Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 5236579, 9 pages
https://doi.org/10.1155/2021/5236579

Research Article

A Privacy-Preserving Blockchain Supervision Framework in the Multiparty Setting

Baodong Wen,[1] Yujue Wang,[2] Yong Ding ,[1,3] Haibin Zheng,[2] Hai Liang ,[1] and Huiyong Wang[4]

[1] *Guangxi Key Laboratory of Cryptography and Information Security, School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin, China*
[2] *Hangzhou Innovation Institute, Beihang University, Hangzhou, China*
[3] *Cyberspace Security Research Center, Pengcheng Laboratory, Shenzhen, China*
[4] *School of Mathematics and Computing Science, Guilin University of Electronic Technology, Guilin, China*

Correspondence should be addressed to Yong Ding; stone_dingy@126.com

Received 2 July 2021; Revised 8 August 2021; Accepted 20 August 2021; Published 24 September 2021

Academic Editor: Weizhi Meng

Data supervision is an effective method to ensure the legality of user data on blockchain. However, the massive growth of data makes it difficult to achieve data supervision in existing blockchain applications. Also, data supervision often leads to problems such as disclosure of transaction data and user privacy information. To address these issues, this paper proposes a privacy-preserving blockchain supervision system (BSS) in the multiparty setting, where a supervision chain is introduced to realize data supervision on blockchain. All sensitive information such as user information in the supervising data is encrypted by the attribute-based encryption (ABE) technology, so that both privacy protection and access control on user data can be achieved. Theoretical analysis and comparison show that the proposed BSS scheme is efficient, and experimental analysis indicates the practicality of our BSS scheme.

1. Introduction

Blockchain is featured with the characteristics of decentralization, autonomy, and immutability [1]. As the key technology in the construction of trust systems, it is envisioned as an effective technology to address security issues faced in finance, property rights, smart cities, government affairs, supply chain, and other fields [2]. With the rapid development and wide application of blockchain, due to its open and transparent characteristics, more and more transaction data, user information, network node address, and other information face the risk of privacy leakage [3]. Unlike the traditional centralized architecture, blockchain does not rely on a central node; thus, it can effectively avoid the single point of failure. However, in order to reach consensus by all blockchain nodes, the data has to be disclosed to all of them, which also brings the risk of privacy leakage.

The lack of centralized entities makes it difficult for relevant government regulators to supervise the blockchain. Lack of regulation will seriously restrict the healthy and sustainable development of the entire blockchain industry. However, there remain some problems in the existing supervision methods on blockchain [4]. Due to the autonomous and decentralized features of blockchain, it is difficult to guarantee the legality of data on blockchain; that is, the data on blockchain cannot be well supervised. Moreover, supervision may bring the issue of privacy protection [5, 6]. Due to the significant difference between the blockchain technology and traditional system architecture, many traditional privacy protection methods are not applicable to blockchain. Therefore, it is necessary to design an effective supervision mechanism with privacy protection on user data in blockchain.

The multilayer structure has been used to achieve supervision on blockchain. Yang et al. [7] realized the monitoring of user behavior and the verification of blocks by employing the multilayer structure. The block verification is executed by the system supervisor, which improves the performance and security of the system. Li et al. [8] designed a two-layer adaptive blockchain-based supervision framework (TABS) to address the supervision issues in off-site modular housing production, where the first layer contains the adaptive private sidechains of participants, and the second layer is the main blockchain for communication and transactions. TABS can effectively prevent the main blockchain from tampering with records, and it can also prompt users to quickly publish their transaction records without revealing their privacy. Note that a single supervisor is easily corrupted by an adversary, which can cause irreparable losses. The problem of single point of failure can be effectively avoided by setting multisupervision in the supervision process. Yang et al. [7] and Li et al. [8] put forward their schemes in the agricultural machinery scheduling and off-site modular housing production scenarios, respectively. However, there was no universal blockchain supervision framework for the application scenarios that need to be regulated. In addition, there is no blockchain supervision framework that allows multiple parties to participate in a multilayer blockchain structure.

1.1. Our Contributions. To address the above mentioned issues, this paper proposes a multiparty blockchain supervision system (BSS) framework. In BSS, a dual-chain architecture is introduced, which contains two types of blockchains, namely, business chain (BC) and supervision chain (SC). SC consists of the regulatory authorities and supervisors, which provides the supervision service for the data on BC. By deploying transaction information and supervision information separately, the scalability of the BSS can be improved.

ABE is employed to realize flexible access control on data; that is, the regulatory authority can set access control policies, so that different supervisors have different permissions. Regulatory authority can encrypt data for multiple supervisors at the same time and build communication channels without obtaining each supervisor's public key in advance. This process can reduce the computing overhead caused by encrypting data for each recipient. Data information will go through two rounds of supervision by regulatory authorities and supervisors. Smart contract in BSS can realize verification and upload supervision information to the blockchain. Thus, BSS supports the management and control on data in BC and also protects the data privacy, which offers trade-off between supervision and privacy protection. Through security and theoretical analysis, it is shown that the proposed BSS framework is suitable for different ABE and application scenarios.

1.2. Related Works. Yong et al. [9] designed a blockchain supervision system to supervise the supply of vaccines through smart contracts and machine learning. Their scheme not only supports the query on individual vaccination records and tracking the vaccine operation records through the smart contract but also allows the regulatory agencies to manage expired vaccines. Meng et al. [10] proposed a security mechanism to build trust-based filtering. This mechanism processes and reduces malicious traffic by using traffic fusion and aggregation. Yin et al. [11] provided an approach using supervised machine learning to implement system supervision, where the gradient enhancement algorithm was used to predict the type of entity. A classifier was established to distinguish 12 categories by using 957 entities as sample data for authentication. The gradient boosting algorithm with default parameters was used to improve the accuracy of average cross validation. Ma et al. [12] proposed a traceable blockchain scheme, SkyEye, which enables the regulatory authority to track the identity of users. In [13], Ma et al. designed a blockchain traceable scheme with oversight function based on SkyEye, from a distributed multikey generation protocol and some other cryptographic primitives. Note that the supervisor must obtain the consent of committees when tracing some users. Meng et al. [14] proposed a blockchain-enabled single character frequency-based exclusive signature matching scheme to secure the security of smart IoT environment.

In terms of privacy protection, many information hiding mechanisms have been proposed for transaction contents, including Monero and Zrash. Monero is mainly based on the Cryptonote protocol, which uses one-time random address and ring signature to randomize the sender and other node information so as to realize the sender's anonymity. Encryption is used to realize the anonymity of the receiver; that is, only the receiver has the private key of the ciphertext. In Monero coin, the anonymity of the sender is determined by the size of the anonymous set. The stronger the anonymity is, the larger the anonymous set is, but the time complexity of encryption and decryption will also increase. Zrash [15] is a cryptocurrency embedded with noninteractive zero-knowledge proof, which divides the address into transparent address and hidden address. The hidden address is used to realize anonymity for users. Unlike Monero, Zrash can authenticate transactions without disclosing transaction data. However, users may not make transparent transactions due to the computational cost of zero-knowledge proof. Blockchain platforms such as Monax and Multichain [16] provide multichain solutions that enable privacy protection of transaction data through interchain isolation.

As a kind of computer protocol, smart contract [17] can realize automatic verification, programmable execution, irreversible, and other functions. The security and privacy of smart contract can be guaranteed by formal verification [18], decompilation [19], etc. Cheng et al. [20] introduced Ekiden, which combines blockchain with trusted hardware. The Ekiden system separates consensus and execution, which offers the high system performance and scalability. In the initialization phase, the smart contract is encrypted and stored on the blockchain after verification. The corresponding public key and private key should be provided when the smart contract is called and acquired. The privacy protection for smart contract is realized by storing encrypted contract.

ABE is developed on the basis of identity-based encryption (IBE) proposed by Boldyreva et al. [21]. Compared with the previous encryption methods, ABE realizes a one-to-many encryption mode, provides fine-grained access control on data, and also supports certain fault tolerance [22]. Goyal et al. [23] designed a key policy attribute-based encryption scheme, where the access policy and attribute set are embedded in the key and ciphertext, respectively. Bethencourt et al. [24] proposed a ciphertext policy attribute-based encryption scheme, where the access policy and user attributes are, respectively, embedded in ciphertext and key, which can be used in access control applications such as private data sharing [25].

1.3. Organization. The remainder of this paper is organized as follows. Section 2 describes the system model, dual-chain architecture, and security requirements. Section 3 introduces the preliminaries for the proposed BSS scheme. A description of our BSS scheme is presented in Section 4. In Section 5, the security and performance of our BSS scheme are evaluated and compared. Section 6 concludes the paper.

2. System Model and Requirements

2.1. System Model. As shown in Figure 1, a BSS system consists of five types of entities, namely, regulatory authority, supervisor, key generation center (KGC), business chain (BC), and supervision chain (SC).

(i) *Regulatory Authority*. For the data to be supervised, they can be judged by the regulatory authority according to some rules. The supervision results are encrypted by the regulatory authority and broadcasted to supervisors.

(ii) *Supervisor*. The supervisors with decryption permission are able to decrypt the information sent by the regulatory authority and supervise the related data.

(iii) *KGC*. The KGC is responsible for generating system public parameters and registering the attributes of supervisor.

(iv) *BC*. BC is mainly used to maintain the business data information.

(v) *SC*. SC mainly manages the supervision information. The supervision information processed by the regulatory authority and the supervisor is transmitted to SC.

The data to be supervised in the BSS system is first delivered to the regulatory authority. They are supervised according to the supervision rules by the regulatory authority and then encrypted by employing the hybrid encryption technology, where the access policy can be set during hybrid encryption. Only the supervisor satisfying the access policy has relevant authority to conduct supervision. The supervisors need to perform the second round of supervision on data. If the supervision results of two rounds are consistent, then the smart contract uploads the supervision information to SC.

2.2. Dual-Chain Architecture. In order to realize data supervision, this paper introduces a dual-chain architecture composed of BC and SC and uses the ABE method to protect the privacy of user data. The dual-chain architecture is shown in Figure 2.

(i) *SC*. SC consists of the regulatory authority nodes (RAN) and the supervisor nodes (SUN). In real world applications, RAN can be the regulatory authority, while SUN may comprise legal departments. RAN is able to perform supervision and encryption on data. Data submitted to the RAN for supervision is reviewed in the first round to detect illegal information. SUN can complete the decryption and supervision on data, so that the supervisor can further supervise the relevant data after decryption. The supervision results in the two rounds of supervision can be confirmed and uploaded to SC through smart contract.

(ii) *BC*. Different types of data are stored on BC, which should have been delivered to SC for supervision before being written to BC. Also, when the data is retrieved from BC, it should be first delivered to SC for supervision. In addition, the data in BC may also be taken out for supervising whenever necessary.

2.3. Security Requirements. A secure BSS system in the multiparty setting has to satisfy the following requirements.

(i) *Anticollusion Attack*. Even when the keys of multiple supervisors are combined, these supervisors cannot obtain the valid ciphertext. Supervisors cannot obtain plaintext data that exceeds their regulatory capability.

(ii) *Multiparty Supervision*. Data on the BC can be supervised by multiple parties. It avoids the problem of excessive concentration of power under the supervision of an individual or separate agency and reduces the security risk caused by the breach of one party.

(iii) *Privacy Protection*. Sensitive data submitted to the SC should be encrypted to guarantee their privacy.

(iv) *Access Control*. The supervisors are not allowed to access data that is not authorized. Different supervisors have their own permission and have different decryption capabilities for the data sent from the regulatory authority.

3. Preliminaries

3.1. Attribute-Based Encryption. A ciphertext-policy attribute-based encryption scheme A consists of four algorithms

$$A = (\text{Setup}, \text{KeyGen}, \text{Enc}, \text{Dec}). \tag{1}$$

(i) $Setup(d) \longrightarrow (PK, MK)$. With input the security parameter d, the system setup algorithm outputs public parameter PK and master key MK

(ii) $KeyGen(MK, U) \longrightarrow SK$. With input the master key MK and the attribute set U, the key generation

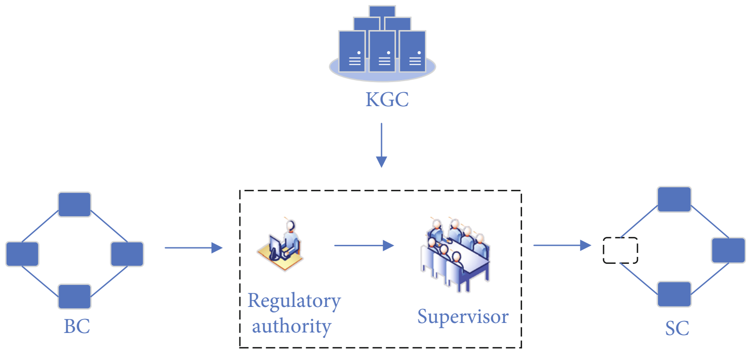


Figure 1: System model of BSS.

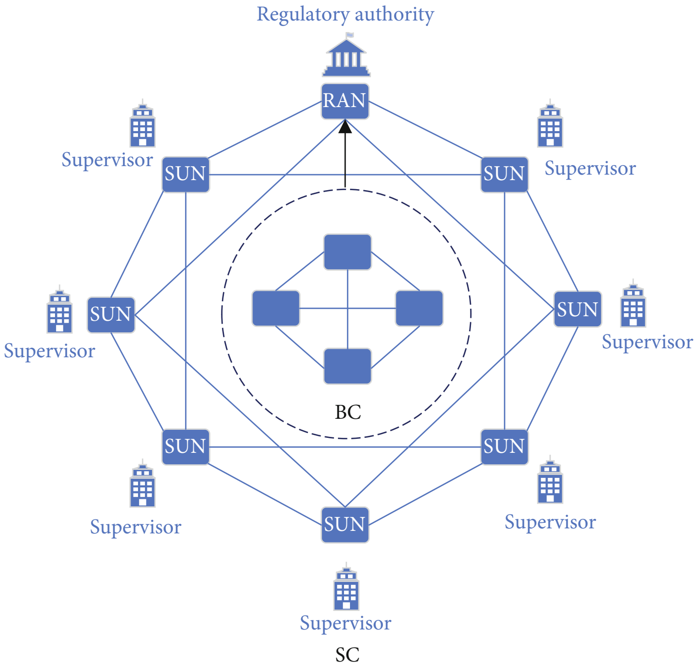


Figure 2: Dual-chain architecture.

algorithm outputs the private key SK associated with the user attribute set U

(iii) $Enc(PK, M, T) \longrightarrow CT$. With input the public parameter PK, a plaintext message M, and an access structure T, the encryption algorithm outputs a ciphertext CT

(iv) $Dec(CT, SK, PK) \longrightarrow M$. With input the ciphertext CT, private key SK, and public parameter PK, if the attributes in the user key match the access policy required by the ciphertext, then the decryption algorithm outputs the corresponding plaintext M

3.2. Bilinear Groups. Let G_1 and G_T be two cyclic groups of prime order p and g be a generator of G_1. A bilinear map $e : G_1 \times G_1 \longrightarrow G_T$ satisfies the following conditions:

(i) *Bilinearity*. For $a, b \in_R Z_p$, we have

$$e\left(g^a, g^b\right) = e(g, g)^{ab}. \tag{2}$$

(ii) *Nondegeneracy*. There exists $r, s \in G_1$ such that

$$e(r, s) \neq 1_{G_T}, \tag{3}$$

where 1_{G_T} is the identity of G_T.

(iii) *Computability*. For $r, s \in_R G_1$, there is an efficient algorithm to compute $e(r, s)$.

4. BSS Construction

Our BSS framework consists of five procedures, namely, system setup, registration, regulatory authority supervision, supervisor second-round supervision, and data processing. The frequently used notations are summarized in Table 1, and the process of supervision is shown in Figure 3.

Table 1: Notations.

Notations	Descriptions
F	Secure symmetric encryption algorithm
A	Ciphertext-policy attribute-based encryption scheme
R	Registration record
U	Attribute set
m	The data to be supervised
I	User information
J_1	The supervision result of the regulatory authority
J_2	The supervision result of the supervisor
N	The signature of KGC
t	Timestamp
β	Supervision record
L	Supervision information

4.1. System Setup. KGC selects a secure symmetric encryption scheme $F = (\text{KeyGen}, \text{Enc}, \text{Dec})$ and a ciphertext-policy attribute-based encryption scheme $A = (\text{Setup}, \text{KeyGen}, \text{Enc}, \text{Dec})$. With input the security parameter d, KGC runs the algorithm $A.\text{Setup}(d)$ to generate the public parameter PK and the master key MK. Then, KGC uploads the encryption scheme F and the public parameter PK to the blockchain, while MK is kept secret and not allowed to be accessed by other users.

4.2. Registration. The supervisor submits its own attribute set U to KGC for registration. KGC first searches the database; if the supervisor has already registered, the registration request is rejected. Otherwise, the attribute set U is added to the local database of KGC. Then, KGC generates a registration record as follows:

$$R \longleftarrow \left(U \| \text{id}_S \| N \| t_{\text{Reg}}\right), \tag{4}$$

which contains the user's attribute set U, identity document of supervisor id_S, KGC's signature N, and registration time t_{Reg}. The registration record R is written to the blockchain. Then, KGC runs the A.KeyGen algorithm with the master key MK and user attribute U to generate the private key SK, which is sent to the corresponding supervisor to complete the registration process. The registration process is shown in Algorithm 1.

4.3. Regulatory Authority Supervision. The data m to be supervised is first uploaded to RAN, so that the regulatory authority can perform supervision based on its own rules. The regulatory authority generates supervision record

$$\beta_{\text{RA}} \longleftarrow (m \| I \| J_1 \| t_{\text{RA}} \| \text{id}_{\text{RA}}), \tag{5}$$

where m is the supervised data, I is the user information, t_{RA} is the regulatory authority supervision time, and id_{RA} is the identity document of regulatory authority. Also, $J_1 \longleftarrow (\text{id}_m \| \text{id}_{\text{BC}} \| V \| \lambda_{\text{RA}})$ denotes the supervision result of the regulatory authority, where id_m is the identity document of m, id_{BC} is the identity document of BC, V is the rule that m violates, and λ_{RA} is the judgment of regulatory authority.

The regulatory authority generates a symmetric key $k \longleftarrow F.\text{KeyGen}(d)$ and calculates

$$\begin{aligned} C_1 &= A.\text{Enc}(\text{PK}, k, T), \\ C_2 &= F.\text{Enc}(k, \beta_{\text{RA}}), \end{aligned} \tag{6}$$

where PK and T are the public parameters and access structure in ABE, respectively. The RAN outputs the corresponding ciphertext $\langle C_1, C_2 \rangle$ and broadcasts it to supervisors.

4.4. Supervisor Second-Round Supervision. For the received ciphertext tuple $\langle C_1, C_2 \rangle$, the supervisor executes $A.\text{Dec}(C_1, \text{SK}, \text{PK})$ with its private key SK. If SK satisfies the access policy T in C_1, then the supervisor is allowed to get the symmetric key k through decryption. Moreover, the supervisor runs the algorithm $F.\text{Dec}(C_2, k)$ to get the corresponding plaintext tuple β_{RA}, which contains data m on BC. The supervisor is then able to run a second round of supervision on data m and outputs the corresponding supervision record

$$\beta_S \longleftarrow (m \| I \| J_2 \| t_S \| \text{id}_S), \tag{7}$$

where t_S is the supervisor supervision time. Here, $J_2 \longleftarrow (\text{id}_m \| \text{id}_{\text{BC}} \| V \| \lambda_S)$ is the supervision result of the supervisor, where λ_S is the judgment of supervisor.

4.5. Data Processing. The smart contract will compare the supervision results generated in two rounds of supervision by the regulatory authority and the supervisor, respectively. If they are consistent, then the smart contract generates the following supervision information

$$L \longleftarrow (\beta \| t_{\text{Pro}}), \tag{8}$$

and adds it to SC, which consists of data information $\beta \longleftarrow (\beta_{\text{RA}} \| \beta_S)$ and data processing time t_{Pro}. If the two supervision results are inconsistent, a new round of supervision should be performed by RAN. The procedure of data processing is shown in Algorithm 2.

5. Analysis and Comparison

5.1. Security Analysis

Theorem 1. *If the symmetric encryption scheme F and ABE scheme A are secure, then the proposed BSS framework can resist collusion attacks.*

Proof. In ABE schemes, SK is associated with a random polynomial $q(x)$ or a random number r. Different random polynomial $q(x)$ or random number r will be selected when generating private key SK for different users. The Lagrange

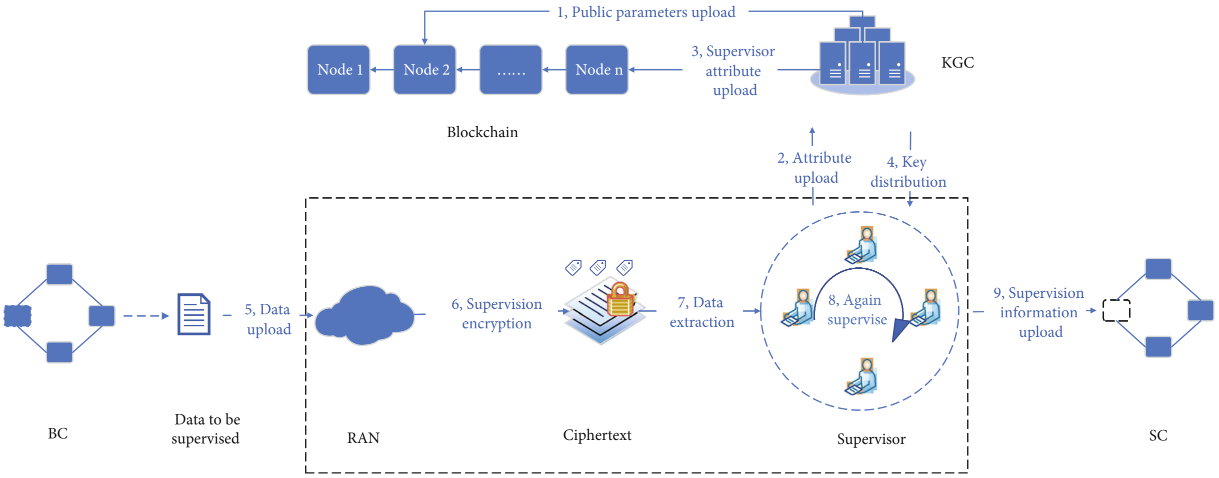


Figure 3: A procedure of BSS.

```
Require: $U, id_S, MK$
Ensure: $success/failure$
    $KGC \longleftarrow U$
    if $id_S$ already registered then
        return $failure$
    else
        $KGC \longleftarrow id_S, U$
        Register $id_S, U$ to local database
        Generate $N, t_{Reg}$
        $R \longleftarrow (U \| id_S \| N \| t_{Reg})$
        Send $R$ to blockchain
        $SK \longleftarrow A.KeyGen(MK, U)$
        Send $SK$ to $id_{S.}$
    else if
```

Algorithm 1: Registration.

```
Require: $J_1, J_2$
Ensure: $success/failure$
    Smart contract $\longleftarrow J_1, J_2$
    if $J_1 = J_2$ then
        Generate $t_{Pro}$
        $\beta \longleftarrow (\beta_{RA} \| \beta_S)$
        Smart contract $\longleftarrow \beta, t_{Pro}$
        $L \longleftarrow (\beta \| t_{Pro})$
        $SC \longleftarrow L$
        return $success$
    else
        return $failure$
    end if
```

Algorithm 2: Supervision data processing.

interpolation method requires that only when all values come from the same polynomial, the value of the target point can be solved. Therefore, when the keys of multiple users are combined, different random numbers and random polynomials cannot be combined to obtain the corresponding plaintext information. Thus, the private keys of different users cannot be combined, which means the proposed BSS framework can resist collusion attacks of multiple users.□□ □

Theorem 2. *The proposed BSS framework can support the multiparty supervision of data on BC.*

Proof. In the proposed BSS framework, SC is used to implement review and supervision on data m, including the data uploaded to the BC, retrieved from the BC, and remain existed in the BC. Users are only allowed to upload and retrieve data that meets certain rules and conditions. Multiple parties are allowed to participate in the supervision process, where only the authorized supervisors are able to jointly supervise certain data. Only when the supervision results J_1 and J_2 are consistent, the supervision information L will be uploaded to SC, which can reduce the risk of privacy leakage caused by the concentration of power in the single supervision authority setting.□□ □

Theorem 3. *If the symmetric encryption scheme F and ABE scheme A are secure, then the proposed BSS framework can provide privacy protection of data on BC.*

Proof. In the proposed BSS framework, the user information I, timestamp t, and data on BC m are encrypted by the hybrid encryption technology. Data information can only be decrypted and viewed by the user who has the corresponding private key, which can reduce the risk of privacy leakage caused by supervision. In addition, SC in the proposed scheme is realized by the consortium chain, so that only the licensed users can join SC. Compared to the public chain, the management of the consortium chain can provide better protection for data privacy and the accountability after privacy leakage.□□ □

Table 2: Theoretical comparison.

Scheme	Supervision method	Access control	Application scenarios
Yong et al.'s scheme [9]	Machine learning	—	Vaccine supply
Yin et al.'s scheme [11]	Machine learning	—	—
Sun et al.'s scheme [26]	Multiblockchain model	—	Central bank digital currency
Peng et al.'s scheme [27]	Double-layer blockchain	—	Vaccine production
Our BBS framework	Dual-chain architecture	√	Financial trade, etc.

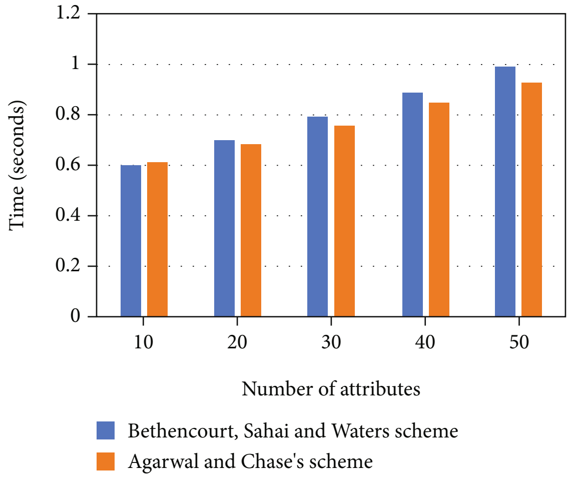


Figure 4: Time cost in the registration phase.

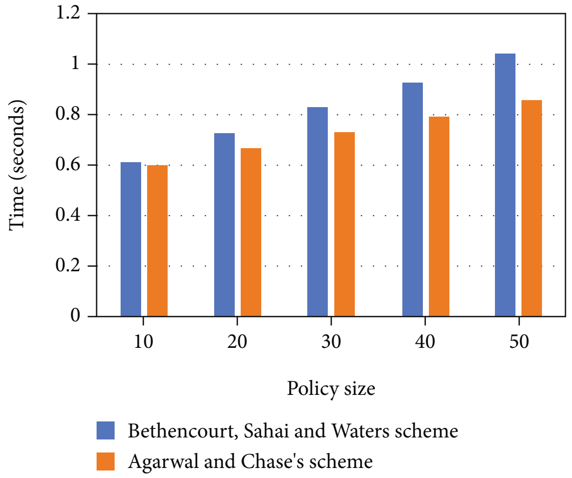


Figure 5: Time cost of encryption.

Theorem 4. *If the chosen ABE scheme A is secure, then the proposed BSS framework can support access control on data.*

Proof. In the proposed BSS framework, the ABE scheme A is used to control the permissions. By embedding access policy T in the encryption process, the specific supervisor is assigned to decrypt and access the data. That is, when the attribute set U of the supervisor satisfies the access policy T, the supervisor has the permission to supervise data m; otherwise, it does not have the permission to decrypt the data. Thus, different supervisors have different supervision permissions for different data.□□ □

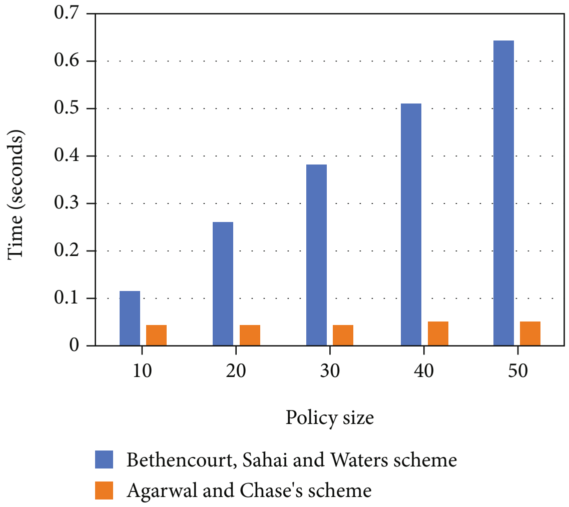
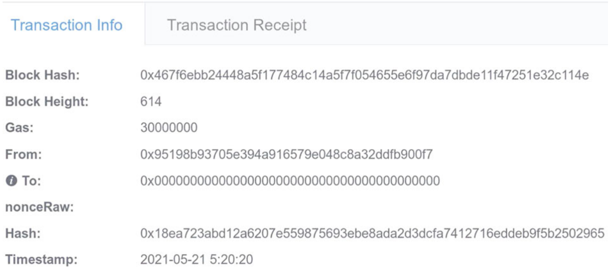


Figure 6: Time cost of decryption.

5.2. Theoretical Analysis. As shown in Table 2, the performance of our BSS framework is theoretical compared with existing supervision schemes. Yong et al.'s scheme [9] and Yin et al.'s scheme [11] mainly use the machine learning method to achieve supervision. Sun et al.'s scheme [26] introduces a multichain structure to complete supervision. Peng et al.'s scheme [27] achieves the supervising through a double-layer blockchain. In our BSS framework, the supervision of data in the blockchain is realized by designing a dual-chain architecture.

In addition, the schemes [9, 11, 26, 27] cannot control the permission of supervisors during the supervision process, whereas our BSS realizes the control on the supervisor's permission through the ABE technology. In terms of application scenarios, Yong et al.'s scheme [9] and Peng et al.'s scheme [27] are suitable to the supervision in the supply and production of vaccine, respectively, while Sun et al.'s supervision scheme [26] can be applied to the central bank digital currency. Our BSS framework is suitable for financial trade information supervision, industrial equipment maintenance information supervision, etc. In different application scenarios, regulatory authorities and supervisors use different rules to supervise different data. Our BSS framework is also suitable to other application scenarios that require multiparty supervision.



Block Hash:	0x467f6ebb24448a5f177484c14a5f7f054655e6f97da7dbde11f47251e32c114e
Block Height:	614
Gas:	30000000
From:	0x95198b93705e394a916579e048c8a32ddfb900f7
ⓘ To:	0x0000000000000000000000000000000000000000
nonceRaw:	
Hash:	0x18ea723abd12a6207e559875693ebe8ada2d3dcfa7412716eddeb9f5b2502965
Timestamp:	2021-05-21 5:20:20

Figure 7: A part information of transaction.

5.3. Experimental Analysis. We conducted the experiments using Python and Solidity programming languages, on a platform with Ubuntu 16.04 operating system and 4 GB memory. The machine is with an AMD Ryzen 5 4600H at 3.00 GHz and 16 GB in memory. FISCO BCOS 2.0 was adopted as the underlying framework of consortium blockchain. In the Setup phase, 256-bit AES-CBC was chosen as the symmetric encryption algorithm F, which is implemented by the Crypto library. For ABE scheme, both Bethencourt, Sahai and Waters scheme [24] and Agrawal and Chase's scheme [28] were employed to process the data on the same chain. A 224-bit asymmetric elliptic curve MNT224 was chosen to realize bilinear mapping.

The performance of our BSS framework is compared by two instantiations from two ABE schemes [24] and [28], respectively. The number of supervisor attributes is a key factor for the timing of registration phase. Figure 4 shows the effect of the registration time when the number of supervisor attributes changes from 10 to 50. It can be seen from Figure 4 that the time in the registration phase enjoys a linear relationship with the number of attributes of the supervisor. When the number of attributes is 10, both instantiations take roughly the same registration time. Although the registration time grows as the number of attributes increases, the overall time increase of Agrawal and Chase's scheme [28] is lower than that of Bethencourt, Sahai and Waters scheme [24].

In the phases of regulatory authority supervision and supervisor second-round supervision, different access policies would affect the efficiency of encryption and decryption of data by regulatory authority and supervisors. Figures 5 and 6, respectively, show the encryption and decryption time of schemes [24] and [28] under different policy sizes. It can be seen from Figure 5 that the increase of the strategy will lead to the increase of encryption time of the system. While the encryption time of Agrawal and Chase's scheme [28] is lower than that of Bethencourt, Sahai and Waters scheme [24]. As shown in Figure 6, in the decryption phase, with the increase of policy size, the decryption time of Agrawal and Chase's scheme [28] does not have significant changes, while the scheme of Bethencourt, Sahai and Waters [24] changes greatly.

In the data processing phase, the smart contract will compare the supervision results J_1 and J_2 generated by the regulatory authority and supervisor, respectively. Then, the smart contract uploads the supervision information L to the SC. The system will output the transaction information when the supervision information L is uploaded successfully. Part of the transaction information in the data processing phase is shown in Figure 7, which includes block hash, transaction hash, contract address, and other information. Here, the block hash is the hash value with regard to the current block, the transaction hash is the hash value generated at the end of supervision, and the contract address shows the address of the invoked contract.

6. Conclusion

This paper studied the problems of difficult supervision in BC, privacy leakage during supervision, and overconcentration of rights. To address these issues, a supervision system architecture BSS for data in BC is proposed. Through SC and the ABE technology, both data supervision and privacy protection can be realized. The supervisor is granted certain permission, and only the supervisor satisfying the relevant authority permission can supervise the data on BC. The proposed BSS framework also supports access control on supervisors and allows multiple supervisors to participate in supervision at the same time. The designed dual-chain architecture can effectively improve the scalability of the BSS system. Theoretical and experimental analysis shows that the BSS instantiations with different ABE schemes are suitable for real world applications.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This article is supported in part by the National Key R&D Program of China under project 2020YFB1006004; the National Natural Science Foundation of China under projects 61772150, 61862012, and 61962012; the Guangdong Key R&D Program under project 2020B0101090002; the Guangxi Natural Science Foundation under grants 2018GXNSFDA281054, 2019GXNSFFA245015, and 2019GXNSFGA245004; the Zhejiang Soft Science Research Program 2021C35044; the Guangxi Young Teachers' Basic Ability Improvement Program under Grant 2021KY0214; the Peng Cheng Laboratory Project of Guangdong Province PCL2018KP004; and the Open Program of Guangxi Key Laboratory of Cryptography and Information Security under Grant GCIS201930.

References

[1] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, pp. 557–564, Honolulu, HI, USA, June 2017.

[2] W. Yang, S. Garg, A. Raza, D. Herbert, and B. Kang, "Blockchain: Trends and Future," *Knowledge Management and Acquisition for Intelligent Systems*, K. Yoshida and M. Lee, Eds., pp. 201–210, Springer, Nanjing, China, 2018.

[3] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *Journal of Network and Computer Applications*, vol. 126, pp. 45–58, 2019.

[4] G. Peters, E. Panayi, and A. Chapelle, "Trends in cryptocurrencies and blockchain technologies: a monetary theory and regulation perspective," *Journal of Financial Perspectives*, vol. 3, no. 3, pp. 92–113, 2015.

[5] P. Pandey and R. Litoriya, "Implementing healthcare services on a large scale: challenges and remedies based on blockchain technology," *Health Policy and Technology*, vol. 9, no. 1, pp. 69–78, 2020.

[6] J. X. Jiang and G. Bai, "Evaluation of causes of protected health information breaches," *JAMA Internal Medicine*, vol. 179, no. 2, pp. 265–267, 2019.

[7] H. Yang, S. Xiong, S. A. Frimpong, and M. Zhang, "A consortium blockchain-based agricultural machinery scheduling system," *Sensors*, vol. 20, no. 9, p. 2643, 2020.

[8] X. Li, L. Wu, R. Zhao, W. Lu, and F. Xue, "Two-layer adaptive blockchain-based supervision model for off-site modular housing production," *Computers in Industry*, vol. 128, p. 103437, 2021.

[9] B. Yong, J. Shen, X. Liu, F. Li, H. Chen, and Q. Zhou, "An intelligent blockchain-based system for safe vaccine supply and supervision," *International Journal of Information Management*, vol. 52, p. 102024, 2020.

[10] W. Meng, W. Li, and J. Zhou, "Enhancing the security of blockchain-based software defined networking through trust-based traffic fusion and filtration," *Information Fusion*, vol. 70, pp. 60–71, 2021.

[11] H. H. Sun Yin, K. Langenheldt, M. Harlev, R. R. Mukkamala, and R. Vatrapu, "Regulating cryptocurrencies: a supervised machine learning approach to de-anonymizing the bitcoin blockchain," *Journal of Management Information Systems*, vol. 36, no. 1, pp. 37–73, 2019.

[12] T. Ma, H. Xu, and P. Li, "Skyeye: a traceable scheme for blockchain," *Cryptology ePrint Archive: Report 2020/034, International Association for Cryptologic Research (IACR)*, vol. 2020, 34 pages, 2020.

[13] T. Ma, H. Xu, and P. Li, "A Blockchain Traceable Scheme with Oversight Function," in *International Conference on Information and Communications Security*, pp. 164–182, Springer, Copenhagen, Denmark, 2020.

[14] W. Meng, W. Li, S. Tug, and J. Tan, "Towards blockchain-enabled single character frequency-based exclusive signature matching in IoT-assisted smart cities," *Journal of Parallel and Distributed Computing*, vol. 144, pp. 268–277, 2020.

[15] E. B. Sasson, A. Chiesa, C. Garman et al., "Zerocash: decentralized anonymous payments from bitcoin," in *2014 IEEE Symposium on Security and Privacy*, pp. 459–474, Berkeley, CA, USA, May 2014.

[16] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Workshop on distributed cryptocurrencies and consensus ledgers*, vol. 310, pp. 1–4, Chicago, IL, 2016.

[17] C. D. Clack, V. A. Bakshi, and L. Braine, "Smart contract templates: foundations, design landscape and research directions," 2016, https://arxiv.org/abs/1608.00771.

[18] J. Woodcock, P. G. Larsen, J. Bicarregui, and J. Fitzgerald, "Formal methods," *ACM Computing Surveys*, vol. 41, no. 4, pp. 1–36, 2009.

[19] T. Chen, X. Li, X. Luo, and X. Zhang, "Under-optimized smart contracts devour your money," in *2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER)*, pp. 442–446, Klagenfurt, Austria, February 2017.

[20] R. Cheng, F. Zhang, J. Kos et al., "Ekiden: a platform for confidentiality-preserving, trustworthy, and performant smart contracts," in *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 185–200, Stockholm, Sweden, June 2019.

[21] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proceedings of the 15th ACM Conference on Computer and Communications Security - CCS '08*, pp. 417–426, Alexandria, Virginia, USA, 2008.

[22] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proceedings of 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 457–473, Aarhus, Denmark, 2005.

[23] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for finegrained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security - CCS'06*, A. Juels, R. N. Wright, and S. De Capitani di Vimercati, Eds., pp. 89–98, ACM, Alexandria, VA, USA, 2006.

[24] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, Berkeley, CA, USA, May 2007.

[25] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in *Proceedings of International Workshop on Public Key Cryptography*, D. Catalano, F. Fazio, R. Gennaro, and A. Nicolosi, Eds., pp. 53–70, Springer, Berlin, Heidelberg, 2011.

[26] S. He, H. Mao, X. Bai, Z. Chen, K. Hu, and W. Yu, "Multi-blockchain model for central bank digital currency," in *2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*, pp. 360–367, Taipei, Taiwan, December 2017.

[27] S. Peng, X. Hu, J. Zhang et al., "An efficient double-layer blockchain method for vaccine production supervision," *IEEE Transactions on NanoBioscience*, vol. 19, no. 3, pp. 579–587, 2020.

[28] S. Agrawal and M. Chase, "Fame: fast attribute-based message encryption," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security - CCS'17*, pp. 665–682, New York, NY, USA, 2017.