Blockchain anonymous trading system based on multi-hop payment

Weiwei Zhang1 and Zhiyuan Li1*
Department of Cybersecurity,Jiangsu University,Zhenjiang,212013,China

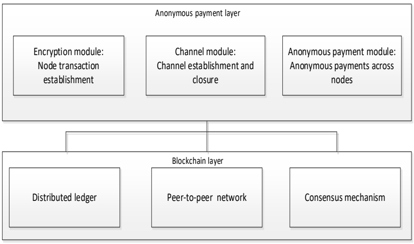
优胜奖

Abstract

In recent years, with the emergence of bitcoin, blockchain technology has attracted more and more attentions from academia and industry. The advantages of blockchain are decentralized trust, not tampered, traceable and consensus features. However, transaction processing speed is 7 transactions per second in the bitcoin network. The transaction processing performance is not suitable to many applications in e-commerce field. Hence, the scalability of transaction consensus on blockchain has become a challenge issue. There are existing works to solve the issue, such as the lightning network, which exploits cross-chain consensus to improve the scalability of the bitcoin transaction. However, the anonymity between seller and buyer is still a privacy challenge for the fast blockchain payments based on the lightning. In this paper, we propose a blockchain anonymous trading framework based on multi-hop payment to solve the scalability problem of the blockchain transactions and improve the efficiency of transactions among nodes. Firstly, we use Three-session encryption to build multiple encryption transaction channels between a pair of nodes. Secondly, in this work route algorithm is used to find a minimal anonymous service fee path. Finally, the experimental results show that lightning network with encryption transaction channels can improve the use efficiency, reduce the extra cost of transaction and guarantee the privacy information of users.

System Design

Overall system architecture


Anonymous payment layer

Encryption module:
Node transaction establishment

Channel module:
Channel establishment and closure

Anonymous payment module:
Anonymous payments across nodes

Blockchain layer

Distributed ledger

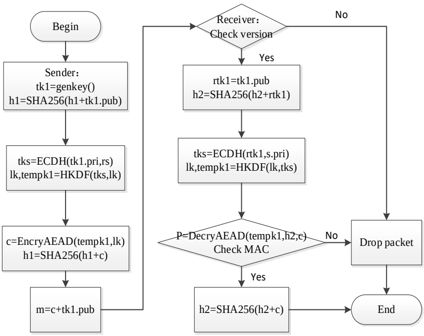
Peer-to-peer network

Consensus mechanism

Figure 1. Overall system architecture

System encryption module

Before a node requests a transaction, an encrypted session state is established, which is used to encrypt and authenticate messages sent between nodes. Among them, before the node enters the authentication and encryption communication state, a three-step communication handshake is needed to ensure the anonymity and security of the communication.


Begin

Sender：
tk1=genkey()
h1=SHA256(h1+tk1.pub)

tks=ECDH(tk1.pri,rs)
lk,tempk1=HKDF(tks,lk)

c=EncryAEAD(tempk1,lk)
h1=SHA256(h1+c)

m=c+tk1.pub

Receiver：
Check version

rtk1=tk1.pub
h2=SHA256(h2+rtk1)

tks=ECDH(rtk1,s.pri)
lk,tempk1=HKDF(lk,tks)

P=DecryAEAD(tempk1,h2,c)
Check MAC

h2=SHA256(h2+c)

Drop packet

End

Figure 2. The first step of encryption module handshake

Anonymous payment module

In order to determine a cross-node anonymous payment path, the node needs to select a relatively optimal path based on the path selection algorithm on its local view.When calculating path needs to forward the channel cost and anonymous messages forwarding cost consideration, because in the network of each channel forwarding cost and its connection nodes forward anonymous messages cost exists the possibility of inconsistency, therefore we will define a path overhead than *PErate*, channel the *PErate* value is the path to forward the ratio of cost and node anonymous message forwarding cost. The path algorithm is shown in algorithm 1. In this algorithm, the sender wants to find a G from their local view inside can be connected to the recipient's path are added to the path list *Pathlist* $path_i$, finish after adding algorithm began to calculate the path forward channel in turn from *Pathlist* $tmpPathfee_i$ anonymous message forwarding fees, fees $tmpPathfee_i$ and node is equal to the $tmpPathfee_i$ HTLC basic fee basefee with other fees such as forwarding $tfee_i$. Then calculate the path $PErate_i = tmpPathfee_i / tmpPeerfee_i$. If the $PErate_i$ is less than the current best fee *bestPErate*, record the path and update the values of *bestPErate* and the *bestpath* until calculating the paths of all *Pathlist*, return *bestpath* and *bestPErate*.

Algorithm 1: Routing algorithm FindRoute(G,F)

```
begin
    $bestpath \leftarrow \{\}$, $bestPErate \leftarrow 0$, $Pathlist \leftarrow \{\}$, $NodeRatio \leftarrow \{\}$
    for find the $path_i$ from G to F do
        $Pathlist \leftarrow$ addpath($Pathlist$, $path_i$)
    end
    for each $path_i$ in the $Pathlist$ do
        Calculate the $path_i$ node anonymous message forwarding cost $tmpPeerfee_i$
        $tmpPathfee_i \leftarrow (basefee_i + tfee_i)$
        $PErate_i \leftarrow (tmpPathfee_i / tmpPeerfee_i)$
        $dit_i \leftarrow |1- PErate_i|$
        if $dit_i < |1-bestPErate|$ then
            $bestPErate \leftarrow PErate_{i;}$
            $bestpath \leftarrow path_{i;}$
        end
    end
    return $bestpath$ and $bestPErate$
end
```

Simulation

We compare the difference between the Dijkstra algorithm and the routing algorithm presented in this paper which variation in anonymous service fees over time. Figure 3 shows that the total cost of service nodes on the path by algorithm proposed in this paper is lower than the Dijkstra shortest path algorithm with the change of time.

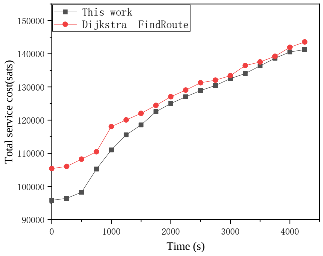


Figure 3. Compare the impact of time on Total service cost

Figure 4 shows 0that the algorithm in this paper compared with the Dijkstra shortest path algorithm, selects more anonymous service nodes when looking for the optimal payment path.

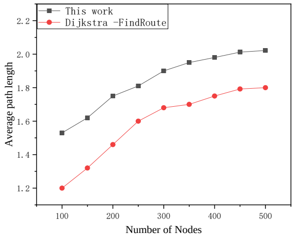


Figure 4. Comparison of the influence of anonymous service node number on routing selection

Conclusion

We introduce the anonymous payment layer on the basis of the Bitcoin network, which can enhance the communication security of the nodes participating in the tran0saction, and provide a secure session guarantee for both sides of the transaction.At the same time, the system seeks the most cost-effective anonymous payment path for each node to enhance anonymity while reducing service consumption costs .Our future work is to deploy the system and validate our work.

References

[1] D. Guinard, V. Trifa, Building the Web of Things: with Examples in Node.Js and Raspberry Pi, Manning Publications Co., 2016. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System[D].2008.

[2] Martinazzi Stefano,Flori Andrea. The evolving topology of the Lightning Network: Centralization, efficiency, robustness, synchronization, and anonymity.[J]. PloS one,2020,15(1).

[3] Bartolucci Silvia,Caccioli Fabio,Vivo Pierpaolo. A percolation model for the emergence of the Bitcoin Lightning Network.[J]. Scientific reports,2020,10(1).

Contents

Linkman：Weiwei Zhang
Telephone：15895042402
E-mail：1725529638@qq.com