Design and Implementation of a Central Node-controlled Off-chain Payment Channel Rebalancing Scheme

Wei-Jun Gao[1], Ya-Qian Yue[2], and Xiao-Qin Wang[3]

(Corresponding author: Ya-Qian Yue)

School of Computer and communication, Lanzhou University of Technology[1]

No. 36, Peng-Jia-Ping Road, Lanzhou 730050, China

Email:yyaqian2023@163.com

(Received Mar. 29, 2023; Revised and Accepted Nov. 24, 2023; First Online Feb. 23, 2024)

Abstract

The emergence of an off-chain payment channel network provides a reliable solution for blockchain scalability. However, channel imbalance in practical applications increases the transaction cost of nodes, leads to poor sustainability of payment channels, and even affects network stability. This paper proposes a central node-controlled off-chain payment channel rebalancing scheme for channel imbalance, using a combination of algorithms and smart contracts to establish a credible, safe, and win-win mutual rebalancing platform for nodes who want to achieve channel balance, and verifies the effectiveness of the scheme, providing a new idea of low consumption and no cost for the rebalancing channel.

Keywords: Blockchain; Channel Imbalance; Off-chain Payment Channel Network; Rebalancing

1 Introduction

With the development of technology and the deepening of information sharing, network attack methods emerge in an endless stream, and attackers try to steal, modify and abuse user information. In this context, network protection technology [1] is increasingly improved, such as privacy protection [2], key management [3], identity authentication [4] and other protective means are constantly optimized, and the birth of blockchain technology has become an effective tool for network security protection. Blockchain provides data security, autonomy, transparency, auditability, privacy, and many other benefits, and has been widely used in various fields such as finance, Internet of Things, healthcare, energy, Biometrics, and government affairs [5–10]. The off-chain payment channel network retains the advantages of blockchain security and decentralization [11], reduces the pressure on on-chain storage by moving transactions down the chain, ensures transaction processing volume, and enables low-cost and low latency transactions for on-chain micro-payments. However, channel imbalance [12] has become an important issue limiting the development of off-chain payment channel networks.

Channel imbalance is caused by excessive one-way payments at one end of the channel. Channel funds are transferred in one direction, and after several transfers, the distribution of funds at one end becomes zero, and if both ends of the channel want to transact at this point, the channel must be closed and a new channel established. The opening and closing of the channel need to be published on the chain, and the closing of the channel will increase the path length of transaction transmission of certain nodes, resulting in long transaction delays and high fees.

At present, there are two common ways to deal with the channel imbalance problem. One is routing to achieve channel rebalancing, which uses channels with a higher balance to transmit transactions, effectively avoiding further deterioration of unbalanced channels, but still lacks in improving the balance of imbalanced channels. Secondly, the node takes the initiative to achieve channel rebalancing and adopts the loop payment to eliminate the fund offset problem when channel imbalance is monitored, which improves the channel balance degree but increases the time and fund cost of the node to rebalance the channel. To address the shortcomings of the current channel rebalancing scheme, this paper proposes a central node-controlled off-chain payment channel rebalancing scheme, which adopts the way of mutual borrowing and lending by nodes at both ends of the channel to solve the channel imbalance problem, aiming to reduce the funds and time spent by nodes in the rebalancing process.

The organization of this paper is as follows. Section 2 mainly introduces the basic knowledge of off-chain payment channel networks. Section 3 describes the research status of the off-chain payment channel network and the main solutions to the problem of channel imbal-

ance. Section 4 shows the "central node control off-chain payment channel rebalancing scheme" model diagram and describes the detailed design and implementation process of each module in the model diagram. In Section 5, the experiment verifies the correctness, effectiveness and expansibility of the "central node-controlled off-chain payment channel rebalancing scheme". Section 6 summarizes the work done in this paper and discusses the limitations, applicability and future research direction of this scheme.

2 Background

Blockchain technology has been implemented in P2P networks without relying on trusted third parties, changing the existing payment model and creating a new type of commercial payment system, but it has problems such as low throughput and extended transaction times. The current mainstream payment platform, Visa, can process an average of *2,000* transactions per second [13], while blockchain can theoretically process up to *7* transactions per second [14]. In order to break the scalability bottleneck of blockchain, on-chain scaling technology, inter-chain scaling technology and off-chain payment channel network have emerged.

The on-chain expansion technology mainly has two ways to adjust the blockchain parameters and update the system consensus algorithm. Such as increasing the block size to increase the block capacity, changing the communication method between blockchain nodes to improve the block out rate, and updating the consensus algorithm to reduce the transaction confirmation time, but the technique has certain limitations, such as increasing the block size may lead to network congestion and updating the system consensus algorithm cannot be completed in a short period of time.

Inter-chain scaling is mainly based on cross-chain technology [15], which realizes blockchain scaling through inter-chain value transfer, however, this technology is in the concept certification stage, lacking commercial landing applications, and can not be quickly put into practical applications.

With the off-chain payment channel network [16], after both parties to a transaction create a payment channel with a smart contract, both parties can make multiple transactions. If one party has a desire to close the channel or disputes a transaction in the process, the blockchain will act as an arbitration platform to check and confirm the status of the channel. The network ensures that transactions are executed correctly and securely by running a Recoverable Sequence Maturity Contrace (RSMC) and single-path atomic transactions and cross-channel transactions by running a Hashed Timelock Contracts (HTLC).

2.1 Payment Channels

A payment channel is a transaction path created peer-to-peer by both parties to a transaction, allowing both parties to update and maintain the funds in the channel off-chain, thereby enabling off-chain payments. The process of off-chain channel payments consists of following steps. First, open a channel. Each party to the transaction takes out funds and deposits them into the channel to generate the initial transaction. Both parties attach signatures to the initial transaction and broadcast it to the chain, indicating the completion of the channel creation. Second, Conduct the transaction. Both sides of the transaction exchange funds in the channel and the distribution of funds in the channel will be updated after each transaction. In the process, if one side maliciously publishes a false transaction, all the funds of the user in the channel will be returned to the other side as a penalty. Finally, Close the channel. When one side of the channel runs out of funds or wants to leave the channel, any side of the channel only needs to publish the latest channel status to the chain, and after the status is published, it means the channel closure is completed.

2.2 Payment Channel Network

The formation of a payment channel network not only enables users to transact across channels, but also reduces the pressure on network channel information storage. In the network, users who do not create a channel want to make transactions, the routing algorithm will find a suitable path for them to transmit the transaction, and the sender of the transaction only needs to pay the intermediate node transaction forwarding fees. For a better understanding, the illustration of the cross-channel trading is given in Figure 1.

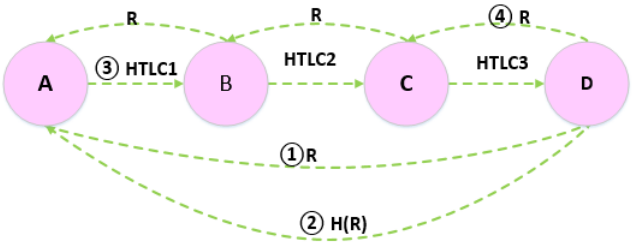

Figure 1: The illustration of the cross-channel trading

Suppose user A wants to transact with D, but no payment channel is established between A and D. The transaction execution process is as follows: A randomly generates the original image R and passes R to D; D hashes the received R to generate H(R) and passes it to A; A executes the routing algorithm to find the transaction transmission path A− >B− >C− >D that can reach D. Each node in the path signs a time lock with the neighboring

node respectively. After the time lock contract on the transmission path is signed, user D presents the original image R of H(R) to C to unlock the funds from C. Then R is passed to the next user in turn to unlock the funds of the neighboring users. Finally, the transaction between user A and D is realized, and for users B and C who transmit the transaction, they will receive a transmission fee, which is generally relatively low.

3 Related Work

When the off-chain payment channel network was created, its research mainly focused on routing algorithms, such as the hybrid routing algorithm Flare [17], which used a combination of common nodes and beacon nodes to find paths for payment nodes, improved the path finding rate and decentralized centralization, and laid a consolidated foundation for the routing algorithms that followed. In recent years, routing algorithms have considered some inherent limitations in the network, such as fund overload [18], channel imbalance [19], routing cost [20], and security issues [21]. For channel imbalance, Giovanni et al. [22] proposed to reduce channel imbalance by charging transaction fees at the gateway nodes, the rate of which depends on the balance difference between the nodes at both ends of the channel; Khalil et al. [23] proposed REVIVE, which allows any set of users to safely rebalance the channel according to the channel owner's preference, to ensure the balance of funds between the forwarding nodes. Mercan et al. [18] proposed balance-aware routing, which calculates the channel imbalance before the transaction is forwarded and then selects the gateway to be forwarded, thus alleviating the channel imbalance. Conoscenti et al. [24] proposed a passive rebalancing scheme to reduce the payment failure rate due to channel imbalance. Hong et al. [25] proposed the asynchronous rebalancing idea CYCLE, where imbalanced nodes eliminate the fund offset by implementing loop payments on closed-loop routing. Avarikioti et al. [26] proposed an optional rebalancing protocol that effectively decomposes the rebalancing solution into incentive-compatible cycles, thus preserving the node balance while atomic payments are executed.

With the development and growth of off-chain payment channel networks, studies on topological properties have emerged, such as Seres [27] on the degree distribution, robustness, and random failures of (Lightning Network LN), Guo et al. [28] on the connectivity, channel capacity, and routing efficiency of LN, Zabka et al. [29] on the geographical distribution of LN, and Lisi et al. [30] on the topology of lightning networks for a specific time period.

Later work has shown that there are security risks in off-chain payment channel networks [31], such as Malavolta et al. [32] described possible wormhole attacks in LN networks, followed by the multi-hop anonymity and privacy-preserving payment channel network MAPPCN [33], and for attack models, such as Thakur et al. [34] proposed a conspiracy attack and Perez et al. [35] proposed a balance detection attack. There are also researches on the privacy protection of off-chain Payment channel networks. Zhang et al. [36] proposed a hybrid multi-hop mechanism, including Payment channel network PCN, Onion routing and side chain, so as to ensure privacy-protecting off-chain payment. The CryptoMaze protocol proposed by Mazumdar et al. [37] not only avoids the formation of multiple off-chain contracts on the side of the path sharing of routing partial payments, but also ensures the no-connectibility of partial payments.

4 Scheme Design

4.1 Design Ideas

In this paper, a channel rebalancing network is formed in which each node has a channel rebalancing mini-network centered on itself, and the channel balancing degree in the mini-network is set by the central node as a way to limit the payment behavior of each node and keep the channel within a certain balancing degree.

For the nodes in the off-chain payment channel network that want to participate in the channel rebalancing network, they need to submit the channel information that they have created. After receiving the channel information from the node, the channel rebalancing network creates a rebalancing channel information table centered on the node. All nodes in the channel rebalancing network that meet the channel rebalancing requirements need to execute the channel rebalancing operation unconditionally. In the design, the following points are considered:

1) Information security, the distribution of funds of the nodes in the channel is not leaked.

2) Capital protection, no loss of node funds during rebalancing operation.

3) No impact on the normal trading activities of the nodes.

According to the above requirements, this paper divides the rebalancing scheme into three modules,channel screening, rebalancing execution and channel clearing. The scheme principle is shown in Figure 2.

Channel Screening Module: Screen the channels in the rebalancing channel information table that needs to adjust the fund distribution and calculate the funds needed to rebalance the channel.

Rebalancing execution module: According to the rebalancing funds calculated by the channel screening module, rebalancing transfers are executed on the corresponding channels.

Channel clearing module: When a node leaves the channel rebalancing network, in order to ensure that the nodes in the network do not lose funds in the rebalancing process, it can leave only after clearing the channel debt relationship connected with the node, at which time the

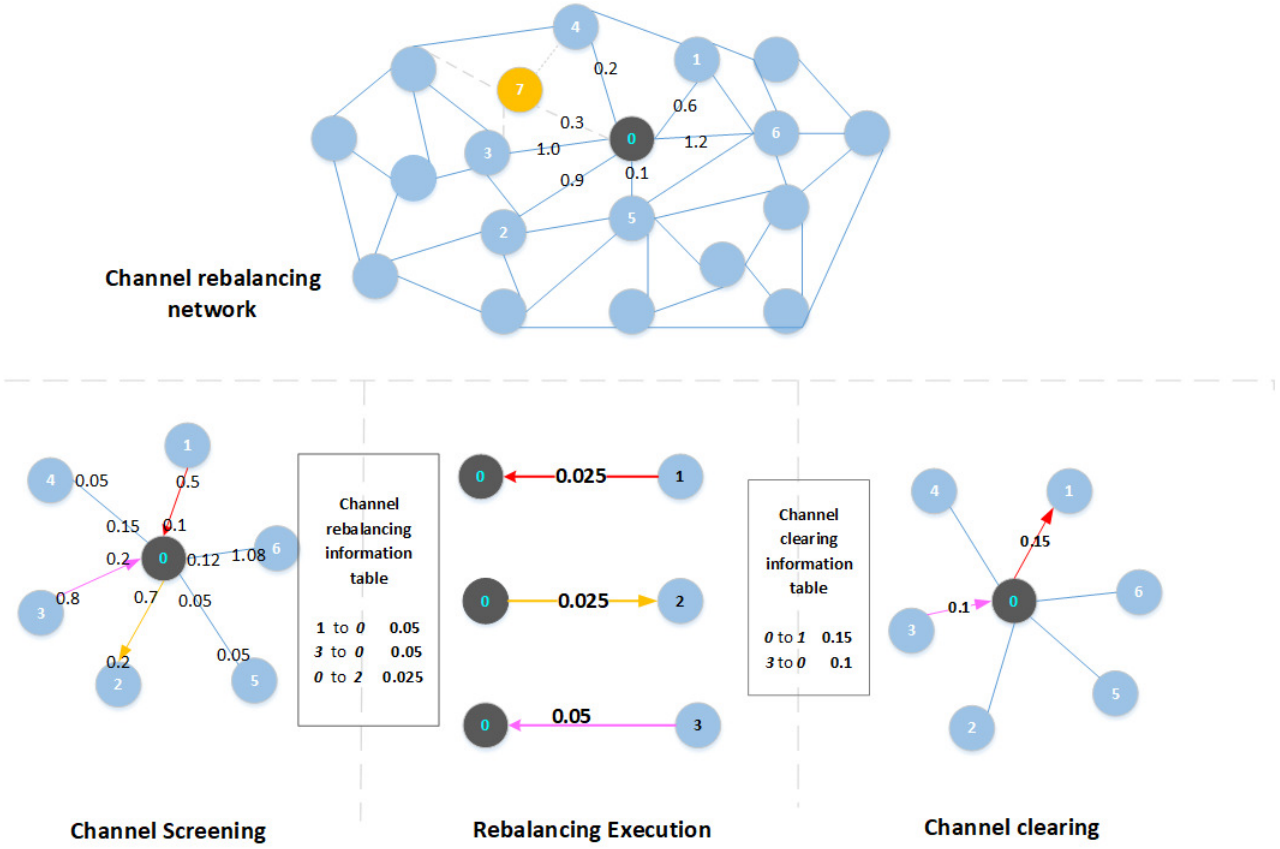

Figure 2: Channel rebalancing scheme diagram

network automatically clears the information of the leaving node and the channel information connected with the node.

Considering that cross-channel rebalancing may affect the trading activities of nodes, the design is such that each node only actively regulates the payment channel it creates and places the execution of rebalancing in idle time when the node has no trading activities. In this way, cross-channel rebalancing will not be involved, and due to the immediacy of the transaction of the created channel, it will not affect the normal transaction activities of nodes.

Nodes that want to participate in the channel rebalancing network, before entering the network, have to submit their own channel information form. Considering the information security, the information provided only includes the addresses and channel capacity of nodes at both ends of established channels that are publicly in the payment channel network. Taking node *0* in 2 as an example, the submitted channel information is shown in Table 1.

After receiving the node channel information, compare the node information of the channel rebalancing network and create a node-centered rebalancing channel information table, which contains the node addresses and fund distribution at both ends of the channel, and the table is only stored at the central node, which is not involved in the channel fund distribution leakage problem because it is established about the channel information table created

Table 1: Node *0* channel information table

Node1	Node2	Capacity
0	1	0.6
0	2	0.9
0	3	1.0
0	4	0.2
0	5	0.1
0	6	1.2
0	7	0.3

by the central node. For example, according to Table 1 submitted by node *0*, after comparing with the nodes in the network, it is found that node *7* is not involved in the channel rebalancing network, so the rebalancing information created for node *0* is shown in Table 2.

4.2 Detailed Design

4.2.1 Model Definition

We represent the channel rebalancing network as a digraph $G^{'} = \left(V^{'}, E^{'}\right)$ where $V^{'} = \{v_1, v_2, v_3, ...v_n\}$ is the set of nodes in $G^{'}$, $e^{'}_{i,j} \in E^{'} = \left\{(v_i, v_j) \,|v_i, v_j \in V^{'}\right\}$

Table 2: Node 0 channel information table

Node1	Node2	Balance1	Balance2	Capacity
0	1	0.1	0.5	0.6
0	2	0.7	0.2	0.9
0	3	0.2	0.8	1.0
0	4	0.15	0.05	0.2
0	5	0.05	0.05	0.1
0	6	0.12	1.08	1.2

is the set of edges in $E^{'}$. Take any node i in $V^{'}$, We define the small network formed by the central node i as a directed graph $G_N^i = \left(V_N^i, E_N^i\right)$, where $V_N^i = \left\{v_{N_1}, v_{N_2}, v_{N_3}, ...v_{N_k|k\leq n}\right\}$ is the set of nodes in $G_N^{'}$, $e_{N_{i,j}}^i \in E_N^i = \left\{\left(v_{N_i}, v_{N_j}\right)|v_{N_i}, v_{N_j} \in V_N^i\right\}$ is the set of channel edges in G_N^i. The funds deposited by nodes i and j when creating a channel are denoted as b_{N_i} and b_{N_j}, and the channel capacity is denoted as $c_{N_{i,j}}$, we have:

$$c_{N_{i,j}} = b_{N_i} + b_{N_j} \tag{1}$$

For the channel $e_{N_{i,j}}^i$, we define the imbalance degree of the channel as $b_{i,j}^{im}$:

$$b_{i,j}^{im} = \frac{|b_{N_i} - b_{N_j}|}{c_{N_{i,j}}} \qquad b_{i,j}^{im} \in (0,1) \tag{2}$$

In Formula (2), when $b_{N_i} = b_{N_j}$, we have $b_{i,j}^{im} = 0$, then equation (2) is also equivalent to:

$$\frac{b_{N_i}}{c_{N_{i,j}}} = \frac{b_{N_j}}{c_{N_{i,j}}} = 0.5 \tag{3}$$

Formula (3) indicates the most ideal channel equilibrium state, that is, the same funds at both ends of the channel, but it is difficult to achieve this situation in the real network, so we set a changeable value $b_{i,j}^{im^{'}}$ to indicate the difference between the channel imbalance degree acceptable to the central node and the optimal balance degree *0.5* in the small network formed by the central node, the value is set by the central node V_{N_i}. That is, the channel unbalance that the central node refuses to accept. The funds of the node i will remain within the variation δ_1 and δ_2, node i funding will meet $b_{N_i} \in (\delta_1, \delta_2)$, there are:

$$\left\{\begin{array}{l} \delta_1 = c_{N_{i,j}} * \left(0.5 - b_{i,j}^{im^{'}}\right) \\ \delta_2 = c_{N_{i,j}} * \left(0.5 + b_{i,j}^{im^{'}}\right) \end{array}\right\} \tag{4}$$

The channel selection algorithm will be designed based on the funding requirements of node i in Formula (4).

4.2.2 Model Implementation

The channel selection module is implemented by FindRebalancingChannel(FRC) algorithm, which is used to find out the imbalanced channel in $G_N^i = \left(V_N^i, E_N^i\right)$ and calculate the funds required for the channel rebalancing. The algorithm pseudo-code is shown in Algorithm 1.

Algorithm 1 FRC

Input: $ReInfor = ReChannelInformlist$, $b_{i,j}^{im^{'}}$
1: $OPB = 0.5$
2: **for** $c_{N_{i,j}}$ in *ReInfor* **do**
3: $\delta_1 = c_{N_{i,j}} * (OPB - b_{i,j}^{im^{'}})$
4: $\delta_2 = c_{N_{i,j}} * (OPB - b_{i,j}^{im^{'}})$
5: **end for**
6: **for** b_{N_i} in *ReInfor* **do**
7: **if** $b_{N_i} < \delta_1$ **then**
8: $ReBalance = b_{N_i} - \delta_1$
9: **end if**
10: **if** $b_{N_i} > \delta_2$ **then**
11: $ReBalance = b_{N_i} - \delta_2$
12: **end if**
13: **end for**
Output: $C\_id, ReBalance$

Algorithm 1 is based on the acceptable imbalance value $b_{i,j}^{im^{'}}$ rejected by the central node to calculate the capital balance range $[\delta_1, \delta_2]$ of all channels centered on this node. If the funds at the end of the central node i are not in the range, the channel is picked out. The calculated rebalancing fund *ReBalance*, a positive value, indicates the the channel imbalance is caused by the higher-end funds of the central node i than the j end funds. At this time, the channel imbalance needs to be solved by transferring funds from i end to the j end. A negative value indicates that the channel imbalance is caused by higher funds at the node j end is higher than the central node i, and the imbalance needs to be resolved by transferring funds from j end to the i end.

In Rebalancing execution module, perform rebalancing transfer on the selected unbalanced channel. Before rebalancing transfer, set up fund detection to ensure that the node funds at both ends of the channel are not lost. The Rebalancing contract designed in this paper is shown in Algorithm 2.

In Algorithm 2, the transfer direction is judged first. A positive *ReBalance* value indicates that the transfer direction is from the node i to j, which means that the node i is helping the node j to balance the channel they have established by borrowing, and then checking whether the node j has the ability to repay, which is shown in the contract as *ReBalance*$<b_{N_j}$ the rebalancing transfer can only be performed if the contract is, otherwise, the rebalancing fails. Similarly when *ReBalance* is negative, to perform a rebalancing transfer, it is necessary to satisfy *ReBalance*$<b_{N_i}$. In this module, it is also necessary to record the *ReBalance* of each rebalancing transfer in each channel, which is used for the liquidation of the next module.

In Channel clearing module, before a node leaves the

Algorithm 2 Rebalancing

Input: $b_{N_i} = getBalance\,(account_i)$
$b_{N_j} = getBalance\,(account_j)$
int[] $ClearBalance = [0]$
if $ReBalance > 0$ **then**
  if $ReBalance < b_{N_j}$ **then**
    reTransfer($account_j$)
    pushContent($ReBalance$)
  end if
else
  if $|ReBalance| < b_{N_i}$ **then**
    reTransfer($account_i$)
    pushContent($ReBalance$)
  end if
end if
Output: $ClearBalance$

network, it must clear the debts of all channels connected to it. This capability is implemented through the CleanChannel contract shown in Algorithm 3.

Algorithm 3 CleanChannel

int $total = 0$
for $i = 0; i <$ ClearBalance.length; i++ **do**
  $total = total + ClearBalance[i]$
end for
if $total > 0$ **then**
  reTransfer($account_i$)
else
  reTransfer($account_j$)
end if

In Algorithm 3, the *ReBalance* of the channel's historical rebalancing transfer is first cleared, and the result is placed in *total*. The positive or negative value of *total* indicates the direction of debt repayment, and the positive values indicate that in the rebalancing prosess with the help of the nodes i of mutual funds is more than node j, then the node j needs to repay the excess fund of node i. Similarly, a negative value of *total* means that the node i needs to repay the excess funds from the node j. Based on the positive and negative values of *total*, the repayment transfer is then executed.

5 Experiments and Analysis of Results

5.1 Validating the FRC Algorithm

5.1.1 Experimental Design

This experiment collectes the channel capacity created at a node named bfx-lnd1 in LN at some point on March 2, 2023, and its frequency distribution is shown in Figure 3.

Figure 3 shows that the channel capacity created by this node is mostly distributed within *0* to *2* BTC, with

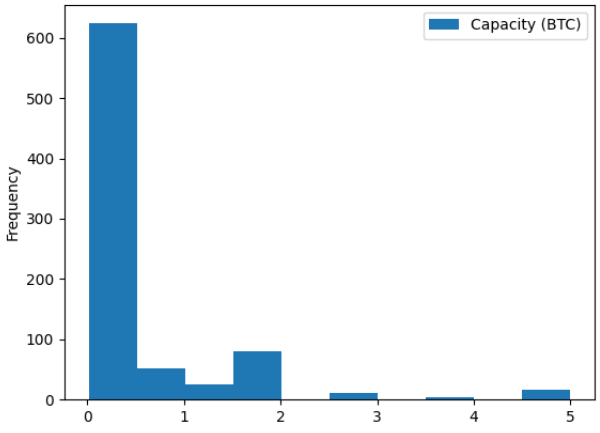

Figure 3: Channel capacity created by bfx-lnd1 nodes

only a few channels exceeding *2* BTC. In the channel capacity shown in the figure above, this paper randomly selected *100* channel capacities to participate in the channel rebalancing network of this scheme. Since the fund distribution at both ends of the channel is not available in the network, for the distribution of funds at both ends of the channel, this paper generates the channel rebalancing network by taking a random number in *0* and $c_{N_{i,j}}$, and the two ends of the funds satisfy the following condition.

$$\left\{ \begin{array}{l} b_{N_i} \quad | \quad b_{N_i} \in [0, c_{N_{i,j}}] \\ b_{N_j} + b_{N_j} = c_{N_{i,j}} \end{array} \right\} \tag{5}$$

The fund distribution at both ends of the *100* channels generated by the above method is shown in Figure 4.

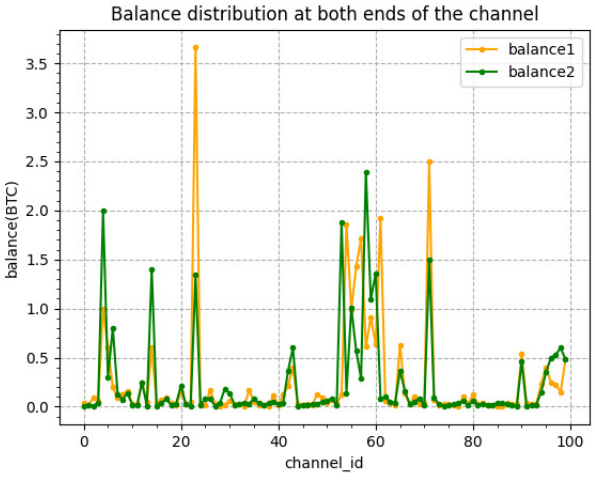

Figure 4: Distribution of funds at both ends of the channel

Figure 4 shows that among the *100* channels, most channels have channel imbalance problems, and among

the unbalanced channels, there are extremely unbalanced channels. But there are a few channels where the distribution of funds relatively balanced. Following that, the channel imbalance $b_{i,j}^{im}$ of the *100* channels selected above is calculated, and their distributions are shown in Figure 5.

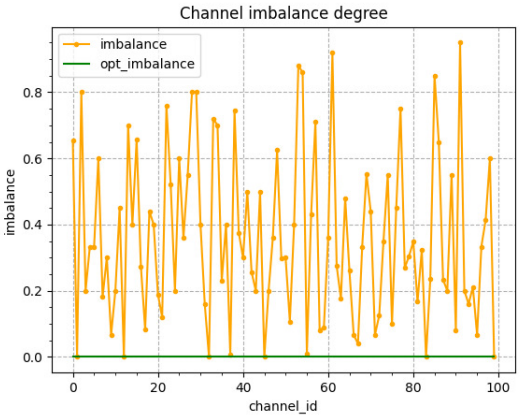

Figure 5: Channel imbalance degree

The green line in Figure 5 shows the optimal balance of *0.5*, and the yellow line shows the imbalance $b_{i,j}^{im'}$ of the channel. As can be seen from Figure 5, most channels deviate from the optimal balance, and the number of channels included in different balance levels is different. For the FRC algorithm mentioned in Section 4.2.2, we make the following analysis:

1) The smaller the $b_{i,j}^{im'}$, the more channels need to be rebalanced. The reason is that most channels will meet the channel balance requirements set by the central node V_{N_i} with the fund range of the node (δ_1, δ_2) increasing.

2) As $b_{i,j}^{im'}$ increases, the gap between the average paying capacity of channels and that of channels before the implementation of the rebalancing scheme will narrow. This is because the (δ_1, δ_2) shrinks with $b_{i,j}^{im'}$ increasing, indicating that the central node has a higher requirement on the balance degree of channels in the network, and at this time, only a few channels participate in the rebalancing scheme. Therefore, the average paying capacity of channels in a small network composed of central nodes will not increase significantly.

According to the above analysis, we need to perform the FRC algorithm under different $b_{i,j}^{im'}$. To measure the number of channels that can perform rebalancing operations and the average payment capacity of channels in the small network composed of central nodes.

5.1.2 Results Analysis

In this paper, we implement the FRC algorithm in Python language and measure the span of *0.005* as $b_{i,j}^{im'} \in [0.00,0.50]$, within the different $b_{i,j}^{im'}$ under the execution of the FRC algorithm, the number of channels that can perform rebalancing operations is collected from volume and the average channel payment capacity in a small network composed of central nodes, and the results are shown in Figure 5 and Figure 6 respectively.

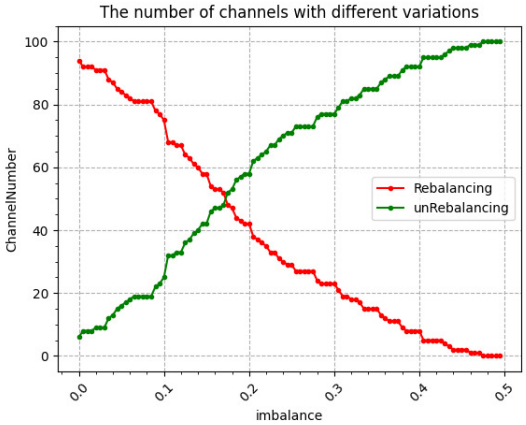

Figure 6: Number of channels

In Figure 6, the red dash indicates the number of channels that can be adjusted by the rebalancing scheme under a certain imbalance degree that the central node refuses to accept. As can be seen from the trend of Figure 6, with the increase of imbalance degree, the number of adjustable channels is decreasing. The green dash line indicates the number of channels which cannot be adjusted by rebalancing scheme under a certain imbalance degree, and their number shows an upward trend with the increase of imbalance. Notably, at the same imbalance, there is $unRebalancing + Rebalancing = 100$.

In Figure 7, the blue broken line represents the average payment capacity of channels in a small network composed of central nodes after the execution of a rebalancing scheme in an imbalance degree. The average payment capacity of channels in the network decreases with the increase of imbalance. The yellow broken line represents the average paying capacity of channels when no rebalancing operation scheme is executedin a imbalance. As can be seen from Figure 7, with the increase of imbalance, the gap between them decreases obviously. When imbalance increases to a certain extent, the two broken lines actually coincide. In this case, it means that the rebalancing scheme loses its rebalancing ability, so the central node should avoid this critical value when choosing an acceptable imbalance degree imbalance. In this experiment, the critical value is equal to *0.475*.

Through the above experiments, the rationality of 5.1.1 analysis on FRC algorithmis proved, and the effectiveness

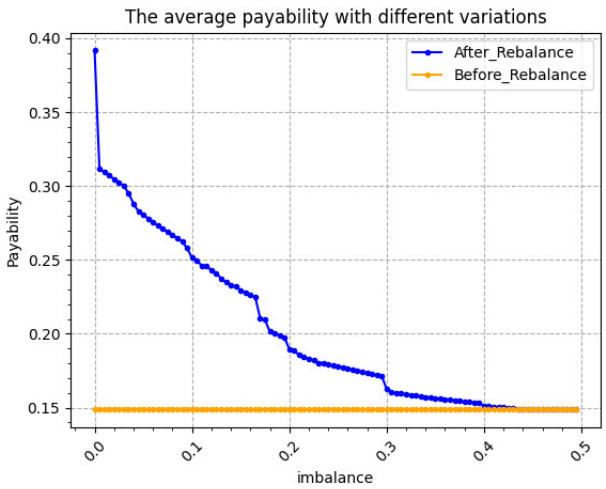

Figure 7: Channel Average Payment Capacity

of FRC algorithm in improving channel balance degree is verified.

5.2 Validating Smart Contracts

5.2.1 Experimental Design

This paper implements the Rebalancing and CleanChannel contracts on Remix, the official open-source online integrated development environment of Ethereum. For the Rebalancing contract, the functional requirements are verified by testing the Rebalancing greater than 0 and less than 0 mentioned in 4.2.2, as shown in Table 3.

The CleanChannel contract needs to calculate the sum of the Rebalancing values recorded by the Rebalancing contract, and realize the repayment operation in the corresponding *ReBalance* account according to the positive and negative values. Its test table is shown in Table 4.

5.2.2 Results Analysis

According to the Rebalancing and CleanChannel contract testing requirements in 5.2.1, the *ReBalance* values shown in Table were set in this paper, and the test results are shown in Table 5.

Let *ReBalance = 100,000,000,000,000,000,000* sat, in Table 5, the first judgment rebalancing transfer direction is b_{N_i} to b_{N_j}, and then determine b_{N_i} whether there is the ability to repay, because the b_{N_i} account balance is *999,999,999,999,993,876,17* sat, less than *100,000,000,000,000,000,000* sat, so it is not executed the b_{N_i} transfers *100,000,000,000,000,000,000* sat to b_{N_j}. When *ReBalance = -200* sat, the first judgment rebalancing transfer direction is b_{N_j} to b_{N_i} transfer *200* sat, and then check b_{N_i} whether there is the ability to repay, and since the b_{N_i} balance at this time is *999,999,999,999,965,105,60* sat, which is completely greater than *200* sat, so the execution of b_{N_j} to b_{N_i} transfer *200* sat, the b_{N_i} balance is *999,999,999,999,965,107,60* sat after transfer b_{N_i}. The analysis of the above results shows that the Rebalancing contract is designed to meet the requirements for rebalancing under certain conditions.

According to the rebalancing values recorded in Rebalancing contract, CleanChannel contract is executed, and the measured funds at both ends of the channel are shown in Table 6.

In Table 6, after the two rebalancing transfers in Table 5, the clearing yields *total = -100* sat, indicating that during the rebalancing b_{N_i} has made use of an extra b_{N_j} *100* sat, at this time, the b_{N_j} balance is *999,999,999,999,989,998,06* sat, and after receiving *100* sat from b_{N_i}, the b_{N_j} balance is *999,999,999,999,989,999,06* sat. The successful transfer from b_{N_i} to b_{N_j} indicates that the CleanChannel contract we designed implements channel clearing function.

In Tables 5 and 6, the data highlighted in red indicate that the experimental values do not match the theoretical values. We find that the experimental values are lower than the theoretical values in red-marked data. The reason for this deviation is that when the contract is deployed on the Remix platform, the platform automatically adds the cost of executing the contract, and the cost is spent by the account where the contract is deployed, so when the account executes the contract, the balance of the account will be lower than the value of balance before the account is spent minus the spent funds. Taking *ReBalance = 100* sat in Table 5 as an example when b_{N_i} paying *100* sat to b_{N_j}, the b_{N_i} balance should be *999,999,999,999,937,279,64* sat, but it is only *999,999,999,999,937,233,52* sat, and the decrease *416,2* sat is used as a fee for the execution of this contract.

5.3 Solution Scalability Verification

In order to verify the scalability of the scheme, *1500* channels in LN were randomly selected for experiments. First, the average channel unbalance degree of these channels is calculated, and the calculated result is *0.0977*. Then, with a span of *0.02*, $b_{i,j}^{im'} \in [0.00, 0.10]$, we measured the change of the average paying capacity of channels in the small network formed by the central node as the number of channels increases, and then calculate the increasing multiple of the average paying capacity of channels after using different schemes. The experimental results are shown in Figures 8 and 9.

In Figure 8, different colors of broken lines represent different $b_{i,j}^{im'}$ values, the virtual broken line represents the average channel payment ability before the implementation of the plan, and the solid line represents the average channel payment ability after the implementation of the plan.The results show that: under the same $b_{i,j}^{im'}$, the average paying capacity of channels is significantly improved after the implementation of the scheme, and the increasing trend is not affected by the number of channels, which indicates that the scheme has good scalability. Under dif-

Table 3: Rebalancing Contract test table

Rebalancing transfer direction	**Rebalancing transfer, conditions**	b_{N_i} **theoretical value**	b_{N_j} **theoretical value**
$ReBalance>0$	$ReBalance<b_{N_j}$	$b_{N_i} - ReBalance$	$b_{N_j} + ReBalance$
	$ReBalance>b_{N_j}$	b_{N_i}	b_{N_j}
$ReBalance<0$	$\|ReBalance\|>b_{N_i}$	b_{N_i}	b_{N_j}
	$\|ReBalance\|<b_{N_i}$	$b_{N_i} + ReBalance$	$b_{N_j} - ReBalance$

Table 4: CleanChannel contract test table

Channel clearing value	**Reimbursement, direction**	b_{N_i} **theoretical value**	b_{N_j} **theoretical value**
$total$	$total>0$	$b_{N_i} + total$	$b_{N_j} - total$
	$total<0$	$b_{N_i} - total$	$b_{N_j} + total$

Table 5: Rebalancing contract execution after both ends of the channel funding table

***ReBalance*(sat)**	b_{N_i}, **(sat)**	b_{N_j} **(sat)**	$\mathbf{1}b_{N_i}$ **(sat)**	$\mathbf{1}b_{N_j}$ **(sat)**	$\mathbf{1}b_{N_i}$ **theoreti. value (sat)**	$1b_{N_j}$ **theoreti. value (sat)**
100	*999,999, 999,999, 937,280, 64*	*999,999, 999,999, 993,875, 17*	*999,999, 999,999, 937,233, 52*	*999,999, 999,999, 993,876, 17*	*999,999, 999,999, 937,279, 64*	*999,999, 999,999, 993,876,* 17
100,000,000,000,000,000,000,	*999,999, 999,999, 936,233, 52*	*999,999, 999,999, 993,876, 17*	*999,999, 999,999, 935,223, 52*	*999,999, 999,999, 993,876, 17*	*999,999, 999,999, 936,233, 52*	*999,999, 999,999, 993,876, 17*
-200	*999,999, 999,999, 965,105, 60*	*999,999, 999,999, 953,583, 80*	*999,999, 999,999, 965,107, 60*	*999,999, 999,999, 953,529, 80*	*999,999, 999,999, 965,107, 60*	*999,999, 999,999, 953,581, 80*
-100,000,000,000,000,000,009	*999,999, 999,999, 996,510, 60*	*999,999, 999,999, 952,529, 60*	*999,999, 999,999, 996,510, 60*	*999,999, 999,999, 951,529, 60*	*999,999, 999,999, 996,510, 60*	*999,999, 999,999, 952,529, 60*

Table 6: CleanChannel contract execution after both ends of the channel funding table

***total*(sat)**	b_{N_i}, **(sat)**	b_{N_j} **(sat)**	$\mathbf{1}b_{N_i}$ **(sat)**	$\mathbf{1}b_{N_j}$ **(sat)**	$\mathbf{1}b_{N_i}$ **theoretical value (sat)**	$\mathbf{1}b_{N_j}$ **theoretical value (sat)**
-100	*999,999, 999,999, 950,375, 11*	*999,999, 999,999, 989,998, 06*	*999,999, 999,999, 950,061, 23*	*999,999, 999,999, 989,999, 06*	*999,999, 999,999, 950,374, 11*	*999,999, 999,999, 989,999, 06*

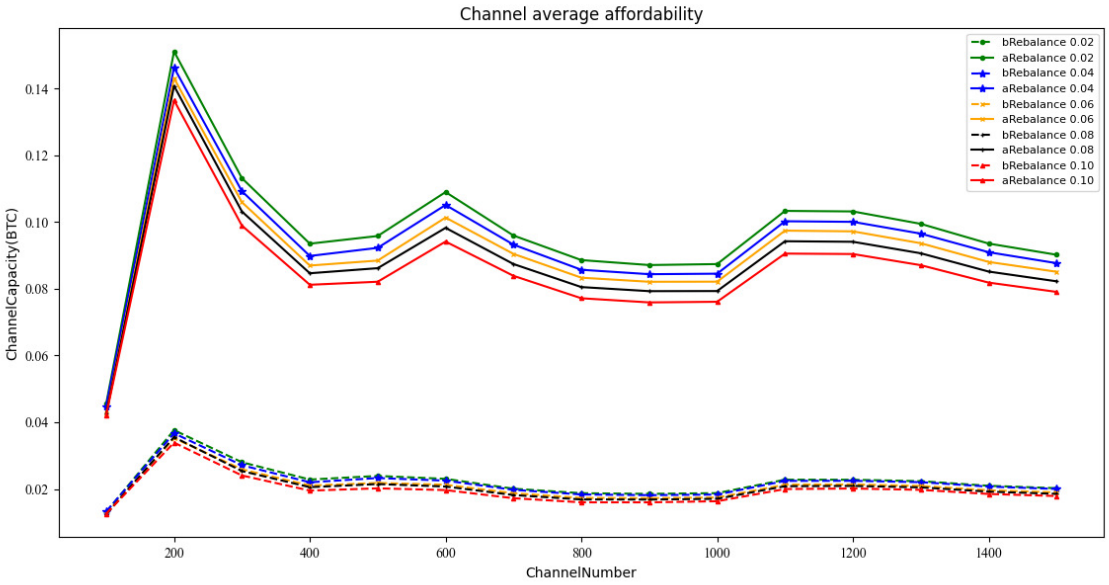

Figure 8: Channel average affordability

ferent scenarios, before and after the implementation of the scheme, there is a significant increase in the average payment capacity of the channel as $b_{i,j}^{im'}$ the average payment capacity of the channels decreases as the number of channels increases, the reason for this phenomenon is that as the $b_{i,j}^{im'}$, which is due to the fact as the number of channels increase, the central node's balancing requirements for the entire network increase, marking the rebalancing ability weaker and therefore the average payment capacity of the channel decreases. Several peaks in the graph casused by the relatively large initial funds at both ends of each newly added channel, and have no special meaning.

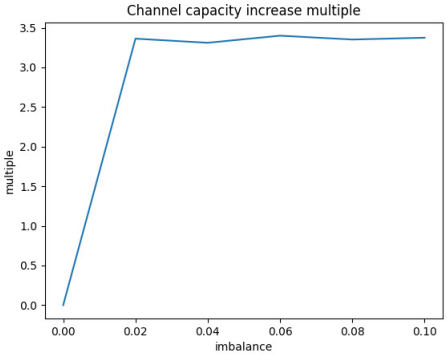

Figure 9: Channel capacity increase multiple

The broken line in Figure 9 shows the increase multiples of the average paying capacity of channels after using the scheme compared with before using it under different $b_{i,j}^{im'}$. As can be seen from the figure, the increase multiples are basically stable between 3 and 3.5 times, indicating that the scheme has a significant effect on improving the average paying capacity of channels.

6 Conclusions

Aiming at the channel imbalance problem in the off-chain payment channel network, this paper proposes an off-chain payment channel Rebalancing scheme controlled by the central node, and designs the channel selection algorithm FRC, smart contract rebalancing and CleanChannel to implement the scheme. The main contributions of this paper are as follows:

1) Through the hierarchical use of node and channel information, not only protects the privacy of nodes and channels, but also ensures the integrity of information required by the central node when rebalancing channels.

2) Channel selection algorithm FRC, so that the nodes in the off-chain payment channel network can flexibly adjust the fund distribution of the fund needs, so as to improve the channel balance.

3) Rebalancing contract is proposed, which realizes the rebalancing operation and avoids the risk of the node losing funds by checking the fund balance at both ends of the channel.

4) The designed CleanChannel contract fully guarantees that the funds of nodes will not be lost in the rebal-

ancing process, and further guarantees the reliability of the rebalancing scheme.

The "off-chain payment channel rebalancing scheme controlled by central node" not noly reduces the cost of node rebalancing channel, but also improves the flexibility and durability of the payment channel. The scheme will hopefully be applied to lightning Network, Raiden Network, Celer Network, etc, thus enabling the off chain payment channel network to provide reliable and efficient payment solutions in various scenarios such as real-time payment, high-frequency trading, micropayment, micropayment and Internet of Things payment, and to promote innovation and development in the payment field.

However, when setting the channel imbalance degree $b_{i,j}^{im'}$ rejected by the central node, the scheme does not consider the difference in the demand for the balance degree of each channel in the small network composed of the central node, and lacks the dynamic analysis of the channel. In the future work, we will study the current mainstream off-chain payment channel network and design a more flexible one for the central node. In addition, the active protection of node channel fund information needs to be strengthened, and then we will create a stronger fortress for channel fund information through information access control, information encryption and other means.

Acknowledgments

This study was supported by the National Natural Science Foundation of China (No.61762059). The authors are also particularly grateful to the reviewers for their suggestions.

References

[1] Z. Guo, "Cryptanalysis of a certificateless conditional privacy-preserving authentication scheme for wireless body area networks," *International Journal of Electronics and Information Engineering*, vol. 11, no. 1, pp. 1–8, 2019.

[2] M. M. Nabi and F. Nabi, "Cybersecurity mechanism and user authentication security methods," *International Journal of Electronics and Information Engineering*, vol. 14, no. 1, pp. 1–9, 2022.

[3] L. Liu and J. Cao, "Analysis of one lightweight authentication and key agreement scheme for internet of drones," *International Journal of Electronics and Information Engineering*, vol. 13, no. 4, pp. 142–148, 2021.

[4] P. Fan, Y. Liu, J. Zhu, X. Fan, and L. Wen, "Identity management security authentication based on blockchain technologies." *Int. J. Netw. Secur.*, vol. 21, no. 6, pp. 912–917, 2019.

[5] L. Xue, "The application of blockchain technology in the financial field," in *2021 International Conference on Forthcoming Networks and Sustainability in AIoT Era (FoNeS-AIoT)*. IEEE, 2021, pp. 130–134.

[6] T. Alam, "A survey on the use of blockchain for the internet of things," *International Journal of Electronics and Information Engineering*, vol. 13, no. 3, pp. 119–130, 2021.

[7] D. Sentausa and D. Habsara Hareva, "Decentralize application for storing personal health record using ethereum blockchain and interplanetary file system," in *2022 1st International Conference on Technology Innovation and Its Applications (ICTIIA)*, 2022, pp. 1–6.

[8] U. Cali, M. Kuzlu, S. N. Gupta Gourisetti, S. Mishra, M. Pasetti, C. Lima, T. Hughes, F. Rahimi, and P. Nitu, "Standardization efforts for blockchain in energy domain and power grid applications," in *2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain)*, 2022, pp. 1–6.

[9] J. Du, L. Li, X. Xiong, and Y. Zheng, "A blockchain covert communication method based on voting contract," in *2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA)*, 2023, pp. 1280–1282.

[10] N. Hamian, M. Bayat, M. R. Alaghband, Z. Hatefi, and S. M. Pournaghi, "Blockchain-based user re-enrollment for biometric authentication systems," *IJ of Electronics and Information Engineering*, vol. 14, no. 1, pp. 18–38, 2022.

[11] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari, and Y. Cao, "A survey on blockchain technology: Evolution, architecture and security," *Ieee Access*, vol. 9, pp. 61 048–61 073, 2021.

[12] R. Pickhardt and M. Nowostawski, "Imbalance measure and proactive channel rebalancing algorithm for the lightning network," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2020, pp. 1–5.

[13] R. Dennis and J. P. Disso, "An analysis into the scalability of bitcoin and ethereum," in *Third International Congress on Information and Communication Technology: ICICT 2018, London*. Springer, 2019, pp. 619–627.

[14] A. Gervais, "On the security, performance and privacy of proof of work blockchains," Ph.D. dissertation, ETH Zurich, 2016.

[15] S. Lin, Y. Kong, S. Nie, W. Xie, and J. Du, "Research on cross-chain technology of blockchain," in *2021 6th International Conference on Smart Grid and Electrical Automation (ICSGEA)*. IEEE, 2021, pp. 405–408.

[16] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. Gün Sirer *et al.*, "On scaling decentralized blockchains: (a position paper)," in *International conference on financial cryptography and data security*. Springer, 2016, pp. 106–125.

[17] P. Prihodko, S. Zhigulin, M. Sahno, A. Ostrovskiy, and O. Osuntokun, "Flare: An approach to routing in lightning network," *White Paper*, vol. 144, 2016.

[18] S. Mercan, E. Erdin, and K. Akkaya, "Improving transaction success rate in cryptocurrency payment channel networks," *Computer Communications*, vol. 166, pp. 196–207, 2021.

[19] L. M. Subramanian, G. Eswaraiah, and R. Vishwanathan, "Rebalancing in acyclic payment networks," in *2019 17th International Conference on Privacy, Security and Trust (PST)*. IEEE, 2019, pp. 1–5.

[20] E. Erdin, M. Cebe, K. Akkaya, S. Solak, E. Bulut, and S. Uluagac, "A bitcoin payment network with reduced transaction fees and confirmation times," *Computer Networks*, vol. 172, p. 107098, 2020.

[21] H. Xue, Q. Huang, and Y. Bao, "Epa-route: Routing payment channel network with high success rate and low payment fees," in *2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2021, pp. 227–237.

[22] G. Di Stasi, S. Avallone, R. Canonico, and G. Ventre, "Routing payments on the lightning network," in *2018 IEEE international conference on internet of things (IThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*. IEEE, 2018, pp. 1161–1170.

[23] R. Khalil and A. Gervais, "Revive: Rebalancing off-blockchain payment networks," in *Proceedings of the 2017 acm sigsac conference on computer and communications security*, 2017, pp. 439–453.

[24] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Hubs, rebalancing and service providers in the lightning network," *Ieee Access*, vol. 7, pp. 132 828–132 840, 2019.

[25] Z. Hong, S. Guo, R. Zhang, P. Li, Y. Zhan, and W. Chen, "Cycle: Sustainable off-chain payment channel network with asynchronous rebalancing," in *2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE, 2022, pp. 41–53.

[26] Z. Avarikioti, K. Pietrzak, I. Salem, S. Schmid, S. Tiwari, and M. Yeo, "Hide & seek: Privacy-preserving rebalancing on payment channel networks," in *Financial Cryptography and Data Security: 26th International Conference, FC 2022, Grenada, May 2–6, 2022, Revised Selected Papers*. Springer, 2022, pp. 358–373.

[27] I. A. Seres, L. Gulyás, D. A. Nagy, and P. Burcsi, "Topological analysis of bitcoin's lightning network," in *Mathematical Research for Blockchain Economy: 1st International Conference MARBLE 2019, Santorini, Greece*. Springer, 2020, pp. 1–12.

[28] Y. Guo, J. Tong, and C. Feng, "A measurement study of bitcoin lightning network," in *2019 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2019, pp. 202–211.

[29] P. Zabka, K.-T. Foerster, S. Schmid, and C. Decker, "Empirical evaluation of nodes and channels of the lightning network," *Pervasive and Mobile Computing*, vol. 83, p. 101584, 2022.

[30] A. Lisi, D. D. F. Maesa, P. Mori, and L. Ricci, "Lightnings over rose bouquets: an analysis of the topology of the bitcoin lightning network," in *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 2021, pp. 324–331.

[31] Y. Qin, Q. Hu, D. Yu, and X. Cheng, "Malice-aware transaction forwarding in payment channel networks," in *2021 IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*. IEEE, 2021, pp. 297–305.

[32] G. Malavolta, P. Moreno-Sanchez, A. Kate, M. Maffei, and S. Ravi, "Concurrency and privacy with payment-channel networks," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 455–471.

[33] S. Tripathy and S. K. Mohanty, "Mappcn: Multi-hop anonymous and privacy-preserving payment channel network," in *Financial Cryptography and Data Security: FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers*. Springer, 2020, pp. 481–495.

[34] S. Thakur and J. G. Breslin, "Collusion attack from hubs in the blockchain offline channel network," in *Mathematical Research for Blockchain Economy: 1st International Conference MARBLE 2019, Santorini, Greece*. Springer, 2020, pp. 31–44.

[35] C. Pérez-Sola, A. Ranchal-Pedrosa, J. Herrera-Joancomartí, G. Navarro-Arribas, and J. Garcia-Alfaro, "Lockdown: Balance availability attack against lightning network channels," in *Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24*. Springer, 2020, pp. 245–263.

[36] Q. Zhang, S. Cao, Y. Ni, T. Chen, and X. Zhang, "Enabling privacy-preserving off-chain payment via hybrid multi-hop mechanism," in *ICC 2022-IEEE International Conference on Communications*. IEEE, 2022, pp. 13–18.

[37] S. Mazumdar and S. Ruj, "Cryptomaze: Privacy-preserving splitting of off-chain payments," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 2, pp. 1060–1073, 2022.

Biography

Wei-Jun Gao received his Bachelor of Science degree from Lanzhou University in 1997 and his Master of Science degree from Chinese Academy of Sciences in 2000. He has been engaged in teaching and scientific research at Lanzhou University of Technology since 2000. His research interests include software engineering, distributed computing and cloud computing, big data processing, and

graphics and image processing.

Ya-Qian Yue received her B.S. degree in Network Engineering from Lanzhou Institute of Technology in 2021, and is now studying for her M.S. degree in School of Computer and Communication at Lanzhou University of Technology. Her main research interests are network and information security, and blockchain.

Xiao-Qin Wang received the B.S. degree in Network Engineering from Xinjiang Normal University in 2021, and is now a master's student in the School of Computer and Communication of Lanzhou University of Technology. Her main research interests are network and information security, blockchain.