Insights of Security Approach on Payment System using Blockchain

Chitra Kiran N (chitrakiran.n@alliance.edu.in)
Alliance University https://orcid.org/0000-0002-8691-1985

Research Article

Keywords: Blockchain, Bitcoin, Routing, Payment Channel Network

Posted Date: June 22nd, 2022

DOI: https://doi.org/10.21203/rs.3.rs-856357/v1

Abstract

Blockchain-based crypto currencies have recently attracted a lot of attention due to their potential uses in a variety of fields. One of these applications is the IoT area, which can use crypto currencies for micropayments without losing their payment privacy. However, the popularity of crypto currency-based micropayments is hampered by long transaction confirmation times and relatively high costs. Payment channel networks are one of the proposed methods to overcome these issues, in which nodes create payment channels without publishing to the blockchain. As long as IoT devices can sustain their overhead, they can benefit from such payment networks. When it comes to the routing difficulty, payment channel networks have their own set of characteristics. They should, in particular, maintain a balanced network in order to continue payments for extended periods of time, which is critical for IoT devices once they are installed. In this study, This paper offer a payment channel network design that uses a common weight strategy across the network to maintain the channels balanced. For unbalanced payment scenarios, we also recommend establishing multipoint connections to nodes for each IoT device. In comparison to the minimal fee approach, the experiment results suggest that keep the network channels more evenly balanced. Furthermore, various connections from IoT devices to the nodes enhance the success ratio significantly.

1 Introduction

The Internet of Things (IoT) has been used in a variety of fields, but its full potential has yet to be realized due to challenges such as scalability, security, privacy, connectivity, and so on. The commerce industry is another area where IoT devices are widely used. When a product or service is purchased (e.g., vehicle charging, parking payment, vending machine purchase, etc), IoT devices will need to send and receive payments at some point. Crypto currency-based payments [1] [2] provide a higher level of privacy and security for both parties by concealing the payee and payer identities, preventing fraud through the use of cryptographic techniques, and providing non-repudiation in the event of a dispute. A consensus method (e.g. Proof of Work, Proof of Stake, etc.) is used in Blockchain technology [3], which eliminates the need for a central authority to authorize and maintain records. The failure of a participant does not cause the system to collapse because the Blockchain ledger is irreversible and anybody can have a copy of it. It not only eliminates the problem of a single point of failure, but it also allows for secure transactions in an untrustworthy environment. The distributed structure of the Blockchain is the source of the strength it holds, which unfortunately becomes the point of weakness in scalability [4], [5] when it comes to increased number of users and payments. Bitcoin's design, in particular, renders it inherently time-consuming and slow. For example, adding a new block to the Bitcoin network takes about 10 minutes by design. Furthermore, the block size limit has an impact on performance. The number of transactions that may be completed in a given time frame is limited not only by these design characteristics, but also by hardware and bandwidth constraints. The theoretical maximum number of transactions per second is calculated to be 7 represents in the [6], which is far less than what Visa and MasterCard can process [7]. Furthermore, the transaction charge, which can skyrocket on busy days [8], is disproportionately high in

comparison to the amount being sent. As a result, hefty transaction fees and long block confirmation times are two major roadblocks to virtual currencies growing and becoming widely utilised for micropayments in everyday life. One of the solutions proposed to alleviate the difficulties of virtual currencies is a payment channel network (also known as off-chain networks) [9]–[11]. It makes use of the smartcontract concept to avoid having to write each transaction to the blockchain. Rather, transactions are carried out off-chain. Basically, once a channel is created between two parties, an infinite number of transactions can be performed in both directions as long as there are available funds. Furthermore, because building a channel is a time and money-intensive procedure, nodes in a payment channel network can send payments to any other node by paying a transaction fee to other existing nodes. This creates an overlay network to simulate the payment channel network, with the nodes' balances acting as links. The Lightning Network (LN) is a recent illustration of this notion, having grown to approximately 10,000 subscribers in less than two years [9]. This payment network has nodes which charge transaction fees to users passing their data over them. The PCN concept will open up new possibilities for users and enterprises in the IoT sphere. An automobile (light node) can, for example, make a payment by connecting to the LN through a full node in the hypothetical design shown in Fig. 1. Because the entire LN node maintains the LN protocol, this concept, which serves as the foundation for the startup company Breez [9], may be adapted to any use case. While establishing a payment channel network is a promising option for addressing the scalability issue of blockchain-based cryptocurrencies for micropayments, it comes with its own set of hurdles in terms of operational efficiency, management, and routing, among other things.

One of the most distinguishing features of these payment channel networks is the manner in which channel capacities are spent, which poses new issues in terms of channel balances during routing. For example, the most well-known application of this notion is LN [9], in which nodes are free to set transaction fees, which are used in conjunction with channel capacity to select sender-to-receiver paths. Obviously, consumers choose routes that have available capacity and charge the least amount of money. As a result of this collection, available funds in one direction may be depleted, resulting in a graph that is poorly connected or even unconnected (i.e., partitioned). As a result of unidirectional payments and a lack of awareness of imbalanced channels, non-conductive nodes emerge, reducing the overall efficiency of payment routing. For example, according to one of the most recent studies, the chance of sending a $5 payment in LN [9] is around 50%, which is unacceptable to consumers. Unfortunately, this issue has received little attention, as the focus has primarily been on routing techniques. In the long run, we believe that balance-aware routing can increase the overall network's stability and success ratio. In the long run, we believe that balance-aware routing can increase the overall network's stability and success ratio. We suggest the use of two unique strategies in this study to overcome the concerns with unbalanced routing in payment channel networks. First, rather than allowing users to choose their own channel weight policy; we adopt a common channel weight policy that all nodes can adapt. The term "weight" refers to a statistic based on channel balance that is employed in Dijkstra's algorithm to discover the cheapest way. Fundamentally, the goal is to encourage nodes to use high-balanced channels for payments and avoid low-balanced ones. This will make it easier to use the channels in a way that maintains available

balances in all directions. Second, in order to optimise the solution further, we recommend utilising various ingress points to the network from customers (i.e., IoT devices). In this approach, an IoT will be able to select the node from which to initiate a payment. Multiple access points will be beneficial, especially if the payment flow is skewed. These two elements will result in symmetrically balanced channels and increased payment channel network efficiency. We implemented and tested the proposed approach's effectiveness in a variety of payment circumstances, and found that the payment routes can be greatly balanced. The following is a breakdown of the paper's structure: Sect. 2 highlights previous research in the field, while Sect. 3 gives background information on payment network principles and our assumptions. The problem specification and our methodology are presented in Sect. 4. In Sect. 5, evaluate the suggested mechanism's performance. Finally, Sect. 6, concludes the entire research work.

2 Existing Work

Various payment channel network techniques have been proposed, and some are presently in use. In practice, the Lightning Network (LN) [9] for Bitcoin and Raiden [11] for Ethereum are two instances. With almost 10000 nodes and 30000 channels, LN is the most active. For sending payments in LN, source-routing is used. The transaction is started after a node finds a path with available channel capabilities. Spider [12] is a payment channel network that uses packet-switching routing algorithms. Micropayments are made in the same way that MTU is done in computer networks.It improves payment throughput by using congestion control and a best-effort methodology. It chooses the paths that equalise the channels specifically. Payments are queued at spider routers and sent as soon as funds become available. To effectively handle rapidly fluctuating balances, Wang et al. [13] uses a distributed routing method. It distinguishes between mouse and elephant payments. Small payments are distributed at random over pre-determined paths. It scans the nodes for large payments to discover the channel with available funds. The payment is then divided into numerous smaller parts. The work of Khalil et al. [14] assumes that a node has several connections, with some of the links being depleted as a result of the skewed payments. It seeks out network cycles, and a user sends a payment to her in order to rebalance the depleted channel through others. By employing an embedding-based routing algorithm, the study of Roos et al. [15] focuses on the anonymity of payments. Malavolta et al. [16] presents landmark routing, which stores routing tables for the whole network in only a few nodes. Only one of the landmark nodes is known to the rest. The payment is sent to the gateway node, which takes care of the remainder. Our effort focuses on a path selection approach for selecting the best payment route so that the overall network can be more sustainable (i.e., more transactions), while we leave the routing details to other projects. The work done by Dr. Chitra Kiran N [16] the book goes into great detail about the history and development of mobile payment systems. The author usually equates the word money with currency in the form of coins and banknotes. Cash is linked to money since it is a form of current asset that is utilised as legal tender and accepted as a payment reserve. Nonetheless, the fundamental meaning of money has evolved over time in terms of how it is perceived. In terms of inventions, bank deposits and banknotes, sometimes known as paper money, are relatively new. A study done is about E-payment system using various existing techniques by Dr. Chitra Kiran. N, Mr. Suhas Suresh, Mrs. Suchira Suresh [17], the main objective is to set-

up a roadmap for the E-payment mechanisms as well as their future opportunities. The work of Jerrin Yomas and Dr. Chitra Kiran [18] have examined all of the security vulnerabilities raised by mobile payment systems that do not provide secure customer verification during transactions. This study presents a hardware-based bidirectional secure payment system that employs biometric authentication at both the vendor and customer ends. This technology eliminates the need for physical cash in all transactions and handles the identity issues that arise with each transaction. The results indicate that the system satisfies all of the secure payment system's requirements and that the full transaction procedure takes less than 30 seconds to complete.

Dr. Chitra Kiran et al. [19] have presented a previous study that looked at the implications of a secure micropayment system that used process-oriented structural design in a mobile network. To provide reliable and secure offline transactions in mobile commerce, the prior system made extensive use of SPKI and hash chaining. However, the current study has attempted to build a new schema called Offline Secure Payment in Mobile Commerce in order to give a much lighter weight secure offline payment system in micro-payments (OSPM). The empirical tests are carried out on three different types of transaction processes, taking into account the most extreme scenario of real-time offline cases. Dr. Chitra Kiran et al. [20] have discussed the contextual applicability of modulation schemes, particularly OFDM and filtered OFDM (F-OFDM), in the context of 5G communications.

3 Preface And Assumptions

3.1 Block Chain and Bitcoin

A blockchain is a distributed database with a block-based data structure. A block in Bitcoin is made up of transactions (data), timestamps, nonces, the block's hash, and the previous block's hash [1]. The block chain’s consistency is ensured by the collaboration of honest nodes. The nodes in cryptocurrency-based networks reach a consensus for a transaction block by demonstrating that they have sufficient interest in the network. Proof of work is employed, for example, in the widely used Bitcoin Hashcash.

A miner node's basic technique is to load transaction requests into a block and then calculate the hash of that block. The final hash should be less than a figure that is determined based on the combined computational power of all miners. The miner seeks to find a suitable solution by adjusting the nonce value. When a block is discovered, it is immediately disseminated to the other nodes. The next block calculation begins when other nodes approve that block.

3.2 Off-Chain Payment Channels

The average time for a block to be approved in Bitcoin is roughly 10 minutes. The Bitcoin's utility and practicality are hampered by this time frame. Specifically, using Bitcoin for everyday spending has become nearly hard. The reason for this is that a payee, as a heuristic, counts a transaction as genuine after waiting at least 6 blocks.

To address this issue, developers devised the "off-chain payment channel" mechanism, which was inspired by the introduction of the smart contract mechanism to the blockchain. In such process, two users, say A and B, agree to start a business together. Then they sign a contract by transferring collateral to a shared 2-of-2 multisignature address and publishing it on the blockchain to start the channel. “Hash Time Locked Contracts” is the name of this contract type (HTLC). When the users reach an agreement on a payment amount, they create a new HTLC, exchange the new contract, and update the channel's status. A challenge, namely a pre-image 864, is delivered to the recipient to initiate a payment from a debtor. The contract becomes legitimate when the recipient successfully responds to the challenge, and ownership of the money is transferred. The off-chain approach has the significant benefit of removing the need for peers to post every transaction on the blockchain. The payments are theoretically instantaneous, in other words. Furthermore, because frequent on-chain transactions are not required, transactions will be shielded from unexpectedly high transaction costs.

The payment matter's direction is an important element of this type of channel. Two flows from opposite directions on the same link, for example, cancel out each other's capacity utilization. Figure 2 depicts this. A channel between two parties A and B is formed at Time = 0. Both A and B put 100 units of cash in the channel, bringing the total capacity to 200 units. The directed capacity from A to B will be zero after A completes two transactions of 50 units each. As a result, A will be unable to transfer funds until B returns the funds. B replies with 130 units, and when the channel is closed, they receive their shares from the multi-signature address.

3.3 Payment Channel Networks

The concept of an off-chain payment channel can be expanded to include a payment channel network. Assume that CH1 and CH 2 have a channel, and that CH 2 and CH 3 have a channel as well, as illustrated in Fig. 3. If A wishes to deal with CH 3 exclusively, he or she must hash-lock a set quantity of money and send it to CH 3 via CH 2. A CH 3 will obtain her/his money from CH 2 by exposing the answer because she/he already knows the answer to the challenge. The HTLC's genius is on display here. CH 2 discovers the answer to the challenge as CH 3 reveals it. CH 2 will now successfully respond to the challenge and receive her/his portion from CH 1. Through multi-hop payments, one can reach everyone in a network, building a payment channel network. Customers can connect to this payment network through any gateway. IoT devices can choose one or more gateways to open an off chain channel using wireless communication in our example.

3.4 Assumptions

In this study, a payment channel network is made up of nodes connected via off-chain payment channels. The quantity of money deposited in a 2-of-2 multi-signature address is represented by the channel capacity. Although each node can send and receive payment from any other node, we want to distinguish between consumers (IoT devices) and stores to replicate the circumstance when IoT devices

wish to utilise bitcoin for micropayments and the cash flow is primarily from a customer to a store for a service.

We base our work on an assumed current routing protocol that nodes use to broadcast weights to the rest of the network and transport a defined payment from a source to a destination. Our goal is to determine the spot to start the payment and find the most acceptable route, thus we aren't concerned with the routing protocol's efficiency or overhead. To calculate the path, each node is expected to have the whole topology.

4 Proposed Approach

The stimulation for our approaches is explained in this part, followed by a description of our solutions.

4.1 Issue Motivation and Overview

A payment starts at a node, travels through intermediary nodes, and finally arrives at its destination. The nodes function as either transit or end nodes. An endnode is a node that is the source or destination of payment, whereas a transit node is one that just transmits from one neighbour to another. Various issues may arise throughout this process, causing the payment to fail or causing transmission inefficiencies. In many IoT applications, where payments must be made in real time and the service must be available at all times, this is unacceptable. These issues are discussed separately below:

4.1.1 Problem: Highly Directional Payments

If a node sends payments in one direction on the same channel all of the time, the channel's balance in that direction will be decreased. It will cause a loose connection or disconnection in the network, which may result in: a) a group of nodes being disconnected from the rest of the network until the channel balance is increased, b) A1 node having to travel longer paths, and c) Two payments arriving at the same node at the same time not being transmitted due to a lack of available funds. In Fig. 4, for example, S1 is unable to send payment to A1. Users in today's payment networks typically calculate routes based on the optimum fee set by node owners. When it comes to determining fees, they are not bound by any rules. The user's ideal flow may differ from the system's ideal flow.

4.1.2 Problem: Overused Nodes

The second issue concerns the payment's source and receiver. When a store's outbound capacity is depleted, the node can no longer initiate payments or act as a transit node. Similarly, if a store has used up all of its incoming capacity, it will be unable to accept payment and serve as a transit node.

In Fig. 4 shows that IoT devices connected to S are unable to make payments via this node. They must wait for S to receive a payment that has been sent to it. S is unable to send money to A. D, on the other hand, is unable to receive any payment and must wait for any IoT device to send payment to D. C, like other circumstances, is unable to send payment to E. We can't control where the money goes, but we can

influence where it comes from to some level by utilising various connections from IoT devices to stores. A node that receives a large amount of payments should be used as the source, while a node with limited outgoing capacity should not be used to initiate payments. In 2018, an experiment on the success rate of transmitting transaction vs the amount sent in USD [21] yielded the data shown in Fig. 5. The average capacity per channel in LN was $20 at the time of the experiment. With a 90% success rate, even sending $1 is not guaranteed, according to the graph.

4.2 Problem Solutions

We now offer two solutions to address the aforementioned problems:

4.2.1 Proposed Solution 1: Balance-aware Routing

One of the most important factors for the success of the payment channel networks lies in keeping the channels balanced. We propose using a mandated weight calculation method which must be adopted by all the nodes in the network. Basically, each directed edge is assigned a weight inversely proportional to its current capacity. The route calculation will be based on this newly assigned weight. This will help keep the channels equally balanced in both ways and the overall network. Specifically, the weight of each channel is computed using the following equation by each node:

$W = (MC - C_o)^{2 \cdots}$ (Eq. 1)

Where W denotes a channel's weight, MC denotes the maximum permissible channel capacity defined centrally, and Co denotes the current outgoing channel balance. This new weight adjusts the balance based on the present situation. The node (user) then calculates the quickest path to transfer the requested payment using these freshly computed weights. It's worth noting that squaring the difference will result in a large gain or decrease in weight. As a result, this new weight will significantly encourage users to use channels with available balance while also assisting them in avoiding routing through channels with low balance. By routing all payments through high-balanced channels, the balance inequality problem, which is a critical component of successful payment network architecture, will be resolved.

4.2.2 Proposed Solution 2: Multi-connection:

IoT devices will be connected to several nodes in the payment network so that they can begin payments from a variety of locations. From all of these places, the path to the destination is computed, and the one that will contribute the most to network stability is chosen.

For example, in Fig. 6, the customer (IoT device) has two alternatives for initiating payment to C: 1) *path1* (which starts from A) and 2) path2 (which starts from D). After the route computation, the IoT device will choose *path2* according to our method. This choice will aid node A in preserving its limited outbound capacity (C_{AB}) and maintaining a balanced channel between A and B in both directions. It will also boost D's incoming capacity, CBD (due to payment delivered to B), and more evenly balance B and D's channels.

Algorithm 1 Route Calculation

Input: C=*Store connection list*, G=*Connected directed graph*
for every edge, e, in G **do**
    $G_e.weight$=$(MC\text{-}G_e.balance)^2$
end for *// weight calculations are done*
min = Integer.Max
for every *connection*, s in C **do** *// Calculate shortest path from each point*
    $Path$=$ShortestPath(G$, from=s, to=$d)$
    if $Path$ less than min **then**
        $min = Path$
    end if
end for
Output: min

Algorithm 1 presents the proposed route calculation in its entirety. Eq. 1 is used to calculate the weight for each link in the outgoing connections. Then, using Dijkstra's shortest path method, each node computes the shortest path to destination from its available connections depending on the link weight. To begin the payments, the lowest cost path is chosen from among these. In order to make payments, an IoT device chooses one of these nodes as a connection point. Based on the available amount of connections, our programme selects these connection locations at random.

5 Performance Assessment

As mentioned in this part, we conducted comprehensive tests to understand the influence of the suggested method on performance.

5.1 Experiment Setup

We created a Java simulator that allows us to perform the experiments and track the metrics. Table 1 lists the many parameters that must be set when executing the tests. We also go through how to deal with different configurations in depth. Configure the network: We assume that each IoT device is only connected to one store in the first set of studies. This enables us to assess the influence of a single weight strategy without the need for several linkages.

Table 1
Study Parameters

Number of Nodes	**100**
Node Degree	3
Intial Channel Capacity	50–150
Payment	5–15
Number of Payment	5000

The results are based on a 100-node random regular network, each with a degree of three. We employ the same network in the second phase, but each IoT device is supposed to have numerous connections to commence payment.

5.1.1 Files Containing Payments

We created 10 different balanced payment sequences, each with 5000 end-to-end transactions, for the first batch. The number of payments is spread evenly among the nodes. Each node transmits and receives 50 $5 to $15 transactions. As a result, total incoming and outgoing may not be equal, but they should be close because they are chosen at random. Node A sends to B but receives from C because the source and destination are not always the same. The second set of payment sequences is imbalanced, allowing us to explore the influence of several connections.

5.1.2 Payment transfer:

Each node calculates the path, and the payment is transferred by decrementing the amount from each channel utilized and incrementing in the opposite way through intermediary nodes.

5.1.2.1 Run the Experiment

The starting channel capacity and payment amount of each payment file are randomized using 100 distinct seeds. As a result, the results are an amalgamation of 1K randomized network experiments.

5.2 Performance Metrics

To evaluate the performance of the suggested strategy, we employ the following metrics:

- **Network Imbalance**: The divergence of channel balances from the general average is shown by this indicator. It's calculated as the average of each channel's difference from average capacity.
- **Path Length**: This is the total number of hops a payment has taken.
- **Network Diameter**: The number of hops between the two farthest nodes.
- **Success Ratio**: This measure indicates how many payments a node has successfully sent from a source to a destination.

For comparison, we created a random fixed weight policy in which the channel weights between nodes are set to a fixed value. These random weights are used to find the least expensive pathways.

5.3 Experiment Outcomes

5.3.1 Single Connection Experiments

A finding is perfom by experiment in which used a single connection from each IoT device to store and used a uniform weight scheme. The channel capacity distribution is shown in Figs. 7(a) and 7(b). The number of channels whose capacity is between x and x + 10 is represented by a bar. There are 300 directional channels, all of which were given an initial balance of 50 to 150 and are spread evenly.The distribution flattens when we apply random fixed weight. A large portion of the channels are unbalanced. A fifth of them go below 50, which was the lowest value in the initial configuration for a channel. The capacity of 25 channels is smaller than 20. The channel capacity distribution resembles a Gaussian distribution with a mean of 100 in the case of our suggested common weight policy, with 85 percent of the channels still in the initial range. There are only three channels with a balance of less than 20. This indicates that the network is more balanced. A fifth of them go below 50, which was the lowest value in the initial configuration for a channel. The capacity of 25 channels is smaller than 20. The channel capacity distribution resembles a Gaussian distribution with a mean of 100 in the case of our suggested common weight policy, with 85 percent of the channels still in the initial range. There are only three channels with a balance of less than 20. This indicates that the network is more balanced.

The network imbalance metric is used to more precisely assess and quantify the divergence. To accurately quantify the variance, we set all of the channels to 100. To visualise the change, we opted to utilise a timeline in the x-axis. The network imbalance is measured after every hundred payments. As seen in Fig. 7(c), it increases quickly in the first scenario, and then gradually increases in the second. The value is substantially lower in our approach, and the growth is gradual. It comes to an average distance of 18 miles. The channel capacities are clearly staying closer to the mean. It is perfomed additional testing to see if our strategy adds any burden to payment performance. The effect of payment path length and network diameter on network topology was explored. First, we determined how many hops each payment in the payment file must traverse. To amplify the results, we used a network of 1000 nodes for this experiment. The quantitative difference between the findings of the two approaches is not significant, as seen in Fig. 7(d). The patterns are similar as well. It rises over time before levelling off. This can be explained in the following way: Our solution employs longer paths at first because we force payments to transit over high-capacity channels, despite the fact that they are longer. The fixed weight technique benefits from shorter pathways at first, but at the expense of balance depletion. As a result, payments are spread out over longer periods of time at subsequent phases. The aforesaid discovery was validated later when we checked the average path length among all nodes in the network after all payments were sent to their destinations.

For varying quantities, Fig. 7 illustrates the average path length from each node to every other node in the network. It's worth noting that the path between two nodes may alter depending on the amount. Higher

amounts must take longer routes. Our method improves network connectivity, allowing us to transmit $50 from one location to another in one hop on average. The diameter of the network for various payment amounts is shown in Fig. 7. The use of a common weight results in a network that is more compact. Overall, there is no overhead and, in the long run, there is a gain.

5.3.2 Multiple Connection Experiments

The payments among the nodes are well distributed in the first batch of experiments, which indicates that the number of payments a node sends and gets is the same, even when the amount is picked at random within a specific range. This allowed us to observe the influence of weight policy without having to engage into discussions about success rates. I have conducted more trials in this part for IoT devices that have numerous connection points to retailers. I have created scenarios in which the funds transmitted and received for a given node are not allocated evenly. When payments are skewed, the quantity of incoming and outgoing payments for a node will not be equal, resulting in rejected payments due to channel depletion. To generate an imbalance between payments issued and received, we altered the disparity between them from 10–50%. If the difference is 10%, for example, the number of payments issued will be 10% higher or lower than the number of payments received. We put single (C1), double (C2), and triple (C3) connections through their paces (10 to 50).

As shown in Fig. 8(a), the success rate for single connections (C1) declines to 50%, whereas the success rate for triple connections hovers around 90%. (C3). Additional connections allow an IoT device to re-balance asymmetric channels and use an alternate route if one store is disconnected due to outgoing capacity erosion. Figure 8(b) depicts the average payment path length for each connection case. These findings suggest that multiconnections lower the overall number of hops a payment must travel. Figure 8(c) depicts the link between the success ratio and the initial capacity of channels when they were first built. The success ratio gets closer to one as the average capacity for the channels is increased from 100 to 300, especially when several connections are used.

6 Conclusion And Future Work

Cryptocurrency payment networks are a new and promising topic that needs more research to improve its efficiency and effectiveness. In this study, we suggest and analyse the use of a network-wide common weight policy for bitcoin payment networks, as well as redundant connections between IoT devices and businesses. By routing payments to high-capacity connections, the suggested solution tries to maintain the links in the payment channel network balanced. The results show that we can keep the network more evenly balanced and achieve a greater success rate even when payment flows are unbalanced.

References

1. J. Sidhu, "Syscoin: A peer-to-peer electronic cash system with blockchain-based services for e-business", *In 26th international conference on computer communication and networks (ICCCN),* pp. 1-6, 2017.

2. E. K-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: A secure, scale-out, decentralized ledger via sharding," *In IEEE Symposium on Security and Privacy (SP),* pp. 583-598, 2018.
3. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain technology: Beyond bitcoin”, *Applied Innovation*, vol. 2, pp.71, 2016
4. C. Berger, and H. P. Reiser, "Scaling Byzantine consensus: A broad analysis," *In Proceedings of the 2nd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers*, pp. 13-18, 2018.
5. W. Xin, T. Zhang, C. Hu, C. Tang, C. Liu, and Z. Chen, "On scaling and accelerating decentralized private blockchains," *In IEEE 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids)*, pp. 267-271, 2017.
6. T. Kim, "On the transaction cost of Bitcoin," *Finance Research Letters*, vol. 23, pp. 300-305, 2017
7. J.S. Bellagarda, "The potential effect off-chain instant payments will have on cryptocurrency scalability issues-The Lightning Network," *In CONF-IRM,* pp. 2, 2019.
8. K. Torpey, "Bitcoin Transaction Fees Are Pretty Low Right Now. Here's Why," *Bitcoin Magazine*, 2018
9. Y. Sompolinsky, and A. Zohar, "Accelerating bitcoin's transaction processing," *Fast money grows on trees, not chains*, 2013
10. F. Armknecht, G. O. Karame, A. Mandal, F. Youssef, and E. Zenner, "Ripple: Overview and outlook," *In International Conference on Trust and Trustworthy Computing* Springer, pp. 163-180, 2015.
11. U. Nisslmueller, K-T. Foerster, S. Schmid, and C. Decker, "Toward active and passive confidentiality attacks on cryptocurrency off-chain networks," *arXiv preprint arXiv: 2003.00003,* 2020
12. V. Sivaraman, S.B. Venkatakrishnan, M. Alizadeh, G. Fanti, and P. Viswanath, “Routing cryptocurrency with the spider network”, arXiv preprint arXiv:1809.05088, 2018
13. P. Wang, H. Xu, X. Jin, and T. Wang, “Flash: efficient dynamic routing for offchain networks”, *arXiv preprint arXiv:1902.05260,* 2019
14. R. Khalil, and A. Gervais, “Revive: Rebalancing off blockchain payment networks”, *In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security,* pp. 439-453, 2017
15. S. Roos, P. M-Sanchez, A. Kate, and I. Goldberg, “Settling payments fast and private: Efficient decentralized routing for path-based transactions”, *arXiv preprint arXiv:1709.05748*, 2017
16. C. Kiran N, “History, Evolution & Future of Mobile Payment System”, Book Chapter, retrieved on 29 July 2021
17. C. Kiran N, S. Suresh, S. Suresh, "Vulnerability, threats, and attacks in E-Payments System: Security Solutions." *International Journal of Psychosocial Rehabilitation,* vol. 24, no. 4, 2020
18. J. Yomas, and N. Chitra Kiran, "An Effective Hardware-Based Bidirectional Security Aware M-Payment System by Using Biometric Authentication", *In Computer Science On-line Conference, pp. 99-108. Springer, Cham,* 2019.

19. N. C. Kiran and G. N. Kumar, "Reliable OSPM schema for secure transaction using mobile agent in micropayment system," *Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT),* pp. 1-6, 2013,
20. K.P. Nagapushpa, and C. Kiran N, "Novel Optimized Filter Design for Filtered-OFDM to Enhance 5G Communication Spectral Efficiency," In Computer Science On-line Conference, pp. 11-20, Springer, Cham, 2019.
21. E. Erdin, M. Cebe, K. Akkaya, E. Bulut, and S. Uluagac, "A scalable private Bitcoin payment channel network with privacy guarantees," *Journal of Network and Computer Applications*, vol. 180, pp. 103021, 2021

Figures

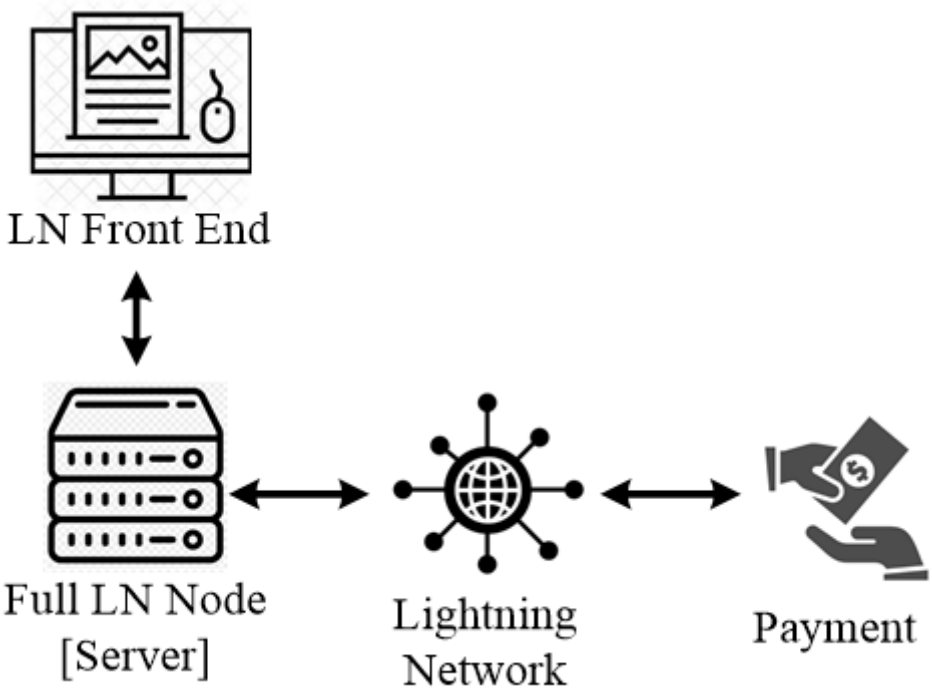

Figure 1

Proceeding the payment by IoT device in the LN

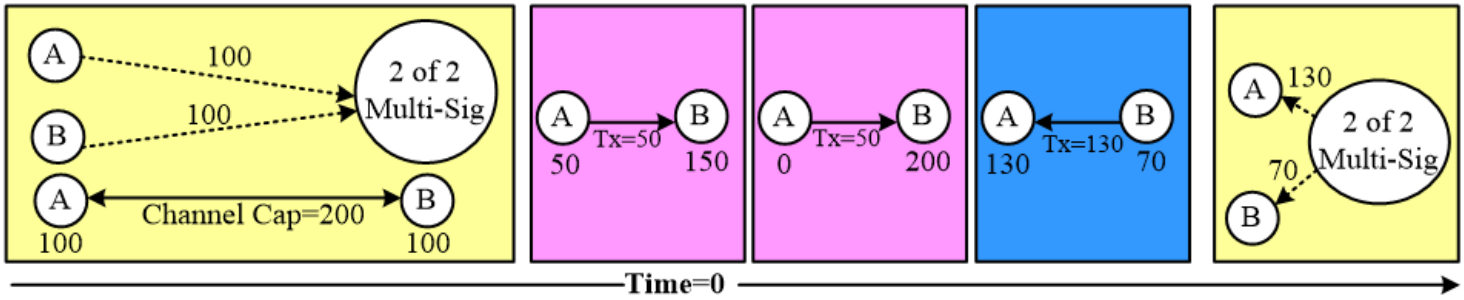

Figure 2

Demonstration of a payment channel

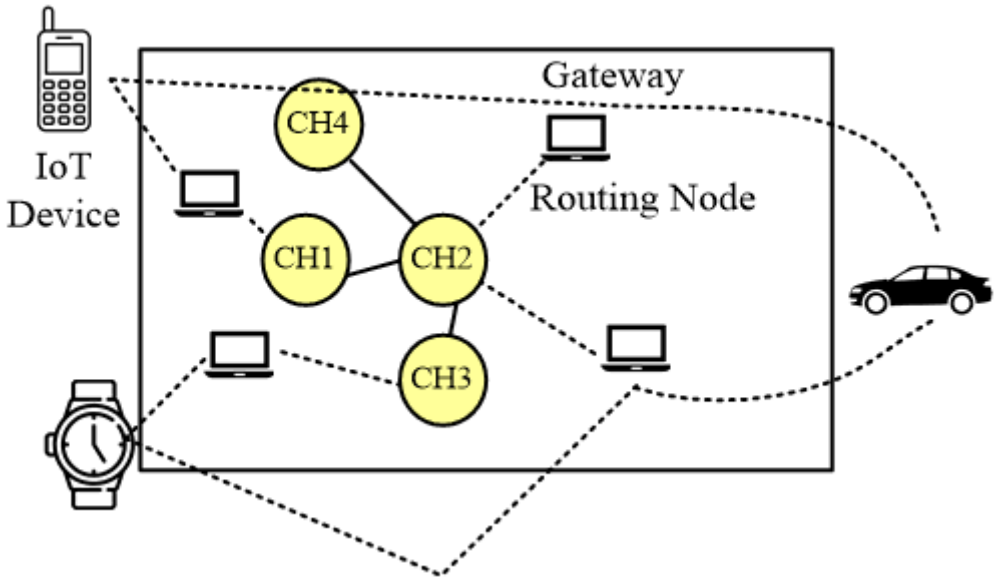

Figure 3

Payment channel network

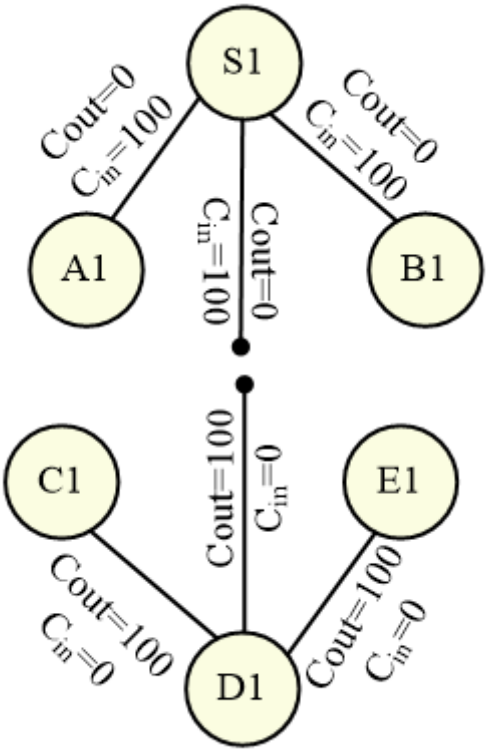

Figure 4

Exhausted channels causes detachment

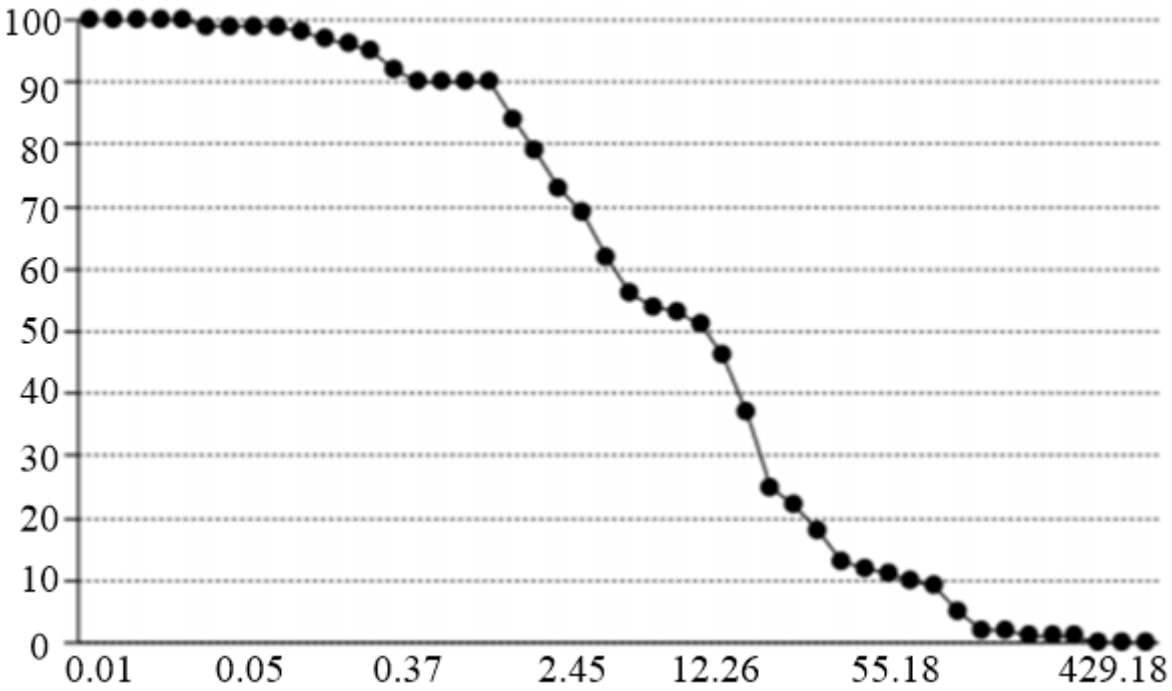

Figure 5

Success rate vs. Amount for the payment [21]

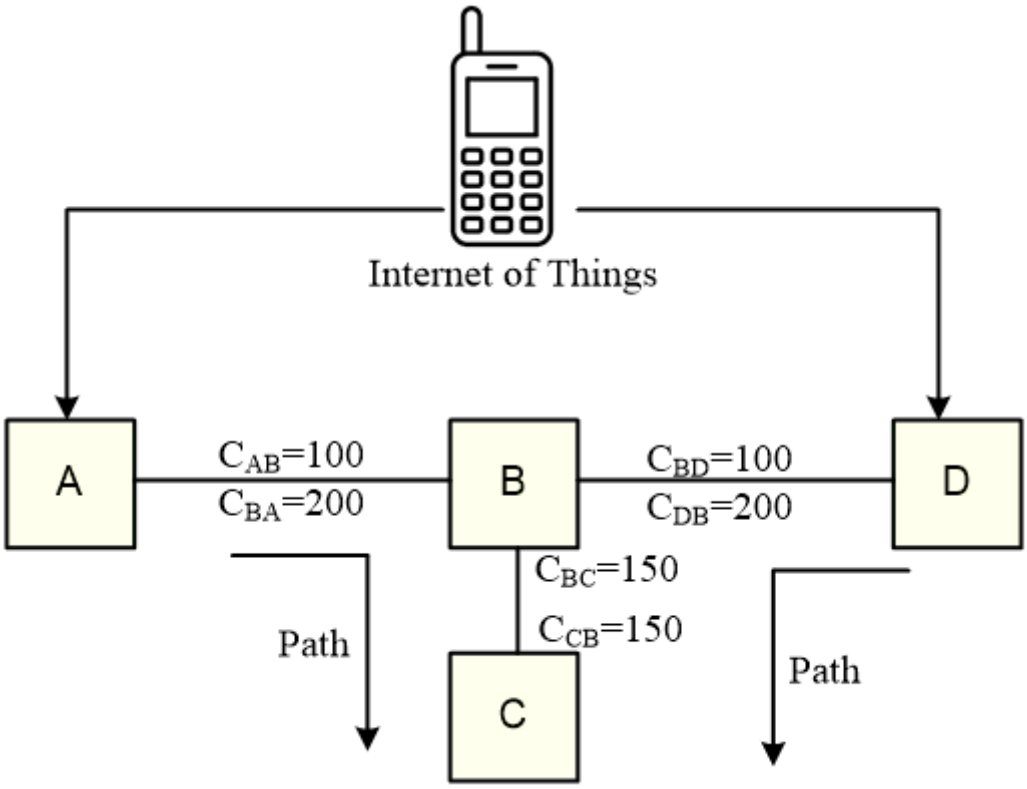

Figure 6

Multi-point connection establish with re-balancing

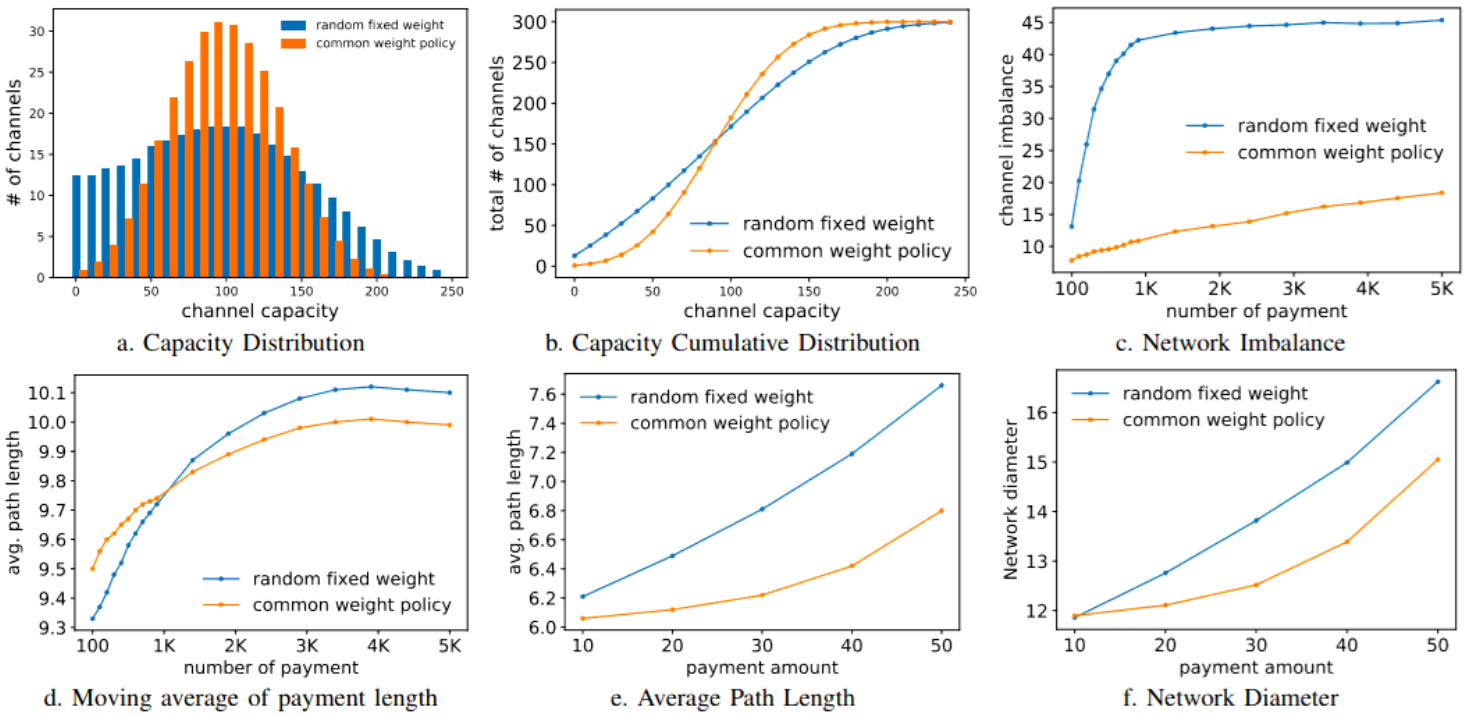

Figure 7

Results of common weight by single connection

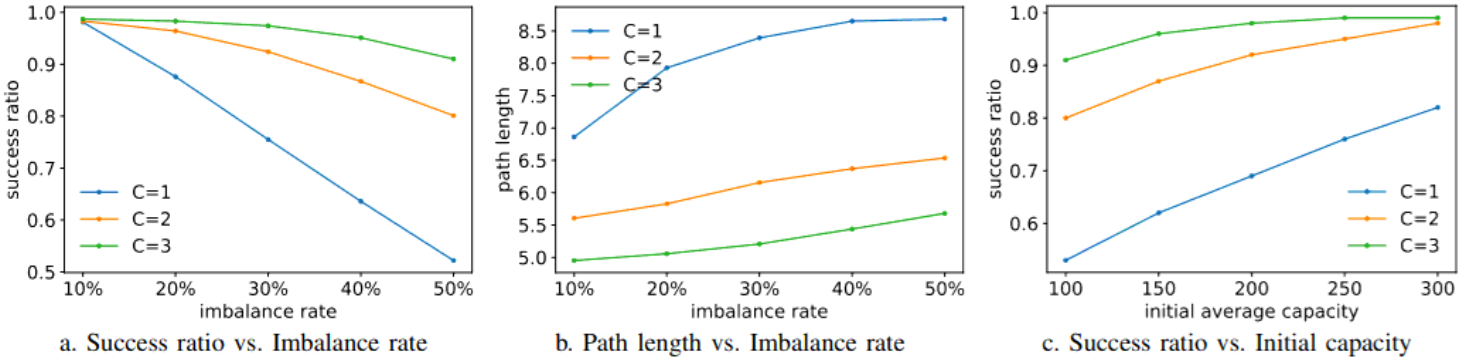

Figure 8

Outcomes of numerous connections