International Journal of Digital Crime and Forensics
Volume 14 • Issue 2

A Privacy Protection Scheme for Cross-Chain Transactions Based on Group Signature and Relay Chain

Xiubo Liang, Zhejiang University, China
Yu Zhao, Zhejiang University, China
Junhan Wu, Zhejiang University, China
Keting Yin, Zhejiang University, China*

ABSTRACT

Recently, with the rapid development of blockchain technology, the information interaction and value transfer problems between different blockchains have become the focus of research. The cross-chain technology is to solve the cross-chain operation problems of assets and data between different chains. However, the existing cross-chain technology has the problem of identity privacy leakage. Therefore, this article proposes a cross-chain privacy protection scheme for consortium blockchains based on group signature, certificate authority, and relay chain. The scheme is divided into three cross-chain service layers, called the management layer, the transaction layer, and the group layer. The management layer is responsible for the forwarding of cross-chain transactions, the transaction layer includes the blockchains that actually participate in cross-chain transactions, and the group layer is responsible for group signature related work. Through this scheme, the identity privacy of both parties to the transaction can be protected during the cross-chain transaction process.

KEYWORDS

Anonymity, Blockchain, Certificate Authority, Cross-Chain, Group Signature, Identity Privacy, Relay Chain, Supervisable

INTRODUCTION

The blockchain proposed by Satoshi Nakamoto(Nakamoto, 2008) in 2008 is a distributed chained data structure, which has many advantages such as decentralization, non-tampering and non-forgeability, and is considered to be the future of financial service infrastructure(Huang, Li, Lai, & Chen, 2017). According to the number of central nodes or privileged nodes, the blockchain can be divided into three categories, namely public blockchain, consortium blockchain and private blockchain(Peters, & Panayi, 2016). The public blockchain is completely decentralized, which allows any node to obtain data and process transactions on the blockchain. However, consortium blockchain and private blockchain need to be authorized and verified by at least one organization before nodes can join. The consortium blockchain has the advantage of fast transaction processing, so it is widely used in cultural relics traceability(Liang, Zhang, Gu, Chen, Zhang, & Liu, 2020), medical data sharing(Shahna, Qamar, & Khalid, 2019), educational data sharing(Liang, Zhao, Zhang, Liu, & Zhang, 2020), etc.

However, the blockchain systems and operating mechanisms are various from different application scenarios. This phenomenon leads to the isolation of block information in different blockchains,

DOI: 10.4018/IJDCF.302876 *Corresponding Author

resulting in the islanding effect of the blockchain("Mauve Paper Vitalik", n.d.). Therefore, how to exchange information and value across different blockchains has become the focus of research. In 2012, the InterLedger protocol was proposed to solve the coordination problem between different blockchain systems(Hope-Bailie, & Thomas, 2016). Since then, cross-chain technology has developed rapidly. Cross-chain technology aims to link independent blockchains and carries the value exchange function of different value system blockchains. Herlihy proposed hash-locking mode(Herlihy, 2018) in 2013. BlockStream proposed sidechain (Asgaonkar, & Krishnamachari, 2019) in 2014. In 2016, BTC-Relay proposed a relay-chain solution (Chow, 2016), which has become the mainstream cross-chain technology. In addition, technologies such as the off-chain payment channel of the Lightning Network at the layer-2 level(Poon, & Dryja, 2016) and the decentralized autonomous incentives in Plasma(Poon, & Buterin, 2017) are also worthy of attention. The architecture proposed in this paper uses the relay-chain scheme.

Blockchain ledger is open and transparent, so privacy protection has become a challenge. Unlike within-chain transactions only in one system, cross-chain will inevitably cause two systems to interact and affect each other. According to atomic transfer(Hope-Bailie, & Thomas, 2016), a problem with the cross-chain information of a chain will affect the entire cross-chain network. Recently, there have been many attacks on cross-chain transactions. In July 2021, due to the theft of the administrator's private key, the cross-chain project AnySwap was hacked and lost more than 8 million dollars. In August 2021, Poly Network, a cross-chain interoperability protocol, was attacked by hackers and lost more than 600 million dollars. It can be seen that the cross-chain security situation is very urgent. Therefore, how to ensure system security and protect privacy in the process of cross-chain transactions is a question worth considering.

In the blockchain, privacy issues are mainly divided into two categories: identity privacy and data privacy(Zhu, Gao, Shen, Li, Zheng, Mao, & Wu, 2017). This paper discusses the issue of identity privacy in the cross-chain process, that is, users hope that the public data content stored on the blockchain cannot obtain any useful information related to their identity. The identity privacy of cross-chain transactions is fundamentally different from that of within-chain transactions. Identity privacy refers to the association between user identity information and blockchain addresses. However, different blockchains have their own addresses to represent identity information. Therefore, cross-chain privacy protection must first solve the intercommunication of different blockchains' identity information.

Main contributions of this work are summarized as follows:

1. This paper has unified the identity information of nodes on different blockchains through a centralized CA organization.
2. This paper improves a group signature algorithm, and uses the improved group signature algorithm to realize the concealment of the identity information of both parties in the cross-chain transaction from the nodes that do not participate in the cross-chain transaction, thereby protecting identity privacy.
3. This paper applies the relay chain, the CA and the group signature technology through a three-layer architecture. The three layers are the management layer, the transaction layer, and the group layer.
4. Through the relay chain, a cross-chain transaction process similar to the handshake mechanism is realized in this paper.

The rest of this paper is organized by the following order: Section 2 discusses related work. Section 3 describes three layers, security model, transaction model and the specific process of cross-chain transaction of our system. Section 4 analyzes the safety and the performance evaluation of our system. Section 5 summarizes the whole paper and discusses the future work.