Secure Data Transfer Through Inter-Planetary File System (IPFS) and Blockchain-Embedded Smart Contract Using Multi-Level Authority and Encryption

Benjamin Ilunuamie Alenoghena[1]

Muhammad Bashir Abdullahi[2]

Solomon Adelowo Adepoju[3]

&

Joseph Adebayo Ojeniyi[4]

Abstract

The introduction of Smart contract-embedded blockchain systems incorporated with building Information model (BIM) in construction projects brought about the transformation of public and corporate management. The system, although it has contributed to infrastructure development, still faces vulnerabilities such as eavesdropping, data tampering, and possible attacks, requiring a secure communication channel. This research aims to develop a secure system for transferring data through the Inter-Planetary File System (IPFS), BIM and a blockchain-embedded smart contract. The system will use multi-level authority and encryption to ensure the confidentiality, integrity, and availability of the transferred data. The use of IPFS and a smart contract will allow for decentralized and distributed storage and transfer of data, while the use of multi-level authority and encryption will provide additional security measures to protect against eavesdropping, data tampering and theft. The resulting system has the potential to revolutionize the way data is transferred and stored, with applications in various industries and contexts.

Key words: Building Information Model (BIM), Inter-Planetary File System (IPFS), Smart Contract, Encryption.

1.0 Introduction

By 2022, global construction spending is expected to reach 12.4 trillion US dollars (Li *et al.,* 2019). The introduction of new technologies such as Building Information Modelling (BIM) in the Architecture, Engineering, and Construction (AEC) industry has resulted in significant advancement, but this advancement comes with an increase in design cost and a steep learning curve (Chang *et al.,* 2017; Zhang *et al.,* 2013). Even though the construction industry has been evolving for centuries and researchers have been seeking innovative solutions for decades, numerous challenges remain in making the construction process faster, safer, cheaper, and more accurate (Zhang *et al.,* 2013).

When contracts are signed between a contractor and a client, the procuring entity provides various contract resources, including budgetary funds and relevant personnel for the contract's effective implementation (Zheng *et al.,* 2020). Payments are the lifeblood of construction projects, but in practice, consistent fund flows are rare, resulting in undesirable consequences such as delays, increased costs, poor performance, disputes, and bankruptcies, all of which could jeopardize the projects' success. Payment issues have been identified as one of the leading causes of construction project disputes

(Ahmadisheykhsarmast & Sonmez, 2020). Although very little research has been put into developing smart contract systems for the security of payments, the introduction of embedded smart contract blockchain systems provided a solution to these problems (Ahmadisheykhsarmast & Sonmez, 2020).

Prior to this research, there exist a Blockchain-enabled smart contract that automates the conditioning of construction payments on the progress assessments. Enabled by an on-site reality-capturing Unmanned Automated Vehicle (UAV) to observe and get the progress from the job site. The system made use of IPFS and BIM (Hamledari & Fischer, 2021). Despite its advantages, IPFS (Inter Planetary File System) lacks a mechanism for content encryption. Instead, IPFS accesses shared content (data) by hashing the data. As a result, users cannot share sensitive information via IPFS (Alwis, 2020).

The most crucial aspects of data protection are secure communication and data confidentiality, which means guarding against unauthorised access or theft. By using data encryption and decryption, cryptography can help achieve these goals (Alenezi *et al.*, 2020). The importance of having a secure communication channel cannot be overstated as the channel can be vulnerable to attacks like man-in-the-middle (MitM) attacks (Mallik *et al.*, 2019), in which the perpetrator places himself between the UAV and the IPFS to either listen covertly or to impersonate one of the parties. He can then alter the data to the benefit or disadvantage of the contractor or the client while making it appear as though an ordinary exchange of information is taking place. To that effect, there is a need for the encryption of the channel of transfer of data from the supervisor (UAV) who inputs the progress of the construction to the IPFS. The rest of this paper is organized as follows. Section 2 discussed the related literature, section 3 dived into the methodology used, section 4 discussed the result and finally conclusion in section 5.

2.0 Literature Review

The research and integration of blockchain smart contracts in other domains have been on the high side as the technology brings about a lot of possibilities, yet little research has gone into examining the feasibility and applicability of this promising tool in AEC. Before the integration of blockchain into construction management, previews research proposed measures to Improve construction contract management. For example, standard construction contracts have been proposed by many countries and regions as references for contract formalization for specific types of construction projects, such as the FIDIC contract (Nael, G., 2005). However, standard construction contracts focus on the improvement of the contract structure and are still difficult to interpret by individuals who are not lawyers by profession. To simplify contract management, e-contracts were proposed. E-contracts are created by analyzing relationships between the contract participants and contractual information, followed by modelling traditional textual contracts in XML format (Cardoso & Oliveira, 2008). However, current applications of e-contracts are mainly found in the electronics trade, where the complexity of relationships between parties, obligations, and activities is simpler compared to that in construction contracts.

Despite the availability of digitized progress data, payment automation in AEC is just beginning to receive attention as projects still rely on traditional payment applications that are time-consuming, information-intensive, and cannot support payment automation (Penzes *et al.*, 2018). Researchers over the years have tried to show how much impactful the integration of blockchain into the AEC. (Hamledari & Fischer, 2021b) who researched the role of Blockchain-Enabled Smart Contracts could play in Automating Construction Progress Payments, due stated that progress payment automation is still far from reality, the writer also presented the theory of social reality to identify the underlying barriers that hinder the automation. The writer also argued that the reliance on centralized control, execution mechanisms, and lack of guaranteed execution, the current payment applications, and their supporting contract documents, even when computerized, cannot support progress payment automation. The paper concluded that the introduction of blockchain-enabled smart contracts could bring about the automation of payments by converting product flow (the observation of as-built conditions) to cash flow (progress payments) without reliance on the role of intermediaries.

Few research has tried to store and automate the payment of contracts using blockchain smart contracts with reviews on how much impact blockchain will bring to the automation of payment systems. (Nanayakkara *et al.,* 2021) carried out a literature review using questionnaires on an expert forum of 24 members including the upstream and downstream of the construction supply chain and university academics to identify the payment and related financial issues in the construction supply chain and construction industry. Opinions were carefully compared and the writers concluded that blockchain and smart contract technologies could assist in overcoming payment-related issues, such as partial payments, payment delays, non-payments, cost of finance, long payment cycle, retention, and security of payment issues, to a great extent.

In the implementation of blockchain-based smart contracts, (Guo *et al.,* 2021) proposed a blockchain-based smart contract to manage contract documents, monitor the signing process, and provide automated contract execution and payment settlement. The system proposed will handle the signing, verification, and validation of certificates and saving contract files using blockchain smart contract technology. The system will ensure that the contracts are protected by digital signatures and certificates. The system proposed cuts the time it takes to sign a contract from 55 to 190 hours (for a conventional paper-based contract) to 16-46 hours. Also, the cost of signing a contract was reduced from RMB2363 to RMB229 per contract. (Ahmadisheykhsarmast & Sonmez, 2020) proposed a system using smart contracts to automate the payment of construction contracts from employers to contractors. Using solidity as the smart contracts design language, the system's architecture consisted of an add-on software developed in Microsoft Project 2019 to transfer the necessary schedule and cost data to the smart contract via a project management software and a smart contract-based decentralized application designed to be deployed on the Ethereum blockchain. The system will ensure direct payments on fixed periods (weekly or monthly) from the employer's wallet to the wallets of subcontractors and suppliers to improve cash flow and reduce payment issues.

(Luo & Cheng, 2019) proposed a smart contract-based blockchain framework to facilitate the automation of contract payment. The model was proposed to automate payments in the supply chain of construction projects by formalizing construction contracts into smart contracts. The contract logic formalization involved the contractor, inspector, quantity surveyor, engineer, and employer. The execution of the smart contract was done through a permissioned blockchain-based framework. Consists of an automated consensus process based on pre-defined conditions of the smart contract, storing information in 2 different locations; Ledger and a data model for tasks completed and payments, and a manual process that requires input from the authorized stakeholder.

The introduction of BIM in the construction sector brought about a huge turnaround. Said to be the most flourishing technology in the construction sector (Martínez-aires *et al.*, 2018), integrating the technology with blockchain and smart contracts will significantly make a huge impact. (Shojaei *et al.*, 2019) proposed a system that was to integrate BIM model into a smart contract and creates a cyber-physical space for administrating the project through the blockchain network. This study was carried out to test the feasibility of blockchain technology as the link between the BIM model and the physical world with the implementation of smart contracts as the business logic of the blockchain network. The system used a private, permission-based blockchain, using Hyperledger fabric due the cryptocurrency aspect of the blockchain was not used, monetary compensations were executed through traditional channels such as electronic deposits. The system used seven (7) participants (client, architect/engineer, General Contractor (GC), regulators, inspectors, suppliers, and sub-contractors). The writers concluded that due the research method used in the study is by no means optimal, and it is only adopted as a starting point to show the feasibility of the approach. (Ye *et al.,* 2020) proposed a framework for automated contract, invoice, and billing management from a BIM model mapped in a blockchain-enabled smart contract. The proposed system process payments automatically through the banks and use a Common Data Environment (CDE) as off-chain storage that handles all the payment-related files for which a BIM Contract Container (BCC) is used, which contains all payment-relevant data. The BIM model and a BoQ with QTO were used to create the billing model which is then automatically processed via smart contracts for payments to be automated thereby completely simplifying the payment process. (Liu *et al.,* 2019).

IPFS due to its limitations of not having content encryption has managed to be used by many sectors in relation to blockchain. The fact that IPFS is decentralized in nature and uses the Distributed Sloppy Hash Table (DFSH), has brought about its popularity.

In the Identity management sector, (Liu *et al.,* 2019) proposed an identity management system on biometrics and blockchain/smart contracts to enable secure and privacy-preserving identity management. The proposed system used both the IPFS well-known one-way hashing algorithm and ground-truth information to verify an individual’s identity (Access control).

As can be seen from the literature reviewed, there is no clear protection provided for the transfer of data between IPFS, BIM, and blockchain-enabled smart.

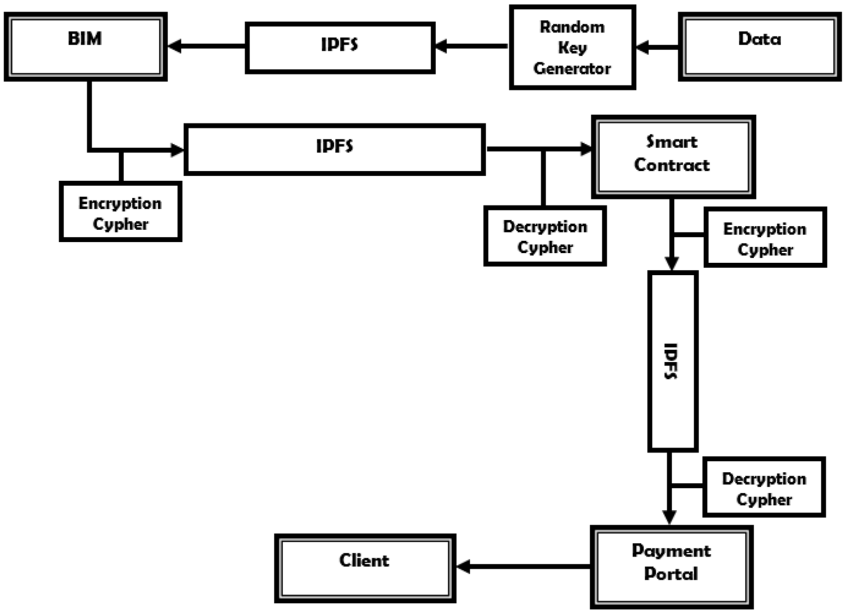
3.0 Methodology

The information transferred between IPFS and BIM may be compromised as a result of the identified research gap and considering IPFS architecture, there is no known data security. In order to secure the channel through which this data is shared in the IPFS network, this research suggests a cryptographic implementation.

The system has two primary goals and at least one party for content sharing. They are data comparison and data exchange in BIM. Time spent adding data and time spent comparing data can be the analysis's parameters. The mechanism is used in this study to analyse the aforementioned test parameters while keeping the other variables constant.

3.1 System Design

The system design is a three-unit tunnelling system by the IPFS. The encryption key used to encrypt the data input by a supervisor is generated randomly by a key generator. The BIM, where the degree of completion is confirmed, receives the encrypted data next via IPFS. The data is further encrypted after verification, sent through IPFS, and then decrypted in the smart contract. After decryption, the data is analysed by the smart contract, and once payment authorization has been granted, the data is once again encrypted before being sent to the payment portal via IPFS. Figure 3.1 displays the procedure.



3.2 Encryption Flow Diagram

A detailed explanation of the proposed algorithm's operation is presented in the encryption flow diagram of figure 3.2.

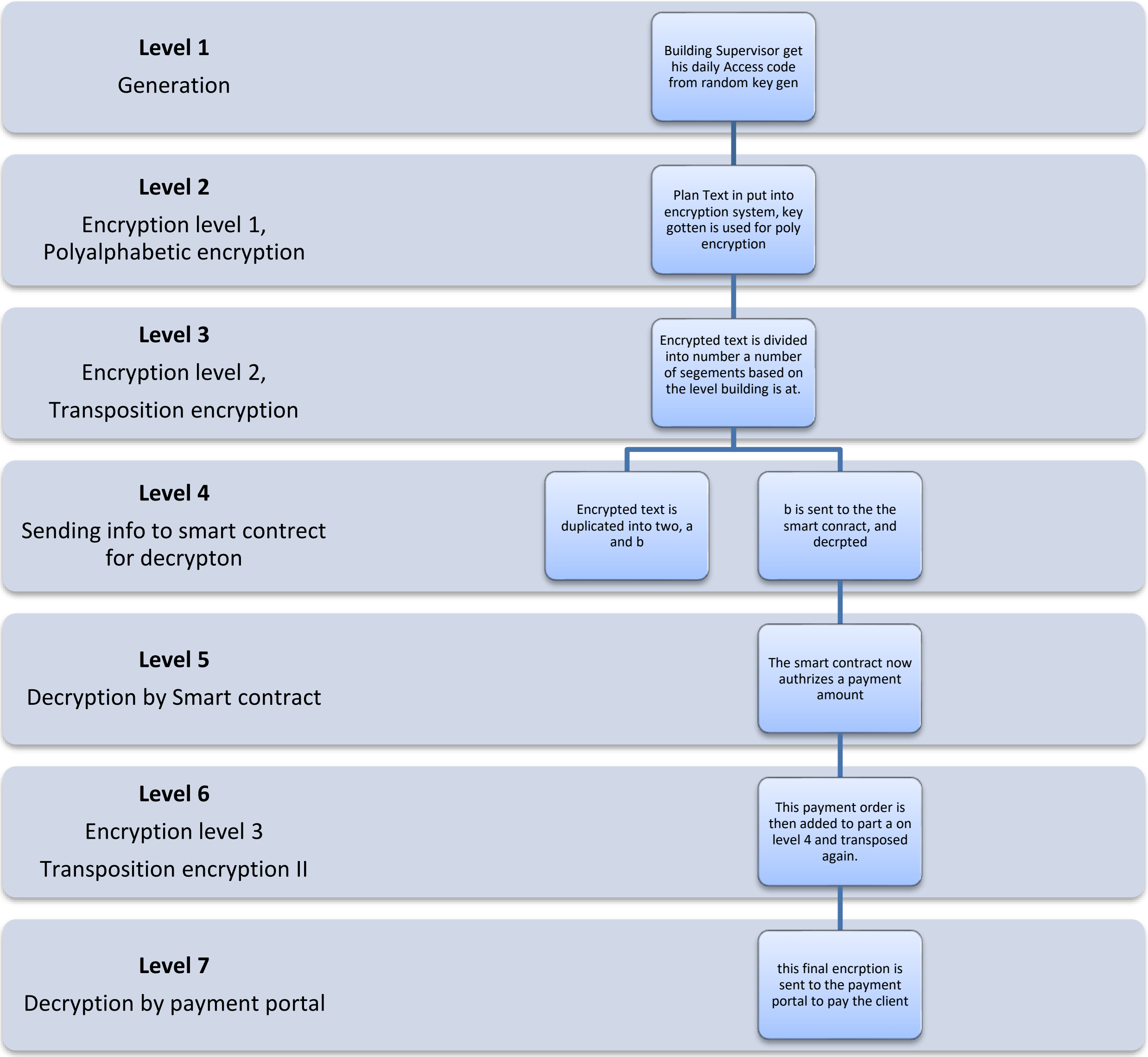

Level 1
Generation
Building Supervisor get his daily Access code from random key gen
Level 2
Encryption level 1, Polyalphabetic encryption
Plan Text in put into encryption system, key gotten is used for poly encryption
Level 3
Encryption level 2,
Transposition encryption
Encrypted text is divided into number a number of segements based on the level building is at.
Level 4
Sending info to smart contrect for decrypton
Encrypted text is duplicated into two, a and b
b is sent to the the smart conract, and decrpted
Level 5
Decryption by Smart contract
The smart contract now authrizes a payment amount
Level 6
Encryption level 3
Transposition encryption II
This payment order is then added to part a on level 4 and transposed again.
Level 7
Decryption by payment portal
this final encrption is sent to the payment portal to pay the client

Figure 3.1: Encryption Flow Diagram

3.3 Algorithm and Mathematical Model

3.3.1 Algorithm

Algorithm 1: Data Encryption

```
Input a: Plaintext
Input b: Building Level
P: convert a to its digital equivalent
R: Random string of 1 – 6 is generated without repetition
foreach
```

```
        $Z = \sum_{1-\infty}^{P} R$
    end foreach
    Km: eliminate digits greater than b in R
    using Km, transpose  Z ←Fx
    Send Fx to Smart contract
```

3.3.2 Mathematical Model

A random code algorithm developed for the model is shown below;

Random code Algorithm

Random String (Count 1 – 6), Integer must be positive and no repetition allowed

Random Key = (R1, R2, R3, R4, R5, R6)

Encryption Level 1: Polyalphabetic Encryption

Plaintext = (P1, P2, P3, P4, P5)

Ef(x) = (P1+R1, P2+R2, P3+R3, …, $P\infty+R\infty$)

$$= \sum_{1-\infty}^{P} R \;\; =Y1, Y2, Y3, \ldots, Yn$$

Buildings are divided into levels; Level logged in by supervisor from levels 2 – 5. The number is then used to divide cypher text into the count e.g.; If count is 3, Y1, Y2, Y3 = Y11, Y22, Y33.

The key for this encryption is private and agreed on to the extent of levels 1 – 6, however, sequences are put in levels available. If the Key is 3, 5, 1, 4, 2 and the current count is 3, then the key will equal 3, 1, 2

Cipher Text 2 = Y3, Y1, Y2

Cipher text 2 is sent to the smart contract. After decryption, the smart contract adds another string to the cipher text, Pn. Y3, Y1, Y2, Pn. The same key is then applied again.

Encryption Level 2: Transposition Encryption

Transposition Y31, Y12, Y23, PN4

3, 5, 1, 4, 2, 6 → 3, 1, 4, 2

Y2, Y3, Pn, Y1 → Final cipher text sent to payment portal

Encryption Example:

Plaintext = f i r s t f l o o r c o m pl e t e d = 6 9 18 19 20 6 12 15 15 18 3 15 13 16 12 5 20 5 4

Random Key = 1, 3, 6, 4, 5, 2

Ef(x) = G L X W Y H M R U V H N S R I Y G E

Level logged in by supervisor = 4

From Key 136452, eliminate numbers greater than the Level logged in by supervisor = 1342

Cipher text 2 = G Y U S G L H V R E X M H I Ω W R N Y Ω

The smart contract will now add “make payment” and add another level

Final Cipher text = G L X W M A T Y H M R A Y B U V H N K M β S R I Y E E B G E Ω Ω β N β

We now proceeded to encrypt the final cipher text “firstfloorcompletedmakepayment” using a classical encryption method (transposition cipher) and a modern encryption method as well.

Transposition Cipher Text= rolamflmdafoeptiopmysreketcten

The key used was ZEBRAS

RSA Cipher Text =bT��?�it4ش�%�NT����}�e�gH,�\TAlX,�l�?n¾yU

4.0 Results and Discussions

The developed algorithm was run in CrypTool 2.1 (Stable Build 9481.2) to test for its performance as a multilevel encryption tool. In order to extend IPFS with an access control mechanism, the following information security requirements need to be considered. They are confidentiality, integrity, availability, non-repudiation and authenticity. Table 4.1 shows the result generated.

Table 4.1: Analysis of results

CRYPTOSYSTEM	**CRYPTO ANALYSIS USED**	**TEXT GOTTEN FROM CRYPTANALYSIS**	**PERCENTAGE CHARACTER PLACEMENT ACCURACY**
Multilevel and Multi authority system	Known Cryptosystem attack	W X L G T A M R M H Y B Y A N H V U²Î M K I R S B E E Y©Î E G ²Î ©Î ²Î N	0%
Transposition cipher	Known Cryptosystem attack	amemtrcffkyiotolesoleemtrpanpd	13.3%
RSA Cipher	Dictionary Attack	�,��gX��?��4��}��U� ��� ��TeAnTl������� �?� l,%ƛ��ƛ�byTHiNt��\	0%
Transposition cipher	Brute Force	rpomlyasmrfelkmedtacftoeenptio	6.6 %
Transposition cipher	Dictionary Attack	lfmoypareomtinteerkecomaldpstf	7%
Multilevel and Multi authority system	Brute Force	GMKB LRMG XAβE WYSΩ MBRΩ AUIβ TVYN YHEβ HNE	0%
Multilevel and Multi authority system	Dictionary Attack	� G� B�ST YH WMAΩBK AEX E�V HI � L� GNRY � EN MRY �UM	0%
RSA Cipher	Brute Force	btT �,¾Tش� \�y�4�eTlU����A�?%�gl ��}HX?iN�, n	0%

4.1 Discussion of Results

The proposed system of this research ensures confidentiality through the cryptographic mechanism. The system would have additional multi-level Authority and encryption. Brute force was used to test the confidentiality of the system. Results show RSA, Multi-Level, and Multi Authority all produced the same outcome and showed no similarities to deciphered text from a cryptanalysis or plain text.

4.1.1 Integrity, non-repudiation and authenticity

IPFS is designed for the permanent web. It accesses the shared contents by the content hashes. Once the content is changed; the hash of the content also has to be changed. IPFS assign a unique node id for every node in the network and it verifies the sender of the data. Therefore integrity, non-repudiation and authenticity are already implemented within the IPFS protocol. The E-IPFS system also ensures these properties because it works on top of the IPFS (Alwis, 2020).

5.0 Conclusion and Recommendations

The use of BIM and IPFS in a smart contract allows for decentralized and distributed storage and transfer of data, while the use of multi-level authority and encryption will provide additional security measures to protect against eavesdropping, data tampering and theft. The algorithm developed from this research has the potential to revolutionize the way data is transferred and stored, with applications in various industries and contexts. For construction projects that require security but do not require the hassles of a complex system, we would advise using our model rather than the more complicated and resource-intensive RSA scheme.

References

Ahmadisheykhsarmast, S., & Sonmez, R. (2020). A smart contract system for security of payment of construction contracts. Automation in Construction, 120, 103401. https://doi.org/10.1016/j.autcon.2020.103401

Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. International Journal of Communication Networks and Information Security, 12(2), 256–272.

Alwis, R. A. H. A. De. (2020). Access level control for shared content in Inter Planetary File System (IPFS). University of Colombo School of Computing.

Cardoso, H. L., & Oliveira, E. (2008). A contract model for electronic institutions. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 4870 LNAI, 27–40. https://doi.org/10.1007/978-3-540-79003-7-3

Chang, C.-Y., Pan, W., & Howard, R. (2017). Impact of Building Information Modeling Implementation on the Acceptance of Integrated Delivery Systems: Structural Equation Modeling Analysis. Journal of Construction Engineering and Management, 143(8). https://doi.org/10.1061/(asce)co.1943-7862.0001335

Guo, L., Liu, Q., Shi, K., Gao, Y., Luo, J., & Chen, J. (2021). A blockchain-driven electronic contract management system for commodity procurement in electronic power industry. IEEE Access, 9, 9473–9480. https://doi.org/10.1109/ACCESS.2021.3049562

Hamledari, H., & Fischer, M. (2021a). Construction Payment Automation Using Blockchain-Enabled Smart Contracts and Reality Capture Technologies By. Automation in Construction, 132, 103926.

Hamledari, H., & Fischer, M. (2021b). Role of Blockchain-Enabled Smart Contracts in Automating Construction Progress Payments. Journal of Legal Affairs and Dispute Resolution in Engineering and Construction, 13(1), 04520038. https://doi.org/10.1061/(asce)la.1943-4170.0000442

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

Liu, Y., Sun, G., & Schuckers, S. (2019). Enabling Secure and Privacy Preserving Identity Management via Smart Contract. 2019 IEEE Conference on Communications and Network Security, CNS 2019. https://doi.org/10.1109/CNS.2019.8802771

Luo, H., & Cheng, J. C. P. (2019). Construction Payment Automation through Smart Contract-based Blockchain Construction Payment Automation through Smart Contract-based Blockchain Framework. IAARC Publications, 36, 1254–1260. https://doi.org/10.22260/ISARC2019/0168

Mallik, A., Ahsan, A., Shahadat, M. M. Z., & Tsou, J. C. (2019). Man-in-the-middle-attack: Understanding in simple words. International Journal of Data and Network Science, 3(2), 77–92. https://doi.org/10.5267/j.ijdns.2019.1.001

Martínez-aires, M. D., López-alonso, M., & Martínez-rojas, M. (2018). Building information modeling and safety management : A systematic review. Safety Science, 101(February 2017), 11–18. https://doi.org/10.1016/j.ssci.2017.08.015

Nael, G., B. (2005). The FIDIC forms of contract (Third Edit). Blackwell Publishing Ltd. https://books.google.com.ng/books?hl=en&lr=&id=hk6gDodpTtsC&oi=fnd&pg=PT16&dq=Bunni+N.+G.+The+FIDIC+forms+of+contract.+Blackwell+Pub,+2005.&ots=gtOctNhWjr&sig=VElYHyCIpd141zuMRFRWoSEPByM&redir_esc=y#v=onepage&q&f=false

Nanayakkara, S., Perera, S., Senaratne, S., & Weerasuriya, G. T. (2021). Blockchain and Smart Contracts : A Solution for Payment Issues. Multidisciplinary Digital Publishing Institute, 8(2), 36.

Penzes, B., KirNup, A., Gage, C., Dravai, T., & Colmer, M. (2018). Blockchain technology in the construction industry: Digital transformation for high productivity. Institution of Civil Engineers (ICE).

Shojaei, A., Flood, I., & Moud, H. I. (2019). An Implementation of Smart Contracts by Integrating BIM and Blockchain. Proceedings of the Future Technologies Conference, October, 519–527. https://doi.org/10.1007/978-3-030-32523-7

Ye, X., Sigalov, K., & König, M. (2020). Integrating BIM- and cost-included information container with Blockchain for construction automated payment using billing model and smart contracts. ISARC. Proceedings of the International Symposium on Automation and Robotics in Construction (ISARC 2020), 37, 1388–1395.

Zhang, Gao, D. and, & Zhili. (2013). Project time and cost control using building information modeling (BIM). ICCREM 2013: Construction and Operation in the Context of Sustainability, November, 545--554.

Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems, 105, 475–491. https://doi.org/10.1016/j.future.2019.12.019