Zero-Knowledge Proof for trusted construction management: A preliminary study of adaptive blockchain BIM identity authentication

Lingming Kong*, Rui Zhao, Fan Xue
*The University of Hong Kong, Hong Kong SAR, China. *: Corresponding author*
u3009509@connect.hku.hk, u3008752@connect.hku.hk, xuef@hku.hk

This is the preprint version of the conference paper:
Kong, L., Zhao, R. & Xue, F. (2023). Zero-Knowledge Proof for trusted construction management: A preliminary study of adaptive blockchain BIM identity authentication. *Proceedings of the 23rd International Conference on Construction Applications of Virtual Reality*. Florence, Italy: University of Florence Press, 347-355.

The final published version of this paper can be found at: [LINK_TO_DOI].

ABSTRACT: *Blockchain technology emphasizes trust and collaboration through distributed networks and is deemed to contribute to building information modeling (BIM) based construction collaboration and management. However, the open nature of blockchain introduces severe cybersecurity attacks that undermine the trustworthiness of construction management. One salient point is identity authentication for security BIM data access in the blockchain environment. The traditional public-private key or password authenticate methods are vulnerable to malicious theft. Zero-Knowledge Proof (ZKP) is an emerging, password-free method for authenticating identities. It allows one party to prove the truth or falsity of a statement to another party without revealing any meaningful information to the counterpart. Therefore, this study proposes a preliminary user authentication protocol based on the non-interactive ZKP protocol, specifically the zk-SNARK protocol, for adaptive authentication of blockchain BIM. The adaptive authentication recognizes a random subset of on-chain historical BIM operation records to prove the identity according to the protocol. Without revealing any meaningful knowledge to the authentication system, this adaptive data access control prevents password attacks using the BIM records on-chain. Finally, the proposed protocol is deployed on the test blockchain and implemented in a preliminary case study to illustrate the feasibility and effectiveness of the proposed method. The main contribution of this paper is twofold. Firstly, the theoretical contribution is proposing a novel zk-SARKs-based identity authentication protocol that utilizes the on-chain BIM operation records. Secondly, the practical contribution relies on presenting a ZoKrates-based workflow of generating proofs, creating smart contracts, and deploying on the blockchain for verification.*

KEYWORDS: *Zero-knowledge proof, Blockchain, BIM, Construction Management, Identity Authentication.*

1. INTRODUCTION

In multi-party construction activities, collaboration and trust emerge as significant yet intricate issues. Building Information Modeling (BIM) stands as a trending and burgeoning technology within the construction industry, facilitating efficient cross-disciplinary collaboration among stakeholders. However, given the inherent characteristics of construction activities—encompassing multiple data contributors, consumers, and geographically dispersed stakeholders—the centralized, file-based BIM collaboration necessitates stringent data access control. This measure is crucial to prevent deliberate cybersecurity attacks, such as login attacks.

Ensuring that the right individuals access the appropriate BIM content – in essence, addressing authentication concerns – has emerged as one of the most critical issues in BIM-based collaboration. For example, Skandhakumar et al. (2018) proposed a BIM-based security model presented by BIM-XACML language to facilitate conditional access to BIM, and Zheng et al. (2019) offered a new context-aware access control model for the decentralized cloud BIM system. These studies cannot avoid password attacks, which represent intentional attacks to steal the authentication credentials such as passwords and private keys.

Blockchain technology brings a transformative alteration from centralized BIM to distributed BIM that is deemed to achieve transparent, traceable, and consensus-based trusted collaboration with better encryption and security (Subangan & Senthooran 2019; Nawari & Ravindran 2019). Blockchain is a distributed ledger network first proposed in 2008 and implemented in 2009 (Zheng et al. 2018). In recent years, the integration of BIM and blockchain has been studied extensively, especially in the data security aspects. Inappropriate distribution and excessive BIM transparency may lead to a loss of reputation and trust.

Considerable literature on trust has grown up around the theme of blockchain BIM in different project aspects (Wu, et al., 2022; Zhao, Chen, & Xue, 2023). For example, Das et al. (2021) categorized BIM data security into five types and emphasized the confidentiality and authenticity of distributed BIM. The confidentiality of BIM represents the necessity of safe data access by authorized people or organizations, and authenticity involves user-related and data-related regions. The Hyperledger community presented a "privacy data" mechanism that only stores the sensitive data as hash code in ledgers and source data such as BIM files off-chain (Androulaki et al. 2018). Accordingly, Tao et al. proposed an access control model based on asymmetric encryption and sensitive BIM model components decomposition (Tao et al. 2022). Much previous research utilized traditional encryption or access control policy to guarantee secure data access in the distributed blockchain environment, which encountered the same challenge as the centralized BIM, password attacks.

Adaptive authentication stands as a potential solution for circumventing password attacks. Zero-knowledge proof (ZKP) constitutes a cryptographic technique that empowers the prover to persuade the verifier without divulging further meaningful information regarding statements. ZKP has three significant properties: (1) completeness. If the statement or witness is true, the verifier can be convinced by the honest prover. (2) reliability. The prover can deceive the verifier with a negligible probability if they do not know the statement. (3) zero knowledge. The verifier only obtains the information "the prover has this knowledge" without extra meaningful information (Goldreich & Oren 1994). These three main properties of ZKP are deemed to contribute to multi-party identity authentication for blockchain BIM. Typically, ZKP can be classified into two types, interactive ZKP and non-interactive ZKP (Hu et al. 2018). The non-interactive ZKP is widely used in the blockchain environment due to its one-way communication between the prover and the verifier, specifically the zero-knowledge Succinct Non-interactive ARguments of Knowledge (zk-SNARKs) protocol (Parno et al. 2016; Groth 2016). Anonymous currencies such as Zerocash (Sasson et al. 2014) and SERO use zk-SNARK in the blockchain domain for implementing privacy transactions. A large volume of published studies describes the role of ZKP in solving identity authentication problems of blockchain. Wang et al. (2020) summarized the existing solutions to privacy protection issues in blockchain and emphasized the effectiveness of ZKP. Yang et al. (2020) formulated an identity management scheme by leveraging smart contract and ZKP algorithms; Sun et al. (2021) proposed a two-part framework of ZKP in blockchain as on-chain and off-chain parts respectively, aiming to provide a solution of security private data access in the blockchain environment. However, due to the high cost of computation and storage of ZKP, the lack of using historical data stored in

the blockchain, and the primitive application of blockchain BIM, research on ZKP-based identity authentication for BIM collaboration in the blockchain environment is still preliminary.

For a construction project, both BIM files and BIM-related operation records are stored in the blockchain system. Due to the limited storage capability of blockchain and the massive-volume nature of BIM files, a typical blockchain BIM system is composed of two parts: on-chain and off-chain parts. The on-chain part stores the metadata of BIM files, including the file name, size, owners, creating time, version information, operation records, and other file-related descriptive data. The off-chain part keeps large-size BIM data such as BIM model files and documents of the project. A representative two-part structure blockchain BIM system is proposed by Tao et al. (2021), and Xue and Lu (2020) introduced a semantic differential approach to capture changes in the local BIM model as transactions on chain. The storage methods of BIM data in the blockchain are out of the scope of this paper, but the BIM data itself is possible to facilitate the ZKP-backed identity authentication of the construction blockchain.

This study proposes a Zk-SNARKs-based identity authentication protocol for blockchain-backed BIM collaboration. By utilizing the random subset of historical data records in the blockchain, stakeholders involved in the construction projects with distinct roles and responsibilities access the blockchain channel through an adaptive authentication process. By leveraging ZKP, a dynamic login function is achieved that avoids password attacks and provides a trusted identity authentication function. The proposed Zk-SNARKs-based BIM user authentication protocol is described in part 2, and a case pilot is illustrated to prove the possible feasibility of the protocol in part 3. Then, the pros and cons of the protocol are discussed in part 4, and part 5 shows the limitations and future works.

2. A ZKP-BASED AUTHENTICATION PROTOCOL FOR BLOCKCHAIN BIM

The two-step authentication processes between BIM stakeholders and the blockchain network is shown in Fig. 1. Firstly, the BIM stakeholders act as provers to prove their authority to the blockchain by providing statements, which are the knowledge of BIM in their mind. Then, the blockchain verifies the correctness of the statement automatically by the deployed smart contract and responds to the BIM stakeholder.

2.1 The zk-SNARKs-based authentication protocol

The structure of the proposed zero-knowledge Succinct Non-interactive ARguments of Knowledge (zk-SNARKs) based authentication protocol is depicted in Fig. 2. The first layer is the blockchain layer which is composed of a block network to store the BIM editing records. On top of the blockchain layer, various smart contracts deployed on the blockchain constitute the second layer. Three types of smart contracts for data storage, data querying, and proof verification are involved. With these smart contracts, BIM stakeholders can interact with the blockchain network, such as uploading the BIM editing records by the data storage smart contract and verifying their identities by the verifying smart contract. The uppermost layer is the application layer, which provides functions for users to interact with the blockchain. Two services, namely identity provider (IdP) and BIM server provider (BIMSP), are designed in this layer. The IdP are various identities, including project manager, civil engineer, designer, BIM engineer, and their combinations. IdP is designed to provide multiple options for users' identification. The BIMSP provides adding, modifying, deleting, and querying operating authorities of BIM models. Authorized users can get editing rights corresponding to their identity in the BIM model.

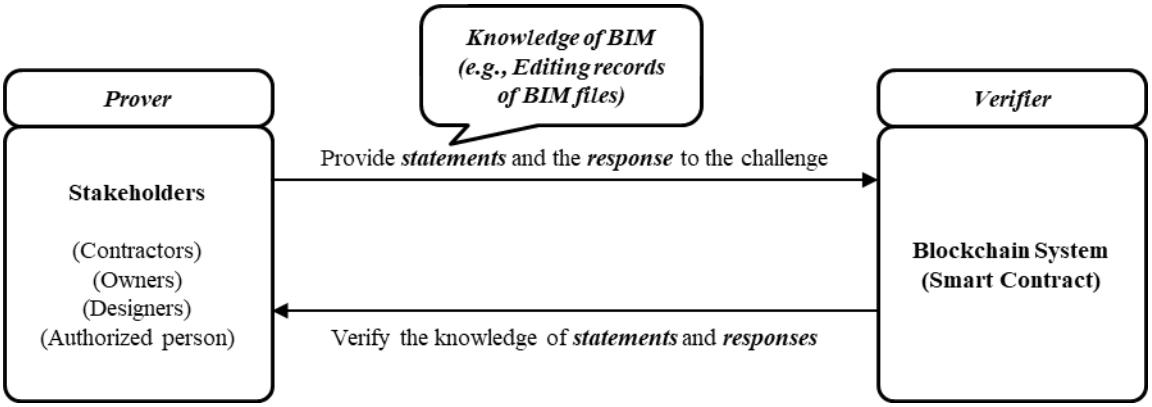


Fig. 1: Possible facilitation of BIM in the structure of ZKP for construction blockchain

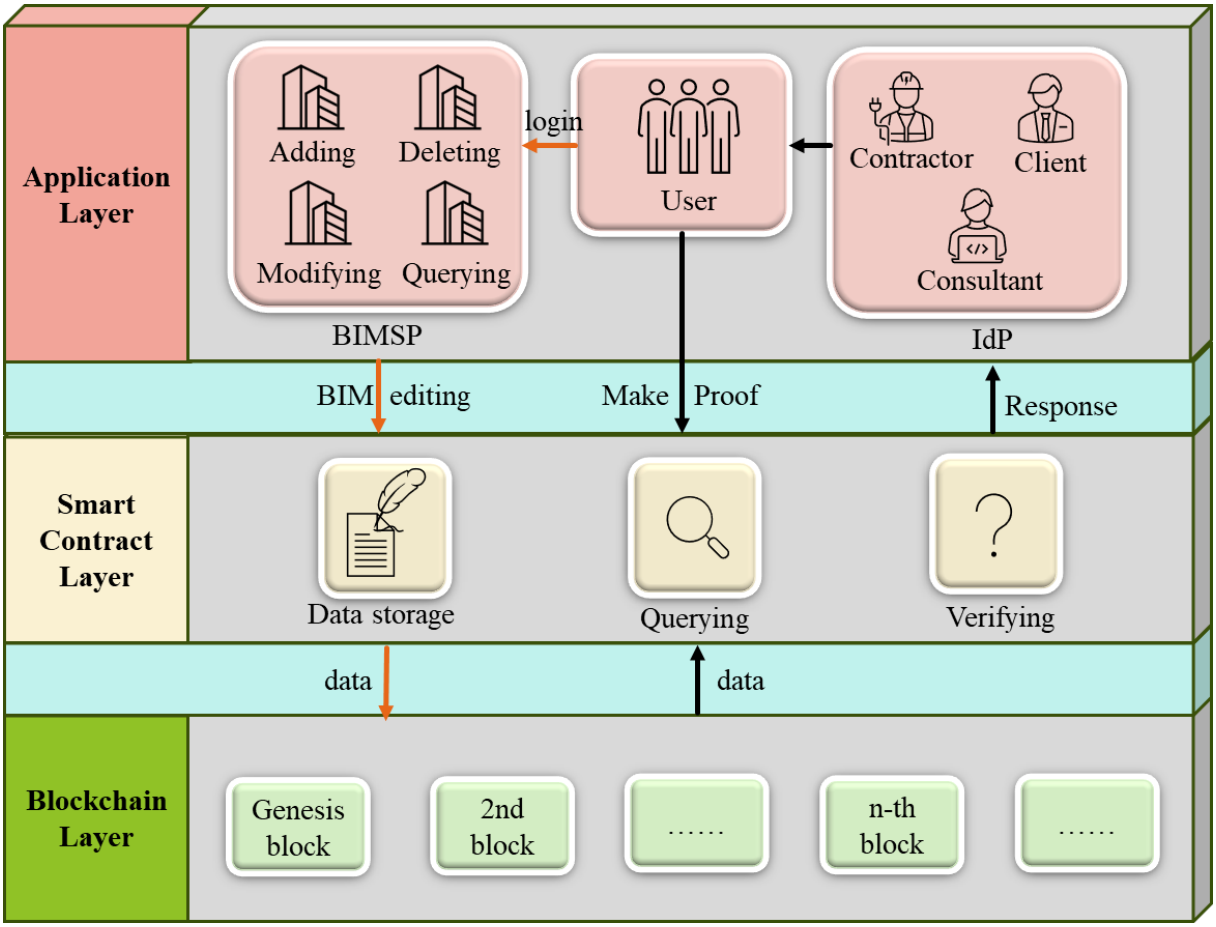


Fig. 2: Structure of the proposed zk-SNARKs-based identity authentication protocol

This paper focuses on the smart contract for proof verification, which implements an automatic authentication model based on the zk-SNARKs protocol. The zk-SNARKs protocol supports succinct proof verification by the one-way message communication between the prover and verifier. Its development processes involve five main steps:

1) Define the domain-specific data model to describe the BIM-related knowledge for identity authentication. For instance, to describe the editing history records of a door, the data of "editing_month", "door_level", and "editing_action" should be involved. The "editing_action" is further categorized into four subtypes: add, delete, modify, and query.

2) Describe the logic of the domain-specific data model to be proved using the NP statement such as Rank-1 Constraint Satisfaction (R1CS). An NP statement means that if you have a solution, it is computationally easy to prove it, but it is not computationally to find the solution. In this way, the ZKP protocol is completeness and soundness.

3) The proof circuit accepts some common parameters as input and generates a Common Reference String (CRS).

4) Generate proof about the proposition.

5) Verify the proof.

The core step is generating the NP statement of the domain-specific data model, namely the logic proof circuit. Many tools are developed to do this work, such as Zokrates, libsnark, snarkjs, etc. In this paper, the Zokrates toolbox, which is developed by Ethereum, is implemented to convert the BIM-related data model to the logic-proof circuit. A detailed example is presented in Part 3.

2.2 Workflow

The workflow of proving the identity to the blockchain system is depicted in Fig. 3. A user defined by IdP first requests a login to the blockchain system with a role confirmation process. Then, BIM stakeholders generate proof of the BIM-related knowledge, such as the editing of a BIM version at a specific time, to the blockchain. The smart contract for verifying the proofs is pre-deployed on the blockchain and verified automatically. If the proof is verified as true, a one-time password authenticates the user to log in. The login event will be recorded on the chain, too.

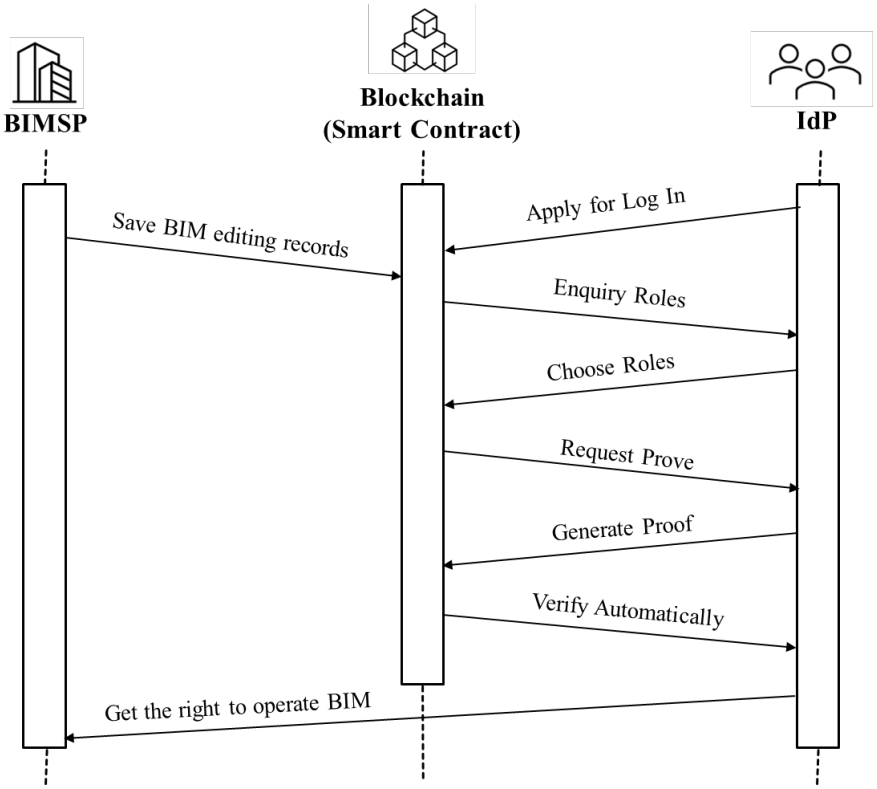
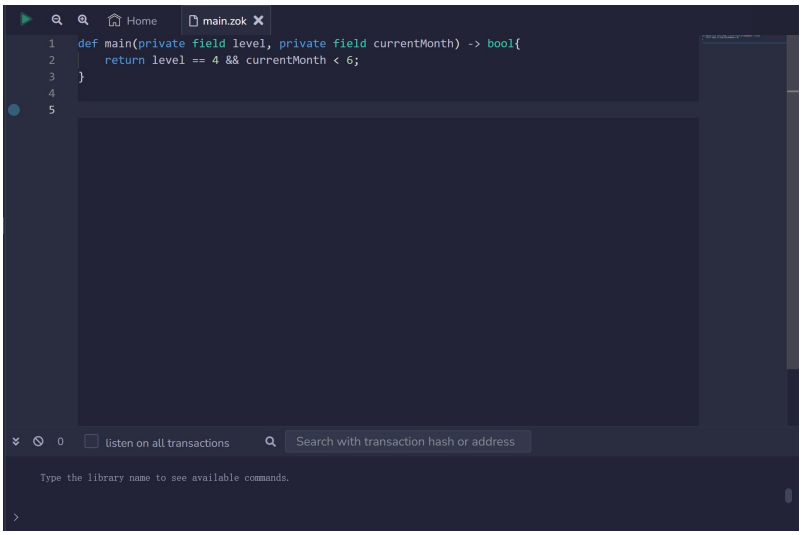


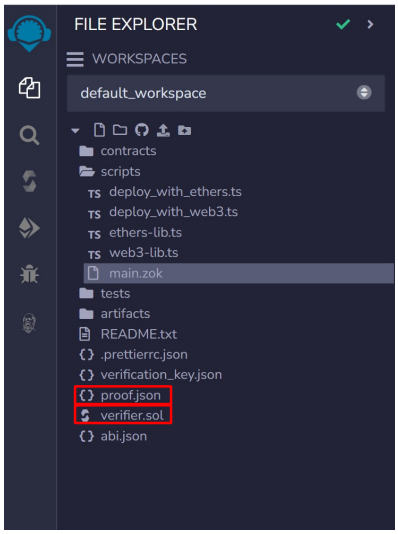
Fig. 3. The workflow of the proposed protocol

2.3 Software implementation

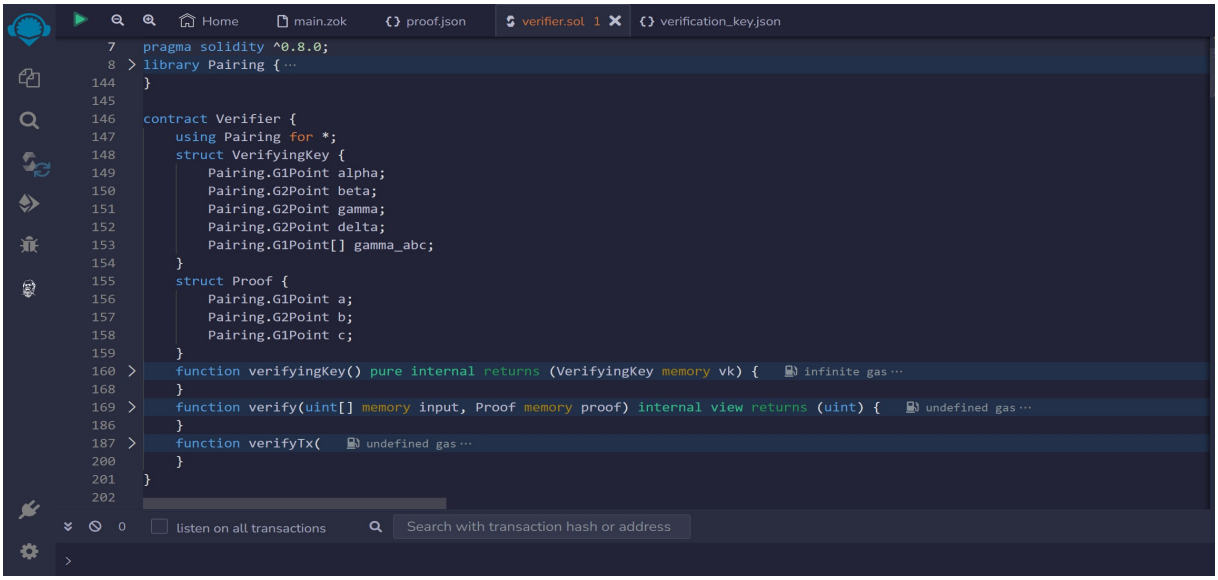
An identity authentication smart contract (IASC) is deployed on the test blockchain network by ZoKrates (Version 0.8, available at https://github.com/Zokrates/ZoKrates). ZoKrates (2023) is a toolbox for implementing zk-SNARKs on Ethereum, which provides functions such as trusted setup, libraries, and proving schemes et al. The Remix IDE is an open-source web-based IDE that creates, compile, tests and deploy Ethereum-based smart contracts on the blockchain network (Jain , 2022). Fig. 4 illustrates the interface of generating an IASC and deploying it on the test blockchain network by the Remix IDE.



(a) Definition of the logic circuit



(b) Generated proof and IASC



(C) An example of IASC

Fig. 4: Interfaces of Remix IDE. (a) define a logic circuit; (b) Generation of proof and identity authentication smart contract; (c) an example of IASC

As Fig. 4(a) shows, the circuit is declared in the ".zok" file alliance with the ZoKrates schema, the private filed type represents the secrete input that will not be revealed in the proof process and return a bool value that represents the verification result. A BIM user is able to generate a proof file, namely the "proof.json" file in Fig. 4(b), which will be sent to the blockchain for verification. The generated IASC is shown in Fig. 4(c), including five parts: (1) two data

155 structures that describe the verification key and proof data; (2) three verification functions.

3. CASE PILOT

3.1 Case selection

A project at the University of Hong Kong (HKU) was selected in this section to demonstrate the proposed zk-SNARKs identity authentication protocol. The project was a modular
160 construction project of a student residential apartment located at Wong Chuk Hong (WCH), involving 1,224 modules. Each module involves three main phases. Each module involves three main phases:

1) Manufacturing phase that the module is manufactured in the factory in Mainland China;
2) Logistics phase that transports the module from Mainland to Hong Kong through
165 maritime transportation and land transport; and
3) On-site installation of modules.

3.2 Mapping of project workflow to zk-SNARKs

The fragmented construction phases and multi-disciplinary participants require high-level access control to the blockchain BIM collaboration platform. The IdP of this project defines
170 three main stakeholders:

1) The main contractor. Paul Y. Engineering is the main contractor, and is responsible for module manufacturing and inspections, module transportation, and on-site installation. Paul Y. utilizes BIM for the on-site instructions and proposes potential changes to the consultant and client.
175 2) The lead consultant. Architecture Design and Research Group Ltd. (AD+RG) is the lead consultant for design and the key author and data contributor of BIM. Architecture, structure, water/drainage, and HVAC designers collaborate on the comprehensive BIM.
3) The client. HKU is the client of this project can access the whole BIM collaboration system.

180 According to the category of roles and responsibilities, the statements of the Zk-SNARKs-based authentication protocol of each group should be as follows:

1) Paul Y. Engineering: Browsing history of BIM. For example, "is the statement 'User A browse the architecture BIM Ver. 1.2 on 29th September' *True or False*?
2) AD+RG Ltd: Browsing and authoring history of BIM, including components' changes
185 and revisions. For example, "Is the statement 'the *DELETE* operation of sliding windows/doors at level 4 was done before June' *True* or *False*?"
3) HKU: Browsing records of BIM models or related project information in the blockchain transactions. For example, "Is the statement 'so far, there have been 4 approved BIM changes in the structure domain' *True* or *False*?"

190 To map the project workflow to the proposed zk-SNARKs-based identity authentication protocol, a statement of BIM-related knowledge should first be converted to a computational problem. For instance, the statement "User A browse the architecture BIM Ver. 1.2 on 29Th September" should be converted as "if version == 1.2 and date == 29th Sep then result == True

else result == False". Then, an NP statement such as R1CS should be developed. Specifically, R1CS is a sequence of three vector sets (*A, B, C*) that satisfy the equation $s \cdot A * s \cdot B = s \cdot C$, where *s* is the solution vector and *A, B, C* are coefficient vectors. The simple "·" represents the inner product operation of vectors. The computational statement is converted into several simple expressions to represent the computation logic, such as $x \oplus y = z$ where " $\oplus$ " represents the "+" or "×" operations in the proof circuit. For the example computation statement, the operation is "+". In this way, the project workflow statement is converted to R1CS circuits for further computation.

3.3 Preliminary results

Step 1: Coding of the statement

Step 2: Compile the circuit to constraints

Step 3: Setup to generate the public -private key pairs

Step 4: Generate proof

Step 5: Deploy the smart contract and verify the proof

Fig. 5: An example of the identity authentication process of the project consultant.

Fig. 5 gives an example of the zk-SNARKs-backed identity authentication process of the project consultant. The Remix IDE (Ethereum 2023) is utilized to deploy the smart contract. The statement "the DELETE operation of sliding windows/doors at level 4 was done before June" is coded as a computation function firstly according to Sec. 3.2. Then, users can compile the function as a logic circuit with 561 constraints by the compile function provided by Remix IDE. The zk-SNARKs require setup to generate a public-private key pair for further proof generating, which is done in Step 3. After the setup process, BIM stakeholders generate proof through their private input, namely their secret knowledge. As Step 4 shows, the generated proof file is a JSON file that involves data of prove schema (elliptic curves) and a hash of proofs. After that, a smart contract with the suffix ".sol" is extracted and deployed on the test blockchain network in Step 5. Finally, the proof file is sent to the smart contract and verified. As Figure 4 shows, the verification of the consultant is true in Step 5.

4. DISCUSSION

The potential influences of the proposed Zk-SNARKs-based BIM user authentication protocol can be analyzed and discussed from different perspectives, including technology, business, and user.

From a technological standpoint, Zero-Knowledge Proof (ZKP) aligns effectively with on-chain knowledge. Through the synergy of Building Information Modeling (BIM) and blockchain, construction knowledge attains inherent transparency and becomes readily accessible via the

distributed ledger. The blockchain records historical BIM operation activities, preserving collaboration traceability. Meanwhile, off-chain BIM files can be securely accessed via on-chain indexes. The amalgamation of on-chain and off-chain BIM-related data presents itself as suitable knowledge for user identity authentication. Consequently, the integration of ZKP and blockchain BIM emerges as a rational and achievable endeavor.

From a business standpoint, the identity authentication protocol based on Zk-SNARKs fosters a higher degree of reliability and trust in BIM-centered collaborations within the blockchain ecosystem. The adaptive access control, rooted in BIM knowledge, safeguards user identity privacy while accommodating an array of application scenarios, including bidding qualifications. Moreover, this identity authentication solution empowers traditional organizations and data providers to securely generate sensitive data.

From a user perspective, the utilization of ZKP empowers BIM stakeholders to efficiently create a suite of identity authentication smart contracts based on their project-specific knowledge. Nonetheless, the adoption of the zk-SNARKs-based identity authentication protocol demands a fundamental grasp of 'computation representation of knowledge.' In essence, users must formulate the logical representation of project-related knowledge. Regrettably, this prerequisite presents a barrier to the widespread adoption of ZKP.

5. CONCLUSION

The advent of blockchain introduces new prospects for transparent, immutable, and secure distributed BIM collaboration. Yet, owing to the inherently open nature of blockchain, the integrity of construction management faces significant threats from severe cybersecurity attacks, particularly password attacks. Establishing secure identity authentication mechanisms for data access within the realm of blockchain BIM becomes the cornerstone of trustworthy collaboration. However, conventional methods of identity authentication, such as the traditional public-private key pair or password, are susceptible to malicious exploitation. Enter zero-knowledge proofs (ZKP), a cryptographic technique empowering the prover to persuade the verifier without disclosing additional meaningful information about their claims. Consequently, ZKP is positioned to endorse password-free identity authentication, basing approvals on users' knowledge, thus effectively sidestepping the risk of malicious password theft.

This paper introduces a ZKP protocol, specifically zk-SNARKs, designed for identity authentication within the context of the blockchain BIM environment. Through the utilization of the zk-SNARKs protocol and on-chain historical BIM editing data, this study establishes an adaptive identity authentication process for collaborative efforts based on blockchain BIM. In contrast to conventional password or public-private key authentication methods, this study employs the knowledge of BIM and construction projects as the primary means of identity verification. ZKP ensures the privacy and security of this knowledge, effectively functioning as the safeguard to authenticate identities.

A pilot case implements the proposed protocol by deploying a smart contract on the test blockchain network. The results vividly illustrate the feasibility of the proposed method. Subsequently, we delve into the potential impact of ZKP from technological, business, and user perspectives. The theoretical contribution of this research hinges on the development of a zk-SNARKs-based identity authentication protocol. This protocol efficiently leverages a subset of on-chain BIM editing records. In practical terms, the workflow of the proposed identity authentication protocol guides BIM users through tasks such as creating domain-specific circuit descriptions of BIM knowledge, developing the smart contract, and deploying it on-chain using tools like ZoKrates and Remix IDE.

This research is subject to several limitations. Firstly, the zk-SNARKs protocol necessitates a trusted setup before generating proofs and theoretically could produce false proofs that appear valid to the verifier. Furthermore, the intricate domain-specific knowledge associated with blockchain-BIM-based construction management remains unexplored, warranting further investigation to formulate a specialized domain-specific language. Lastly, the case pilot's scope is confined to laboratory testing, necessitating more extensive trials in complex real-world project scenarios. As a recommendation for future studies, we propose the exploration of more advanced ZKP protocols, such as zk-STARK, to effectively address the aforementioned limitations.

ACKNOWLEDGEMENT

The work presented in this paper was supported by the Hong Kong Research Grants Council (RGC) (No. 17200221).

REFERENCES

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., Caro, A. D., . . . Yellick, j. (2018). Hyperledger fabric: a distributed operating system for permissioned blockchains. *EuroSys '18: Proceedings of the Thirteenth EuroSys Conference*, (pp. 1-15). doi:10.1145/3190508.3190538

Das, M., Tao, X., & Cheng, J. (2021). BIM security: A critical review and recommendations using encryption strategy and blockchain. *Automation in Construction, 126*. doi:10.1016/j.autcon.2021.103682

Ethereum. (2023, 8, 10). *Remix*. Retrieved from https://github.com/remix-run

Groth, J. (2016). On the Size of Pairing-Based Non-interactive Arguments. *Advances in Cryptology – EUROCRYPT 2016* (pp. 305–326). Berlin, Heidelberg: Springer. doi:10.1007/978-3-662-49896-5_11

Hu, S., Cai, C., Wang, Q., Wang, C., Luo, X., & Ren, K. (2018). Searching an Encrypted Cloud Meets Blockchain: A Decentralized, Reliable and Fair Realization. *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications* (pp. 792-800). Honolulu, HI, USA: IEEE. doi:10.1109/INFOCOM.2018.8485890

Jain , S. (2022). Introduction to Remix IDE. In J. S.M., *A Brief Introduction to Web3* (pp. 89–126). Berkeley, CA: Apress.

Nawari, N., & Ravindran, S. (2019). Blockchain and Building Information Modeling (BIM): Review and Applications in Post-Disaster Recovery. *Buildings, 9*(6). doi: https://doi.org/10.3390/buildings9060149

Parno, B., Howell, J., Gentry, C., & Raykova, M. (2016). Pinocchio: nearly practical verifiable computation. *Communications of the ACM, 59*(2), 103-112. doi:10.1145/2856449

Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin. *2014 IEEE Symposium on Security and Privacy* (pp. 459-474). Berkeley, CA, USA: IEEE. doi:10.1109/SP.2014.36

Skandhakumar, N., Reid, J., Salim, F., & Dawson, E. (2018). A policy model for access control using building information models. *International Journal of Critical Infrastructure Protection*, pp. 1-10. doi:https://doi.org/10.1016/j.ijcip.2018.08.005

Subangan, S., & Senthooran, V. (2019). Secure Authentication Mechanism for Resistance to Password Attacks. *2019 19th International Conference on Advances in ICT for Emerging Regions (ICTer)* (pp. 1-7). Colombo, Sri Lanka: IEEE. doi:10.1109/ICTer48817.2019.9023773

Sun, X., Yu, F., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021). A Survey on Zero-Knowledge Proof in Blockchain. *IEEE Network, 35*(4), 198-205. doi:10.1109/MNET.011.2000473

Tao, X., Liu, Y., Wong, P.-Y., Chen, K., Das, M., & Cheng, J. (2022). Confidentiality-minded framework for blockchain-based BIM design collaboration. *Automation in Construction, 136*. doi:10.1016/j.autcon.2022.104172

Wang, D., Zhao, J., & Wang, Y. (2020). A Survey on Privacy Protection of Blockchain: The Technology and Application. *IEEE Access, 8*, 108766-108781. doi:10.1109/ACCESS.2020.2994294

Wu, L., Li, X., Zhao, R., Lu, W., Xu, J., & Xue, F. (2022). A blockchain-based model with an incentive mechanism for cross-border logistics supervision and data sharing in modular construction. *Automation in Construction, 375*. doi:10.1016/j.jclepro.2022.133460

Yang, X., & Li, W. (2020). A zero-knowledge-proof-based digital identity management scheme in blockchain. *Computers & Security, 99*. doi:10.1016/j.cose.2020.102050

Zhao, R., Chen, Z., & Xue, F. (2023). A blockchain 3.0 paradigm for digital twins in construction project management. *Automation in Construction, 145*. doi:10.1016/j.autcon.2022.104645

Zheng, R., Jiang, J., Hao, X., Ren, W., Xiong, F., & Zhu, T. (2019). CaACBIM: A Context-aware Access Control Model for BIM. *Information, 10*(2). doi:https://doi.org/10.3390/info10020047

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Gid Services, 14*(4), 352-375. doi:10.1504/IJWGS.2018.095647

ZoKrates. (2023, 08 11). *Introduction-ZoKrates*. Retrieved from Zokrates: https://zokrates.github.io/