Spectrogram Encryption in Consortium Blockchain Based Authorization

Zhicheng Zhu[1,a], Zhipeng Dong[1,b] and Qingmin Meng[1,c,*]

[1]School of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China.
a. 2207814311@qq.com, b. dongzp.kwan@qq.com, c. mengqm@njupt.edu.cn.
**Qingmin Meng*

Keywords: Consortium blockchain; authorization; hash; traceability.

Abstract: Blockchain can be divided into three categories, namely public blockchain, private blockchain and consortium blockchain. The consortium blockchain will be open to a specific organization and it is not completely decentralized since every ordinary user in the consortium blockchain must accept the authorization of the regulator. This work discusses the authorization based on the consortium blockchain, which can face the coexistence of human and robot transaction scenarios. The first step in the authorization process is to enter user information or device information. This information often does not contain the user's personal biological characteristics, which is not conducive to the regulator to quickly distinguish whether the trader is a normal human or a robot. In order to solve this problem, a spectrogram encryption design is proposed for consortium blockchain authorization. In this design, the voice information of multiple users is made into a spectrogram, which is then encrypted by hash operation, and finally stored in the consortium blockchain. The preliminary verification results show that the process can safely save user information and part of the transaction information.

1. Introduction

Blockchain is a technology that emerged in 2010. It integrates decentralized structure, distributed accounting and smart contract, consensus algorithm, storage mechanism and other characteristics to ensure the security and transparency of data sharing. In a blockchain, all transactions are verified and recorded by users within the network, which are timestamped, arranged chronologically, and connected to the previous block. Once a new block is added into the network, it will be unmodifiable [1]. The entire structure of blockchain determines that it is an authentic technology [2]. First and second generation blockchains have a completely decentralized structure, and the consortium blockchain is viewed as the third-generation blockchain. The consortium blockchain is not completely decentralized, it is a semi-centralized system with regulators, because each user in it needs to be authorized. Consortium blockchain is widely used in smart contract and other fields to provide decentralized data protection. Meanwhile, consortium blockchain has the inherent security of public blockchain, and its permission mechanism allows us controlling the edge nodes and its scale [3]. This feature makes it easy to be integrated in large-scale Internet of Things (Iot)

application, which forms the Internet of Things consortium blockchain. Moreover, this feature enables the autonomous collaboration of Iot consortium blockchain to have security features, such as the protection of data and authorization privacy, non-tampering and traceability [4].

As different consortium blockchain entities have different regulators, a complex blockchain ecosystem with multiple centres is formed, which makes data sharing among consortium blockchains face great challenges. [5] proposes an authorization and verification mechanism among multiple consortium blockchain entities. Authorization between existing consortium blockchains is conducted through two keys, the public key and the private key, private keys are used to sign the transaction, and the public key is used as address in the system. For example, some telecom operators together form a distributed consortium blockchain. Users or Iot machines need various authorization mechanisms to get in the operators' infrastructure to share data. Authorization mechanism requires not only public and private keys, but also relevant data encryption methods to protect the user privacy. The following section is a brief review of related works, followed by the presentation of the problem and proposed design, which will study the new encryption methods and authorization mechanism in the consortium blockchain to improve the security and efficiency of the consortium blockchain network.

2. Related Works

In the direction of data transmission and data protection based on consortium blockchain, predecessors have made many contributions. In terms of data storage, [6] proposed a dynamic data security storage scheme based on consortium blockchain. [7] proposed an efficient storage and processing technology based on consortium blockchain by dividing the stored data into continuous data and state data. [8] uses the authorization mechanism of consortium blockchain to realize the authorization and consensus process among smart vehicles. [9] proposed an efficient consensus algorithm based on data transmission in the consortium blockchain to improve the data transmission speed in the consortium blockchain. In addition, in order to solve the cross-chain authorization collaboration of different consortium blockchain entities and improve the scalability of consortium blockchain, [10] proposed a proof-of-concept method for blockchain communication.

3. Problem and Solution

The consortium blockchain is usually used in Iot, telecom operators and data storage, because it is easy for secure authorization, network access and other data sharing activities. The regulator of the consortium blockchain network needs more users or device information to achieve secure authorization and fast network access. Although regulators have access to encrypted pure trading data, it is often costly for regulators to backtrack transaction data. To reduce computing costs and related computing time, regulators want users or robots to input more user or device data like human biometric characteristics into the consortium blockchain. These biometrics not only help to reduce regulators' computing time during backtracking, but also help to distinguish users more quickly. For example, in an application scenario where human and robot coexist, if the original trading information does not contain the trader's biological characteristics, it is difficult to distinguish between human and robot. In order to identify the identity of traders, it is necessary to create a transaction encryption that contains the trader's biological information and a related authorization mechanism. Therefore, we propose the following contributions:

- An embedded biometric encryption and authorization mechanism based on consortium blockchain is proposed.
- The proposed encryption method is designed to encrypt spectrograms, which is conducive in storing user information and transaction information at the same time.

- Human biological characteristics are included in the process of information transmission and storage, which is conducive in the rapid differentiation of human and machine in the rapid consortium blockchain system.

The organization of this article is summarized below. Section I and section II are the introduction and related works respectively, followed by section III presenting the problem and solutions. Section IV shows the proposed system model, and section V is the experimental verification. Finally, the conclusions are summarized in Section VI.

4. System Model

Figure 1 shows the processing method of users' biometric information. For the sake of illustration, only phonetic biometric characteristics are considered here. Figure 1 is illustrated as follows.

1) The voice of the authorized user is collected, and the voice contains numbers related to the transaction. 2) After signal processing, MFCC feature is extracted from the voice data [11], and then the feature data is converted into a spectrogram. 3) Send the spectrogram to the input port of hash function to get hash picture. 4) Images with user or device information are merged and uploaded to edge nodes for re-encryption.

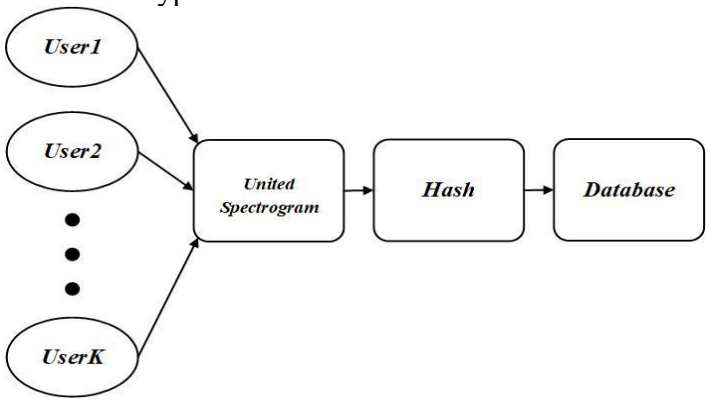

Figure 1. Encryption of traders' biometric data.

Figure 2 shows the authorization mechanism in the consortium blockchain network. First, biometric images of different traders and information about users or devices are uploaded to the edge nodes and sent to the regulatory centre of the consortium blockchain. Second, the federated chain network generates a block and invokes a transaction to store the relevant information. Each unique ID and key is distributed to the user terminal. Upon authorization, the consortium blockchain creates a smart contract for it. Smart contracts are scripts with unique addresses stored in the consortium blockchain that execute independently and automatically on each node in the network in a prescribed manner based on the data contained in the triggering transaction [12]. By sending transactions to this address, trusted nodes in the system can access smart contracts and invoke their functions, thereby directly authenticating registered traders without compromising the privacy of users or devices.

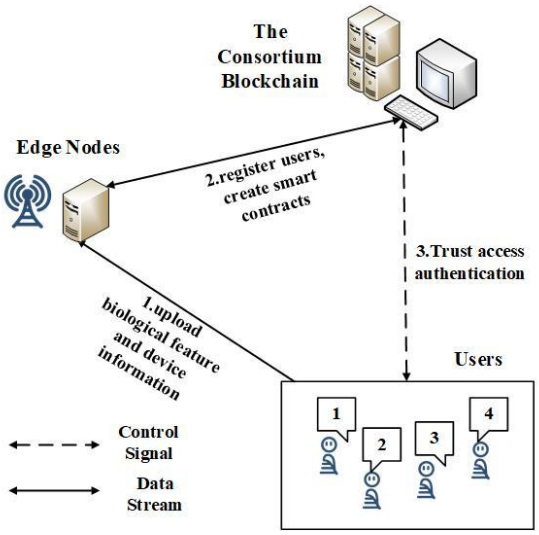

Figure 2. Overview of the studied authentication with consortium blockchain.

To authorize user access, the consortium blockchain distributes a pair of private keys and a pair of public keys to the user or device. When a transaction is signed or modified, the consortium blockchain needs to keep the private key secret, and the user's public key will be transferred to the edge node. Thus, when a registered trader initiates a trade, the public key can be sent directly to the federated chain network for authentication. The proposed biometric encryption and authorization mechanism is helpful for regulators to quickly authenticate and backtrack transaction data. Because the encrypted biometric data not only contain the identity of the trader (which makes it easier to distinguish between humans and internet-of-things robots), it also contains some of the transaction information. Therefore, the design of this paper improves the effective authentication, integrity and security of user transactions in consortium blockchain applications.

5. Experimental Verification

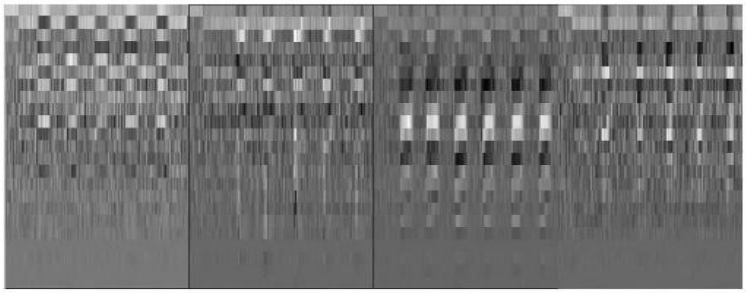

Figure 3. Biometrics from four traders converted into a primitive pattern.

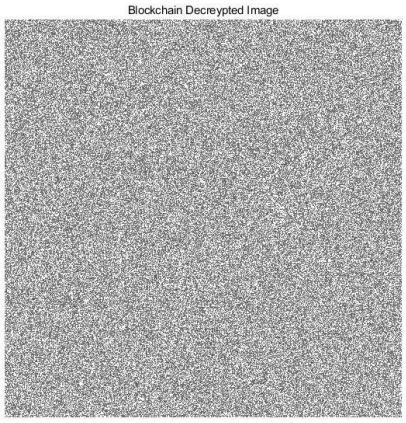

Figure 4. Hash map of the users' spectrogram.

Voice data were collected from four traders. To keep things simple, four people said the Numbers 1, 2, 3 and 4 (presumably in relation to trading ratios), each about twice a second, and for five seconds. Secondly, Mel reciprocal spectrum features were extracted from 4 audio files to generate 4 different data sets. The four data sets are combined into a data matrix and converted to the original graph. As shown in Figure 3, each gray grid in the figure represents biological information. As shown in Figure 4, after the hash function, the original graph is transformed into a hash graph, thus realizing the encryption of user information.

6. Conclusions

The user encryption and authorization in an incomplete decentralized consortium blockchain network is studied in this paper. In the proposed authorization mechanism containing biometrics, the voice information of transaction users contains information related to transactions, and after signal processing, the voice information is first converted into MFCC characteristics, and then converted into the original sound spectrogram. After hashing, the spectrogram is converted to an encrypted graph. Edge nodes or miners have difficulty identifying encrypted patterns, but regulators in the chain can still quickly identify traders by backtracking. This is because the encrypted graph also contains part of the transaction information. The mechanism studied is unique in that it can effectively distinguish between human traders and robots in the Internet of things. The proposed encryption and authorization of embedded biometrics will facilitate the registration and contract, fast and reliable access authorization of consortium blockchain users.

References

[1] Choi T M , "Creating All-Win by Blockchain Technology in Supply Chains: Impacts of Agents' Risk Attitudes towards Cryptocurrency," in Journal of the Operational Research Society, (Taylor & Francis, Oxfordshire United Kingdom, 2020).

[2] Queiroz M M and Telles R, "Blockchain and supply chain management integration: a systematic review of the literature," in Supply Chain Management, (Emerald, the UK, 2019), pp. 241-254.

[3] Zyskind G and Zekrifa D M S, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," IEEE Security & Privacy Workshops, (San Francisco, 2015), pp. 180-184.

[4] Conoscenti M and Antonio Vetrò, "Blockchain for the Internet of Things: A systematic literature review," in The Third International Symposium on Internet of Things: Systems, Management and Security (IOTSMS-2016), (Morocco, 2017), pp. 1-6.

[5] Shuai Zeng and Yong Yuan, "Scaling blockchain towards Bitcoin: key technologies, constraints and related issues," in Acta Automatica Sinica, (China, 2019), pp. 1015−1030.

[6] Qiao R and Zhu SF, "Optimization of dynamic data traceability mechanism in Internet of Things based on consortium blockchain," in International Journal of Distributed Sensor Networks, (SAGE Publications Ltd, New York, 2018) pp. 1-15.

[7] Xiao Chen and Zhigang Zhang, "HyperBSA: A High-Performance Consortium Blockchain Storage Architecture for Massive Data," IEEE Access, (2020) pp. 178402-178413.

[8] Guo S and Hu X, "Trust Access Authentication in Vehicular Network Based on Blockchain," in China Communications, (2019), pp. 18-30.

[9] Jian Y and Ding S, "A High Performance Consensus Algorithm for Consortium Blockchain," in 2018 IEEE 4th International Conference on Computer and Communications, (Chengdu China, 2018), pp. 2379-2386.

[10] Adamik F and Kosta S, "SmartExchange: Decentralised Trustless Cryptocurrency Exchange," in Business Information Systems Workshops, edited by Abramowicz, (Springer, 2019), pp. 356-367.

[11] Zhipeng D and Jingcheng W, "Voiceprint recognition based on BP Neural Network and CNN," in Journal of Physics Conference Series, (2019), pp. 1-7.

[12] Christidis K and Devetsikiotis M , "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, (2016), pp. 2292-2303.