allow botnet construction within the network.

Vulnerabilities in contracts source code: The functions related to specific transactions might execute

undesired results. In the case outlined, a transaction about the location of the material does not include necessary information either on the longitude or latitude, and the system can experience errors, leading to the execution of a malicious fallback function. Type errors can be experienced, as well. Therefore, the wrong code might be executed without the participant being aware of it.

Countermeasures: The code must always be checked multiple times. However, these vulnerabilities are sometimes unavoidable because construction projects involve too many transactions and participants.

5 Conclusions and future work

The CSC is a complex network of multi-stage participants exchanging information, materials, and cash. Due to the nature of construction projects, the process is highly fragmented. Also, the different amount of participants and the large amount of data exchanged make the process highly inefficient. Blockchain applications could considerably change the CSC process. This study sets the bases to show that blockchain could be used to address the issues of productivity and efficiency and reduce the level of fragmentation present in the construction industry. From the blockchain taxonomy derived in this paper, the benefits from the application of blockchain to the CSC process, when implemented correctly within high-security requirements, were deduced to outweigh the harms and risks associated with the flowing of information and data protection.

In addition to the literature review, a hypothetical CSC scenario served as a case study to perform a partial threat analysis of the blockchain model was applied, indicating potential attacks and the countermeasures required to prevent them. Although blockchain will promote transparency and help to increase efficiency in construction projects, it will also create the possibility for malicious attacks to be executed, hence impacting construction participants. Ongoing work by the authors include the development of 1) a detailed framework with a quantifiable threat model simulation that can be optimized with trial and error or probabilistic analyses of detected threats and attacks, and 2) countermeasures for the different blockchain attacks discussed in this study.

Acknowledgements The authors are grateful for the support from the Center for Cyber Security (CCS) at New York University Abu Dhabi (NYUAD).

References

Aloini D, Dulmin R, Mininno V, Ponticelli S (2012). Supply chain management: A review of implementation risks in the construction industry. Business Process Management Journal, 18(5): 735–761

Atzei N, Bartoletti M, Cimoli T (2017). A survey of attacks on Ethereum smart contracts (SoK). In: Proceedings of 6th International Conference on Principles of Security and Trust. Uppsala: Springer, 164–186

Barbosa F, Woetzel J, Mischke J, Ribeirinho M J, Sridhar M, Parsons M, Bertram N, Brown S (2017). Reinventing construction: A route to higher productivity. McKinsey Global Institute

Behera P, Mohanty R, Prakash A (2015). Understanding construction supply chain management. Production Planning and Control, 26(16): 1332–1350

Bhargava V, Chander R, Favilla J R, Kaijim W, Lin S (2019). Engineering and construction digital supply chains. IBM Institute for Business Value

Cachin C (2016). Architecture of the Hyperledger blockchain fabric. In: Workshop on Distributed Cryptocurrencies and Consensus Ledgers, 310: 4

Dasgupta D, Shrein J, Gupta K D (2019). A survey of blockchain from security perspective. Journal of Banking and Financial Technology, 3: 1–17

Feng C, Ma Y, Zhou G, Ni T (2018). Stackelberg game optimization for integrated production-distribution-construction system in construction supply chain. Knowledge-Based Systems, 157: 52–67

Garay J A, Kiayias A (2020). SoK: A consensus taxonomy in the blockchain era. In: Cryptographers' Track at the RSA Conference. San Francisco, CA: Springer, 284–318

Garcia de Soto B, Agusti-Juan I, Hunhevicz J, Joss S, Graser K, Habert G, Adey B T (2018). Productivity of digital fabrication in construction: Cost and time analysis of a robotically built wall. Automation in Construction, 92: 297–311

Gerbet P, Castagnino C, Rothballer S, Rothballer C, Renz A, Filitz R (2016). The transformative power of building information modelling. Digital in Engineering and Construction, Boston Consulting Group

Groce A, Feist J, Grieco G, Colburn M (2019). What are the actual flaws in important smart contracts (and how can we find them)? Cornell University, arXiv: 1911.07567

Heiskanen A (2017). The technology of trust: How the Internet of Things and blockchain could usher in a new era of construction productivity. Construction Research and Innovation, 8(2): 66–70

Hughes D (2020). The impact of blockchain technology on the construction industry. Medium

Johnston D A, McCutcheon D M, Stuart F I, Kerwood H (2004). Effects of supplier trust on performance of cooperative supplier relationships. Journal of Operations Management, 22(1): 23–38

Kadefors A (2004). Trust in project relationships—inside the black box. International Journal of Project Management, 22(3): 175–182

Karame G O, Androulaki E, Capkun S (2012). Double-spending fast payments in bitcoin. In: Proceedings of the ACM Conference on Computer and Communications Security. Raleigh, NC, 906–917

Kinnaird C, Geipel M (2017). Blockchain Technology: How the inventions behind bitcoin are enabling a network of trust for the built environment. London: Arup

Konashevych O, Poblet M (2018). Is blockchain hashing an effective method for electronic governance? In: 31st International Conference on Legal Knowledge and Information Systems. Groningen: IOS Press, 195–199

Kopczak L R, Johnson M E (2003). The supply-chain management

effect. MIT Sloan Management Review, 44(3): 27–34

Kshetri N (2017). Will blockchain emerge as a tool to break the poverty chain in the global south? Third World Quarterly, 38(8): 1710–1732

Li J, Greenwood D, Kassem M (2018). Blockchain in the built environment: Analysing current applications and developing an emergent framework. In: Proceedings of the 6th Creative Construction Conference. Ljubljana: Diamond Congress Ltd.

Li J, Greenwood D, Kassem M (2019). Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases. Automation in Construction, 102: 288–307

Maciel A (2020). Use of blockchain for enabling Construction 4.0. In: Sawhney A, Riley M, Irizarry J, eds. Construction 4.0: An Innovation Platform for the Built Environment. London: Routledge

Mantha B R K, Garcia de Soto B (2019). Cyber security challenges and vulnerability assessment in the construction industry. In: Proceedings of the 7th Creative Construction Conference. Budapest: Diamond Congress Ltd.

Mantha B R K, Jung Y, Garcia de Soto B (2020). Implementation of the common vulnerability scoring system to assess the cyber vulnerability in construction projects. In: Proceedings of the 8th Creative Construction Conference. Budapest: Diamond Congress Ltd.

Marks M (2017). Construction: The next great tech transformation. McKinsey & Company

Mason J (2017). Intelligent contracts and the construction industry. Journal of Legal Affairs and Dispute Resolution in Engineering and Construction, 9(3): 04517012

Mason J, Escott H (2018). Smart contracts in construction: Views and perceptions of stakeholders. In: Proceedings of FIG Conference. Istanbul

Mathews M, Robles D, Bowe B (2017). BIM + blockchain: A solution to the trust problem in collaboration? In: CITA BIM Gathering. Dublin

Mendling J, Weber I, van der Aalst W, vom Brocke J, Cabanillas C, Daniel F, Debois S, Di Ciccio C, Dumas M, Dustdar S, Gal A, Garcia-Banuelos L, Governatori G, Hull R, La Rosa M, Leopold H, Leymann F, Recker J, Reichert M, Reijers H A, Rinderle-Ma S, Solti A, Rosemann M, Schulte S, Singh M P, Slaats T, Staples M, Weber B, Weidlich M, Weske M, Xu X, Zhu L (2018). Blockchains for business process management—challenges and opportunities. ACM Transactions on Management Information Systems, 9(1): 4

Mosakheil J H (2018). Security threats classification in blockchains. Culminating Projects in Information Assurance, 48. St. Cloud, MN: Department of Information Systems, St. Cloud State University

Nguyen B, Buscher V, Cavendish W, Gerber D, Leung S, Krzyzaniak A, Robinson R, Burgess J, Proctor M, O'Grady K, Flapper T (2019). Blockchain and the built environment. London: Arup

Nowiński W, Kozma M (2017). How can blockchain technology disrupt the existing business models? Entrepreneurial Business and Economics Review, 5(3): 173–188

Nomura Research Institute (2015). Survey on blockchain technologies and related services. FY2015 Report

O'Brien W J, Fischer M A (1993). Construction supply-chain management: A research framework. In: Proceedings of Civil-COMP, Information Technology for Civil & Structural Engineers. Edinburgh, 61–64

Omohundro S (2014). Cryptocurrencies, smart contracts, and artificial intelligence. AI Matters, 1(2): 19–21

Papadopoulos A G, Zamer N, Gayialis P S, Tatsiopoulos P I (2016). Supply chain improvement in construction industry. Universal Journal of Management, 4(10): 528–534

Pärn E A, Garcia de Soto B (2020). Cyber threats and actors confronting the Construction 4.0. In: Sawhney A, Riley M, Irizarry J, eds. Construction 4.0: An Innovation Platform for the Built Environment. London: Routledge

Penzes B (2018). Blockchain technology in the construction industry: Digital transformation for high productivity. London: Institution of Civil Engineers (ICE)

Project Provenance Ltd. (2015). Blockchain: The solution for transparency in product supply chains. London

Queiroz M, Telles R, Bonilla S (2019). Blockchain and supply chain management integration: A systematic review of the literature. Supply Chain Management, 25(2): 241–254

Saad M, Spaulding J, Njilla L, Kamhoua C, Shetty S, Nyang D, Mohaisen A (2019). Exploring the attack surface of blockchain: A systematic overview. Cornell University, arXiv: 1904.03487

Saberi S, Kouhizadeh M, Sarkis J, Shen L (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7): 2117–2135

Schrauf S, Berttram P (2016). Industry 4.0: How digitization makes the supply chain more efficient, agile, and customer-focused. Strategy&, PWC

Sepasgozar S M, Razkenari M A, Barati K (2015). The importance of new technology for delay mitigation in construction projects. American Journal of Civil Engineering and Architecture, 3(1): 15–20

Shen C, Pena-Mora F (2018). Blockchain for cities—A systematic literature review. IEEE Access, 6: 76787–76819

Streule T, Miserini N, Bartlomé O, Klippel M, García de Soto B (2016). Implementation of Scrum in the construction industry. Procedia Engineering, 164: 269–276

Swan M (2016). Blockchain temporality: Smart contract time specifiability with blocktime. In: International Symposium on Rules and Rule Markup Languages for the Semantic Web. Rule Technologies. Research, Tools, and Applications. Stony Brook, NY: Springer, 184–196

Tezel A, Papadonikolaki E, Yitmen I, Hilletofth P (2020). Preparing construction supply chains for blockchain technology: An investigation of its potential and future directions. Frontiers of Engineering Management, in press, doi: 10.1007/s42524-020-0110-8

Turk Ž, Klinc R (2017). Potentials of blockchain technology for construction management. Procedia Engineering, 196: 638–645

Viriyasitavat W, Xu L, Bi Z, Sapsomboon A (2018). Blockchain-based business process management (BPM) framework for service composition in Industry 4.0. Journal of Intelligent Manufacturing, doi: 10.1007/s10845-018-1422-y

Vrijhoef R, Koskela L (2000). The four roles of supply chain management in construction. European Journal of Purchasing and Supply Management, 6(3–4): 169–178

Wang J, Wu P, Wang X, Shou W (2017). The outlook of blockchain technology for construction engineering management. Frontiers of

Engineering Management, 4(1): 67–75

Wang Y, Han J, Beynon-Davies P (2019). Understanding blockchain technology for future supply chains: A systematic literature review and research agenda. Supply Chain Management, 24(1): 62–84

Wong P, Cheung S (2005). Structural equation model of trust and partnering success. Journal of Management Engineering, 21(2): 70–80

Xue X, Wang Y, Shen Q, Yu X (2007). Coordination mechanisms for construction supply chain management in the Internet environment. International Journal of Project Management, 25(2): 150–157

Ye Z, Yin M, Tang L, Jiang H (2018). Cup-of-Water theory: A review on the interaction of BIM, IoT and blockchain during the whole building lifecycle. In: Proceedings of the 35th International Symposium on Automation and Robotics in Construction (ISARC). Berlin: IAARC Publications, 1–9

Zheng Z, Xie S, Dai H, Chen X, Wang H (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4): 352–375