A bike sharing system based on Blockchain platform

Hanyue Guo[1,a], Jiting Zhou[1], Jiaqi Wang[1] and Xiaodong Wang[2]

[1]Shanghai Film Academy, Shanghai University, Shanghai 200072 P.R. China
[2]FNFN FUND LIMITED, Kunming, Yunnan650032 P.R. China

Abstract. Leakage of user privacy and vandalism of the sharing bike have been the most serious problem since sharing bike came on the scene. Accordingly, it is very urgent to rebuild the underlying trust mechanism. Most bike sharing systems are centralized, leading to overpressure on the central server. This paper proposes a bike sharing system based on blockchain service platform and a shared operation mode of C2C. The system uses the blockchain system as the trust guarantee. The extra chain payment - lightning network is used to improve the efficiency of the blockchain system and the smart contract is used to provide the rights and interests of the two parties.

1 Introduction

1.1 Current bike-sharing system

At present, there are some problems in the bike sharing system, as follows:

- Trust mechanism problem: there are a lot of human damage to the shared bicycle. The sharing bicycle platform usually uses the security deposit to solve the problem of trust mechanism, but the loss is still serious.
- Privacy issues: central institutions to grasp the platform user information, vulnerable to the disclosure of user privacy.
- Data processing problem: Once the computing mode centered on the core server is paralyzed, it will cause the paralysis of the shared bicycle using system and cause unnecessary loss to the users [1].

1.2 Analysis of bike-sharing system based on Blockchain Technology

The bike-sharing system under the blockchain platform constructs a decentralized operation platform by means of the technical features of encrypted storage and immutability. The users' data on the chain can be monitored in real time, and the smart contract will be triggered after the transaction takes place. The dynamics of the tenant, platform, and user are monitored and recorded in real time.

Through blockchain technology, we can do three points: first, we can trace back to which party divulges user data to eliminate user privacy disclosure purposes. Second, we can record every transaction information in real time to generate user credit score. Credit score determines whether users can use shared bicycles and ride time and frequency, thereby reducing the loss of shared bicycles. Finally, we can also perform data distributed storage to reduce the pressure of the central server.

2 Technical principle

2.1 Distributed database: blockchain

In 2008, the paper "Bitcoin: a peer-to-peer electronic cash system" [2] discussed in detail the electronic cash system of bitcoin, which was supported by blockchain technology and realizes point-to-point transaction.

Blockchain technology is a completely new distributed infrastructure and computing paradigm. The blockchain data structure of blockchain technology verifies and stores data. The cryptographic approach guarantees the security of data transmission and access. Smart contract programming and operational data consisting of automated script code. [3]. Blockchains are combined into specific data structures in chronological order, and the centralized data sharing is guaranteed by the principle of cryptography. The SHA 256 algorithm and Merkle tree are used to implement it's simple and secure data management system with sequential relationship and efficient and rapid verification [4].

2.1.1 PoW consensus mechanism

The consensus mechanism is an algorithm that allows participants to form a common understanding. The consensus mechanism adopted is PoW: when miners dig a new block, they must calculate the sha-256 password hash function. Random hash values in the block start with one or more zeros. As the number of zeroes rises, the amount of work required to find the solution increases exponentially, and the miners try to find the solution over and over again [2]. the node that calculates

[a] Corresponding author: 15632280060@163.com

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).

the correct answer first can obtain the billing right of the current block and the reward of newly issued "token".

The advantages of this consensus mechanism are complete decentralization, free access of nodes, easy implementation, high cost of destroying the system and high security coefficient [5].

2.1.2 Security mechanisms

The PoW consensus mechanism and the longest chain mechanism can guarantee the Immutable property of the blockchain.

With the PoW mechanism, the probability of obtaining the result is close to the proportion of computational force, the cost of cheating is higher than the cost of mining when the malicious node is less than 51% of the computational force. Thus, the probability of block bifurcation is extremely low.

The longest chain mechanism requires that new blocks be linked to the end of longer blockchain branches. After the new block is linked to six blocks, its validity can be confirmed.

2.1.3 Efficiency of blockchain

In order to ensure the reliability of the transactions, the blockchain system stipulates that each transaction must be confirmed 6 times to pass. The system can only process 7 transactions per second, and each transaction needs to wait 10 minutes to confirm. Trading often takes an hour to complete verification.

2.2 Out-of-chain transactions-Lightning Networks: addressing blockchain's efficiency issues

In February 2015, the paper "The bitcoin lightning Network: Scalable off-chain instant payments" [6] proposed an off-chain transaction method of blockchain, which is very suitable for multi-frequency, micro-payment bike sharing transactions.

The Lightning Network is based on two trading intelligence contracts, RSMC (Revocable Sequence Maturity Contract) and HTLC (Hashed Time lock Contract). RSMC guarantees that direct transactions between two people can be done under a chain. HTLC guarantees that any transfer between two people can be completed through a "payment" channel. This contract is used for two nodes with no trading channel to complete the transaction through the intermediate node (there is a payment channel between the intermediate node and the two nodes).

2.2.1 RSMC

As shown in figure 1, which illustrates the transaction structure of RSMC.

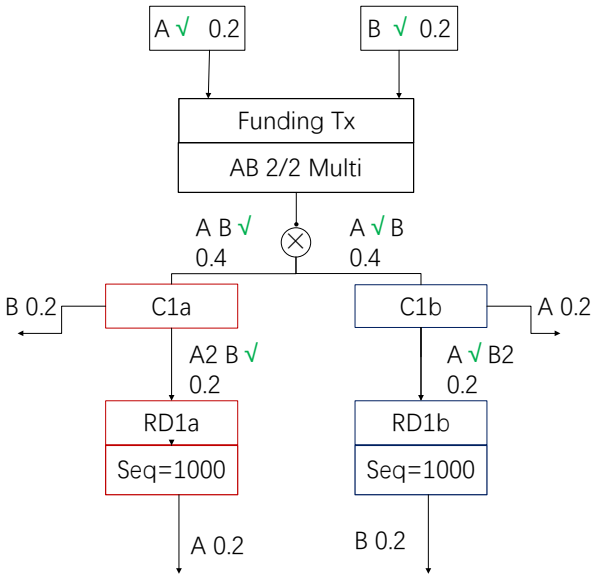

Figure 1. Structure of the RSMC transaction.

There are four steps from the beginning to the end of the transaction.

The first step: A and B take out 0.2BTCs each, construct Funding TX, and output 2 / 2 multiple signatures of A and B.

The second step: A constructs Commitment Tx:C1a and RD1a, A gives the signature to B. RD1a is the cost transaction for the first output of C1a and sends 0.2BTC to A. B constructs Commitment Tx:C1b and RD1b and hands them to A for signature. The structure is symmetrically related to C1a and RD1a.

Step three: B signs C1a and RD1a and signs them to A. A to C1b and RD1b signature, after the completion of B. At this point, since both parties have not signed Funding Tx, neither party can cheat.

Step four: After the two parties have finished signing and exchanging the commitment Tx, they will sign and exchange the Funding Tx respectively. The transaction can be broadcast on the blockchain at this time.

2.2.2 HTLC

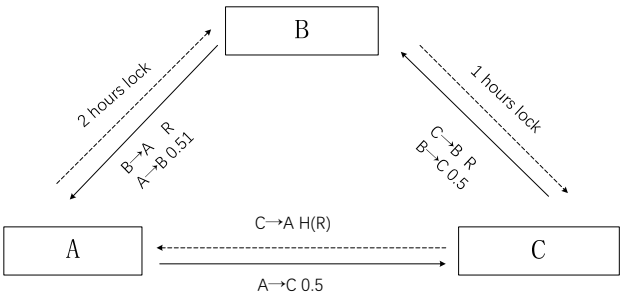

Figure 2. HTLC transaction diagram.

As shown above, A wants to send 0.5 BTCs to C, but there is no payment channel between A and C. But it can be made up of two micropayment channels, such as A / B and B/C.

C generates a secret R and sends the Hash (R) to A, Alice and Bob agree to an HTLC contract: as long as B can produce the correct hash to A within two hours, A

will pay 0.51 BTCs. If Bob fails to produce the R, the money will be returned to A two hours later. Similarly, B and C agreed to a HTLC contract: as long as Carol can show B the correct hash within 1 hour, Bob will pay C 0.5 BTCs.

In this way, the transaction can be completed through the middleman B, A and C, of which the difference of 0.01 is regarded as the commission of B.

2.2.3 Safety and security

In order to prevent any party from issuing abandonment distribution plan during the transaction process, Lightning Network Technology provides security protection through the following measures:

(1) sequence field: a party unilaterally terminating a transaction needs to wait for the previous block to confirm the length of the 1,000 data blocks set up in the sequence field before it can get its allotment.

(2) every time the balance allocation scheme is updated, both parties send the private key used in the last transaction to each other.

(3) punishment mechanism for evil: if one side cheats, the other side will take all the funds in the passage.

3 Bike sharing scheme based on blockchain

This system uses the blockchain system to build the trading platform, and solves the problem of low efficiency of the system through the lightning network technology. The authentication information and transaction information of all nodes on the blockchain will be stored on the blockchain in time order. Blockchain technology provides trust guarantee and bookkeeping. All transaction information and registration information of nodes will be recorded on the blockchain. The blockchain technology can guarantee the real existence of every transaction, so as to protect users' rights and interests.

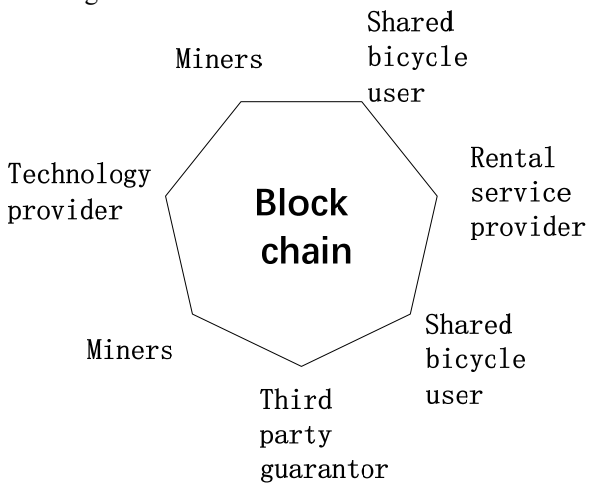

Figure 3. Blockchain platform structure.

As shown, the following nodes exist on the entire blockchain node:

"miners": in order to win the “token” award for node bookkeeping rights, responsible for bookkeeping work.

Shared bike users: including users who use shared bicycles and users who provide high-quality bicycle rental services.

Blockchain technology provider: provide blockchain technical support, maintain platform security, provide platform data analysis services.

Rental service provider: provides the sharing bicycle rental service.

third-party guarantor: for C2C mode to provide notarization services.

There is a micro-payment channel of lightning network between the users of shared bicycle and the renter and the third-party guarantor.

Blockchain platform mainly provides two services: one is in the B2C mode of operation, for ordinary users to implement, rental bicycle renter sharing bike. The second is in the operating mode of C2C, for users with cycling quality requirements, most of these users are cycling enthusiasts who want to rent a high-quality bicycle . This kind of bicycle sharing model belongs to the sharing economy model, with high-quality bicycle users providing their idle and temporarily unused cars at home to earn commission. Users can choose between each other. The renter can search nearby suitable bicycles. The provider can also use the blockchain records to investigate the lease situation of the other party to choose whether to lease or not.

3.1 The Operation Mode of B2C

Ordinary users only need to establish a lightning network payment channel with the leasing company and publish it on the blockchain after completing the transaction. The specific operation is as follows:

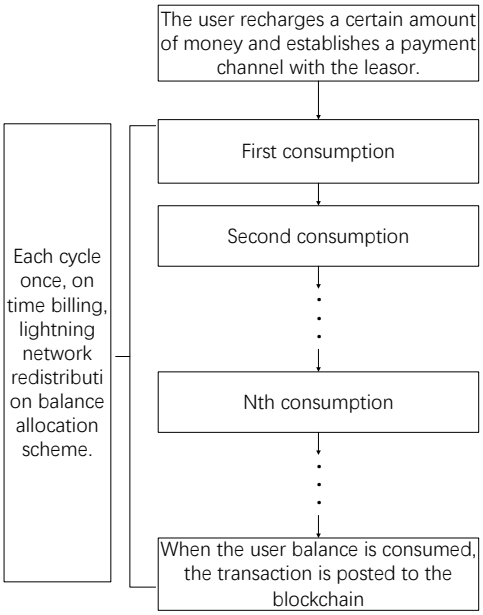

Figure 4. B2C pattern transaction graph.

The user recharges a certain amount of money and establishes a payment channel with the Leasing company. Each cycle once, on time billing, lightning network redistribution balance allocation scheme. After the user

balance is consumed, both parties sign together and announce the transaction to the blockchain.

3.2 Operation mode of C2C

This economic model is aimed at cyclists, and high-quality cyclists are also platform users, who have bikes that sit idle at home for the time being and want to rent them to cyclists.

First, the rent-seekers finds the qualified bicycle through the blockchain platform and obtains the consent of the provider. Second, two people in the platform generally need a third-party guarantor (can be a leasing company) to ensure the security and reliability of the transaction, the two sides and the third-party guarantor establish payment channels to complete the payment. In order to ensure the interests of the provider, we also need to introduce smart contract technology, and to collect a certain amount of deposit from the lessor.

The process is shown in figure 4.

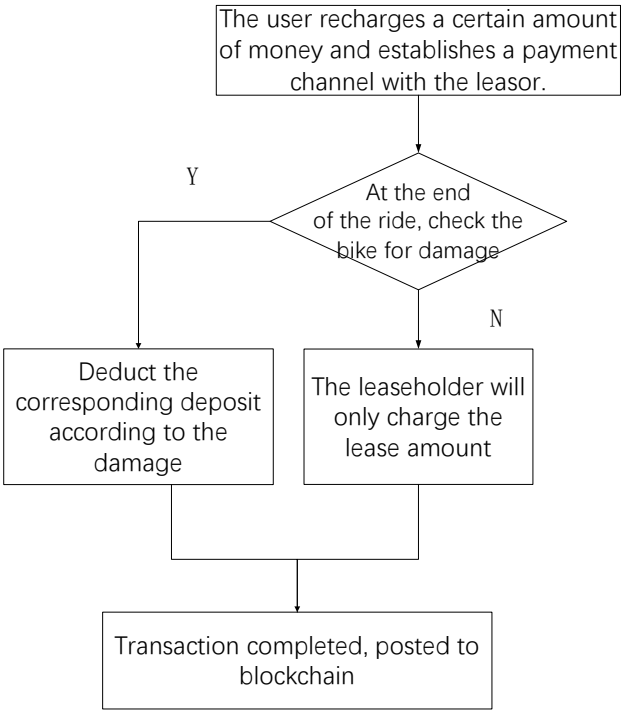

Figure 5. transaction diagram of C2C pattern.

First, the leasing party enters the deposit and the rental amount agreed by both parties in the wallet address. Second, after the end of the ride, the bicycle would be checked. If the bicycle is not damaged, the tenant only pays the rent. If the bicycle is damaged, the tenant should also deduct part of the deposit according to the loss of the bicycle. In the second cases, if the tenant refuses to pay, he will not be able to benefit from the platform services again, and the provider may sue the tenant under an electronic contract.

The payment process is as follows.:

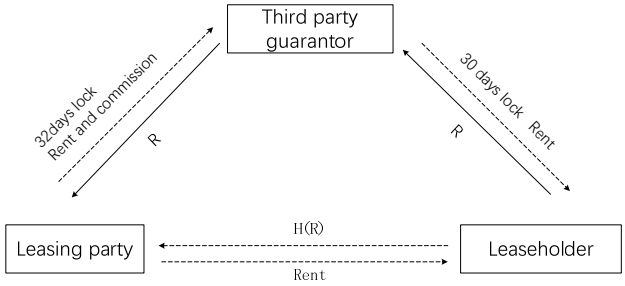

Figure 6. flow chart of C2C payment.

As shown in figure 6, both parties complete the transaction through a payment channel with a third-party guarantor.

4 Summary

In this paper, a bike sharing platform system based on the blockchain system is designed. It solves the problem of trust mechanism and the pressure of the central server under the central platform which has been paid much attention to by the society up to now. The efficiency of blockchain is solved by lightning network technology, and a new operation mode of C2C is proposed.

Reference

1. S. Nanda, T. J. Hacker and Y. H. Lu, "Predictive Model for Dynamically Provisioning Resources in Multi-Tier Web applications," 2016 IEEE International Conference on Cloud Computing Technology and Science 240 (CloudCom) [C], Luxembourg City, 2016, pp. 326-335.
2. S. Nakamoto Bitcoin: A peer-to-peer electronic cash system [J]. Consulted, 2008.
3. Niu Luqing. New trend of application of chain gold blockchain [J]. New economy Guide, 2017 (8): 10-18.
4. Xia Qing, Zhang Fengjun, Zuo Chun. A Survey of consensus mechanisms in cryptographic Digital currency Systems [J]. Computer Systems applications, 2017,26 (4): 1-8.
5. Yuan Yong, Wang Feifei. Development status and Prospect of Blockchain Technology [J]. Acta Automatica Sinica, 2016,42 (4): 481-494.
6. JOSEPH P, THADDEUS D. The bitcoin lightning network: Scalable off-chain instant payments [R / OL].2017.13(4)