Mobile Blockchain for Mutual Fund Co-investment

Tianfeng Liu
Tsinghua University
ltf17@mails.tsinghua.edu.cn

Ming Ren
Tsinghua University
mu571@sina.com

Dan Li
Tsinghua University
tolidan@tsinghua.edu.cn

Zhiming Chen
China CITIC Bank
chenzhiming1@citicbank.com

Peng Jiang
China CITIC Bank
jiangpeng@citicbank.com

ABSTRACT

In this paper we design a mobile blockchain application for mutual fund co-investment. Blockchain helps guarantee the data correctness and integrity of investment records, which improves the confidence of users when conducting co-investment. Considering the property of the application scenario, we use distributed ledger yet centralized consensus algorithm in the blockchain system. In order to speedup checking the data integrity on mobile phones with limited resource, we propose a fast verification process with a novel two-layer merkle tree, or named *hybrid merkle tree*.

1 INTRODUCTION

Blockchain is a distributed computing system with a distributed ledger to provide trust transactions across the Internet. Every peer maintains a duplicated ledger, and executes a consensus algorithm to validate transactions, grouping them into blocks. Once a transaction has been recorded in the blockchain distributed ledger, it is immutable and undeniable. It is helpful to guarantee data security, privacy and integrity. Lots of works based on blockchain have emerged in various fields, such as healthcare, insurance and industry to solve data integrity problems.

Mutual funds, managed by fund managers, pool money from retail and institutional investors. Although, in finance field, centralized institutions authorize all transactions and monitor the entire financial market, fund managers also have chances that they may, consciously or unconsciously, delete or substitute some transactions, which lead to huge losses, to persuade other investors. It is very hard for investors to find out these actions in traditional ways.

To solve problems mentioned above, we propose a blockchain application with a distributed ledger to deploy on mobile phones[1][2]. This system consists of two main parts, cluster servers in a financial center and mobile nodes. Servers are in charge of storing and instantaneously broadcasting the information of financial transactions, and mobile nodes are capable of verifying data correctness and integrity independently when needed.

When deploying a system on mobile phones, the limitation of storage space and computational resource should be taken into account. Like Simplified Payment Verification (SPV) procedure in Bitcoin, we design a cheap and fast data integrity verification process. We propose a new data structure, named *hybrid merkle tree*, combined with fully merkle tree and partial merkle tree, to verify the integrity of users and transactions data at the same time.

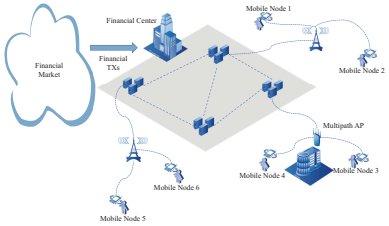

Figure 1: System overview

Our contributions in this paper are: (1) identify a strong trusted assumption in financial field, which is different from other public domain system. (2) propose a distributed ledger optimized for limited resources on mobile. (3) propose a new data structure, named *hybrid merkle tree*, to speed up the verification process.

2 DESIGN

2.1 Challenge

When blockchain technology is implemented on mobile nodes, there are three differences from common blockchain systems. Firstly, the computing ability of mobile nodes is limited. Secondly, the storage capacity of mobile nodes is much smaller than servers. Thirdly, the network communication between servers and mobile nodes is different from common blockchains.

This system should also guarantee data correctness and integrity: (1) If severs declare that this transaction is belonged to a user, mobile nodes can verify this declaration independently. (2) This system guarantees the integrity of transaction in a specific time interval of history, which means servers should provide all transactions of a specific user in a particular time interval, without any deletion and substitution of transactions. This is the main challenge in system design.

2.2 System Overview

The proposed system is illustrated in Figure 1. There are three entities in this system: the financial market[3], the financial center with a server cluster, and massive mobile devices.

Financial Market: This entity is an abstraction of true financial markets, like funds or stocks. All transactions including in this system come from financial market. In reality, every financial market will have regulators to check whether transactions are legal or not and reject illegal transactions. So, if a transaction is sent into this system, this transaction will be considered as legal and stored in server cluster.

APNet'2018, August 2018, Beijing, China

Server Cluster: The financial center consists of server clusters and is responsible for confirming and storing transactions sent by financial market[3]. The functions of servers are in charge of calculating block headers and two-layer merkle tree with transactions once a day, then publish block headers to all mobile nodes. In verification process, after receiving queries from mobile nodes, they extract hybrid merkle tree and related transactions from database and send them to corresponding mobile nodes.

Mobile Device: It is basic entity in this system. Every mobile node will receive and store block headers published by servers every day. When a user wants to check data correctness and integrity of a specific user in a particular time interval, this action will trigger the verification process in mobile node. Mobile nodes will query these information to servers. After receiving all information, mobile nodes use same hashing function as server to calculate final merkle root independently. Eventually, mobile nodes can compare results with the corresponding merkle roots stored before. According to the comparison results, mobile users can determine whether the financial center can be trusted.

2.3 Assumption

In other distributed ledger systems, like Bitcoin or Ethereum, developers should design an exquisite mechanism to ensure every participant has initiative to be honest not only in data storing but also in transaction making. But in financial market, regulators will check whether every transaction is legal or not. So this system should only focus on trying to ensure honest in data storing.

We notice an interesting phenomenon that the importance and meaning of every transaction is determined by other transactions and market information in the future. When a transaction occurs just now, there is no motivation that servers delete or substitute this transaction. However, when there are a lot of transactions and market information about price gathered in a long term, servers can determine whether past transactions should be reserved, deleted or substituted according to their interests. This phenomenon occurs various financial fields, not only in co-investment scenario. In a nutshell, servers will be honest for transactions occurring just now, but may be dishonest for transactions occurring long time ago.

2.4 Central Consensus

Using the key insight in §2.3, we can simply use a central consensus algorithm in servers.

The consensus algorithm is working as follows: (1) Mobile nodes sends all transactions to servers. After servers receive the transaction, it will notify the mobile nodes which sends this transaction. (2) Servers will gather all transactions in one day, construct a block with transactions and hybrid merkle tree (described in next section) and send the block header back to every mobile nodes. (3) Mobile nodes receive the block header every day, save these headers in their storage spaces and use these block headers to verify the correctness and integrity of transactions. Detail of verification process will described in next section.

2.5 Fast Verification

Considering limitations in mobile nodes, we design a fast verification process. It is similar to Simplified Payment Verification (SPV) in bitcoin[4], we use a two-layer merkle tree to speed up the verification process[5]. This data structure is illustrated in Figure 2.

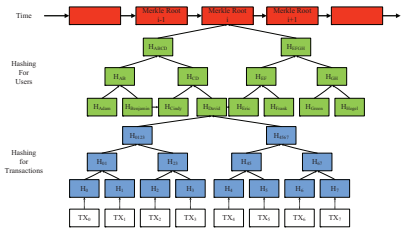

Figure 2: Two-layer merkle tree for verification

It is two-layer merkle tree, stored in server nodes. First layer is transaction layer. The leaves of merkle tree of transaction layer are all transactions of a particular user and a particular day, and hashed into one root represented the user who transactions belong to. Second layer is user layer. Using the hash root in transaction layer as leaves of merkle tree of user layer, and hashed into one merkle root. Finally, using the merkle roots in user layer, we can construct blocks and block headers

To verify the integrity of transaction, mobile nodes will query all transactions of a specific user in a particular time interval, such as user A and time interval T. Servers will send all transactions of A in T. Additionally, servers will send all hashes which can construct merkle paths in user layer from user A to merkle root. Mobile nodes will firstly calculate the full merkle tree in transaction layer using transactions provided by servers. Then they will calculate partial merkle tree in user layer, and compare results with block headers stored before. Because mobile nodes only receive fully merkle tree in transaction layer and partial merkle tree in user layer, we call this *hybrid merkle tree* .

3 CONCLUSION

Both public environment and financial environment should guarantee the correctness and integrity of data. Especially in mutual fund co-investment, it is very hard for investors to find out cheating actions of fund managers in traditional ways. With a strong assumption, we propose a distributed ledger system in mobile phones with a central consensus algorithm to solve this problem. Due to limitations in mobile nodes, we design a new data structure, named hybrid merkle tree, to speed up verification process in mobiles.

REFERENCES

[1] Kongrath Suankaewmanee, Dinh Thai Hoang, Dusit Niyato, Suttinee Sawadsitang, Ping Wang, and Zhu Han. Performance analysis and application of mobile blockchain. In *2018 International Conference on Computing, Networking and Communications (ICNC)*, pages 642–646. IEEE, 2018.

[2] Zehui Xiong, Yang Zhang, Dusit Niyato, Ping Wang, and Zhu Han. When mobile blockchain meets edge computing: challenges and applications. *arXiv preprint arXiv:1711.05938*, 2017.

[3] Gareth W Peters and Efstathios Panayi. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In *Banking Beyond Banks and Money*, pages 239–278. Springer, 2016.

[4] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[5] Johannes Buchmann, Erik Dahmen, and Michael Schneider. Merkle tree traversal revisited. In *International Workshop on Post-Quantum Cryptography*, pages 63–78. Springer, 2008.