A Conceptual Framework for Secure BIM-based Design: Using Blockchain and Asymmetric Encryption

Xingyu Tao[a], Moumita Das[a], Yuhan Liu[a], Peter WONG Kok Yiu[a], Keyu Chen[b], and Jack C. P. Cheng [a] *

[a]Department of Civil and Environmental Engineering, Hong Kong University of Science and Technology, Hong Kong SAR
[b]College of Civil Engineering and Architecture, Hainan University, Haikou, China.
E-mail: xtaoab@connect.ust.hk, moumitadas@ust.hk, yliugk@connect.ust.hk, kywongaz@connect.ust.hk, kchenal@connect.ust.hk, cejcheng@ust.hk (corresponding author)

Abstract –

Blockchain is a disruptive technology that has great potential in securing BIM data immutability and traceability. However, integrating BIM management with blockchain still faces a risk of sensitive information leaking because blockchain is such a transparent network that BIM data are disclosed to every member. Therefore, this paper proposes a blockchain-encryption integrated (BEI) framework to protect the access of sensitive BIM data when collaborating in a blockchain. The proposed framework contains two parts. Firstly, a "greatest common zone" (GCZ) method is developed to decompose BIM models for data segregation. Besides, an asymmetric encryption-based method is designed as the access control approach. In this way, sensitive BIM data would be encrypted and then shared in the blockchain ledger, which are maintained by all project members. Only authorized members can decipher the confidential information using a private key. The feasibility of the conceptual framework is validated through an illustrative example, showing that the BEI framework is a promising solution in securing the BIM-based design process.

Keywords –

BIM-based design; Blockchain; Asymmetric encryption; Greatest common zone (GCZ) method; IPFS

1 Introduction

Building Information Modelling (BIM), a game-changing technology that has been mainstreamed across the global construction industry, plays a significant role in design collaboration, in which BIM serves as the digital representation and shared knowledge resource of a physical building [1]. Designers can define and modify any design attributes in BIM and share them with the whole project team digitally, rather than working in isolation. Therefore, various BIM-based collaboration platforms have been developed to enable real-time and smooth communication, reduce the risk of rework, coordinate design changes, and federate models [2]. However, these existing platforms have a centralized system architecture, suffering a high cybersecurity risk of data manipulation [3]. For example, malicious insiders with authorized access have the motivation and opportunity to unwittingly modify design records or BIM models to run away from responsibilities. As a result, the project team cannot secure data integrity, traceability, and accountability.

Blockchain is a promising solution in keeping data security by integrating technologies including peer-to-peer (P2P) networks, decentralized data storage, and consensus mechanism [4]. Information shared in a blockchain network would be synchronized to every peers' local database (i.e., blockchain ledger) to avoid unilateral data manipulation [5]. Recent research efforts presented the feasibility and benefits of integrating blockchain into construction processes to accelerate collaboration. Initial explorations in construction interim payment [6], supply chain management [7], and on-site quality management [8] highlighted that blockchain could address some key concerns hindering collaboration. The Winfield-Rock report [9] indicated that blockchain could provide a secure and collaborative environment for BIM processes by emphasizing network security and data traceability.

Very few studies have investigated methods to facilitate access control methods in blockchain-based BIM design collaboration. Blockchain is a transparent network, and every member could access design data in his local blockchain ledger without any limitation, leading to data breaches and compromising intellectual property and commercial secrets. The latest ISO 19650-5: 2020 [10] standers have pointed out that controlling unauthorized access to information that can be confidential or sensitive is one of the primary tasks in

BIM-based collaboration. Traditional access control approaches like log in control or table lock for centralized databases are not suitable for blockchain due to its special chained data structure and distributed data storage manner. In a blockchain ledger, data are placed in different blocks, preventing setting access control to every block. because there would be thousands of blocks in a ledger and not each block contains sensitive data. Besides, distributed data storage makes synchronously managing access control to multiple peers' repositories difficult [11].

Thus, this paper proposes a conceptual blockchain-encryption integrated (BEI) framework to protect sensitive BIM data access. In this framework, a "greatest common zone" (GCZ) method is designed to decompose BIM models into sensitive and non-sensitive components for data segregation. Besides, an asymmetric encryption-based method is designed in the BEI framework to enable sensitive data access control. In this way, the proposed BEI framework ensures design data integrity using blockchain, while keeping sensitive data confidentiality using asymmetric encryption. Finally, the conceptual BEI framework is deployed in an illustrative design example to validate its feasibility.

2 Blockchain in Construction

Blockchain, known as a distributed ledger technology (DLT), is the underlying technology of Bitcoin [11]. Figure 1 shows the blockchain structure. Blockchain is a peer-to-peer network where no central servers control the network. Every peer in blockchain network maintains an identical copy of data (i.e., blockchain ledger). Each block is chained with the previous one via a hash, an irreversible value based on the content of the previous block. Any slight modification on block data would dramatically change the hash value of block, leading to invalidation of the entire chain [12].

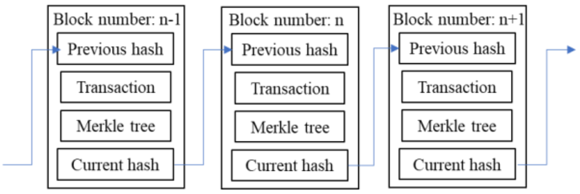


Figure 1. Blockchain structure

Blockchain is a disruptive technology to create a trusted and secure environment in the construction industry. Li et al. [13] reviewed potential blockchain applications in the built environment, revealing its potential to promote efficiencies and drive digital transformation in construction. Nawari and Ravindran [14] proposed a blockchain-based framework and applied it in post-disaster recovery. Wang et al. [7] introduced blockchain in construction supply chain management, within which a blockchain framework and a smart contract algorithm were developed to ensure data traceability. Sheng et al. [8] investigated blockchain employment in on-site construction quality management. Das et al. [6] designed a blockchain-based interim payment system to protect payment records and execute payment automatically. However, very few studies have developed methods to facilitate sensitive BIM data access control in the blockchain environment.

Blockchain is inherently unsuitable for storing large-sized files like BIM models, which may cause high latency and network congestion. Thus, an interplanetary file system (IPFS) [15] is integrated with blockchain to solve such problems. IPFS is a peer-to-peer, decentralized data storage system where every peer connecting to IPFS is a "file server". When a file is uploaded to IPFS, a cryptographic hash value named content identifier (CID) is generated based on the file content. This value is authenticity proof and a "hyperlink" of the file. It should be noted that the files are still stored in providers' local database, and only people who have corresponding CIDs could access files. Thus, several studies have designed an integrated method that large-sized data are placed in the IPFS, while CIDs are distributed in the blockchain to enable data traceability [16]. However, very few studies have developed methods to facilitate sensitive BIM data access control in the blockchain environment, posing a high risk of sensitive data leaking.

3 Conceptual BEI Framework

This paper proposes a conceptual blockchain-encryption integrated (BEI) framework (Figure 2), whose scientific contribution lies on two parts: (1) proposing a "greatest common zone" (GCZ) to decompose BIM model for data segregation and (2) developing an asymmetric encryption-based method for sensitive BIM data access control. Section 3.1 introduces the GCZ method, and the development of access control method is in Section 3.2.

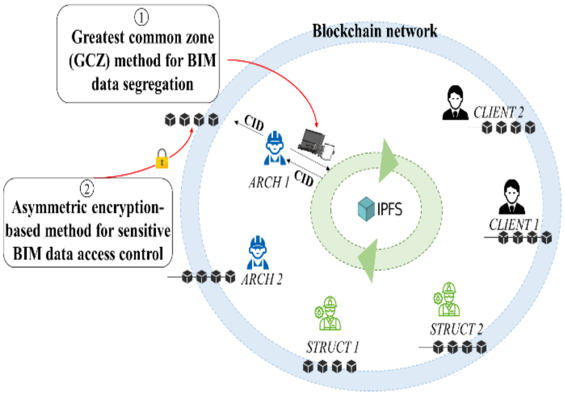

① Greatest common zone (GCZ) method for BIM data segregation
② Asymmetric encryption-based method for sensitive BIM data access control
Blockchain network
CID
CID
ARCH 1
ARCH 2
IPFS
CLIENT 2
CLIENT 1
STRUCT 1
STRUCT 2

Figure 2. Conceptual BEI framework

3.1 GCZ Method for BIM Model Decomposing

A GCZ method is designed to decompose BIM models into sensitive and non-sensitive (public) BIM components to facilitate data segregation. The basic idea of GCZ is to remove sensitive zones (e.g., the layout of zones) in a BIM model and pass the remaining non-sensitive components to members who have no rights to access sensitive zones. Components contain sensitive zones are only shared with authorized members. The decomposing process involves two steps. Firstly, for each zone in each component, members who can access the zone are selected. Then, GCZ reserves the common zones that they all can access in this component.

For example, Figure 3 shows a BIM model example containing multiple sensitive zones (i.e., zone 1, 2, 3) and a non-sensitive zone (i.e., zone 4). Table 1 displays the zone access metric where ARCH 1 (design leader in architecture team), STRUCT 1 (design leader in structure team), and CLIENT 1 (leader client) can access all zones, ARCH 2 (an architecture design helper) can only access zone 2 and 4, STRUCT 2 (a structure design helper) can only access zone 4, and Client 2 can only access zone 1,2 and 4. Figure 4 shows the model decomposing process using the proposed GCZ method. Project members who can access zone 1 can also access zone 2 and 4. Thus, in BIM component 1, zone 3 is removed while zone 1, zone 2, and zone 4 are kept. Similarly, people who can access zone model 2 can also access zone 4. So, component 2 contains both zone 2 and zone 4. It should be noted that component 1 model is only used for zone 1 coordination, and so as the remaining component models. For example, when there are design changes in zone 1, design team would update component 1 and share it with other disciplines.

Figure 5 shows the results of decomposing BIM models, including a root BIM model and BIM components. Three benefits are summarized as: (1) GCZ facilitates BIM data segregation, (2) GCZ is practical, efficient, and easy to handle, and (3) GCZ helps to reduce unnecessary work of removing zones (e.g., we don’t need to remove zone 2 and 4 in zone model 1).

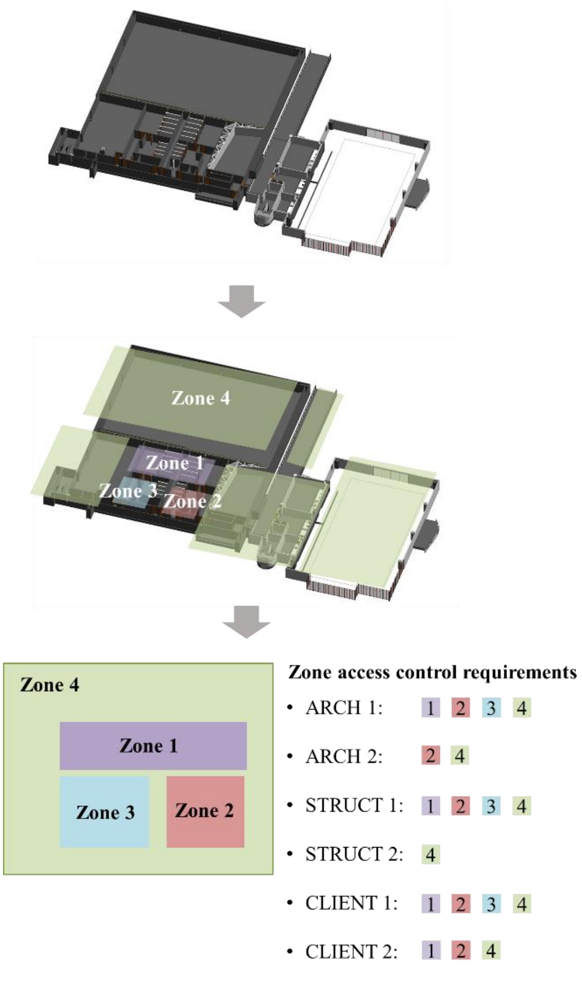


Figure 3: BIM model example with multiple sensitive zones

Table 1: Zone access metric

	Zone 1	Zone 2	Zone 3	Zone 4
ARCH 1	√	√	√	√
ARCH 2	×	√	×	√
STRUCT 1	√	√	√	√
STRUCT 2	×	×	×	√
CLIENT 1	√	√	√	√
CLIENT 2	√	√	×	√

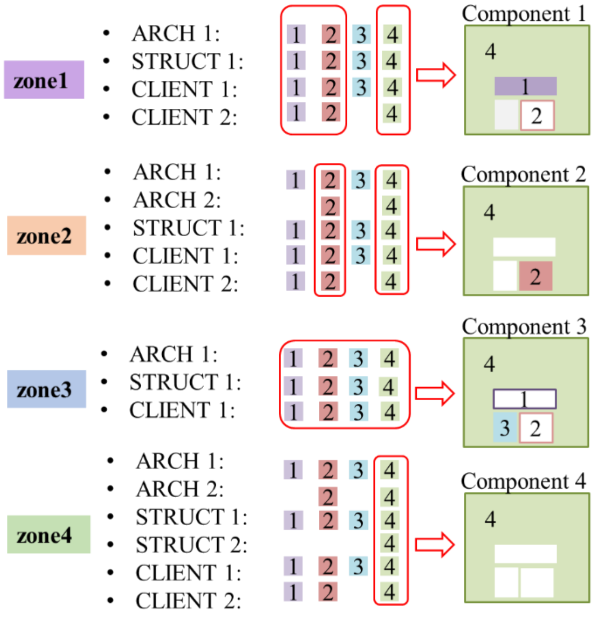


Figure 4: Model decomposing process using GCZ method

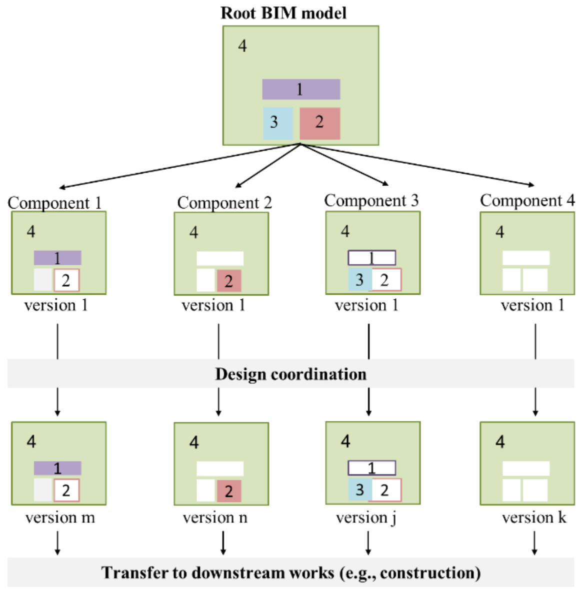


Figure 5: BIM model decomposing results

3.2 Asymmetric Encryption-based Method for Access Control

As every peer could see any shared transaction in the blockchain network; thus, this paper integrates asymmetric encryption protocol with blockchain to facilitate sensitive BIM data access control. Asymmetric encryption is a cryptographic protocol that encrypts and decrypts data using two separate keys: a public key and a private key. The public key is known to others, while the private key is kept secretly. Any person can encrypt a message using the receiver's public key, and that encrypted message can only be decrypted with the receiver's private key.

Figure 6 shows the access control method. In Figure 6, designers would store BIM components in the IPFS network in Step 1. Before sharing CIDs to blockchain network, the designer would first check if this is a CID for a sensitive component. If no, the CID would be directly distributed to other disciplines in the blockchain network through proposing a transaction (Step 2). Otherwise, the CID would be encrypted using public keys of authorized receivers (Step 3) and then shared in blockchain (Step 4). In Step 5, design information (e.g., CID or encrypted CID) would be synchronized to every member's local blockchain ledger as a design record. Subsequently, any member who wants to access a BIM component for design coordination could download it using CID he receives (Step 6). As for the encrypted CID, he could decipher it (Step 7) using a private key and download the component from IPFS (Step 8) if he is an authorized member of this component.

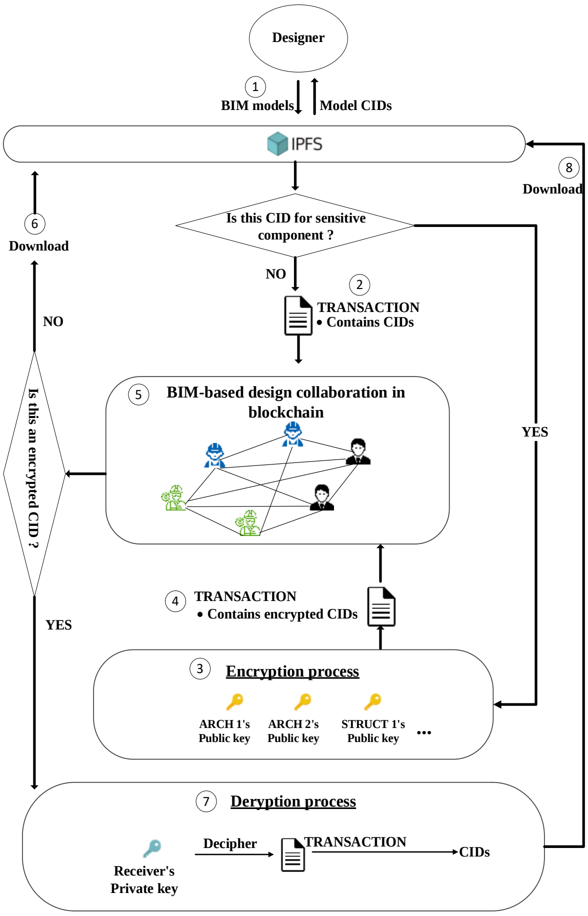


Figure 6. Asymmetric encryption-based method

for access control in blockchain

4 Illustrative Example

4.1 Prerequisites

A private blockchain platform, Hyperledger Fabric [17], is configured with three organizations (i.e., architecture team, structure team, and client). Besides, an IPFS desktop is set up for storing BIM components. The RSA (Rivest–Shamir–Adleman) [18], an asymmetric encryption protocol that is widely used for secure data transmission, is selected in this example.

4.2 Validation Process

Step 1: decomposing BIM model. As mentioned in previous sections, it is the very first step to partition BIM data into sensitive and non-sensitive part. The illustrative example utilizes the components and access requirements that are defined in Section 3.1. Figure 7 shows the BIM models and components. A root BIM model with three sensitive zones is decomposed into four BIM components. Components 1, 2 and 3 are sensitive for they contain sensitive zones. The remaining component 4 is non-sensitive. Figure 8 shows the blockchain configuration and BIM data storage in the IPFS.

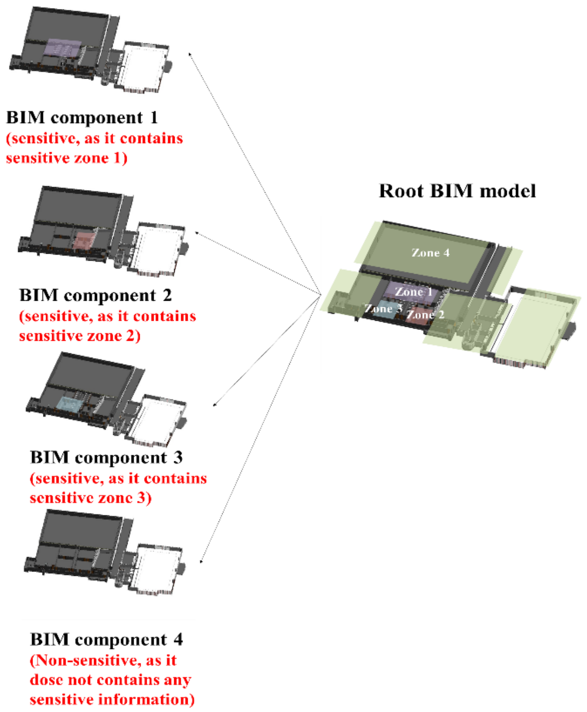
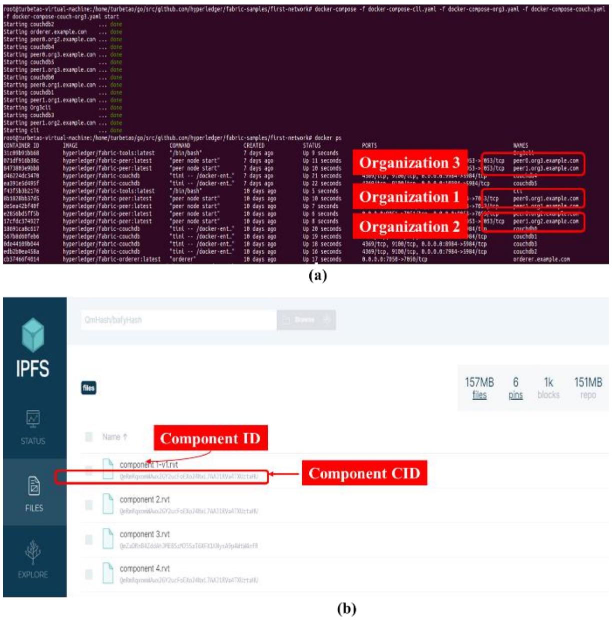

BIM component 1
(sensitive, as it contains sensitive zone 1)
BIM component 2
(sensitive, as it contains sensitive zone 2)
BIM component 3
(sensitive, as it contains sensitive zone 3)
BIM component 4
(Non-sensitive, as it dose not contains any sensitive information)
Root BIM model
Zone 4
Zone 1
Zone 3
Zone 2

Figure 7. BIM model decomposing process in illustrative example



```
root@turbetao-virtual-machine:/home/turbetao/go/src/github.com/hyperledger/fabric-samples/first-network# docker-compose -f docker-compose-cli.yaml -f docker-compose-org3.yaml -f docker-compose-couch.yaml
-f docker-compose-couch-org3.yaml start
Starting couchdb2              ... done
Starting orderer.example.com   ... done
Starting peer0.org2.example.com ... done
Starting couchdb4              ... done
Starting peer0.org3.example.com ... done
Starting couchdb5              ... done
Starting peer1.org3.example.com ... done
Starting couchdb0              ... done
Starting peer0.org1.example.com ... done
Starting couchdb1              ... done
Starting peer1.org1.example.com ... done
Starting Org3cli               ... done
Starting couchdb3              ... done
Starting peer1.org2.example.com ... done
Starting cli                   ... done
root@turbetao-virtual-machine:/home/turbetao/go/src/github.com/hyperledger/fabric-samples/first-network# docker ps
CONTAINER ID   IMAGE                               COMMAND                  CREATED       STATUS          PORTS                                          NAMES
31c09b91bb68   hyperledger/fabric-tools:latest     "/bin/bash"              7 days ago    Up 9 seconds                                                   Org3cli
071df916b38c   hyperledger/fabric-peer:latest      "peer node start"        7 days ago    Up 11 seconds   53->053/tcp                                    peer0.org3.example.com
0473803e9bb0   hyperledger/fabric-peer:latest      "peer node start"        7 days ago    Up 10 seconds   53->053/tcp                                    peer1.org3.example.com
d46274dc3470   hyperledger/fabric-couchdb          "tini -- /docker-ent…"   7 days ago    Up 21 seconds   4369/tcp, 9100/tcp, 0.0.0.0:9984->5984/tcp     couchdb4
ea391e5d495f   hyperledger/fabric-couchdb          "tini -- /docker-ent…"   7 days ago    Up 22 seconds   4369/tcp, 9100/tcp, 0.0.0.0:10984->5984/tcp    couchdb5
f43f5b3b2176   hyperledger/fabric-tools:latest     "/bin/bash"              10 days ago   Up 5 seconds                                                   cli
8b1828bb37d5   hyperledger/fabric-peer:latest      "peer node start"        10 days ago   Up 10 seconds   ->7053/tcp                                     peer0.org1.example.com
de5ea42bf40f   hyperledger/fabric-peer:latest      "peer node start"        10 days ago   Up 7 seconds    ->7053/tcp                                     peer1.org1.example.com
e2656bd5ff5b   hyperledger/fabric-peer:latest      "peer node start"        10 days ago   Up 6 seconds    ->7053/tcp                                     peer0.org2.example.com
17cfdc374027   hyperledger/fabric-peer:latest      "peer node start"        10 days ago   Up 8 seconds    53->053/tcp                                    peer1.org2.example.com
18691ca8c617   hyperledger/fabric-couchdb          "tini -- /docker-ent…"   10 days ago   Up 20 seconds   84/tcp                                         couchdb0
567b8d60feb6   hyperledger/fabric-couchdb          "tini -- /docker-ent…"   10 days ago   Up 19 seconds   84/tcp                                         couchdb1
0de44109b044   hyperledger/fabric-couchdb          "tini -- /docker-ent…"   10 days ago   Up 18 seconds   4369/tcp, 9100/tcp, 0.0.0.0:8984->5984/tcp     couchdb3
edb2b0ea458a   hyperledger/fabric-couchdb          "tini -- /docker-ent…"   10 days ago   Up 16 seconds   4369/tcp, 9100/tcp, 0.0.0.0:7984->5984/tcp     couchdb2
cb37466f4014   hyperledger/fabric-orderer:latest   "orderer"                10 days ago   Up 17 seconds   0.0.0.0:7050->7050/tcp                         orderer.example.com
```

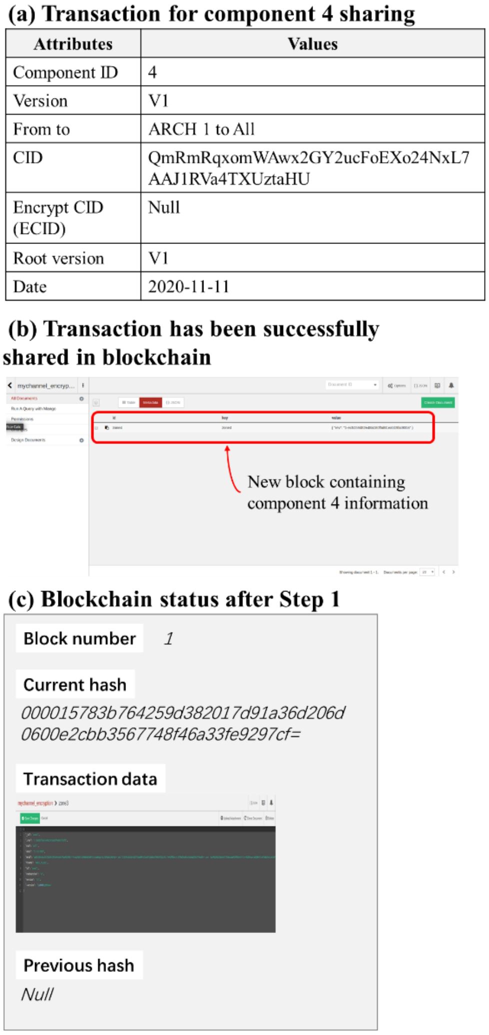
(a)

(b)

Figure 8. Blockchain configuration and IPFS data storage

Step 2: collaborating on a non-sensitive component. ARCH 1 uploads component 4 (non-sensitive component) to IPFS and gets its CID. This is followed by proposing a transaction (Figure 9 (a)) in blockchain to share component CID. As this component is non-sensitive, there is no encrypted CID (ECID) in the transaction. Figure 9 (b) shows that the transaction has been successfully shared. Figure 9 (c) shows that a block has been generated in the blockchain network.

Step 3: collaborating on a sensitive component. To share a sensitive model (e.g., component 3), ARCH 1 would encrypt its CID using authorized receivers' public keys and proposes a new transaction. Thus, in Figure 10 (a), the CID is encrypted to two ECID for CLIENT 1 and STRUCT 1, respectively. Figure 10 (b) shows that the transaction has been successfully shared in blockchain network. Everyone can check the encrypted CID of component 3 in their blockchain ledger. However, only the right receivers can decipher the encrypted CID and download component 3. Figure 10 (c) shows a new block has been generated and chained to the previous one.



(a) Transaction for component 4 sharing

Attributes	Values
Component ID	4
Version	V1
From to	ARCH 1 to All
CID	QmRmRqxomWAwx2GY2ucFoEXo24NxL7AAJ1RVa4TXUztaHU
Encrypt CID (ECID)	Null
Root version	V1
Date	2020-11-11

(b) Transaction has been successfully shared in blockchain

New block containing component 4 information

(c) Blockchain status after Step 1

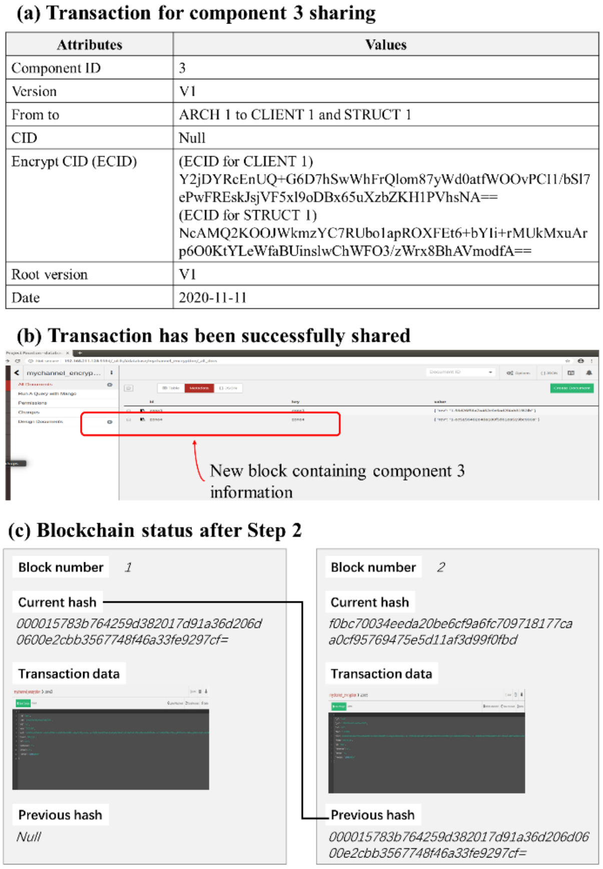
Block number 1

Current hash
000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe9297cf=

Transaction data

Previous hash
Null

Figure 9. Results of sharing non-sensitive component in blockchain



(a) Transaction for component 3 sharing

Attributes	Values
Component ID	3
Version	V1
From to	ARCH 1 to CLIENT 1 and STRUCT 1
CID	Null
Encrypt CID (ECID)	(ECID for CLIENT 1) Y2jDYRcEnUQ+G6D7hSwWhFrQlom87yWd0atfWOOvPC11/bSl7ePwFREskJsjVF5xl9oDBx65uXzbZKH1PVhsNA== (ECID for STRUCT 1) NcAMQ2KOOJWkmzYC7RUbo1apROXFEt6+bYIi+rMUkMxuArp6O0KtYLeWfaBUinslwChWFO3/zWrx8BhAVmodfA==
Root version	V1
Date	2020-11-11

(b) Transaction has been successfully shared

New block containing component 3 information

(c) Blockchain status after Step 2

Block number 1

Current hash
000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe9297cf=

Transaction data

Previous hash
Null

Block number 2

Current hash
f0bc70034eeda20be6cf9a6fc709718177caa0cf95769475e5d11af3d99f0fbd

Transaction data

Previous hash
000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe9297cf=

Figure 10. Results of sharing sensitive component in blockchain

5 Conclusion

This study proposes a blockchain-encrypted integrated conceptual framework for a secure BIM-based design process. The main scientific contributions are summarized as this study developed a GCZ decomposing method to enable BIM data segregation. Besides, a blockchain-encryption integrated solution is designed to protect BIM data immutability and data confidentiality. The illustrative example section validates the feasibility BEI framework. However, this framework is an initial exploration of blockchain application in the construction industry. Potential future work includes (1) integrating technologies such as machine learning to automatically decompose BIM models and (2) implementing the framework in an actual project to evaluate its performance on network latency and throughput.

References

[1] Xue, F. and W. Lu, *A semantic differential transaction approach to minimizing information redundancy for BIM and blockchain integration.*

Automation in Construction, 2020. **118**: p. 103270.

[2] Preidel, C., et al., *Seamless integration of common data environment access into BIM authoring applications: The BIM integration framework*, in *eWork and eBusiness in Architecture, Engineering and Construction*. 2017, CRC Press. p. 119-128.

[3] Boyes, H., *Building Information Modelling (BIM): Addressing the cyber security issues*. 2014, The Institution of Engineering and Technology.

[4] Li, J., D. Greenwood, and M. Kassem, *Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases.* Automation in Construction, 2019. **102**: p. 288-307.

[5] Das, M., X. Tao, and J.C. Cheng. *A secure and distributed construction document management system using blockchain*. in *International Conference on Computing in Civil and Building Engineering*. 2020. Springer.

[6] Das, M., H. Luo, and J.C. Cheng, *Securing interim payments in construction projects through a blockchain-based framework.* Automation in Construction, 2020. **118**: p. 103284.

[7] Wang, Z., et al., *Blockchain-based framework for improving supply chain traceability and information sharing in precast construction.* Automation in Construction, 2020. **111**: p. 103063.

[8] Sheng, D., et al., *Construction quality information management with blockchains.* Automation in Construction, 2020. **120**: p. 103373.

[9] Winfield, M., *The winfield rock report: Overcoming the legal and contractual barriers of BIM*. 2018, UKBIM alliance. p. 1-60.

[10] ISO, *Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling Part 5: Security-minded approach to information managem*. 2020, International Standardization Organization. p. 43.

[11] Penzes, B., et al., *Blockchain technology in the construction industry: digital transformation for high productivity*. 2018, Institution of Civil Engineers

[12] Turk, Ž. and R. and Klinc, *Potentials of blockchain technology for construction management.* Procedia Engineering, 2017. **196**: p. 638-645.

[13] Li, J., D. Greenwood, and M. and Kassem, *Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases.* Automation in Construction, 2019. **102**: p. 288-307.

[14] Nawari, N.O. and S. Ravindran, *Blockchain technology and BIM process: review and potential applications.* ITcon, 2019. **24**: p. 209-238.

[15] Benet, J. *InterPlanetary File System (IPFS)*. 2016 [cited 2020 1 Aug]; Available from: https://ipfs.io/.

[16] Steichen, M., et al. *Blockchain-based, decentralized access control for IPFS*. in *2018 IEEE International conference on Internet of Things and IEEE green computing and communications and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data*. 2018. Halifax, Canada: IEEE.

[17] Foundation, L. *Hyperledger Fabric*. 2015 Available from: https://www.hyperledger.org/use/fabric.

[18] Badertscher C., M.C., Maurer U., *Strengthening access control encryption*, in *Advances in Cryptology – ASIACRYPT 2017*. 2017.