An Edge Colouring-based Collaborative Routing Protocol for Blockchain Offline Channels

Subhasis Thakur
National University of Ireland, Galway
Ireland
Email: subhasis.thakur@nuigalway.ie

John G. Breslin
National University of Ireland, Galway
Ireland
Email: john.breslin@nuigalway.ie

***Abstract*—A Path-based Fund Transfer (PBT) in blockchain offline channel networks or in credit networks, uses a path among the offline channels to transfer funds among the peers who do not have mutual channels. A routing algorithm for PBT finds a suitable path for PBT execution. The problems with the landmark-based routing algorithms for PBT executions are as follows: (1) PBTs through hubs may cause privacy problems as a few landmarks can collude to find the sender and the receiver of a PBT, (2) Landmarks can be targeted with DoS or Eclipse attack. Unavailability of landmarks will lead to a high failure rate of PBT and (3) the unavailability of nodes for PBT execution creates cuts in the trees maintained by landmark-based routing protocols, which will lead to failure of PBT execution. In this paper, we mitigate the above problems with routing algorithms for PBT execution with a graph edge colouring-based routing protocol. In this routing protocol, every peer maintains a set of small subgraphs of the channel network with a particular topology. The peers exchange such subgraph information to find an appropriate path for PBT execution. Our contributions are as follows: (1) We develop a distributed algorithm to find subgraphs maintained by a peer. We prove that despite sharing subgraph information, our protocol preserves the privacy of the sender and the receiver of a PBT. (2) We prove that the proposed protocol is secure against adversarial peers initially agrees to participate in PBT execution and included in the trees or subgraphs computed by landmark-based or our edge colour-based routing algorithm, but later they do not participate in PBT execution. (3) We show that trees built by landmark-based algorithms require more frequent rebuilding as values in individual channels are changed over time compared with subgraphs to be maintained by the peers. (4) We show that the success rate and time to execute PBT for the proposed edge colouring-based routing algorithm is competitive against the landmark-based routing algorithm. (5) We show that DoS attacks resulting unavailability of peers have less impact on the proposed routing algorithm compared with landmark-based routing algorithms.**

***Keywords*-Bitcoin Lightning Network; Offline Channels; Fund Transfer Protocols**

I. Introduction

Blockchain offline channels (such as the Lightning network of Bitcoin [1]) are designed to improve the scalability of blockchain. A payment network over offline channels allows path based fund transfer among peers who do not have mutual channels. A Path-based Fund Transfer (PBT) uses a path in the offline channel network to transfer funds between two peers without a mutual channel. In general, the sequence of steps to execute PBT is as follows:

1) The sender and receiver find a path in the channel network that connects them and which has sufficient funds in their channels to support the proposed PBT. The sender and the receiver probe the channel network to enquire if the peers in such a path are willing to participate in the PBT.
2) After confirming such as a path (by creating a sequence of contracts [1]), the sender and the receiver use Onion routing to propagate a key (Hash of a string) to execute these contracts sequentially to execute the PBT (The process is discussed in Section 3).

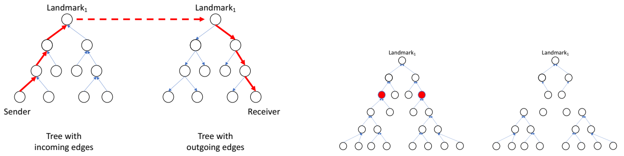
The state of art routing algorithms uses landmark-based routing algorithms. In such a routing algorithm a few landmark-nodes (nodes with high degree and willing to facilitate PBT execution may be in exchange for transfer fees) maintain and share rooted spanning trees (with the landmark as the root) over the network with other peers. The path for PBT execution is found in such a spanning tree. Although landmark-based routing [2], [3] can be efficient in terms of length of the path used in PBT execution, there are few problems as follows:

1) Landmark-based routing may cause privacy problems as a few landmarks can collude to find the sender and the receiver of a PBT. In a landmark-based routing, each landmark maintains two rooted trees with itself as the root, one tree with incoming edges and another tree with outgoing edges. In order to execute a PBT, the sender requests the theses two tree information from a landmark. It finds a path in such a tree from the sender to the root of the tree and another path from the root to the receiver. A combination of these two paths composes the path for PBT execution. The privacy concern for this type of routing is if the landmark knows the identity of the peer who has requested information on trees maintained by the landmark then, it can identify the path (at least partially) for the PBT execution. This is because in a tree there is a unique

978-0-7381-0495-9/20/$31.00 ©2020 IEEE
DOI 10.1109/Blockchain50366.2020.00050

path from each node to the root. Such identification of the PBT execution path can lead to censoring the PBT execution or altering PBT transfer fees as the PBT execution path can be anticipated.

2) Landmarks can be targeted with DoS or Eclipse attack. Unavailability of landmarks will lead to a high failure rate of PBTs. Further, the unavailability of nodes for PBT execution will lead to a high rate of failure in PBT execution. This is because unavailability node leads to cuts the trees built by the landmark.



(a) (b)

Figure 1: Landmark-based routing algorithms. [Left:] Privacy problem for landmark-based routing: The red coloured path shows a PBT execution path. Note that, each such paths are unique as a rooted tree is used in constructing it. The root (landmark) can at least know the path from the sender (or the receiver) to it as these paths are unique and either the sender or the receiver have requested tree information from it. [Right:] Landmarks can be targeted with DoS or Eclipse attack. Unavailability of landmarks will lead to a high failure rate of PBTs. Further, the unavailability of nodes for PBT execution will lead to a high rate of failure in PBT execution. This is because unavailability node leads to cuts the trees built by the landmark.

Routing with landmarks will lead to the creation of landmarks with a high degree. We have already seen the emergence of very high degree nodes in Bitcoin Lightning network. Such a centralisation of the offline channel network will further enhance these problems. In this paper, we mitigate the problem of finding a suitable path for PBT execution using a novel graph edge colouring-based PBT protocol. In this routing protocol, each peer finds and maintains a few small subgraphs of the channel network with a particular topology. The peers exchange such subgraph information to find an appropriate path for PBT execution. Our contributions are as follows:

1) Distributed algorithm (Algorithm 1): We develop distributed algorithm that a peer can use to find its local subgraph.
2) Privacy enhancement (Theorem 1): We prove that despite sharing subgraph information, our protocol preserves the privacy of the sender and the receiver of a PBT.
3) Resilience (section VI-D): We prove that the proposed protocol is secure against adversarial peers who become unavailable after the construction of the subgraphs by the peers. Unavailability of peers may a result on DoS attacks on them.
4) Performance (section VI-B): We prove that the proposed routing protocol is efficient (measured as the time for PBT execution and success rate) compared with state of art landmark-based routing protocols using Bitcoin Lightning network data.
5) Tree / subgraph update (section VI-C): We prove that trees built by landmark-based algorithms require more frequent rebuilding as values in individual channels are changed over time compared with subgraphs to be maintained by the peers.

The paper is organised as follows: in section 2 we discuss related literature, in section 3 we discuss the basics of PBT protocol for Bitcoin, in section 4 we present our PBT protocol, in section 5 we analyse the privacy-preserving property of the protocol, in section 6 we study Bitcoin Lightning network to evaluate performance of the proposed protocol and we conclude the paper in section 7.

II. Related literature

Bitcoin lightning network was proposed in [1] which allows peers to create and transfer funds among them without frequently updating the blockchain. Similar networks are proposed for Ethereum [4] and credit networks [2]. A routing algorithm for Bitcoin lightning network was proposed in [5]. [6] proposed a routing protocol that balances the network. It requires finding cycles in the channel network for fund transfers to keep the channels balanced. [7] investigated the eclipse attack on offline channel network. [8] proposed a protocol for balancing the channel network. [2] proposed a landmark-based routing protocol for fund transfer in the credit network. [3] enhanced the landmark-based routing algorithm developed in [2] by reducing the path length for PBT execution.

III. Routing in offline channel networks

The offline channel creation for Bitcoin was proposed in [1] as the Bitcoin Lightning network We will use the protocol for offline channel formation developed for Bitcoin Lightning network [1]). A PBT protocol for this offline channel network is as follows:

1) Say Alice wants to send fund to Carol via Bob.
2) Carol will create a lock and a key.
3) In the multi-signature address between Carol and Bob, a contract will be created as follows:
   a) Bob will send 5 tokens to this address.
   b) Bob will get these tokens back after 9 days if Carol does not claim it.
   c) Carol can claim it anytime if it can produce key to the lock.
4) Similarly, another contract will be created between Alice and Bob as follows:

   a) Alice will send 5 tokens to this address.
   b) Alice will get these tokens back after 10 days if Bob does not claim it.
   c) Bob can claim it anytime if it can produce key to the lock.

5) Thus Carol reveals the key to Bob as it collects the fund, which Bob uses to get refunded from Alice.

In this paper, we develop a routing protocol for the above mentioned PBT procedure. The protocol finds an appropriate path for PBT execution in a privacy preserving manner without help from any landmarks (high degree nodes).

IV. Collaborative Routing Protocol

A. Overview of the Protocol

A brief description of our proposed routing protocol is as follows:

Step 1: We will use edge coloring of the channels in an offline channel network for the routing purpose. We will use a special form of edge coloring called road-colouring. A road-colourable graph can be coloured in such a way that certain nodes can be assigned a unique sequence (synchronising word) of edge colors. One can reach any of these nodes by following its synchronising word. For example, if the synchronising word of a node is $Red, Blue, Red$ where edges of the graph are coloured with the colors Red and Blue then, by traveling edges as per the sequence $Red, Blue, Red, Red, Blue, Red, \ldots$ will eventually lead to this node. We will use such synchronising word for finding a path for PBT execution. Note that, a node can be reached from ANY other by following its synchronising word. Hence it creates ambiguity about the start location. We will use this ambiguity to hide the identity of the sender and the receiver.

Step 2: Ideally, we would like to create one road-colourable graph for an arbitrary offline channel network. But a graph becomes a road-colourable graph only if it satisfies certain topological constraints. It is not possible that any arbitrary graph road-colourable. Hence we use multiple road-colorable graphs where each of them is isomorphic to a subgraph of the channel network. We use a sufficient number of such road-colourable graph to cover all nodes and edges of the offline channel network.

Step 3: Next, we introduce a concept of reachability from the synchronising word notion of road-colouring. Reachability in this context can be interpreted as the number of nodes which can be reached by following a specific synchronising word.

Step 4: Next, we formulate the routing problem as finding a path between the sender and the receiver using a synchronising word of the receiver. It happens that multiple nodes have the same synchronising word. Hence a route following a synchronising word can lead to any of a set of nodes with the same synchronising word. This is a desirable property as it creates the ambiguity to hide the identity of the receiver of a PBT.

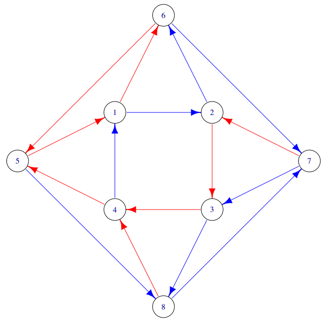


Figure 2: A road colourable graph with 8 nodes.

B. Road Coloring

Let H be a finite, directed, strongly-connected, even out-degree, and aperiodic graph. A directed graph is aperiodic if there is no integer > 1 which divides all cycles of the graph. The graph H admits synchronized colouring, i.e., there are certain nodes who can be assigned unique edge color sequence such that they can be reached by following edges with such a sequence irrespective of the starting location. Such an edge coloring sequence is called the synchronising word. The road-colouring conjecture was proposed in [9] and proved in [10]. In [11], [12] algorithm to compute the synchronising words for road-colourable graphs was investigated.

The set of synchronising words for the road colourable graph shown in Figure 2

1) Sequence for node 2 is $Blue \rightarrow Blue \rightarrow Red$, $Blue \rightarrow Blue \rightarrow Red$, $Blue \rightarrow Blue \rightarrow Red$.
2) Sequence for node 7 is $Red \rightarrow Blue \rightarrow Blue$, $Red \rightarrow Blue \rightarrow Blue$, $Red \rightarrow Blue \rightarrow Blue$.
3) Sequence for node 8 is $Red \rightarrow Red \rightarrow Blue$, $Red \rightarrow Red \rightarrow Blue$, $Red \rightarrow Red \rightarrow Blue$.

Road-colourable graphs are a good fit for automating the path finding problem as we can use the synchronising word of a node to find a path that leads to this node. Further, this can hide the source location as by starting at any node will lead to this node. But the constraints on the structural properties(aperiodic, even out-degree, strongly connected) makes it difficult to convert any arbitrary graph into a road-colourable graph. Hence we will use multiple road-colorable graphs to cover a channel network where each graph is isomorphic to a subgraph of the channel network.

C. Cover by Road-colorable graphs

Let $G = (V, E)$ be the offline channel network with n nodes V and m edges E. $H = (N, L)$ be a road colourable graph with a set of nodes N and set of edges L. $\theta(n_i) \cup \emptyset$ be the synchronising word for the node n_i. Θ be the set of all non-empty synchronising word for the road-colourable

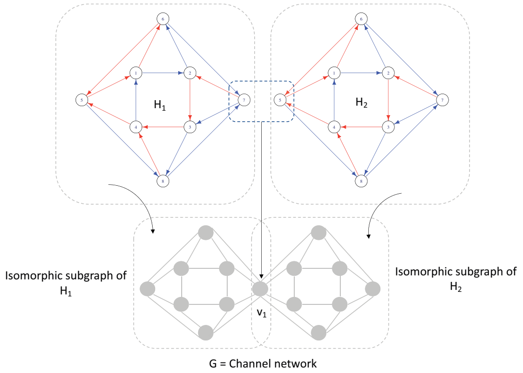


Figure 3: Reachability in the road-colourable graph cover is defined using the common nodes between every pair of road-colourable graph.

graph H. $|\Theta| \leq |N|$, i.e., not every node in H has a synchronising word. $\mathbb{H} = \cup_{i=1}^{k} H_i(N_i, L_i)$ be a collection of road-colourable graphs.

Definition 1. *$\mathbb{H}$ is a cover of the channel network G if the following holds:*

- *For every graph $H_i \in \mathbb{H}$, there is an isomorphic subgraph $G_i = (V_i, E_i)$ of G. Let $f(H_i)$ be the isomorphic map from H_i to G_i.*
- *The set of all isomorphic sub-graphs $\{G_i\}$ covers G, i.e., $\cup_{i=1}^{k} f(N_i) = V, \cup_{i=1}^{k} f(L_i) = E$.*
- *It is possible that $f(N_i) \cap f(N_j) \neq \emptyset$ and $f(L_i) \cap f(L_j) \neq \emptyset$, i.e., the isomorphic subgraphs overlaps.*

Definition 2. *$\mathbb{H}$ is the minimum cover of the channel network G if it is cover of G as defined Definition 1 and the number of road-colourable graphs in the set $\mathbb{H}$ is the minimum.*

D. Reachability

Note that, in order to cover all nodes and edges of a channel network, there are overlaps among isomorphic subgraphs of the channel network corresponding to the set of graph $\mathbb{H}$. We define the concept of connecting nodes among the graphs in the set $\mathbb{H}$.

Definition 3. *$\mathbb{H}$ be a cover of the channel network G with the isomorphism map f. The set of nodes $N^* \in \cup_{i=1}^{k} N_i$ will be called the connecting nodes if for every $n_x \in N^*$ there is a at least one another node $n_y \in N^*$ such that $f(n_x) = f(n_y)$. $C(H_i \in \mathbb{H}) \subset N_i$ be the set of connecting nodes for the graph H_i.*

Reachability can be expressed with the above-defined concept of connecting nodes and synchronising words of the connecting nodes. As shown in Figure 3 road-colourable graph $H_1, H_2 \in \mathbb{H}$ overlapped for the node v_1 in the channel network. The connecting node is 7 for the graph H_1 and 5 for the graph H_2. Both nodes correspond to the node v_1 in the channel network. But node 7 has a synchronising word while the node in 5 does not have a synchronising word. Hence certain nodes can be reached from H_1 to H_2 by following the synchronising word for the node 7. In this case, any node in H_1 can reach node 7 in H_1 by following the synchronising word of node 7 and then, the same sequence will lead to node 7 in H_2. But the similar traversal is not possible from H_2 to H_1 because the node 5 in H_2 has no synchronising word. Hence there is no sequence to reach it from a node in H_2 and travel to H_1.

Definition 4. *$\mathbb{H}$ be a cover of the channel network G with the isomorphism map f and set of connecting nodes $N^* \in \cup_{i=1}^{k} N_i$. The connected subset $\mathbb{H}^{\theta_i}$ for the synchronising word θ_i is a subset of the graphs in the set $\mathbb{H}$ such that the following holds:*

- *for every graph $H_x \in \mathbb{H}^{\theta_i}$ there another graph $H_y \in \mathbb{H}^{\theta_i}$ such that $f(C(H_x)) \cap f(C(H_y)) \neq \emptyset$, i.e., there is at least one node in the channel network which corresponds to both graphs H_x and H_y. Say such nodes are $v_x \in V_x$ and $v_y \in V_y$.*
- *The synchronising word for both v_x and v_y is the same and not $\emptyset$.*

Definition 5. *$\mathbb{H}$ be a cover of the channel network G with the isomorphism map f, set of connecting nodes $N^* \in \cup_{i=1}^{k} N_i$ and the connected subsets $\{\mathbb{H}^{\theta_i}\}$ for all synchronising words in the set Θ. $\mathbb{H}$ will be called a δ reachable cover if all connected subsets $\{\mathbb{H}^{\theta_i}\}$ has at least δ graphs from the set $\mathbb{H}$ and the following holds:*

- *Let M be a directed graph created from $\mathbb{H}^{\theta_i}$ where for each $H_i \in \mathbb{H}^{\theta_i}$ we create a node and for each connecting node in $\mathbb{H}^{\theta_i}$ we create either an unidirectional or bidirectional edge depending on the synchronising word of the connecting node for both graphs in $\mathbb{H}^{\theta_i}$ (as shown in figure 4).*
- *It is required that M be a weakly connected graph.*

E. Finding a local road-colorable graph

Peers will volunteer to construct the cover by a set of road-colorable graphs as discussed in the previous section. Each peer will create at least one road-colorable subgraph and broadcast this graph information to all peers.

A peer will use Algorithm 1 to find a road-colorable graph in its close proximity in the channel network. In such road-colorable subgraph each peer will be represented by a node in a road-colorable graph with a syncronizing word. For example, the road-colorable graph used in this paper has 3 nodes with syncnronizing words. In algorithm 1, each creator of the road-colorable graph is given the node 2. Algorithm 1 first first finds a cycle graph from 1 → 2 → 3 → 4 then it sequentially adds nodes $5, 6, 7, 8$. Note that finding road colarable is an NP-hard problem [10]. But algorithm 1 efficiently generates a road-coloarable graph with 8 nodes. In this paper, we will use road-colorable graphs of size 8. Hence high time complexity of finding road-colorable graphs is not an obstacle to use it in the routing algorithm 1. It is as follows:

- A peer v_i finds a subgraph similar to the road-colorable graph shown in figure 3 where it is the node labeled as ‘2’.
- v_i first forms the subgraph with nodes labelled as ‘1’, ‘6’ , ‘3’, and ‘7’. It does so by choosing a random subset of its neighbours ($N(v_i)$).
- Next, it sequentially adds the remaining nodes labelled as ‘4’, ‘5’ and ‘8’.

Algorithm 1: Road-colorable subgraph finding lgo-rithm

```
Data: $P2P = (V, E)$ as the channel network, $v_i$ is
      the peer who creates the road-colorable
      subgraph
Result: $Ret$ a $1 \times 8$ matrix as the set nodes of the
        road-colorable for $v_i$
begin
    $v2 = v_i$, $n1 = N(v2)$, $ret = [-1 \times 8]$,
      $ret[2] = v2$
    for $i \in [1 : Max\_Attempts]$ do
        if $-1 \in ret$ then
            $n2 = sample(n1, 4)$, $v1 = n2[1]$,
              $v6 = n2[2]$, $v7 = n2[3]$, $v3 = n2[4]$
            if $v6 \in N(v1)$ & $-1 \in ret$ &
              $v7 \in N(v6)$ & $v3 \in N(v7)$ then
                $v5\_set = N(v1) \cap N(v6)$,
                $v8\_set = N(v3) \cap N(v7)$,
                $v4\_set = N(v1) \cap N(v3)$
                if $|v5\_set| > 0$ & $|v8\_set| > 0$ &
                  $|v4\_set > 0|$ then
                    for $j \in [1 : |v4\_set|]$ do
                        if $-1 \in ret$ then
                            $v4 = v4\_set[j]$,
                            $v4\_nei = N(v4\_set[j])$,
                            $v5' = v5\_set \cap v4\_nei$,
                            $v8' = v8\_set \cap v4\_nei$
                            if $|v5'| > 0$ & $v8' > 0$
                              then
                                for $k \in [1 : |v5'|]$ do
                                    $v5 = v5'[k]$,
                                    $nei\_v5 = N(v5)$,
                                    $v8'1 =$
                                      $nei\_v5 \cap v8'$
                                    if $|v8'1| > 0$ then
                                        $v8 = v8'1[1]$,
                                        $ret$ =
                                          [v1,v2,v3,v4,
                                        v5,v6,v7,v8]
                                        $Break$
```

F. PBT Execution Protocol

The PBT execution protocol for road-coloring routing is as follows:

1) Let v_a wants to transfer fund to v_b.
2) v_b forms a random string as key_1 and generate its Hash as H_1. It sends H_1 to v_a.
3) v_b informs v_a about the road-colorable graph where it is a node with synchronizing word. It also informs v_a about the synchornizing word (say θ_7).
4) v_a finds the set of road-colored graphs which are reachable for θ_7 and finds the path which connects v_a with v_b by following the sequence of edge colors mentioned in θ_7.
5) Let the path is $V_a \rightarrow v_1 \rightarrow v_2 \rightarrow v_3 \ldots v_k \rightarrow v_b$. Let sequence of colors is $\theta_=(”Red”, ”Blue, ”Blue”)$. Let all peers agrees to use key K_1 to encrypt information to be sent along edge colored $Blue$ and K_2 for the color ”Red”. Let E_1, E_2 are cliphertext generated by encryption with key K_1 and K_2 respectively.
6) Let $P_1, P_2, \ldots$ are cliphertext generated by encryption with public key of peers $v_1, v_2, \ldots$ respectively.
7) v_a initiates creation of sequence of Hashed Time Locked Contract similar to PBT protocol for Bitcoin Lightning network discussed in previous section. It informs v_1 the following message:

$$Msg_1 = P_1(\theta_7, P_1(E_1(P_2(E_2(P_3(E_3(\ldots)))))))$$

8) Msg_1 can be decrypted by v_1 using its private key. v_1 will create a HTLC with v_a where the lock is $P_1(E_1(P_2(E_2(P_3(E_3(\ldots))))))$. It will interprete that this sequence of HTLCs is guided by the edge coloring sequence θ_7. It will check the edge color of its edge with v_a and find the next color as ”Blue”. v_1 will send the following messgae to v_2 if it has an outgoing edge to v_2: $Msg_2 = P_2(\theta_7, P_2(E_2(P_3(E_3(\ldots)))))$
9) Similarly v_2 will decrypt the message with its private key and proceed with HTLC creation.
10) This process will continue till node v_k who will create a HTLC with v_b where the lock is H_1.

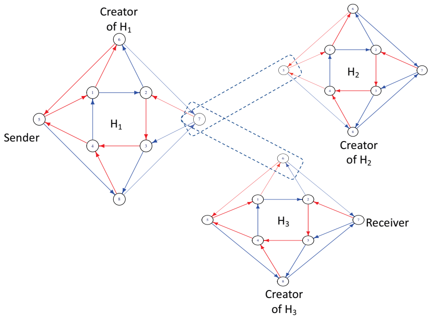


Figure 4: Example: It shows three road-colorable subgraphs, the sender and the receiver and a bridge node.

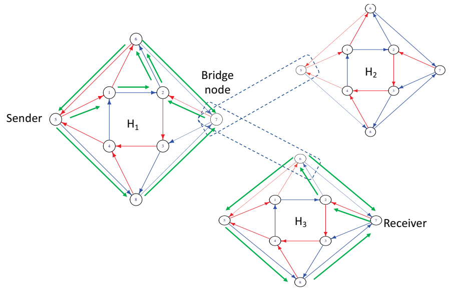


Figure 5: The path marked with green color shows the PBT execution path.

11) v_b will claim funds from the HTLC with v_k by providing Key_1 and sequence HTLCs will be executed as this key will travel to v_a.

V. Privacy of PBT execution

Theorem 1. *A set of adversarial peers whose road-colorable graphs are used in a PBT execution can not reveal the sender and the receiver information of the PBT.*

Proof: Consider the scenario illustrated in Figure 4, there are three road-coloring subgraphs created by peers. These peers broadcast information on these road-colorable graphs and all peers collect such information to build the reachability graphs. In this example, we show the reachability graph for the road coloring sequence of vertex 7. After building the reachability graph, the sender forms the path to the receiver using the edge coloring sequence for node 7. The sequence of colors is (Red, Blue, Blue, Red, Blue, Blue, Red, Blue, Blue). The path is shown in figure 5 with green color.

Let a set of adversarial peers wants to identify the sender and the receiver of a PBT. Let these adversarial nodes are part of a PBT execution, i.e., their road-colorable graphs are used in PBT execution path. These adversarial nodes can not identify the sender or the receiver because:

- All road-colorable subgraphs (H_1, H_2, H_3 in this example) are broadcasted. Hence the sender does not ask the creator of these road-colorable graphs for graph information. Hence creator of the road-colorable graphs does not know the identity of the sender. In a contrast, landmark-based routing (as shown in Figure 1) may know the identity of a sender or receiver as the sender or receiver ask a landmark for a path or sub-path.
- At a bridge node, in this example, the common node among H_1, H_2, H_3 will send PBT message to its neighbour in both H_2 and H_3. But the sender will encrypt the PBT information with its neighbour in H_3. Hence only the node in H_3 will be able to interpret the message. The advantage here is, the PBT can go to any subgraphs from the bridge node where the bridge node is a member. Hence it improves the privacy of the receiver as there are multiple nodes that can be reached with the color sequence for node 7.
- Finally, the adversarial nodes know the edge colour sequence of a PBT, but any node can use such a sequence for a PBT execution and multiple receivers may be reached by the same edge color sequence.

■

VI. Experimental Evaluation

A. Data and Experimental Setup

We use the Bitcoin Lightning network data [1] to analyze the proposed routing algorithm. [1] provided an API to access the Lightning network data. The downloaded data is in JSON format and the RJSONIO package was used to process the data. The data contains (a) information about each node, i.e., public key, and (b) network structure as the edge list. The data was accessed on 1st March 2019. It should be noted that the current size of the Lightning network is slightly larger. The data contains the network structure of the Lightning network and it has the following properties:

# Nodes	# Edges	Avg Degree
4794	61860	24

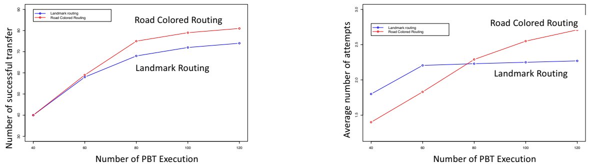
We will compare the performance of our routing algorithm with a landmark-based routing algorithms. There are two prominent landmark-based routing [3], [2]. Landmarks are set of high degree nodes and other non-landmark nodes depend on these landmark nodes to find paths. Each landmark creates tow rooted trees (with itself as the root). One tree for outgoing edges and one edge for incoming edges. First, the sender and the receiver agree on using a particular landmark. The sender finds a path to the landmark by using the rooted

[1] Bitcoin lightning network graph. https://graph.lndexplorer.com/api/graph (2019 (accessed March 1, 2019))

tree built with incoming edges. The receiver finds a path from the landmark to itself using the rooted tree built with out-going edges. The landmarks regularly probe the offline channel network and update its trees. The routing algorithm [3] improves the routing algorithm [2] by finding shortening paths built using rooted trees of landmarks.

B. Success rate of fund transfer

We measure the performance of the proposed road coloring-based algorithm compared with landmark-based algorithms [3], [2]. We use Bitcoin Lightning network data for this evaluation. We choose the induced subgraph of the Lightning network for nodes with a degree of more than 50. In this subgraph, there are 404 nodes with 23942 edges. We randomly choose 10 pairs of senders and receivers from these nodes. We assume the initial channel value of each channel is 4 and the amount of fund transfer is .5 for every transfer. We execute [3] for fund transfer between these pairs of senders and receivers. In 5 execution of PBT execution, we execute 40,60,80,100 and 120 transactions for these sender-receiver pairs. We evaluate the performance of the PBT routing in terms of (a) success rate: the number of successful transactions and (b) the number of attempts in executing each transaction (a new path is used in every attempt). We use 10 landmarks in executing the [3] routing algorithm. We compare the outcome of these PBT executions with [3] with the proposed road coloring-based algorithm using the same set of parameters. The outcomes are shown in Figure 6. Figure 6 (left) clearly shows that the proposed road-coloring-based routing has a better success rate than landmark-based routing. Figure 6 (right) shows that the average number of attempts to execute a PBT becomes more for the road-coloring-based algorithm. This is because in the case of the road-coloring-based routing algorithm there are more paths between a sender and a receiver. Hence the success rate is more and the number of attempts is also greater.



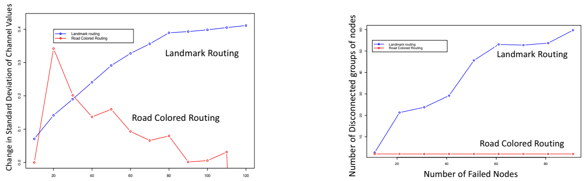
(a)

(b)

Figure 6: Success rate of fund transfer. [Left:] The success rate for landmark-based routing and road-coloring-based routing. It shows that we more we try to execute greater number of transfer between a fixed set of sender and receiver pairs, the road-coloring-based algorithm performs better. [Right:] The average number of attempts for PBT execution for a fixed set of pairs of sender and receiver. It shows that average number of attempts becomes more as the number of PBT execution becomes greater. It shows that the number of paths which can be used for each PBT transfer is more in case of road-coloring-based algorithm.

C. Frequency of rebuilding the subgraphs or trees

Next, we present an analysis of how frequently landmarks should rebuild their trees or peers should rebuild their subgraphs. In this experiment, we use a fixed set of 10 pairs of sender-receiver pairs. In 5 execution of PBTs, we transfer funds among these pairs of sender and receivers 10,20,30,40,50,60,70,80,90,100,120 times. We want to evaluate the impact on trees built by a landmark as we increase the number of transactions before rebuilding the tree. Due to repeated usage, a channel balance may get low and it may not support PBT execution. Hence the landmarks should rebuild their trees periodically. We want to analyze how frequently they should perform such a rebuilding procedure. Similarly, we want to evaluate how frequently a peer should rebuild its subgraphs. We use the same parameters as we execute fund transfers in 12 sets of executions. Figure 7 (left) shows the outcome of these experiments. We plot the change in standard deviation on the values of the edges corresponding to the tree created by a landmark as more and more transactions are executed. We also plot the average rate of change in standard deviation for the subgraphs built by the peers. We found that such a change in standard deviation is increasing for landmark-based routing and it is decreasing for road-coloring based routing. This means, in road-color-based routing uses alternate paths for PBT executions, and the availability of more paths (compared with landmark-based routing) keeps the change in standard deviation low. Hence trees built in landmark-based routing need more frequent rebuilding than the same for subgraphs built by the peers.



(a)

(b)

Figure 7: Success rate of fund transfer: [Left:] We measure the rate of change in standard deviation of channel values of trees built by the landmarks. Also, we measure the same for subgraphs built by the peers. It clearly shows that change in standard deviation is more for landmark-based routing. Hence trees built for landmark-based routing require more frequent rebuilding. [Right:] Impact tested on 30 landmarks.

D. Impact of unavailable nodes

We measure the impact on fund transfer as a node who has previously agreed to participate becomes unavailable. We will assume that initially, all nodes agree to participate in PBT execution. The trees for the landmark-based routing and the road-colorable graphs are built with such information. In both cases, we generate connected graphs as all nodes agree to participate. Next, we measure the impact of adversarial nodes who becomes unavailable after the formation of these trees and road-colourable graphs for routing. In this experiment, we consider a subgraph of the Bitcoin Lightning network with a high degree. The network has 404 nodes with 23942 edges (channels) and the average degree is 59. We construct a road-colorable for each node, i.e., 404 road colorable graphs are built. Next, We construct a reachability graph from these road-colorable graphs. The reachability graph for the color sequence θ_2 (or θ_7 or θ_8) has 14881 edges and the average degree 74. We construct a set of nodes who will become unavailable by choosing 100 nodes from in this network uniformly at random. We create 9 sets of unavailable nodes with 10,20,30,40,50,60,70,80,90 nodes in each set. We will test the impact on unavailable nodes by increasing the number of unavailable nodes. Figure 7 (right) shows the outcome. It shows the number of disconnected groups of peers due to the unavailability of nodes is gradually increasing for the landmark-based algorithm. But for road-color-based routing, such a set of disconnected sets of nodes remains 2. In each road-colorable node, the number of nodes is 8. Hence the at most 16 nodes are impacted for the road-color-based routing. In the case of landmark-based routing in the best-case scenario, a group will have 1 node. Hence road-color-based routing works better than landmark-based routing even if more than 20 nodes fail.

VII. Conclusion

In this paper, we proposed a road-coloring-based routing algorithm for fund transfer in blockchain offline channels. We show that the proposed routing algorithm performs better than landmark-based routing algorithms. We prove that the proposed routing algorithm preserves the privacy of the sender and the receiver of a fund transfer. We show that the landmark-based routing algorithm requires more frequent updating of their trees to support routing. We prove that the unavailability of nodes impacts landmark-based routing more than the proposed road-coloring-based algorithm.

Acknowledgment

This publication has emanated from research supported in part by a research grant from Science Foundation Ireland (SFI) and the Department of Agriculture, Food and the Marine on behalf of the Government of Ireland under Grant Number SFI 16/RC/3835 (VistaMilk), and also by a research grant from Science Foundation Ireland (SFI) under Grant Number SFI/12/RC/2289_P2 (Insight), with both grants co-funded by the European Regional Development Fund.

References

[1] J. Poon and T. Dryja, “The Bitcoin Lightning Network:Scalable Off-Chain Instant Payments.” [Online]. Available: https://lightning.network/lightning-network-paper.pdf

[2] G. Malavolta, P. Moreno-Sanchez, A. Kate, and M. Maffei, “Silentwhispers: Enforcing security and privacy in decentralized credit networks,” *IACR Cryptology ePrint Archive*, vol. 2016, p. 1054, 2016.

[3] S. Roos, P. Moreno-Sanchez, A. Kate, and I. Goldberg, “Settling payments fast and private: Efficient decentralized routing for path-based transactions,” *CoRR*, vol. abs/1709.05748, 2017. [Online]. Available: http://arxiv.org/abs/1709.05748

[4] “Raiden network,” http://raiden.network/, accessed 2018.

[5] P. Prihodko, S. Zhigulin, M. Sahno, A. Ostrovskiy, and O. Osuntokun, “Flare : An approach to routing in lightning network white paper,” 2016.

[6] R. Khalil and A. Gervais, “Revive: Rebalancing off-blockchain payment networks,” in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS ’17. New York, NY, USA: ACM, 2017, pp. 439–453. [Online]. Available: http://doi.acm.org/10.1145/3133956.3134033

[7] S. Thakur and J. Breslin, “Collusion attack from hubs in the blockchain offline channel network,” in *1st International Conference on Mathematical Research for Blockchain*, 2019.

[8] S. Thakur and J. G. Breslin, “A balanced routing algorithm for blockchain offline channels using flocking,” in *Blockchain and Applications*, J. Prieto, A. K. Das, S. Ferretti, A. Pinto, and J. M. Corchado, Eds. Cham: Springer International Publishing, 2020, pp. 79–86.

[9] B. Adler, R.L.; Weiss, “Similarity of automorphisms of the torus,” in *Memoires of the American Mathematical Society*, 1970.

[10] A. N. Trahtman, “The road coloring problem,” *Israel Journal of Mathematics*, vol. 172, no. 1, pp. 51–60, Jul 2009. [Online]. Available: https://doi.org/10.1007/s11856-009-0062-5

[11] A. Trahtman, “An algorithm for road coloring,” *Journal of Discrete Algorithms*, vol. 16, pp. 213 – 223, 2012, selected papers from the 22nd International Workshop on Combinatorial Algorithms (IWOCA 2011). [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570866712001001

[12] M.-P. Béal and D. Perrin, “A quadratic algorithm for road coloring,” *Discrete Applied Mathematics*, vol. 169, pp. 15 – 29, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0166218X13005751