(IJIEST) 2019, Vol. No. 5, Jan-Dec **e-ISSN: 2454-9584; p-ISSN: 2454-8111**

# AN IN-DEPTH ANALYSIS OF THE BLOCKCHAIN TECHNOLOGY IN IMPROVING THE EFFICACY OF THE FINANCIAL DATA SECURITY SAFEGUARDS

**Kanishka Kashyap**
*Vandana International Sr. Sec. School, New Delhi*

## ABSTRACT

*Proposed a secure data-sharing solution based on proxy re-encryption technology and the difficulties of sharing sensitive data among financial institutions, hidden risks in data security, and high financial risk control costs in the paper. A data-sharing model and a data-sharing protocol make up the solution. First, we used the blockchain's distributed storage, decentralized management, and non-tampering characteristics to create a data security sharing model. To keep sensitive data from being tampered with or leaked, the model implements access control strategies on the blockchain platform and stores encrypted data in distributed databases. Utilized identity-based proxy re-encryption technology and distributed key generation technology in the data-sharing Protocol. By re-encrypting sensitive data, the Protocol enables data sharing among users and selects proxy nodes using the proof-of-stake algorithm. In terms of key generation security, the solution analysis discusses the proposed scheme's correctness.*

## INTRODUCTION

The emergence of cloud computing technology [1] offers a practical technical method for exchanging financial data. The cloud service provider receives business information that financial institutions upload. Cloud verification is required for other users who require the relevant data. They will be able to obtain data access rights once the verification is passed. That makes the sharing of data process real. However, there is still a flaw in cloud computing-based data storage: centralized data storage. The cloud servers centrally store all sensitive data. All sensitive data will be leaked once the cloud servers are maliciously compromised, resulting in significant losses for users and financial institutions and jeopardizing national financial security.

New hopes for resolving this issue have emerged due to blockchain technology's development and application[2, 3]. A paper by Satoshi Nakamoto titled "Bitcoin: In 2008, a peer-to-peer electronic cash system" [3] The paper used blockchain technology to create a Bitcoin construction method, thereby establishing blockchain technology. When this Technology was first proposed, many businesses were immediately concerned. Anti-tampering, decentralization and distributed storage are some of the benefits of blockchain technology, as is the potential for more secure and reliable storage. Additionally, these benefits are very well suited to the requirements of the financial sector[4]. In a decentralized system, blockchain can spontaneously generate credit. With credit endorsement from business centre agencies, it can largely establish a financial market, achieving "financial disintermediation". It can greatly reduce data-sharing costs using programmable blockchain technology features and automatic smart contracts [5-6]. It offers a practical means for

the secure transfer of financial data. Throughout data circulation and traceability, make sure that traces remain.

To meet the requirements of the industry and solve the issues above. A data security sharing model and Protocol are developed as part of this paper's financial data security sharing scheme that incorporates proxy re-encryption technology and blockchain technology. The identity-based proxy re-encryption solution and the distributed key generation technology are combined in the sharing Protocol, enabling participating blockchain platform users to negotiate and generate private keys. The solution ensures financial data confidentiality, integrity, and privacy by sharing encrypted data among users using IBPRE technology. When PKG is maliciously attacked, this solution effectively resists user collusion attacks. It prevents the private key leakage of various institutions compared to the traditional centralized PKG key generation technology.

## RELATED TECHNOLOGIES

### A. Blockchain Technology

A blockchain is a particular data structure that arranges data blocks chronologically in a chain[10]. Data is permanently stored in the form of blocks in blockchain technology. A chain structure connects each block, generated chronologically, to form a blockchain. There is a block header and a block body in each block. The version number, timestamp, hash value of the previous block, and any relevant data participating in the consensus mechanism make up most of the block header. The blocks are interlocked by the previous block's hash value, which is a hash operation on the data of each module that reaches the block header. From the creation of the blockchain to the generation of this block, the block body stores all transaction data [11]. Additionally, the blockchain is a distributed, decentralized database. The blockchain is maintained by all nodes in the blockchain network, whereas the traditional distributed database has only one central server for data maintenance. Each node will make a backup. The blockchain's data will not be affected if a single node's data is altered or destroyed.

### B. Proxy Re-encryption Technology

Blaze et al. proposed proxy re-encryption technology [ 12]. It is a mechanism for converting ciphertexts that, following particular rules, can transform a ciphertext decrypted by one key into another ciphertext decrypted by another key in the ciphertext state. Users Alice and Bob each have their own keys in this scheme. A re-encryption key is set on a proxy server that is only partially trusted, and the proxy server uses the re-encryption key to transform the ciphertext that Alice encrypted using her public key into the ciphertext that Bob encrypted using his public key. During the ciphertext conversion process, the plaintext and Alice and Bob's private keys will not be made available to the proxy server. Under the premise of cryptography, this makes it easier to entrust or redistribute ciphertext, reduces trust and dependence on the intermediate conversion server, guarantees information security for plaintext and bilateral users, and is relatively convenient [13].

Enciphered into ciphertext that can be decrypted using the delegatee's private key. The server uses the appropriate re-encryption key to re-encrypt the cypher text whenever the delegate accesses the

file. Taking the example of financial transactions, user Alice stores encrypted files on an unreliable server and allows users to access them. However, Alice cannot perform online ciphertext conversion whenever data is accessed. Using proxy re-encryption technology, Alice can calculate and set a re-encryption key based on her private and public keys. The proxy re-encryption scheme guarantees that the proxy server can access neither the private key nor the plaintext. The correct implementation of the re-encryption algorithm is required to provide the server with a minimum level of trust. As a result, the delegator can use proxy re-encryption to quickly and effectively gain access control over its ciphertext files during financial transactions.

## SOLUTION OVERVIEW

### A. Model Design

Gui and Asghar's peer-to-peer model[14] is the basis for this improved model. Our model consists of four roles, as depicted in figure 1. a member of the blockchain, a data consumer, a data holder, and a proxy service provider. The solution's nodes can play one or more roles, but they cannot simultaneously be both blockchain members and proxy service providers.

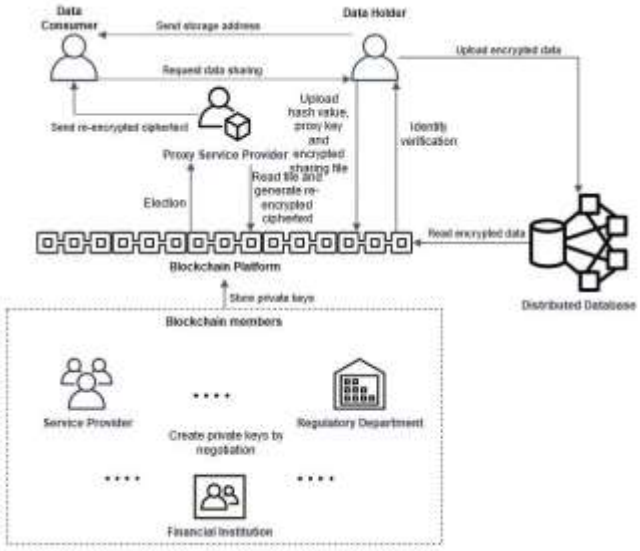


Fig 1. Secure financial data sharing model based on the blockchain

• Data Holder: The data holder has sensitive financial information like the account balance, user ID, password, and transaction history, among other things. Users of data have permission to access their data. The distributed database stores sensitive data encrypted. Data holders upload their hash value, a storage address, and access strategy on the blockchain platform. Holders of data have the ability, through the use of blockchain technology, to safeguard financial data against malicious manipulation. The data owner must generate a proxy re-encryption key and broadcast it to the proxy service provider during the data-sharing process.

• The User of the Data: By submitting an authentication request to the data owner, a data consumer can exercise the right to access the data. The data consumer uses their private key to decrypt the ciphertext and obtain sensitive financial data when they obtain access permission.

• Member of the Blockchain: Banks, government regulatory agencies, and related service providers make up the blockchain members. These members maintain the blockchain platform's functionality. They also calculate and broadcast a secret value to negotiate and generate their private key.

• The Provider of Proxy Services: Delegated proof of stake (DPOS)[15] can be used to select a node to act as a proxy service provider. The proxy service provider encrypts the ciphertext of sensitive financial data using this node's proxy re-encryption algorithm by the re-encryption key sent by data holders.

This model stored sensitive financial information in the blockchain platform and distributed database. The ciphertext of sensitive financial data is stored in distributed databases, and the blockchain platform stores the data's hash value, storage address, and access control rules. The centralized data storage mode is avoided with this storage strategy, and high-frequency access and storage space pressure on the blockchain platform is also reduced.

**B. Protocol**

As a data-sharing protocol, the paper proposed a multi-centre identity-based proxy re-encryption solution. Based on Matthew Green's IBPRE solution, the Protocol is improved. The user's private key is created by the master key, created by the PKG algorithm, in the initial solution. This method cannot protect the PKG from malicious attacks or guarantee its authenticity. This will expose the user's private key due to these risks, which will result in the disclosure of the master key. This paper optimizes the IBPRE solution using the distributed key generation (DKG) algorithm to enhance user key generation security. It guarantees that the secret value is used to generate each user's private key, which is then negotiated with the other users; It can still provide security even if only one user is the target of an intentional attack. The particular Protocol for sharing data consists of the following five steps: initial configuration, generation of keys, storage, sharing, and data decryption.

• The Initial Situation: The server will generate the system's public parameters after entering the server's security parameters. Each member of the blockchain is required to set its polynomial algorithm after obtaining the public parameters. The master key will then be created using the distributed key generation algorithm. Each member of the blockchain chooses a polynomial algorithm at random, and the algorithm broadcasts the calculation result. Each member of the blockchain sends its secret value simultaneously to the rest of the blockchain. After receiving the personal value, the receiver verifies its validity. An error prompt will be returned if the secret value verification is invalid, and the sender will recreate the value until it is valid. Finally, the master key will be generated once each blockchain member's value is verified.

• The production of keys: A private key is returned by each member of the blockchain by the identification value and input parameters.

• The storage of data: The data holder of the sensitive data encrypts the data using the public key, creates the first-layer ciphertext with the identity id and plaintext, and stores the ciphertext in the distributed database when the sensitive data is generated. After that, the data holder electronically signs the sensitive data, writes the signed data, the data hash value, storage location, access control strategy, and other information broadcasts the transaction and inserts it into the transaction as a file. The relevant nodes will approve the transaction before being written into the blockchain.

• Sharing of information: A signature request is first sent to the data owner by a data consumer wishing to obtain a specific sensitive data authority. Through the request message, the owner confirms the consumer's identity. Second, the file access control strategy says that the data holder will use the consumer's identity id and private key to create a proxy re-encryption key if the consumer's identity is legal and has read permissions. should then send the proxy re-encryption key and the address for the data storage to the proxy service provider. The ciphertext is re-encrypted with the proxy service provider's help of the re-encryption key. The data consumer is then sent the second layer of ciphertext. The ciphertext of the second layer is the new cyphertext.

• Unencryption of Data: After receiving the second layer ciphertext, the data consumer can use his private key to decrypt it and obtain the plaintext file.

## SOLUTION ANALYSIS

### A. Correctness of the Key

In the solution, the master key is first generated, and the user private key is then generated based on the master key's value. A reliable third-party authority is required to safeguard the master key and generate the user's private key in similar solutions [16, 17]. An improved plan is presented in this paper that makes use of distributed key generation (DKG) Technology to generate personal value without the assistance of a reputable third party. This plan achieves decentralization while guaranteeing the accuracy of private key generation through DKG technology.

### B. Analysis of Security

In this article, the security and privacy of data are jointly ensured by the model and Protocol. Regarding the model suggested in the paper: The model stores encrypted sensitive financial data in a distributed database, making it impossible for an attacker to decrypt the encrypted data without the private key even if it is leaked. The model also stores the data's hash value, a storage address, and access control strategy on the blockchain. Due to the anti-tampering features of the blockchain platform, the data's security and privacy are greatly enhanced. Particularly, since there are many nodes in the blockchain, once data is written to it, each node will back it up; we can only alter the data stored on the blockchain if a 51 per cent attack occurs. Since the original data is not stored on the blockchain, tampering will not affect sensitive data, even if a 51 per cent attack succeeds.

The solution employs an optimized non-identity-based proxy re-encryption protocol so that the user's private key generation does not rely on PKG from a protocol standpoint. Second, to generate a personal value, each blockchain user selects a polynomial and uses the secret value to create a private key. Distributed key generation can effectively prevent the leakage of private keys in comparison to the centralized PKG method. Even if a single user is targeted maliciously, the attacker cannot obtain the user's private key or secret value. As a result, it is impossible to decrypt sensitive data stored in the distributed database using the user's public key. Because the personal value of each user is verified in the Protocol, the attacker cannot generate the private key if the verification fails, even if multiple users are maliciously attacked. Can conclude that malicious attacks cannot easily leak the user's private key.

## CONCLUSION

Data sharing between subjects that is secure and dependable is always a hot topic in research. The secure sharing of sensitive data and privacy of sensitive financial data greatly impact the financial industry's risk management and safeguarding of national financial security. This paper proposes a secure sharing of financial data based on blockchain technology with the assistance of the decentralization and non-comparability of the blockchain. Conceived a financial data security sharing model and suggested a protocol for data sharing to carry out the point-to-point data sharing function between data holders and consumers. However, this solution's efficiency of DPOS consensus has hindered the framework's performance. The next step's main work is improving the consensus algorithm, making consensus more efficient, and making data sharing from one user to multiple users possible.

## REFERENCES

[1] Dudin E B, Smeranin Y G, “A review of cloud computing,” Scientific and Rechnical Information Processing, Vol. 38(4), pp. 280-284, 2011.

[2] Vujicic D, Jagodiac D, Randic S, “Blockchain rechnology, bitecoin, and Ethereum: a breif overview,” 17th International Symposium Infoteh-Jahorina, Piscataway, pp. 1-6, 2018.

[3] Underwood S, “Blockchain beyond botcoin,” Communications of the ACM, Vol. 59(11), pp. 11-17, 2016.

[4] Yong Yuan, Feiyue Wang, “Blockchain: The State of the Art and Future Trends,” Acta Autiomatic Sinica, Vol. 42(4), pp. 481-494, 2016.

[5] Yong Yuan, Tao Zhou, Aoying Zhou, Yongchao Duan, Feiyue Wang, “Blockchian Technology: From Intelligent Data to Automatic Knowledge,” Acta Automatic Sinica, Vol. 43(9), pp. 231-237, 2017.

[6] Feiyue Wang, “The Destiny: Towards Knowledge Automation,” Acta Automatic Sinica, Vol. 39(11), pp. 1741-1743, 2013.

[7] Gennaro R, Jareckib S, Krawczyk H, et al, "Robust Threshold DSS Signatures," Information and Computation, Vol. 164(1), pp. 54-84, 2001.

[8] Gennaro R, Jareckib S, Krawczyk H, et al. "Secure Distributed Key Generation for Discrete-log based Cryptosystems," Journal of Cryptology, Vol. 20(1), pp. 51-83, 2007.

[9] Green M, Ateniese G. "Identity-based Proxy Re-encryption," Proceeding of the 2007 International Conference on Applied Cryptography and Network Security, Berlin. pp. 288-306, 2007.

[10] Qifeng Shao, Cheqing Jin, Zhao Zhang, Weining Qian, Aoying Zhou. "Blockchain: Architecture and Research Progress," Chinese Journal of Computers, online, 2017.

[11] Zhicheng Zhou, Lixin Li, Zuohui Li. "Efficient cross-domain authentication scheme based on blockchain technology," Journal of Computer Applications, Vol. 38(2), pp. 310-320,326, 2018.

[12] Blaze M, Bleumer G, Strauss M. "Divertible protocols and atomic proxy cryptography," Proceedings of the 1998 International Conference on the Theory and Applications of Cryptographic Techniques, Berlin, pp. 127-144, 1998.

[13] Jing Zhao, Dengguo Feng, Lin Yang, Linru Ma. "CCA-Secure Type-Based Proxy Re-encryption Without Pairings," Acta Electronic Sinica, Vol. 39(11), pp. 260-267, 2011.

[14] Cui S, Asghar M R, Russello G. "Towards blockchain-based scalable and trustworthy file sharing," Proceeding of the 27th International Conference on Computer Computation, Piscataway, pp. 1-2, 2018.

[15] Luo Y, Chen Y, Chen Q, et al. "A new election algorithm for DPoS consensus mechanism in blockchain," Proceeding of the 7th International Conference on Digital Home, Piscataway, pp. 116-120, 2018.

[16] Lin Q, Yan H, Huang Z, et al. "An ID-based linearly homomorphic signature scheme and its application in blockchain," IEEE Access, Vol. 6, pp. 20632-20640, 2018.

[17] Jia X, He D, Zeadally S, et al. "Efficient revocable ID-based signature with cloud revocation server," IEEE Access, Vol. 5, pp. 2945-2954, 2017.