Optimized Security Mechanism for publicly Secret Key Sharing over Cloud using Blockchain

Haewon Byeon[1], Aadam Quraishi[2], Praveen Thuniki[3], Ismail Keshta[4], Mukesh Soni[5] and Mohammad Shabaz[6,*]

[1]Department of AI and Software, Inje University, Gimhae 50834, Republic of Korea
[1]Inje University Medical Big Data Research Center, Gimhae 50834, Republic of Korea
[2]M.D. Research, Intervention Treatment Institute, Houston Texas, USA
[3]Independent Research, Sr Program Analyst, Georgia, Cumming, GA, USA 30040
[4]Computer Science and Information Systems Department, College of Applied Sciences, AlMaarefa University, Riyadh, Saudi Arabia
[5]Dr. D. Y. Patil Vidyapeeth, Pune, Dr. D. Y. Patil School of Science & Technology, Tathawade, Pune, India
[6]Model Institute of Engineering and Technology, Jammu, J&K, India

Abstract

A publicly verifiable key sharing mechanism based on threshold key sharing is provided to explore the security of users' private keys on the blockchain. Participating nodes check the key fragment after receiving it, effectively preventing it from being abused. The crucial sections of the nodes that participated in the critical splicing are made public during the critical recovery stage to prevent them from performing harmful things during the critical recovery stage. Add IDs to the nodes that participated in the crucial splicing during the key distribution stage; a dynamic threshold system is intended to track and update the status of malicious nodes in real time. When the node that possesses the crucial component fails, the owner of the critical component and the main node relocate a key element to the new participating nodes. To safeguard sensitive information. The experimental results show that this system has a key recovery rate of 80% and threshold qualities such as traceability, enforceability, and recoverability.

Keywords

Key sharing mechanism, Blockchain, Secret key, Privacy, Security, Encryption.

1. Introduction

The blockchain is essentially a non-administrative decentralized storage system in which each node owns all data. Due to its unique trust establishment mechanism supply chain [7-8], blockchain is extensively employed in the worldwide deployment of the Internet of Vehicles [2], Internet of Things [3], financial services [4-5], smart grid [6], and other industries as a new computing paradigm and Collaboration mode [1]. Blockchain [9], big data [10], artificial intelligence [11], cloud computing, and network security are all important avenues for the present rising digital industry's development. While demonstrating its vigor, the security flaws of its underlying decentralized technology are becoming increasingly apparent.

Proceedings of SNSFAIT 2024: International Symposium on Securing Next-Generation Systems using Future Artificial Intelligence Technologies, Delhi, India, August 08-09th, 2024

* Corresponding author: bhatsab4@gmail.com (M. Shabaz)
† These authors contributed equally.
bhwpuma@naver.com (H. Byeon); aadamquraishi@yahoo.com (A. Quraishi); basavadeepthihm@gmail.com Praveenthuniki@gmail.com (P. Thuniki); imohamed@um.edu.sa (I. Keshta); mukesh.research24@gmail.com (M. Soni); bhatsab4@gmail.com (M. Shabaz)

In 2014, the well-known Bitcoin trading platform Mt.Gox claimed to have been the victim of a malleability attack and lost 850,000 Bitcoins, establishing a new theft record. In 2017, the MIT Academic Research Expert Group sent an email to IOTA (a new micropayment crypto currency freshly tailored for the Internet of Things), the Internet's backbone, reminding it of Curl-P in its hash algorithm. The existence of gaps has drawn the academic community's attention to the security technology of blockchain cryptography. The private key, as the sole proof required to identify the user's identity in the blockchain realm, cannot be restored if lost.

"Vernacular Blockchain" [12] states that According to the information released, there are numerous addresses in the Bitcoin system with forgotten private keys, the entire worth of which might be in the billions of dollars. As a result, it is critical to offer a secure and viable blockchain user private key management system to address the issue.

At present, given the security management of users' private keys in the blockchain network, the academic circles mainly focus on how to improve the generation of users' private keys, how to store them, and the scalability and security of the use of private keys [13]. In the user secret key stage, Panda et al. [14] proposed to use one-way hash chain technology to generate public and private key pairs and allow the critical team to be self-verified at any time. The single-item hash chain technology increases the difficulty for attackers to steal keys. In storing the private key, the academic community proposed solutions such as local storage, account custody [15-16], offline storage [17-18], cloud storage and encrypted wallet protection. In using the private key, the academic community proposed threshold-based signatures [19-20] and multi-signature schemes. Authoroffer an approach to account recovery through an arbitration process that includes a spam filter that separates legitimate requests from malicious or spam submissions whose votes. The mechanism is supported by game theory and control measures to avoid malicious attacks. Author proposed an efficient and optimal threshold digital signature scheme, which only requires the participation of honest nodes greater than or equal to the threshold to guarantee bits Security of coin wallet effectively. Author proposed a weighted threshold scheme with a Bitcoin elliptic curve digital signature algorithm, in which participants have different priorities and have different weights, if and only if all shares of Positive consequences are only associated with each participant when the sum of the products is greater than or equal to a fixed threshold, and signatures can be reconstructed.

To sum up, most existing research focuses on the private key management of users' accounts. Because users choose to save the private key differently, it will be inaccessible if the user accidentally loses the private key. Therefore, the remote key fragment holder must It is always online. Otherwise, the user's private key cannot be recovered because the threshold is not reached, and the threshold key sharing technology cannot guarantee that the node that splits the crucial and the participating nodes that join the key will not do evil when the key is broken.

This research is optimized based on the above. After each node votes to elect the controller node, the controller node splits the private key. When distributing the split personal key fragments to each participating node, the identity ID of each participating node is added so that the identity ID of each participating node can be added according to the identity. The ID tracks the participating nodes, and when a new controller node is elected in each round of voting, the new controller node redistributes the private key fragments to each participating node; after the participating nodes receive the personal key chips, Verification to prevent the controller node from doing evil when the private key is split; in the stage of splicing the private key, after the participating nodes verify the individual key fragments held, the verification algorithm broadcasts the verification results in the blockchain network to prevent the participating nodes from splicing The private key stage is malicious, and prevents the controller node and the participating nodes from colluding and doing evil. Even if the user accidentally loses the private key, the original private key can be recovered by collecting or splicing key fragments equal to or greater than the threshold. This study verifies the critical segmentation and recovery phases. It is difficult for an attacker to steal the user's private key by collecting key fragments that exceed the threshold or attacking participating nodes. The owner node of the critical component and the controller node undertake to release new vital pieces together to ensure the dynamic management of the key fragments and the recoverability of the user's private key in the active network.

2. Blockchain Implementation

Blockchain is a distributed general ledger system that ensures that it has the advantages of anti-tampering, decentralization, openness and transparency, and unforgivable block data through cryptography-related technologies.

The blockchain realizes the distributed storage and decentralized data through the peer-to-peer (P2P) network protocol and chain structure. The consensus mechanism is used to constrain each decentralized node in the blockchain network and maintain the block. The order of operation and fairness of the chain network system enables each unrelated node to verify and confirm the data in the network, thereby generating trust and reaching a consensus. Cryptography technology is used to ensure the confidentiality of users in the blockchain network confidentiality, integrity, availability and immutability of keys, transmitted information. It supports users to use automated scripts to generate intelligent contracts quickly, accurately and securely, greatly expanding the application of blockchain. The security model of blockchain is bottom-up. It can be abstracted into three levels, as shown in Figure 1.

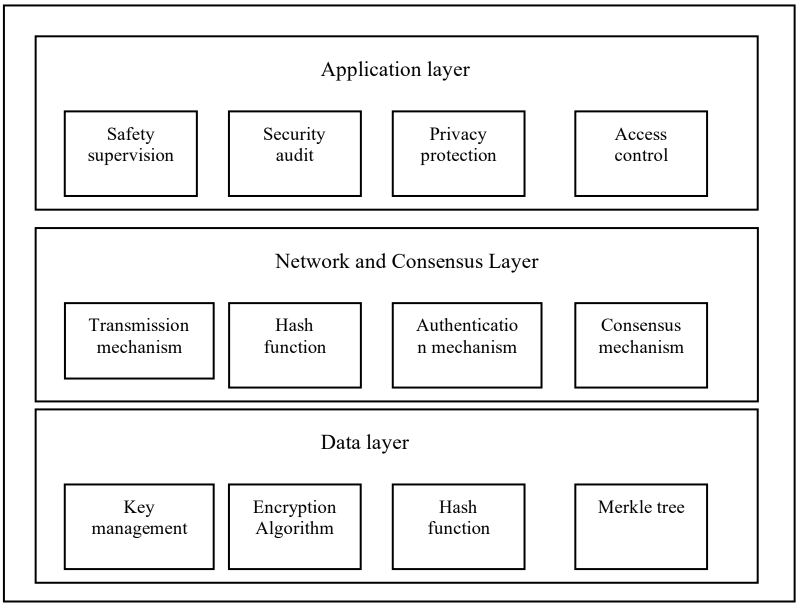

Figure 1 Blockchain security model

1. Data layer. The data layer uses various cryptographic techniques such as hash functions, encryption algorithms, Merkle trees, key management, etc., to ensure the security of data in the blockchain network.

2. Network and consensus layer. It mainly includes the networking method and consensus mechanism of the blockchain. Blockchain uses a peer-to-peer protocol for network transmission. Nodes verify that transaction information is reliable and store it in blocks. In addition, nodes use a consensus mechanism for blockchain consensus.

3. Application layer. It mainly includes various upper-layer applications and platforms with blockchain as the underlying application platform. The application layer adopts the blockchain's high-security privacy protection technology, access control and security auditing to ensure its security. From the perspective of the composition of the blockchain security model, each layer is inseparable from cryptography, which is the core support for the security implementation of blockchain technology.

3. Shamir(T, N) Threshold Key Sharing

Shamir(u, m) threshold key sharing technique is a key sharing technique based on the Lagrangian interpolation algorithm for reliable and secure distribution of account keys to multiple participants. In this scheme, the shared keys are divided into m parts and distributed to m participants. Each participant has a key, the shard is. The shared keys can be recovered as long as at least u shards ti

are collected. The key distributor randomly chooses a polynomial where,
$g(x) = b_{u-1}y^{u-1} + b_{u-2}y^{u-2} + .. + b_1y + t$at b1, and g(0) = $b_{u-1} \in A$; m The key distributor chooses a random polynomial that satisfies the condition, then assigns ti = g(i) to each participant Qi, i = 1 ,2, . Any t participants Q = {Q1,Q2,...,Qu} reconstructed using Lagrangian interpolation:

$$g(x) = \sum_{i=1}^{k} t_i \prod_{1\le j\le k, i\ne j} \frac{y-y_j}{y_i-y_j} \quad (1)$$

The formula: g(x) is the original reconstructed key, the threshold. After the construction is completed, the shared key t can be calculated by t=g(0).

4. Proposed blockchain-based publicly verifiable threshold secrets

Key Sharing Scheme The research scheme is based on Shamir(u, m) threshold key sharing technique and Pedersen's verifiable critical method. By using the publicly verifiable threshold key sharing technology in the blockchain network, the traditional threshold key sharing technology can solve the problem that the user's private key is leaked due to its defects, or the user's private key cannot be leaked due to the offline node holding the key fragments recover.

4.1. Initialization

All nodes in the blockchain network elect the controller node by voting. Let q and r be large prime numbers, respectively, where r is a large prime number of q-1. The only subgroup of order r of the multiplicative cyclic group, g, h, are generators, and no one (except the controller node) knows the discrete logarithm. Assume that the voting controller node is the key distributor, and n sub-nodes are participating nodes, denoted as Q1;Q2; _ _ _ ;Qn respectively and the threshold is k.

4.2. Key Distribution

For a group of integers of key order q, master node E broadcasts a commitment to a pair with a secret value chosen at random by master node E. Master Node E randomly selects a polynomial of degree in and calculates. The controller node randomly selects, calculates and broadcasts the promise of the pair, where. Let calculate. The controller node will (tj, uj) and the identity ID that can be used to verify the child nodes Secretly sent to participating nodes as a shared key fragment held by them, where is the critical element.

4.3. Key Fragment Verification

After each participating node Qj receives the critical segment, it verifies $F(t_j, u_j) = \prod_{i=0}^{k-1} F_i^j$ whether the vital part it has received is valid. If the participating node fails to prove the crucial fragment, it can complain or reject and does not participate in the subsequent key recovery. Assuming one share of failed verification (k; n-c) the scheme becomes a threshold scheme c⩾n-k. At that time, it can be determined that the controller node is fraudulent. Then, the nodes re-vote to elect a new controller node.

4.4. Key Recovery

To participate in the execution of one or more sub-nodes of key recovery to prove $h^{t,u} = \prod_{i=0}^{k-1} F_i^j$ whether their key segments are correct the sub-nodes execute the verification algorithm, and after the performance is completed; the verification algorithm will publish the verification results in the blockchain network. Only the sub-nodes that pass the verification can use the Lagrangian polynomial interpolation method to perform key splicing. The identity ID keeps track of this node and refreshes it.

Key Fragment Append
When the node holding the critical fragment goes offline, the owner node of the essential component and the controller node distribute the critical element to the unassigned nodes. The controller node summons other participating nodes greater than or equal to the threshold value. After the vital fragment is verified, it is restored. After the original key is restored, the key is re-split

and then distributed to other participating nodes.

4.5 Reputation Sharing

High task issuers have access to reputation comments. The scheme in this paper is based on the assumption that only a few task publishers in the mobile network are malicious. During the sharing process, modifying a single task publisher after generating a local opinion has little effect on the reputation value of the data owner because the proposed scheme will be based on the data. The historical interaction records of the owner and the indirect reputation opinions of other multiple task issuers are combined with the theory of entropy to define adaptive weights to conduct a comprehensive reputation evaluation for the data owner so that the reputation evaluation is objective accurate. Reputation opinion sharing is shown in Algorithm 1.

Algorithm 1: Reputation Sharing Algorithm
Input url, url_hash , address, [smk] pkp, pkp 1. The task publisher calls the contract function contribute_reo(url, url_hash, address, [smk]pkp, pkp) 2. if verify_pk(address,pkp) = true 3. The contract stores the reputation opinion information into the reo_share[url_hash] variable 4. The contract calls the internal function set_url_pk(url_hash,pk)p to record the relationship between the reputation opinion and the task issuer into the variable url_pk[url_hash] 5. The contract initializes the whitelist of reputation opinions, and adds the task issuer's information to the whitelist url_whitelist[url_hash] 6. The contract queries other registered task issuers and adds them to the whitelist respectively 7. return REO_TXID 8. else 9. return default 10. end

4.6. Reputation Access

Before each federated learning, the task issuer executes the reputation opinion access algorithm to request the information opinion of other task issuers to select a reliable data owner. The requester inputs the public key pk p of the accessed task issuer, the reputation opinion index path hash url_hash and its public key pk r. After calling the function request_smk(), the contract verifies the requester's identity. If the verification is successful, the contract will judge the request whether the party is in the whitelist of the accessed task issuer. If it exists, it will update the access time of the requesting party and return the encryption key [smk]pkr, the requester can decrypt the symmetric key with the private key; otherwise, the requester's local reputation in the task issuer being accessed is considered low, the task issuer refuses access, and the access fails. In addition, when accessing the corresponding resources on the chain, identity authentication is also required by the audit node on the blockchain service platform. Therefore, if the task issuer in the non-whitelist obtains the symmetric key through collaboration with the task issuer in the whitelist, the task issuer who is not in the whitelist will not be authenticated and thus cannot obtain the reputation opinion reo. Access to reputation opinions is shown in Algorithm 2.

Algorithm 2: Reputation Access Algorithm
Input pk p , url_hash , pk r , address 1) The requester calls the contract function request_smk(pkp, url _ hash, pk) 2) if verify_pk(address, pk) = fakery 3) return fakery

4) if url_whitelist[url_hash][is_white][pk] = true
5) The access timestamp timestamp of pk is updated
6) return Request_TXID, [smk]pk
7) else
8) return default
9) end if
10) end if

4.7. Reputation update

The requester will evaluate the reputation of other task issuers locally. If the number of times that a task issuer has a low reputation exceeds the set threshold, the requester will call the function update_smk_remove() to remove the task issuer from itself. removed from the whitelist. **The** update of reputation opinion is shown in Algorithm 3.

Algorithm 3: Update of Reputation
Enter pkp, url_hash, pk, address 1) The requester calls the contract function update_smk_remove(pk, url_hash, pkp) 2) if verify_pk(address, pk) + fakery 3) return fakery 4) Record the update timestamp of pk 5) Call the contract function remove_whitelist(url_hash, pkp) to remove the task issuer from the whitelist 6) return Remove_TXID 7) end if

5. Scheme Security Analysis

5.1. (t, n) Threshold Characteristics

It threshold feature means dividing and distributing the key to each participating node. The original key can be recovered only if it is equal to or greater than the number of correct nodes, and the original key cannot be retrieved if it is less than one key. Even if an attacker obtains a key fragment, he can only construct a system of equations with unknowns:

$$\begin{cases} t + G_1(t_1,u_1) + G_2(t_1,u_1)^2 + \cdots + G_{u-1}(t_1,u_1)^{u-1} = G_1(t_1,u_1), \\ t + G_1(t_2,u_2) + G_2(t_2,u_2)^2 + \cdots + G_{u-1}(t_2,u_2)^{u-1} = G_2(t_2,u_2) \\ \quad \cdots . \\ t + G_1(t_{t-1},u_{t-1}) + G_2(t_{t-1},u_{t-1})^2 + \cdots + G_{u-1}(t_{t-1},u_{t-1})^{u-1} = G_2(t_{t-1},u_{t-1}) \end{cases} \quad (2)$$

In the formula: (ti; ui) it is the crucial fragment possessed by a particular node. When the number of unknowns is greater than the number of equations, the above equation G(x) has no solution, and the specific form cannot be obtained G(0). That is, the original shared key cannot be accepted t = g (0) = b0. Therefore, this research scheme has the threshold characteristic, and the original shared key can be recovered only when at least one participating node is satisfied.

5.2 Unforgeability and traceability

The enforceability of each participating node means that no participating node can generate legal key segments in the name of other participating nodes. Assume that the identity set of participating nodes is ID = {ID1;ID2; _ _ _ ;IDt}, for Participating nodesQj, whose identities are known Idi

Attack 1 Attacker posing asQj a key splicing. The verification function fails, and the subsequent verification failure results $F(t_j, u_j) = \prod_{i=0}^{k-1} F_i^j$ are published in the blockchain network. The blockchain network traces it back according to the identity ID and then refreshes the node. Therefore, it cannot be impersonated.

The security of this research scheme is compared with Scheme 1, Scheme 2, and the Shamir threshold key sharing scheme, and the analysis results are shown in Table 1. This research method is resistant to collusion attacks and does not need to be trusted. Nodes participate and allow the dynamic addition of participating nodes, ensuring the security and privacy of the user's private key.

Table 1. Safety comparison between this study protocol and existing typical protocols

Program	Whether trusted nodes are required to participate in the reconstruction phase	Can resist collusion	Whether to dynamically add participating nodes
Program	unnecessary	Yes	no
Program	unnecessary	Yes	no
Shamir threshold key sharing scheme	need	no	no
Proposed Work	unnecessary	Yes	Yes

6. Experimental analysis of the scheme

The experimental environment of the publicly verifiable key sharing technology and Shamir threshold key sharing technology scheme in the blockchain is as follows: The operating system is Windows10 Home Chinese version 64-bit, and the CPU is Intel(R)Core(TM)i7-10510U CPU@ 1.80 GHz 2.30 GHz, the memory size is 16 GB, implemented using the Java development language.

6.1. Private key recoverability

Private Key recoverability means that when the participating nodes in the blockchain network change dynamically, the user can recover his private key by collecting enough critical fragments through the controller node. As shown in Figure 2 with table 2, the comparison of the four schemes is set up. There are 20 participating nodes. In the scheme proposed in this study, all nodes use dynamic allocation to distribute critical fragments, and the threshold value is 11; Scheme 1, Scheme 2 and Shamir threshold encryption. The threshold value of the critical scheme is fixed at 10, and nodes join or leave the network randomly in the experiment. Ru is the update rate of blockchain nodes in the figure, and r is the private key recovery rate. It can be seen that with the node update rate, Scheme 2 and the Shamir threshold key party.

Table 2. Private Key recovery rates for a single user

Serial	Proposed Work	Program	Shamir threshold key scheme
0	100	100	100
5	90	92	95
10	80	82	92
15	60	65	90
20	40	45	87
25	20	25	85
30	23	25	80
35	15	18	78

40	10	13	74

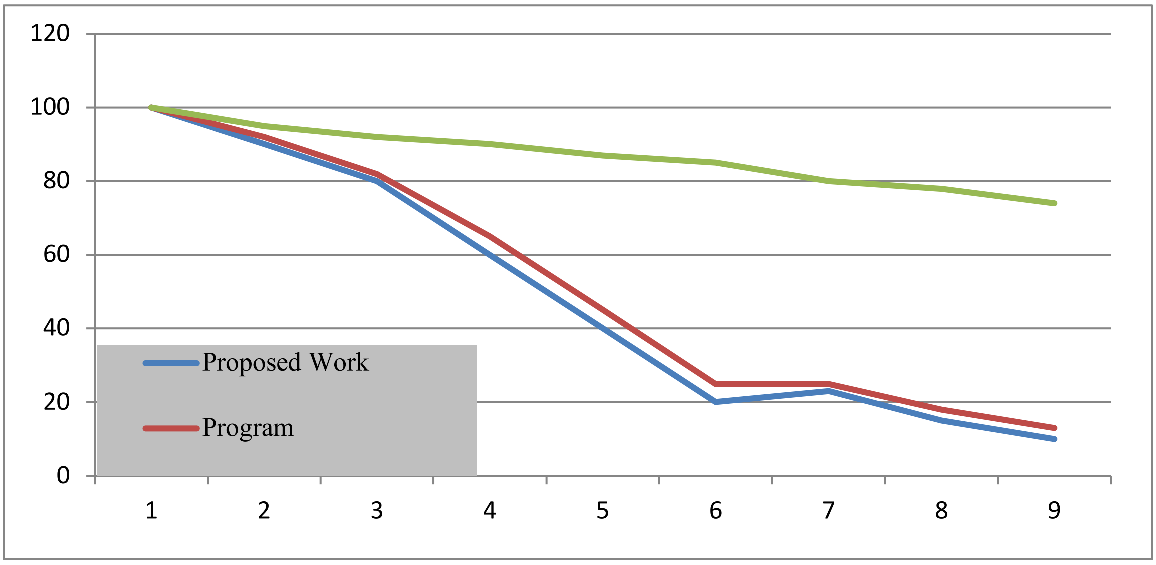

Figure 2. Private Key recovery rates for a single user

The private key recoverability rate of scheme 1 is relatively high. When the update rate of the node reaches 35%, scheme 2 has different weights of the critical fragments held by the nodes. Its private key recovery rate is close to 0, the personal key recovery rate of the Shamir threshold key scheme is close to 15%, and the private key recovery rate of scheme 1 has decreased. Therefore, the plan recommended in this study can effectively deal with node exit in the case of joining. The new joining node also has key fragments through the method of the controller node calling the participating nodes, ensuring the fragment size so that the recoverability of the private key is maintained at a high level. Even if the network node update rate reaches 40%, more than 80% of the private keys can still be recovered in the scheme recommended in this study. Therefore, the method suggested in this study is more suitable for dynamic blockchain networks and can effectively tolerate the exit of nodes carrying key fragments and the addition of new nodes.

Table 3. User private critical recovery time

Serial	Proposed Work	Program	Shamir threshold key scheme
10	90	150	150
11	110	160	100
12	115	150	120
13	120	130	110
14	125	140	105
15	130	120	100
16	135	100	90
17	140	130	95

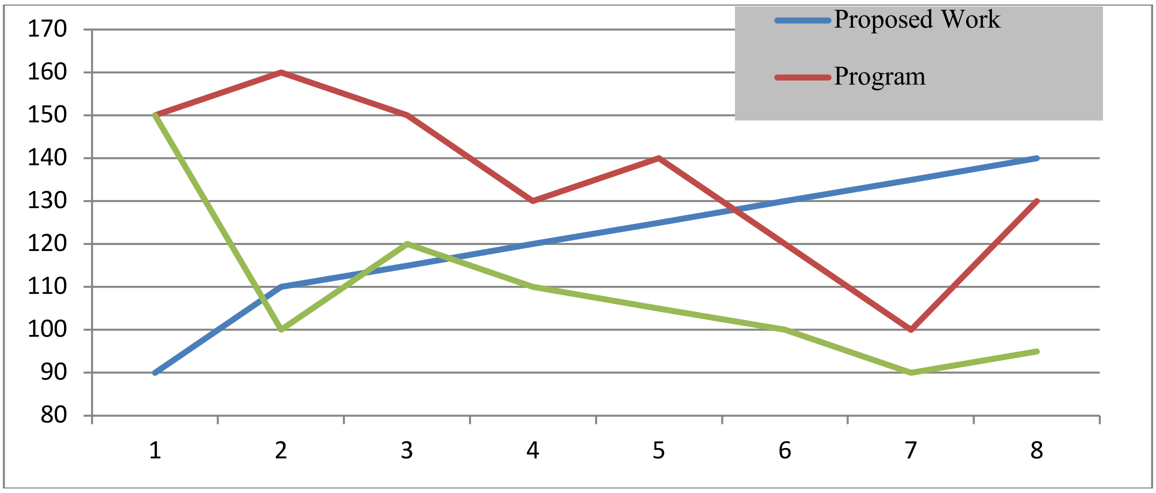

Figure 3. User private critical recovery time

6.3. Nodes do evil

Node evil means that malicious nodes in the blockchain network tamper with their keys, resulting in the failure of private key splicing in the recovery phase. For the scheme proposed in this study and the Shamir threshold key sharing scheme, the situation of node evil is simulated. As shown in Figure 4 with table 4, critical recoverability is displayed when the point is malicious. There are 20 participating nodes in the setting scene, 1 controller node, and the threshold value is 12. In the figure, ne is the number of malicious nodes the number of malicious nodes > When the number of participating nodes–threshold value, the private keys of all schemes cannot be recovered. Therefore, a situation where a maximum of 8 nodes are malicious is simulated. It can be seen that with the increase in the number of malicious nodes, the private critical recoverability rate increases when the number of malicious nodes exceeds 4, the personal key recovery rate of the Shamir threshold key scheme drops rapidly. In contrast, the private key recovery rate of the proposed method in this study is maintained at about 85%. Therefore, the system recommended in this study is that resisting malicious nodes is more secure and can tolerate more malicious nodes.

Table 4. Private key recovery rate when the node is malicious

Serial	Proposed Work	Program	Shamir threshold key scheme
10	90	95	98
11	110	110	98
12	112	135	120
13	114	140	105
14	120	145	95
15	140	110	93
16	145	105	89
17	160	100	85

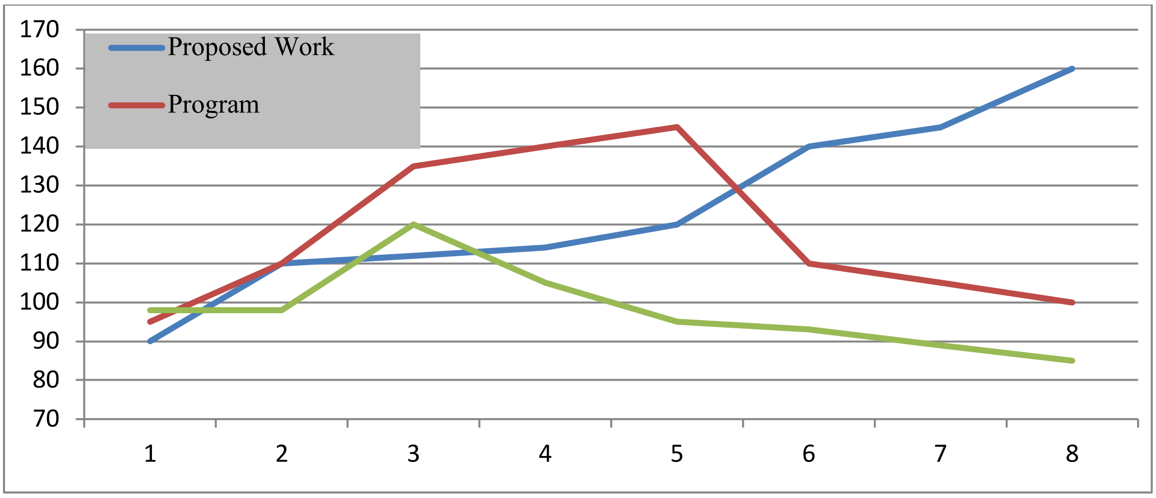

Figure 4. Private Key recovery rate when the node is malicious

6.4. Private key recoverability when the number of users is different

The recoverability of the private key when the number of users is different refers to the recoverability rate of the private key when the number of users is different. The number of nodes participating in the recovery of the private key is different in the blockchain network—the personal key recoverability rate when the number of user's nu is other. The number of users in the blockchain network increases from 1 to 12, the participating nodes are 15 (threshold value 10) and 20 (threshold value 14), and nu is the blockchain the number of users in the network. When the number of participating nodes in the blockchain network is 15, and the number of users does not exceed 4, the private key recovery rate is 100%. When the number of user's increases to 12, the personal key recovery rate is close to 60%; when the number of participating nodes in the blockchain network is 20, and the number of users does not exceed 3, the private key recovery rate is 100%. When the number of users increases, the personal key recovery rate is about 60%. When users increase to 12, the private key recovery rate is 50%. Even if the number of nodes and users continues to grow, the private key of the proposed scheme in this study can be recovered. The rate is about 50%, so the method recommended in this study is suitable for small and medium-sized blockchain networks. Table 5 and Figure 5 shows the Private Key recoverability with different numbers of users.

Table 5. Private Key recoverability with different numbers of users

Serial	Proposed Work	Shamir threshold key scheme
0	100	100
1	99	98
2	98	95
3	97	90
4	96	88
5	98	20
6	99	15
7	96	10

Figure 5. Private Key recoverability with different numbers of users

6.5. Standard Deviation

There are two random processes in the Serials: the features of the random subspace are randomly generated based on the variance contribution rate of the features, and the training data of each base classifier is randomly selected based on the sample selection probability. Therefore, this section studies the effect of randomness on the Serials and performance impact.
Theoretically, on the one hand, the subspace is generated based on the variance contribution rate of the features. The more informative features are included, the greater the probability of being selected, the less informative features are, the smaller the probability of being selected. This guarantees the validity of each subspace; on the other hand, the training data for each base classifier is randomly selected based on the example selection probability, which is
Converted from the positive score, the representative example selection strategy stipulates that in the positive bag and the negative bag, the higher the positive score is, the greater the probability of being selected, and the probability of being selected for each example in the bag is different. On the one hand, from the perspective of the positive bag, the selection strategy tries to avoid selecting negative examples from the positive bag, thereby preventing the trained example-level classifier from predicting false positives; on the other hand, from the perspective of the negative bag See, moving the decision boundary of the example-level classifier towards the positive class increases the number of true negatives. Therefore, the classification effect of the package is guaranteed, and the randomness will not have a great impact on the performance of the classifier.
Experimentally, this paper conducts experiments on Serial 1 to 5. On a Serial, repeat the experiment 100 times with the same experimental settings (split and parameters of cross-validation), and then calculate the standard deviation of the results of the 100 experiments. The experimental results are shown in Table 6, in seial 1-5, The standard deviations of the accuracy rates are 0.42%, 0.32%, 0.17%, 0.79%, and 0.38%, respectively, and the standard deviations of the AUCs are 0.43%, 0.32%, 0.19%, 0.86%, and 0.38%, respectively. Smaller, therefore, randomness has little effect on classifier performance. Figure 6 shows the Comparison of Standard deviation of performance graphically.

Table 6. Standard deviation of performance for 100 repetitions

Data set	Standard deviation of accuracy	Standard Deviation of AUC
Serial 1	0.41	0.48
Serial 2	0.37	0.31
Serial 3	0.19	0.16

Serial 4	0.76	0.82
Serial 5	0.37	0.34

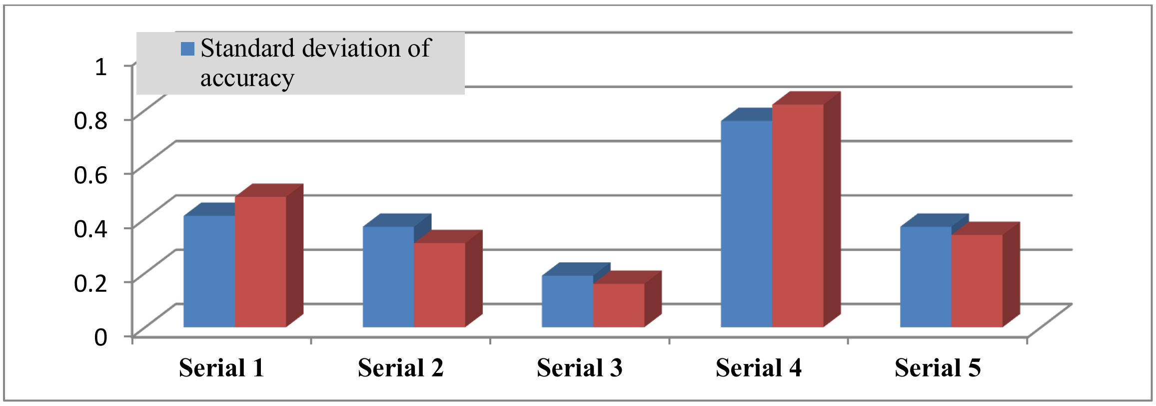

Figure 6. Comparison of Standard deviation of performance

7. Conclusion

A publicly verifiable threshold key sharing method in the blockchain is aimed to address the security issue of the loss or leaking of the user's private key in the present blockchain network. The dynamic threshold's design assures that even if the node containing the important fragment is offline, the recoverability of the user's private key may still be assured. According to the security analysis, the scheme in this study has threshold characteristics, enforceability, and traceability, and is appropriate for dynamic blockchain networks. The crucial splicing algorithm will be investigated in the following study. The recoverability rate of the user's private key will improve as the number of users in the blockchain network grows, making it suited for large-scale blockchain networks.

References

[1]. Z. Su, H. Wang, H. Wang and X. Shi, "A Financial data security sharing solution based on blockchain technology and proxy re-encryption technology," 2020 IEEE 3rd International Conference of Safe Production and Informatization (IICSPI), 2020, pp. 462-465, doi: 10.1109/IICSPI51290.2020.9332363.

[2]. B. Xu, F. Yang, D. Zhang, L. Tang and T. Xia, "Security sharing model of power material logistics information based on blockchain Technology," 2020 13th International Conference on Intelligent Computation Technology and Automation (ICICTA), 2020, pp. 539-544, doi: 10.1109/ICICTA51737.2020.00119.

[3]. X. Wu, C. Ai and J. Chen, "Research on the Development of Computer Network Platform under Big Data and Blockchain Technology," 2021 IEEE 3rd International Conference on Civil Aviation Safety and Information Technology (ICCASIT), 2021, pp. 636-638, doi: 10.1109/ICCASIT53235.2021.9633752.

[4]. Y. Zhang, S. Deng, Y. Zhang and J. Kong, "Research on Government Information Sharing Model Using Blockchain Technology," 2019 10th International Conference on Information Technology in Medicine and Education (ITME), 2019, pp. 726-729, doi: 10.1109/ITME.2019.00166.

[5]. S. Lin, X. Wang, S. Nie, W. Kou and J. Du, "Research on the Sharing of Equipment Data Based on Blockchain," 2021 6th International Conference on Smart Grid and Electrical Automation (ICSGEA), 2021, pp. 435-438, doi: 10.1109/ICSGEA53208.2021.00105.

A. Omar, R. Jayaraman, M. S. Debe, H. R. Hasan, K. Salah and M. Omar, "Supply Chain Inventory Sharing Using Ethereum Blockchain and Smart Contracts," in IEEE Access, vol. 10, pp. 2345-2356, 2022, doi: 10.1109/ACCESS.2021.3139829.

[6]. X. Cheng and F. Qu, "Ocean Data Sharing Based on Blockchain," 2021 IEEE 6th International Conference on Big Data Analytics (ICBDA), 2021, pp. 155-159, doi:

10.1109/ICBDA51983.2021.9402995.
[7]. C. Wang and N. Liu, "Research on Spectrum Sharing of Cognitive Satellite Network Based on Blockchain," 2020 7th International Conference on Information Science and Control Engineering (ICISCE), 2020, pp. 1215-1219, doi: 10.1109/ICISCE50968.2020.00246.
[8]. K. Moschou et al., "Performance Evaluation of different Hyperledger Sawtooth transaction processors for Blockchain log storage with varying workloads," 2020 IEEE International Conference on Blockchain (Blockchain), 2020, pp. 476-481, doi: 10.1109/Blockchain50366.2020.00069.
[9]. Qi Xia; Jianbin Gao; Sandro Amofa, "Blockchain Medical Data Sharing," in Wireless Blockchain: Principles, Technologies and Applications , IEEE, 2022, pp.245-268, doi: 10.1002/9781119790839.ch11.
[10]. H. C. Chou, "A Blockchain-based Collaboration Framework for Educational Material Sharing," 2020 IEEE 8th R10 Humanitarian Technology Conference (R10-HTC), 2020, pp. 1-5, doi: 10.1109/R10-HTC49770.2020.9356955.
[11]. P. Jiang, Y. Feng and Y. Dai, "Design of college student information sharing system based on blockchain," 2021 IEEE 2nd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA), 2021, pp. 568-572, doi: 10.1109/ICIBA52610.2021.9687951.
[12]. Soni, M., & Singh, D. K. (2021). LAKA: Lightweight Authentication and Key Agreement Protocol for Internet of Things Based Wireless Body Area Network. In Wireless Personal Communications (Vol. 127, Issue 2, pp. 1067–1084). Springer Science and Business Media LLC. https://doi.org/10.1007/s11277-021-08565-2
[13]. Y. Cao and J. Zhang, "Network Information Technology Application Based on Blockchain," 2020 International Signal Processing, Communications and Engineering Management Conference (ISPCEM), 2020, pp. 193-195, doi: 10.1109/ISPCEM52197.2020.00045.
[14]. M. Kaur, M. Murtaza and M. Habbal, "Post study of Blockchain in smart health environment," 2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA), 2020, pp. 1-4, doi: 10.1109/CITISIA50690.2020.9371819.
[15]. K. Kim, T. Kim and I. Y. Jung, "Blockchain-based Information Sharing between Smart Vehicles for Safe Driving," 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), 2020, pp. 1-2, doi: 10.1109/VTC2020-Spring48590.2020.9128995.
[16]. G. Zhong, "The Role of Blockchain Technology in the File Management Distributed System under the Background of Big Data," 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021, pp. 1370-1373, doi: 10.1109/ICOSEC51865.2021.9591896.
[17]. Soni, M., & Singh, D. K. (2022). New directions for security attacks, privacy, and malware detection in WBAN. In Evolutionary Intelligence (Vol. 16, Issue 6, pp. 1917–1934). Springer Science and Business Media LLC. https://doi.org/10.1007/s12065-022-00759-2
[18]. M. M. Mahdy, "Semi-Centralized Blockchain Based Distributed System for Secure and Private Sharing of Electronic Health Records," 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE), 2021, pp. 1-4, doi: 10.1109/ICCCEEE49695.2021.9429554.
[19]. F. X. Liu, Q. Wang and F. X. Chi, "Research on Financial Scheme of Digital Motor Vehicle Certification Based on Blockchain Technology," 2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), 2020, pp. 2365-2368, doi: 10.1109/ICMCCE51767.2020.00511.