Volume XXVII 2024
ISSUE no.2
MBNA Publishing House Constanta 2024

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Security for Data Exchange in a Blockchain Ecosystem

To cite this article: Marius Iulian Mihailescu, Stefania Loredana Nita, Valentina Marascu, Marius Rogobete, Ciprian Racuciu, Scientific Bulletin of Naval Academy, Vol. XXVII 2024, pg. 63-73.

Submitted: 28.04.2024
Revised: 25.09.2024
Accepted: 07.10.2024

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-24-I2-006
SBNA© 2024. This work is licensed under the CC BY-NC-SA 4.0 License

Security for Data Exchange in a Blockchain Ecosystem

Marius Iulian MIHAILESCU[1,2], Stefania Loredana NITA[2,3], Valentina MARASCU[1,4], Marius ROGOBETE[5], Ciprian RACUCIU[3]

1) Faculty of Engineering and Computer Science, Scientific Research Centre in Mathematics and Computer Science, SPIRU HARET University, Bucharest, Romania
2) Institute for Computers, Bucharest, Romania
3) Military Technical Academy, "Ferdinand I", Bucharest, Romania
4) National Institute for Laser, Plasma and Radiation Physics, Magurele, Romania
5) HARMAN International

Corresponding author name and e-mail address: Marius Iulian Mihailescu (m.mihailescu.mi@spiruharet.ro)

Abstract. As blockchain technologies increasingly underpin significant economic and social interactions, the need for advanced security mechanisms to protect data exchanged across these decentralized networks becomes crucial. This paper introduces a novel cryptographic scheme designed specifically for blockchain ecosystems to ensure the security, integrity, and confidentiality of data transactions. Our proposed scheme leverages a combination of homomorphic encryption and zero-knowledge proofs, integrated seamlessly with blockchain's inherent properties, such as decentralization and immutability.

Keywords: blockchain; homomorphic encryption; zero-knowledge proofs; data confidentiality; adaptive consensus mechanism, decentralized identity verification

1. Introduction

The importance of safe data exchange in the quickly developing field of blockchain technology cannot be emphasized. Blockchains have become widely used in a wide range of industries, including supply chain management, banking, healthcare, and even government operations [1]-[7]. They were first made prominent by their fundamental role in cryptocurrencies. Because these systems allow decentralized transactions without the need for reliable middlemen, they offer increased efficiency, decreased operational costs, and more transparency. But as blockchain applications become more and more essential to vital infrastructures, the need to protect the data that is shared inside these ecosystems grows significantly.

While decentralization, immutability, and transparency are intrinsic qualities of blockchain technology, they also present special security problems, especially when dealing with sensitive and private data. Traditional cryptography methods and security controls frequently don't work well with blockchain's transparent and decentralized architecture. Moreover, the issue of guaranteeing data security and privacy is made more difficult by the

growing complexity of blockchain networks, which involve numerous parties and differing degrees of access rights.

In this context, our proposed cryptographic scheme is designed to fortify the security of data transactions on blockchain networks. This scheme is particularly vital for applications where data sensitivity is high and the stakes of data breaches are severe, such as in financial services, healthcare records management, and confidential governmental data exchanges. By introducing a method that leverages both homomorphic encryption and zero-knowledge proofs, our approach not only maintains the confidentiality and privacy of data but also allows for the verification of transactions without exposing underlying data. This dual capability is critical in scenarios where data must remain confidential yet verifiable, accommodating the demands for both transparency and privacy that define blockchain's most challenging use cases.

Our work's main contribution is the creation of a strong framework that permits data to be encrypted while maintaining its confidentiality and allowing sophisticated inquiries and calculations to be performed on it. The framework offers multiple deployment options based on security and transparency needs, supporting both public and private blockchains. Additionally, we use zero-knowledge proofs so that no one on the network can compromise privacy or divulge the underlying data in order to confirm that transactions and calculations are right.

The main contributions are summarized as follows:

- Development of a cryptographic framework integrating homomorphic encryption and zero-knowledge proofs tailored for blockchain environments.
- Proposal of a layered security model and adaptive consensus mechanism for enhanced protection based on data sensitivity.
- Implementation of a decentralized identity verification system within the blockchain for improved data integrity and authentication.

Our scheme also introduces a novel protocol for secure data exchange that includes:

- A layered security model that ensures comprehensive data protection from the point of generation to its destination within the blockchain network.
- An adaptive consensus mechanism that enhances security protocols based on the sensitivity and type of data being exchanged, adapting to various threat models dynamically.
- A decentralized identity verification system that uses cryptographic attestations to ensure the authenticity and integrity of all participating nodes.

We analyze the efficacy of our suggested method in simulated blockchain environments and conduct thorough security research. Comparing the results to current approaches, they show improved security for data transactions with negligible effects on transaction performance and latency.

Our plan addresses particular vulnerabilities related to data exchange, making it compatible with the larger framework of blockchain security. It expands the range of applications for blockchain technology by offering a strong architecture that guarantees data integrity and confidentiality on both public and private blockchain networks. The dynamic security requirements of various blockchain applications are met by the implementation of a

layered security model and an adaptive consensus process that is adapted to the sensitivity of the data, improving the systems' dependability and trustworthiness.

By implementing this plan, more businesses will be able to use blockchain technology with assurance since they would know that their data exchanges are secure. As a result, blockchain use may spread more quickly across a range of industries, fostering innovation and enhancing productivity while maintaining strict security guidelines. Therefore, creating and implementing our cryptographic scheme is more than just a technical improvement; rather, it's a necessary step towards utilizing blockchain technology to its fullest in a trustworthy and safe way.

This work paves the path for the implementation of blockchain technology in domains where data security and secrecy are crucial, in addition to addressing the crucial challenge of safeguarding data exchange in blockchain ecosystems. The discovery has practical implications for industries including finance, healthcare, and government services, where safe and effective data sharing is crucial.

2. Development of a cryptographic framework integrating homomorphic encryption and zero-knowledge proofs tailored for blockchain environments

The goal of this proposal is to provide a sophisticated cryptographic framework that will greatly improve data security, integrity, and confidentiality in blockchain ecosystems. Understanding the difficulties presented by blockchain technology, especially regarding protecting data privacy and guaranteeing transparency, the suggested framework combines homomorphic encryption (HE) with zero-knowledge proofs (ZKP), two potent cryptographic approaches. The goal of this integration is to make it possible to compute and verify encrypted data without disclosing the data itself securely and privately.

The primary goals that should be considered when creating a cryptographic system customized for blockchain applications that combines homomorphic encryption and zero-knowledge proofs are as follows.:

- Develop homomorphic encryption techniques for blockchain
    - Implement encryption methods that allow computations to be performed on ciphertexts, producing an encrypted result that, when decrypted, matches the result of operations performed on the plaintext.
    - Tailor these techniques to support typical blockchain operations such as transactions, smart contracts, and consensus mechanisms.
- Integrate zero-knowledge proofs for enhanced privacy and security
    - Develop ZKP protocols that enable the validation of transactions and smart contracts without revealing any underlying sensitive data.
    - Ensure these protocols are efficient enough to maintain high transaction throughput typical of blockchain networks.
- Create a hybrid cryptographic model
    - Combine HE and ZKP to form a hybrid model that leverages the strengths of both techniques, enhancing both privacy and computational efficiency in blockchain applications.
    - Address potential vulnerabilities introduced by each cryptographic method through the synergistic use of both technologies.
- Implementation and testing
    - Implement the cryptographic framework within a test blockchain environment to assess its practical applicability and performance.

    - Conduct thorough testing to evaluate security robustness against various attack vectors and performance impact on blockchain operations.
- Scalability and adaptability analysis
    - Analyze the scalability of the proposed cryptographic framework to handle large-scale blockchain networks.
    - Examine the adaptability of the framework across different blockchain architectures, including both public and private networks.

To achieve the main objectives, the following research and development plan should be followed and adjusted per needs:

1. **Phase 1. Conceptualization and initial development**
    - Research existing implementations of HE and ZKP in blockchain contexts.
    - Develop initial cryptographic prototypes for integrating HE and ZKP within a blockchain simulation.
2. **Phase 2. Framework enhancement and optimization**
    - Enhance cryptographic protocols to optimize speed and security, addressing specific blockchain needs.
    - Test and refine the integration of HE and ZKP, focusing on reducing computational overhead and latency.
3. **Phase 3. Real-World implementation and evaluation**
    - Deploy the framework on a pilot blockchain project with controlled real-world data.
    - Evaluate the framework's performance, focusing on transaction processing speed, data privacy, and security efficacy.
4. **Phase 4. Scaling and commercial deployment**
    - Address any scalability issues found during testing, optimizing the framework for larger blockchain networks.
    - Prepare for commercial deployment by ensuring the framework's compatibility with major blockchain platforms.

If the research the development plan is followed accordingly, the expected impact and contributions should be measured in terms of success as follows:

- Providing robust data privacy and security without sacrificing the decentralization and transparency that are hallmarks of blockchain technology.
- Enabling the broader adoption of blockchain technology in sectors where data confidentiality and security are paramount, such as finance, healthcare, and government.
- Offering a scalable and adaptable solution that can be tailored to a wide range of blockchain applications and architectures.

3. Proposal of a layered security model with adaptive consensus mechanism for enhanced protection based on data sensitivity

It is crucial to protect sensitive data's security and confidentiality in the rapidly developing field of blockchain technologies. With the integration of an adaptive consensus mechanism, our suggested layered security model may react dynamically to different degrees of data sensitivity. In addition to improving security, this method maximizes blockchain performance by adjusting to the varying security requirements of transactions.

1. **Layered security model.** The layered security model is designed to provide differential security protocols based on the type and sensitivity of the data involved in blockchain transactions. Here's how the layers are structured:
   - *Layer 1. Data encryption*
     - *Purpose.* Ensures the confidentiality of data stored on the blockchain.
     - *Implementation.* Use of robust encryption algorithms suitable for blockchain environments, such as AES for standard data and homomorphic encryption for data requiring processing in its encrypted state.
   - *Layer 2. Transaction security*
     - *Purpose.* Safeguards the integrity and authenticity of transactions.
     - *Implementation.* Implementation of digital signatures using public-key cryptography to verify transaction authenticity and integrity.
   - *Layer 3. Network security*
     - *Purpose.* Protects the blockchain network from unauthorized access and malicious attacks.
     - *Implementation.* Deployment of firewalls, intrusion detection systems (IDS), and anti-malware solutions that are tailored to the specific needs and architecture of the blockchain network.
   - *Layer 4. Consensus security*
     - *Purpose.* Enhances the security of the consensus process based on the sensitivity of the transaction data.
     - *Implementation.* An adaptive consensus mechanism that adjusts its parameters based on the assessed risk and importance of the data involved.
2. **Adaptive consensus mechanism.** The adaptive consensus mechanism is designed to adjust the difficulty and robustness of the consensus process in response to the sensitivity of the data being transacted. This mechanism enables the blockchain to maintain high throughput and efficiency without compromising the security of sensitive transactions.
   - *Consensus adjustment parameters*
     - *Data sensitivity rating.* Each piece of data is rated based on its sensitivity (e.g., public, confidential, secret, top secret). This rating influences the consensus requirements.
     - *Transaction value and type.* Higher-value transactions or those involving sensitive data types may require a more rigorous consensus process.
     - *Network state and threat level.* Real-time monitoring of network health and threat levels to dynamically adjust consensus requirements.
   - *Implementation strategies*
     - *Multi-Factor consensus requirements.* Depending on the sensitivity rating, transactions may require different numbers of validations. For example, top secret data might require validations from a larger number of nodes or nodes with higher trust ratings.
     - *Variable block confirmation times.* Increase the number of confirmations required for blocks containing highly sensitive data to enhance security at the expense of slower processing times.
     - *Specialized node requirements*. Transactions involving highly sensitive data might only be processed and verified by nodes that meet specific security criteria, such as geographic location, compliance certifications, or hardware specifications.

The benefits of the proposed model can be summarised as follows:

- *Enhanced data protection.* By applying security measures tailored to the sensitivity of the data, the blockchain can provide stronger protection where it is most needed, reducing the risk of data breaches and leaks.
- *Optimized performance.* The adaptive nature of the consensus mechanism allows for the balancing of security and performance, ensuring that the blockchain can operate efficiently without unnecessary delays for less sensitive transactions.
- *Increased trust and compliance.* With advanced security measures in place, the blockchain network can meet various regulatory compliance standards, making it suitable for applications in industries with stringent data protection laws.

This complete approach offers a strong framework for safeguarding blockchain networks, especially in situations where data sensitivity varies greatly. It does this by combining an adaptive consensus mechanism with a layered security model.

4. Implementation of a decentralized identity verification system within the blockchain for improved data integrity and authentication

Decentralized identity verification systems (DIVS) are necessary to improve data integrity and authenticity across blockchain networks. This system offers a safe, open, and unchangeable way to manage identities by utilizing the decentralization and immutability that blockchain technology offers by nature. A solution like this is especially important in settings where transaction validity and network security are directly affected by identity verification.

The DIVS offers a way to validate user identities without depending on central authority, and it is made to work easily within both new and existing blockchain frameworks. To guarantee the integrity and validity of user identities, this system combines smart contracts, consensus methods, and cryptographic approaches.

The main core components of the proposed DIVS are summarized as follows:

1. **Identity Registration Protocol**
    - *Public Key Infrastructure (PKI).* At the time of registration, each user generates a cryptographic key pair (public and private keys). The public key is used as a part of the user's digital identity.
    - *Identity verification.* Users submit identity proofs to one or more trusted entities (validators) on the network. These entities verify the proofs and vouch for the authenticity of the identity.
    - *Smart contract for identity registration.* Once verified, the user's identity details along with the public key are stored in a smart contract. This contract emits events and records transactions pertaining to identity verifications, updates, and revocations.
2. **Decentralized Identity Smart Contract (DISC)**
    - *Storage.* DISC maintains a ledger of registered identities, hashed personally identifiable information (PII), and associated public keys.
    - *Access control.* Smart contract functions ensure that identity data can only be accessed by authorized parties, and any access is transparent and traceable on the blockchain.
    - *Updates and revocation.* Provides mechanisms for updating or revoking identities, requiring multi-signature verification from multiple trusted entities to prevent unauthorized changes.
3. **Authentication protocol**
    - *Challenge-response mechanism.* To authenticate, a user signs a randomly generated challenge (timestamp or nonce) issued by the requesting party (another user or service) using their private key.
    - *Verification via smart contract.* The requesting party verifies the signature using the public key retrieved from DISC, ensuring the authenticity of the user.

The implementation steps that should be considered are listed as follows:

1. **Development of smart contracts**
   - *Identity registration contract.* Handles the registration and verification process.
   - *DISC.* Manages storage, access, and lifecycle of identity data.
2. **Integration with blockchain network**
   - Deploy smart contracts on the blockchain.
   - Ensure compatibility with existing blockchain infrastructure and protocols.
3. **User interface and experience**
   - Develop user-friendly interfaces for identity registration, management, and authentication.
   - Provide integration support for third-party services to utilize the identity verification system.
4. **Security measures and testing**
   - Implement advanced cryptographic safeguards to protect identity data.
   - Conduct thorough testing, including penetration testing and smart contract audits, to ensure system integrity and security.
5. **Deployment and continuous improvement**
   - Roll out the system in phases, starting with a pilot to gauge user feedback and system performance.
   - Continuously monitor, update, and improve the system based on user needs and emerging security threats.

The following benefits observed after the implementation state and point out the best out from the scheme, and are summarized as follows:

- *Enhanced security and privacy.* By decentralizing identity verification, the system reduces the risk of identity theft and fraud.
- *Increased trust and transparency.* All transactions related to identity verification are recorded on the blockchain, providing a transparent audit trail.
- *Interoperability*. Designed to be compatible across various blockchain systems, facilitating wider adoption and cross-platform transactions.

With the purpose of transforming identity management on the blockchain, this decentralized identity verification system offers a strong foundation for safe, transparent, and effective identity verification and authentication.

4.1. Mathematical background and the implementation for decentralized identity verification system (DIVS)

The proposed DIVS (see Figure 1) in a blockchain utilizes cryptographic algorithms, including public key cryptography and hash functions, along with smart contracts to manage and verify identities securely and efficiently.

The mathematics of the main functions are:

1. **Public key cryptography**
   - Each user generates a key pair consisting of a private key (sk) and a public key *(pk)*.
   - Key generation function is defined as $(pk, sk) = KeyGen()$
   - Signature function is defined as $\sigma = Sign(sk, m)$, where m is the message to be signed.
   - Verification function is defined as $isValid = Verify(pk, \sigma, m)$, where $isValid$ is a boolean indicating whether the signature is valid.

2. **Hash functions**
    - Used to hash identity information to ensure privacy and integrity.
    - The hash function is defined as $h = Hash(data)$, where $data$ includes personally identifiable information (PII).

The smart contracts functions are shown as bellow:

1. **Register identity**
    - Stores user's pk and hashed PII.
    - Register function in smart contract is defined as $register(pk, h)$
2. **Retrieve public key**
    - Retrieves a public key based on user ID or another identifier.
    - Retrieve function in smart contract is $pk = retrievePublicKey(userID)$
3. **Update and revoke identity**
    - Updates or revoke's identity information, requiring consensus among multiple validators.
    - Update function in smart contract is $updateIdentity(userID, newPk, newH)$
    - Revoke function in smart contract is defined as $revokeIdentity(userID)$

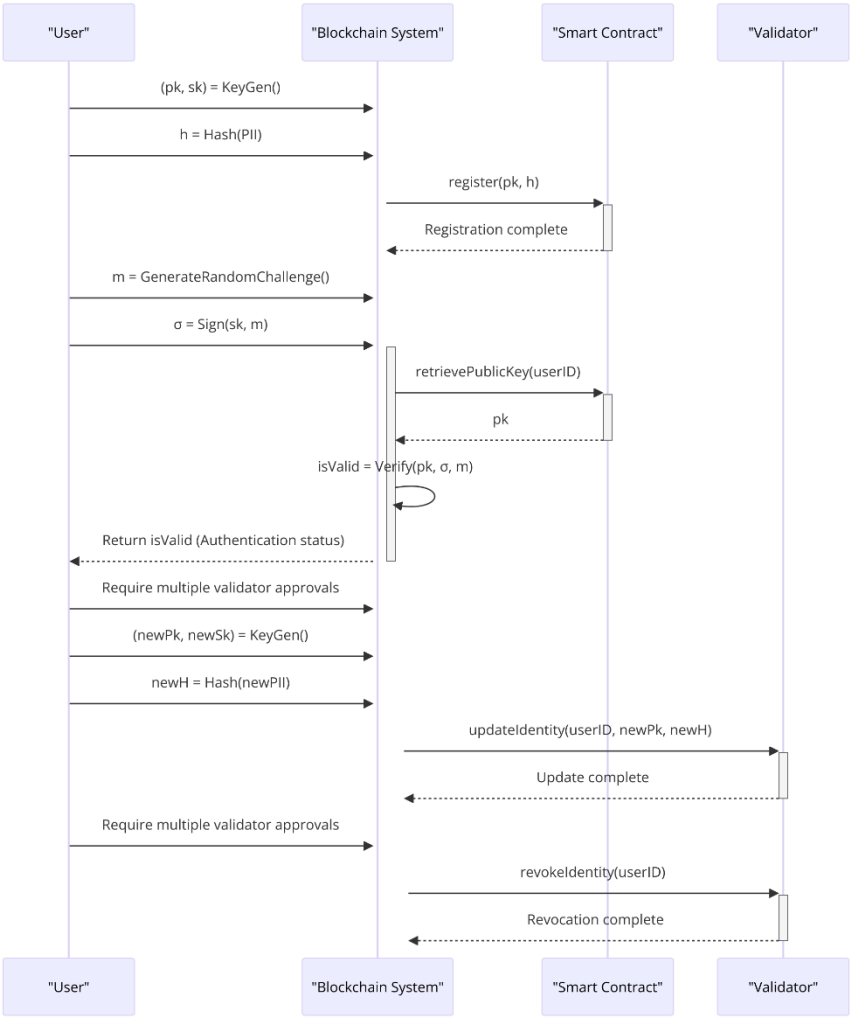

Figure 1. The DIVS

4.2. The pseudocode for the key process

In the process of generating the key we will need the following actors: User, Client Application, Blockchain Network (Smart Contract), which are involved in the following flow:

1. User requests to generate keys.
2. Client Application executes $KeyGen()$.
3. User provides PII.
4. Client Application hashes PII using Hash(data).
5. Client Application calls $register(pk, h)$ to store public key and hashed PII on the blockchain.

```
Function KeyGen():
    Generate key pair (sk, pk)
    Return (pk, sk)

Function Sign(sk, m):
    Compute signature σ using sk on message m
    Return σ

Function Verify(pk, σ, m):
    Check if σ is a valid signature of m under pk
    Return isValid

Function Hash(data):
    Compute hash h of data
    Return h

SmartContract Functions:

Function register(pk, h):
    Store pk and h in blockchain storage

Function retrievePublicKey(userID):
    Retrieve pk for userID from blockchain storage
    Return pk

Function updateIdentity(userID, newPk, newH):
    Require verification from multiple validators
    Update pk and h for userID with newPk and newH

Function revokeIdentity(userID):
    Require verification from multiple validators
    Mark the identity of userID as revoked
```

4.3. The system interaction

```
User Registration:
    (pk, sk) = KeyGen()
```

```
    h = Hash(PII)
    register(pk, h)

User Authentication:
    m = GenerateRandomChallenge()
    σ = Sign(sk, m)
    pk = retrievePublicKey(userID)
    isValid = Verify(pk, σ, m)
    Return isValid

Identity Update:
    Require multiple validator approvals
    (newPk, newSk) = KeyGen()
    newH = Hash(newPII)
    updateIdentity(userID, newPk, newH)

Identity Revocation:
    Require multiple validator approvals
    revokeIdentity(userID)
```

5. Conclusion

A comprehensive answer to the problems of protecting the data sharing in blockchain ecosystems is provided by the suggested cryptographic framework. The framework provides efficient and safe transaction verification while simultaneously guaranteeing data confidentiality and privacy using homomorphic encryption and zero-knowledge proofs. A dynamic approach to security is offered by the layered security model and adaptive consensus mechanism, which scale protections in accordance with the sensitivity of the data. To further improve security, the decentralized identity verification system makes sure that every user on the blockchain is authenticated and reliable.

This strategy has important ramifications for industries like finance, healthcare, and government where private and secure data exchanges are essential. When this framework is successfully put into practice, it may open the door for blockchain technology to be adopted more widely. Blockchain technology offers a balance between anonymity and transparency that satisfies the strict security requirements seen in many professional domains. The investigation and creation of this framework established a standard for upcoming advancements in blockchain security, which could have an impact on a variety of applications and promote the development of safe, decentralized technology.

References

[1]. J. Ma *et al*., "Research On Electricity Spot Market Trading System Based On Blockchain Technology," *2023 3rd International Conference on Computer Science and Blockchain (CCSB)*, Shenzhen, China, 2023, pp. 101-106, doi: 10.1109/CCSB60789.2023.10398820.

[2]. S. R. Niya, I. Mesić, G. Anagnostou, G. Brunini and C. J. Tessone, "A First Analytics Approach to Cardano," *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Dubai, United Arab Emirates, 2023, pp. 1-5, doi: 10.1109/ICBC56567.2023.10174896.

[3]. X. Wang *et al*., "Application of data storage management system in blockchain-based technology," *2023 IEEE 2nd International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA)*, Changchun, China, 2023, pp. 1437-1440, doi: 10.1109/EEBDA56825.2023.10090564.

[4]. Y. Wang, J. Ali, J. Arshad and Y. Liu, "A Proxy-Layer Approach to Secure Smart Contract Deployment on Private EVM-Based PoA Blockchains," *2023 IEEE International Conference on Blockchain (Blockchain)*, Danzhou, China, 2023, pp. 109-112, doi: 10.1109/Blockchain60715.2023.00027.

[5]. M. Piskorec, B. D. James Murphy, F. Rüegsegger, S. R. Niya and C. J. Tessone, "Bow-tie structure of the Polkadot transfer network," *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Dubai, United Arab Emirates, 2023, pp. 1-4, doi: 10.1109/ICBC56567.2023.10174939.

[6]. G. Ramezan, M. Schneider and M. McCann, "MACS: A Multi-Asset Coin Selection Algorithm for UTXO-based Blockchains," 2023 IEEE International Conference on Blockchain (Blockchain), Danzhou, China, 2023, pp. 121-126, doi: 10.1109/Blockchain60715.2023.00029.

[7]. W. Song et al., "A Blockchain Based Fund Management System for Construction Projects - A Comprehensive Case Study in Xiong'an New Area China," 2023 Tenth International Conference on Software Defined Systems (SDS), San Antonio, TX, USA, 2023, pp. 28-33, doi: 10.1109/SDS59856.2023.10329054.