Transaction Propagation on Permissionless Blockchains: Incentive and Routing Mechanisms

Oğuzhan Ersoy, Zhijie Ren, Zekeriya Erkin and Reginald L. Lagendijk
Cyber Security Group, Department of Intelligent Systems,
Delft University of Technology
Delft, The Netherlands
Email: o.ersoy@tudelft.nl, z.ren@tudelft.nl, z.erkin@tudelft.nl, r.l.lagendijk@tudelft.nl

***Abstract*—Existing permissionless blockchain solutions rely on peer-to-peer propagation mechanisms, where nodes in a network transfer transaction they received to their neighbors. Unfortunately, there is no explicit incentive for such transaction propagation. Therefore, existing propagation mechanisms will not be sustainable in a fully decentralized blockchain with rational nodes. In this work, we formally define the problem of incentivizing nodes for transaction propagation. We propose an incentive mechanism where each node involved in the propagation of a transaction receives a share of the transaction fee. We also show that our proposal is Sybil-proof. Furthermore, we combine the incentive mechanism with smart routing to reduce the communication and storage costs at the same time. The proposed routing mechanism reduces the redundant transaction propagation from the size of the network to a factor of average shortest path length. The routing mechanism is built upon a specific type of consensus protocol where the round leader who creates the transaction block is known in advance. Note that our routing mechanism is a generic one and can be adopted independently from the incentive mechanism.**

***Index Terms*—Blockchain, transaction propagation, incentive, routing.**

I. Introduction

In this work, we investigate transaction propagation on permissionless blockchains with respect to incentive compatibility and bandwidth efficiency. The former, incentive compatibility, is an essential component of permissionless blockchain to maintain its functionality with rational participants [1], [2]. The latter, bandwidth efficiency, is an important factor for efficient use of limited resources available in the network.

Although a number of works have studied incentive compatibility problem of blockchains, they are limited to mining mechanism, e.g. investigating *selfish mining attacks* [3]–[6], and *block withholding attacks* [7]–[10]. The existing blockchain solutions such as Bitcoin [11] and Ethereum [12] do not pay attention to incentives for transaction propagation in the network. This is due to the fact that the mining networks in those solutions are centralized in practice [13]–[15] and thus, they do not exhibit a fully decentralized structure. There are only two works that address incentive compatibility of transaction propagation in blockchain by Babaioff et al. [16] and Abraham et al. [17]. Unfortunately, both works suggest a specific solution for the incentive compatibility but do not provide a formal definition of the problem. Furthermore, the proposed solutions are also designed for certain network topologies.

In terms of bandwidth inefficiency, existing solutions suffer from multiple broadcasting of the same transaction over the network. For example, in Bitcoin, each transaction is received by the nodes (miners) in the network twice: once during the advertisement, i.e. broadcasting of the transaction at the beginning, and once after the validation, i.e. broadcasting of the block including the transaction. While validation is essential since each node in the network stores every validated transaction, the advertisement does not need to be received by all nodes. However, redundancy for advertisement is inevitable in such cases where the round leader who creates the validated block is unknown in advance since the transaction needs to be broadcast to all potential round leaders. In recent blockchain proposals where the round leader is known in advance, what we call *first-leader-then-block* (FLTB) type of consensus protocols [18]–[21], it is possible to improve bandwidth efficiency by reducing the communication cost by directly routing the transaction to the round leader. To the best of our knowledge, there is no prior work on optimizing bandwidth efficiency for fully decentralized blockchain.

In this work, our contribution is three-fold: 1) Sybil-proof incentive compatible propagation mechanism, 2) bandwidth-efficient routing mechanism, and 3) bandwidth and storage efficient transaction propagation mechanism which combines the first two mechanisms.

We formally define incentive compatibility of propagation mechanisms in fully decentralized blockchain networks. We show that there is no Sybil-proof and incentive compatible propagation mechanism for poorly connected networks (specifically for 1-connected networks). For other network topologies, we find the following incentive compatible and Sybil-proof formula, which distributes the transaction fee among propagating nodes:

$$f^k_{[i]} = \begin{cases} F \cdot C(1-C)^{i-1} & \text{for } i < k, \\ F \cdot (1-C)^{k-1} & \text{for } i = k, \end{cases}$$

where F is the fee, k is the length of the propagation path, $f^k_{[i]}$ is the share of the i^{th} node in that path, and C is a parameter related to the network topology. The incentive mechanism is

978-1-5386-7204-4/18/$31.00 ©2018 IEEE
DOI 10.1109/CVCBT.2018.00008

IEEE computer society

independent of the choice of consensus protocol and works with any consensus protocol.

We propose a routing mechanism compatible with FLTB-type consensus protocols. Our proposal reduces the communication cost of the transaction propagation from the size of the network to the scale of average shortest path length. In a random network topology of more than 500 nodes, we achieve over 97% communication cost reduction compared to de facto propagation mechanism for the advertisement. Furthermore, we also present a propagation mechanism which combines our incentive and routing mechanisms in a storage and bandwidth efficient way. For incentive mechanism, our combined protocol requires storing only a single signature to provide the integrity of the path, unlike the existing works, which use a signature chain including signatures of each node in the path.

The rest of the paper is organized as follows: Section II presents the related work. Our blockchain model and notations are defined in Section III. Section IV formulates requirements of the incentive problem and computes the generic solution. Smart routing mechanism is presented in Section V and combined with incentive mechanism in Section VI.

II. Related Work

The lack of incentive for information propagation in a peer-to-peer network has been known and studied in different settings [22]–[25]. Kleinberg and Raghavan [24] proposed an incentive scheme for finding the answer for a given query in a tree-structured network topology. Li et al. [25] focused on node discovery in a homogeneous network where each node has the same probability of having an answer for the query. In [22], [23], the authors analyzed the incentive problem for multi-level marketing which rewards referrals if the advertisement produces a purchase. In these marketing models, the reward is shared among all nodes in the tree including the propagation path.

The proposed solutions for peer-to-peer networks [22]–[25] are not applicable for the permissionless blockchains. In peer-to-peer solutions, nodes are asked to provide a specific datum like the position of a peer or the answer to a query. In blockchains, however, transaction propagation is requested to advertise the transactions and eventually place them into a valid block. Alternatively, finding an answer to a query is equivalent to validation of a transaction by round leader in the blockchain. Query propagation in a peer-to-peer network has two main differences compared to a blockchain transaction propagation: nodes do not compete against the ones who forwarded the message to them and nodes cannot generate a response to a query that they do not have the answer, i.e. either they have the right answer or not. Whereas in a blockchain, a block is generated by the round leader and every node is a potential round leader. Essentially, nodes in a blockchain are competitors that have an incentive not to propagate whereas other peer-to-peer nodes do not have the incentive since they cannot generate the answer to the query by themselves.

Recently, blockchain oriented propagation mechanisms have been proposed [16], [17]. In [16], Babaioff et al. uncovered the incentive problem in the Bitcoin system where a rational node (miner) has no incentive to propagate a transaction. They focused on a specific type of network, namely regular d-ary directed tree with a height H, and assumed that each node has the same processing power. In that setting, the authors proposed a hybrid incentive (rewarding) scheme and proved that it is also Sybil-proof. In [17], Abraham et al. proposed a consensus mechanism, Solidus, offering an incentive to propagate transactions and validated blocks (puzzles). In their incentive mechanism, the amount of processing fee passed to the next node is determined by the sender. Both works rely on a signature chain to prevent any manipulation over the path and thereby, to secure the shares of propagating nodes.

[16] and [17] provided analyses of their proposals based on game theory. For the analysis, [16] assumes a tree-structured network which eliminates the case of competition against common neighbors and it is not realistic for blockchain network topology. Whereas, the analysis in [17] is limited to the case of competition between nodes that have common neighbors.

For bandwidth efficiency, to the best of our knowledge, there is no prior work for fully decentralized blockchain without dedicated miners (round leaders). Nevertheless, Li et al. [25] presented a distributed routing scheme for peer-to-peer networks. The authors focused on one-to-one routing which is dedicated to a single target node. Whereas in blockchain it needs to be one-to-all routing, which connects the complete network to the round leader. In addition, [25] does not take into account the possibility of a failing routing caused by a failing or malicious node in the routing path.

III. Our Blockchain Model and Notations

In this section, we describe our blockchain model and the notation used in the paper.

Network. It is a dynamic peer-to-peer network means that there are nodes joining and leaving constantly. Unlike to the existing works [16], [17], we do not have a restriction on the network topology.

Participants. Each participant is denoted by a node in the network. We assume a permissionless blockchain where anyone can participate and contribute to the ledger directly. Moreover, there is no discrimination between nodes (participants), i.e., they can all be the owner of a transaction and propose a block as a miner (round leader). For identification, each node has a public and private key pair and can be validated by his public key.

Consensus and leader election. Incentive mechanism defined in Section IV works regardless of the consensus structure. Whereas, the routing mechanism requires special treatment, which we call *first-leader-then-block* (*FLTB*) type consensus protocols.

FLTB protocols can be defined as the consensus model where the round leader is validated before he proposes the block. Any leader election mechanism which is independent of the prospective block of that leader can be converted into FLTB type. Examples of the FLTB consensus protocols

are Proof-of-Work (PoW) based Bitcoin-NG [18] and several Proof-of-Stake (PoS) based ones [19]–[21].

The rest of the definitions and notations are listed below:

- *Neighbor nodes*: Directly connected nodes in the network, adjacency in the graph.
- *Client*: The source or the sender of a transaction. Client of a transaction T, denoted by c_T.
- *Round Leader*: The legitimate node (participant) who constructs the current block.
- *Intermediary Node*: A node on the transmission path between the round leader and a client.
- $\mathcal{L}^r$: The credential of round leader which validates the round leader of round r and can be verified by all nodes in the network. For example, it could be a special hash value in a PoW protocol or the proof of possessing the chosen coin in a PoS protocol. In general, regardless of the consensus mechanism, credentials are linked to the public key of the leader and can be verified by a corresponding signature.
- $\pi(n_i)$: The probability of node n_i being the round leader, also referred as the capacity of node n_i. It corresponds to the mining power in PoW or the stake size in PoS protocols and is assumed to be greater than zero for every node in the network. $\pi(S)$ corresponds to the total capacity of the all nodes in set S.
- $\mathcal{N}_K^T$: The set of nodes who know (received) the transaction T. $\mathcal{N}_K^{n,T}$ presents the set from the point of view of node n (including n itself).
- $\mathcal{N}_{NK}^T$: The set of nodes who do not know (received) transaction T yet. $\mathcal{N}_{NK}^{n,T}$ denotes the set from the point of view of node n and includes only the neighbors of n.

IV. Incentive Mechanism

We now describe our incentive mechanism. For the sustainable functioning of a fully decentralized blockchain where the nodes (participants) are able to create new identities and behave according to their incentives, propagation mechanism needs to be Sybil-proof and incentive compatible [1].

Conventional incentive instrument, namely transaction fee, almost always refers to the reward of the round leader. Here, we refer transaction fee as it consists of the reward to propagate and to validate transactions. Thereby, rational nodes are encouraged not only to validate transactions but also to propagate them. How to determine the fee is out of the scope of this paper but we assume that each transaction fee is predefined by either the client or a known function. We focus on how to automatically allocate the fee among all the contributors of the process.

Fee sharing function (rewarding mechanism). The fee sharing function distributes the transaction fee among the propagating nodes and the round leader. Note that it is highly probable that the same transaction is received more than once by the round leader (and intermediary nodes) because of the propagation mechanism. A rational round leader would choose the one which maximizes his profit. Like existing works [16], [17], the fee sharing function described here deals with the path which is included in the block. For a transaction (added to the block) with fee F and propagation path P, the function $\mathcal{F}$ determines the shares of each node involved:

$$\mathcal{F} : \{F, P\} \longrightarrow \{f_{[i]}^{|P|}\}_{i=1}^{|P|} \text{ where } \sum_{i=1}^{|P|} f_{[i]}^{|P|} = F.$$

$|P|$ denotes the number of nodes involved in the processing of a transaction with fee F, where $|P| - 1$ of the nodes are in the propagation path between the client and the round leader. Let $|P| = k$, i.e., length of the propagation path of the transaction is k. Then, $f_{[i]}^{|P|}$ denotes the share of i^{th} node in the propagation path, $f_{[k]}^k$ is the share of the round leader and $\sum_{i=1}^k f_{[i]}^k = F$.

In the rest of the section, we formulate the necessities of the fee sharing function to incentivize propagation of an arbitrary transaction T with fee F. An ideal incentive compatible propagation mechanism should satisfy the following properties:

1) *Sybil-proofness*: An intermediary node, as well as the round leader, should not benefit from introducing Sybil nodes to the network.
2) *Game theoretically soundness*: A transaction should not be kept among a subset of the network. There should be adequate incentive for rational nodes willing to propagate, thence it will eventually reach to the whole network.

By formulating these conditions, we achieve the following theorem (where C is a constant which can be chosen according to the network connectivity):

Theorem 1. *In a 2- or more connected blockchain network, each rational node $n \in \mathcal{N}_K^T$ with $\pi(n) < C \cdot \pi(\mathcal{N}_K^{n,T})$ propagates transaction T without introducing Sybil nodes, if the transaction fee F is shared by the following method:*

$$f_{[i]}^k = \begin{cases} F \cdot C(1-C)^{i-1} & \text{for } 1 \leq i < k, \\ F \cdot (1-C)^{k-1} & \text{for } i = k. \end{cases}$$

Proof of the theorem is divided into the following sections. The requirements are formulated in Sections IV-A and IV-B, and the fee sharing function satisfying them is computed in Section IV-C.

A. Sybil-Proofness

Here, we use the same definition of Sybil nodes in [16]: fake identities sharing the same neighbors with the original node that do not increase the connectivity of the network. Because of the Sybil-proof consensus algorithm, Sybil nodes do not increase the capacity of their owner, i.e., the probability of being the round leader.

We investigate the problem in two different settings: 1-connected networks and the rest. k-connected network means that removal of any $k - 1$ nodes does not disconnect the network. In 1-connected networks, there exists a bridge which is the only connection between two distinct subnetworks. Though 1-connected network model seems to be unrealistic

topology for permissionless blockchains, it is important to see the intuition behind the non-competition effect.

1-connected networks. In 1-connected networks, there are critical nodes which have special positions in the propagation paths between some node pairs. A critical node for a node pair appears in all possible paths between these two nodes. The following lemma shows that non-competing advantage of critical nodes makes it impossible to have a Sybil-proof incentive mechanism for 1-connected networks.

Lemma 2 (Impossibility Lemma)**.** *For 1-connected networks, there is no Sybil-proof and incentive compatible propagation mechanism which rewards every node in the propagation path.*

Proof. Assume that, because of 1-connectedness of the network, a node n_i have a critical position for a transaction T, meaning that it is certain he will be included in the propagation path of that transaction. If n_i is one side of the bridge combining two distinct subnetworks, n_i can be sure that each transaction coming from its subnetwork and validated in the other one has to pass through n_i. In Figure 1, we illustrate the two possible paths of a transaction passing through n_i. Since the round leader and also intermediary nodes after n_i will receive one of the paths, they do not have any choice but accept the path sent by n_i.

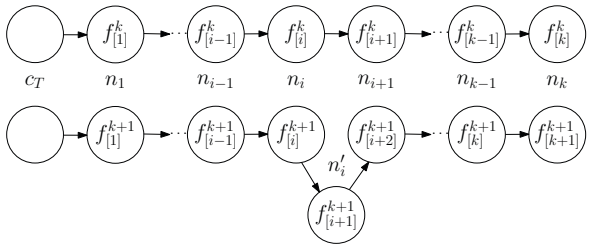

Fig. 1. The fee sharing before and after a Sybil node $n_{i'}$ added by n_i

Now, we investigate the share of a node n_i with and without a Sybil node. As given in Figure 1, n_i is the i^{th} node in the original propagation path and his corresponding fee shares are $f^k_{[i]}$ and $f^{k+1}_{[i]} + f^{k+1}_{[i+1]}$. In order to demotivate n_i, $f^k_{[i]}$ should be greater than or equal to $f^{k+1}_{[i]} + f^{k+1}_{[i+1]}$. Since the position of the node would change for different transactions and rounds, the condition should hold for all positions:

$$\begin{aligned}
&\forall\, i \in \{1,\dots,k\}, \quad f^k_{[i]} \geq f^{k+1}_{[i]} + f^{k+1}_{[i+1]} \\
\text{(summing for all } i\text{'s)} \implies &\sum_{i=1}^{k} f^k_{[i]} \geq \sum_{i=1}^{k} f^{k+1}_{[i]} + \sum_{i=1}^{k} f^{k+1}_{[i+1]} \\
\text{(Definition of } \mathcal{F}\text{)} \implies &F \geq F - f^{k+1}_{[k+1]} + F - f^{k+1}_{[1]} \\
\implies &f^{k+1}_{[k+1]} + f^{k+1}_{[1]} \geq F \\
\text{(Definition of } \mathcal{F}\text{)} \implies &f^{k+1}_{[k+1]} + f^{k+1}_{[1]} = F\,.
\end{aligned}$$

Therefore, other than the first propagating node and the round leader, there is no reward for the rest of the propagating nodes which contradicts with rational behavior. □

Eclipse and partitioning. Note that this monopolized behavior is similar to the eclipse and partitioning attacks where the adversary separates the network into two distinct group and controls all the connections between them [26], [27]. Indeed, Lemma 2 can be generalized to the case where the adversary is able to control all the outgoing connections of a client. In that case, there is no way to deviate the adversary from creating Sybil nodes for that specific transaction. We assume that client nodes are able to defend against the eclipse attacks using the countermeasures defined in [26].

In a 2- or more connected network, there are multiple paths between any two nodes. Therefore, we can immediately focus on the multiple paths case where there are competing paths for the same transaction and the round leader includes one of them to the block.

A node can profit from a fee by either being an intermediary node who propagates it or being the round leader who creates the block. We investigate the Sybil-proof conditions of intermediary nodes and the round leader separately.

a) Intermediary nodes: An intermediary node can be deviated by the actions of the nodes who receive the transaction afterwards. Since there are multiple paths, the round leader will receive the same transaction from at least two different paths. In other words, the round leader would decline all but one of the paths (for each transaction). An intermediary node will be demotivated if introducing a Sybil node would increase the chance of rejection of his path.

If the share of the round leader decreases as the propagation path length increases, then he will choose the shortest path for each transaction. In that case, introducing Sybil nodes will decrease his chance to be included in the block. Therefore, providing larger gain to the leader for choosing the shortest path is sufficient and can be formulated as $f^k_{[k]} > f^{k+1}_{[k+1]}$.

b) Round leader: In some cases, round leader is determined before the block is created or even several rounds earlier [18]–[20]. Since the round leader is guaranteed to be in the propagation path, it is needed to be taken into account separately. In addition, an intermediary node can propagate righteously to his neighbors and then add Sybil nodes for his own mining process. Therefore, in any case (predefined leader or not), it is necessary to make an additional policy for the round leader.

In the case of s Sybil nodes, share of the round leader will change from $f^k_{[k]}$ to $\sum_{i=0}^{s} f^{k+s}_{[k+i]}$ for some k. In order to deviate the round leader, $f^k_{[k]} \geq \sum_{i=0}^{s} f^{k+s}_{[k+i]}$ is required.

Since the latter condition includes the former one (as $f^{k+1}_{[k]} > 0$), Sybil proofness condition can be formulated as:

$$\forall\, k \geq 1, \forall\, s \geq 1, \quad f^k_{[k]} \geq \sum_{i=0}^{s} f^{k+s}_{[k+i]}\,. \tag{1}$$

B. Incentive Compatibility

The decision of the propagation of a transaction can be analyzed as a simultaneous move game where each party takes action without knowing strategies of the others. All players (nodes in our case) are assumed to be rational and they decide

their actions deducing that the others will also act rationally. Some nodes may cooperate with each other. We assume that colluding neighboring nodes already share every transaction with each other and take actions as one. In other words, they act as a single combined node in the network which can be seen as Sybil nodes.

Here, we investigate the propagation decision by comparing the change in the expected rewards for a transaction T. In the beginning, each transaction is shared with some nodes, at least with the neighbors of the client. We will find the required condition to propagate through the whole network. We first investigate the propagation decision by comparing the change in the expected rewards immediately after the action. Then, we extend our analysis with a permanence condition which guarantees that the ones who propagate will not suffer from any future actions.

We show that the sharing decision of a node is independent of the probability of his neighboring nodes being the round leader. Instead, it depends on his own probability against the rest who knows the transaction.

Lemma 3 (Equity Lemma)**.** *Propagation decision of a node is independent from the neighbors' capacities. A rational node would propagate to either all of its neighbors or none of them.*

Proof. Let a transaction T with fee F is known by a node n, and its distance to the c_T is k. The expected reward of node n can be defined as a function $R(\cdot)$ whose input corresponds to the capacities of the nodes who received T from n, then

$$R(X) = \frac{f^k_{[k]} \cdot \pi(n) + f^{k+1}_{[k]} \cdot X}{\pi(\mathcal{N}^{n,T}_K) + X}.$$

We show that $R(\cdot)$ is a monotone function. In order to show that a function is a monotone, it is enough to show that the sign of its derivative does not change in the domain range. For our case, it can be seen that the sign is independent of the input:

$$\begin{aligned} R'(X) &= \frac{f^{k+1}_{[k]} \left(\pi(\mathcal{N}^{n,T}_K) + X\right) - \left(f^k_{[k]}\pi(n) + f^{k+1}_{[k]} X\right)}{\left(\pi(\mathcal{N}^{n,T}_K) + X\right)^2} \\ &= \frac{f^{k+1}_{[k]}\pi(\mathcal{N}^{n,T}_K) - f^k_{[k]}\pi(n)}{\left(\pi(\mathcal{N}^{n,T}_K) + X\right)^2}. \end{aligned}$$

Since $R(\cdot)$ is a monotone function, then it achieves the maximum value at one of the boundary values. In our case, the boundary values are $X = 0$ where no neighbors received the transaction and $X = \pi\left(\mathcal{N}^{n,T}_{NK}\right)$ where all neighbors received it. Here, we omit the fact that $\pi(\cdot)$ is also a monotone function. Thus, we can say that a rational node maximizes his profit by propagating to either all of its neighbors or none of them. □

Lemma 3 simplifies to evaluate interfering multiple node decisions which is discussed in the following Lemma.

Lemma 4 (Propagation Lemma)**.** *Let a node $n \in \mathcal{N}^T_K$, $\mathcal{N}^{n,T}_{NK} \neq \emptyset$ where the distance between n and c_T is k. All neighbors of n will be aware of T if*

$$\frac{f^{k+1}_{[k]}}{f^k_{[k]}} > \frac{\pi(n)}{\pi(\mathcal{N}^{n,T}_K)}.$$

Proof. Assume that some of the neighbors of n are not aware of T, i.e., $\mathcal{N}^{n,T}_{NK} \neq \emptyset$. From Lemma 3, we know that n did not propagate the transaction to any of his neighbors. Therefore, at the moment, the only way that n profits from T is being the round leader with a reward $f^k_{[k]}$.

Table I presents expected reward of n with respect to each possible action of n and $\mathcal{N}^{n,T}_K$. The propagation decision of $\mathcal{N}^{n,T}_K$ may not include all its members, thereby all possible decisions are taken into account. Here, CN corresponds to the common neighbors of n and $\mathcal{N}^{n,T}_K$, NCN_1 distinct neighbors of n and NCN_2 distinct neighbors of $\mathcal{N}^{n,T}_K$ (who decide to propagate), i.e., $CN \bigcup NCN_1 = \mathcal{N}^{n,T}_{NK}$. Since CN is received the transaction from both n and the rest of the $\mathcal{N}^{n,T}_K$, α represents the percentage of the ones in CN decided to continue with the one including n.

If all nodes of $\mathcal{N}^{n,T}_K$ decide not to propagate with their neighbors, then n will benefit from propagating T in the case of

$$\frac{f^k_{[k]}\cdot\pi(n)+f^{k+1}_{[k]}\cdot\pi(\mathcal{N}^{n,T}_{NK})}{\pi(\mathcal{N}^{n,T}_K)+\pi(\mathcal{N}^{n,T}_{NK})} > \frac{f^k_{[k]}\cdot\pi(n)}{\pi(\mathcal{N}^{n,T}_K)} \iff \frac{f^{k+1}_{[k]}}{f^k_{[k]}} > \frac{\pi(n)}{\pi(\mathcal{N}^{n,T}_K)}.$$

If (some) nodes in $\mathcal{N}^{n,T}_K$ decide to propagate T, then n will benefit from propagating T in the case of

$$\frac{f^k_{[k]}\cdot\pi(n)+f^{k+1}_{[k]}\cdot\pi(NCN_1)+\alpha f^{k+1}_{[k]}\cdot\pi(CN)}{\pi(\mathcal{N}^{n,T}_K)+\pi(\mathcal{N}^{n,T}_{NK})+\pi(NCN_2)} > \frac{f^k_{[k]}\cdot\pi(n)}{\pi(\mathcal{N}^{n,T}_K)+\pi(CN)+\pi(NCN_2)}$$
$$\impliedby \frac{f^{k+1}_{[k]}}{f^k_{[k]}} > \frac{\pi(n)}{\pi(\mathcal{N}^{n,T}_K)+\pi(CN)+\pi(NCN_2)} \text{ and } NCN_1 \neq \emptyset.$$

Note that $NCN_1 = \emptyset$ means that all the neighbors of n are also neighbors of $\mathcal{N}^{n,T}_K$ who decide to propagate. In addition, the sufficiency condition is independent of α. Therefore, in any case, if $\frac{f^{k+1}_{[k]}}{f^k_{[k]}} > \frac{\pi(n)}{\pi(\mathcal{N}^{n,T}_K)}$ is satisfied, then all neighbors of n will be aware of the transaction. □

Corollary 5. *Let $f^{k+1}_{[k]} \geq C \cdot f^k_{[k]}$ for some constant $C \in (0, 1)$. $\mathcal{N}^T_K$ will continue to expand until there is no more node $n \in \mathcal{N}^T_K$ having neighbors in $\mathcal{N}^T_{NK}$ and satisfying $\pi(n) < C \cdot \pi(\mathcal{N}^{n,T}_K)$.*

Remark I. Here, it is possible to define different C_k values for each distance k, i.e., $f^{k+1}_{[k]} \geq C_k \cdot f^k_{[k]}$. One might argue that, as the distance increases, it could be possible to find nodes satisfying $\frac{\pi(n)}{\pi(\mathcal{N}^{n,T}_K)} < C_k$ for smaller C_k values. However, as seen in Section VI, this is not always the case. In addition, the intermediate node may not know the exact distance, thus using the same C value would make the decision simpler.

Remark II. Note that the propagation decision is based on $\mathcal{N}^{n,T}_K$ instead of $\mathcal{N}^T_K$ since the latter one may not be available. This could lead to better consequences for propagation because nodes may predict $\mathcal{N}^T_K$ greater than its actual size and decide

TABLE I
THE EXPECTED REWARD OF n FROM T REGARDING POSSIBLE DECISIONS OF n AND THE REST OF $\mathcal{N}_K^{n,T}$.

		$\mathcal{N}_K^{n,T}$ (excluding n)	
	Decision	Not Propagate	(some) Propagate
n	Not Propagate	$\frac{f_{[k]}^k \cdot \pi(n)}{\pi(\mathcal{N}_K^{n,T})}$	$\frac{f_{[k]}^k \cdot \pi(n)}{\pi(\mathcal{N}_K^{n,T})+\pi(CN)+\pi(NCN_2)}$
	Propagate	$\frac{f_{[k]}^k \cdot \pi(n)+f_{[k]}^{k+1} \cdot \pi(\mathcal{N}_{NK}^{n,T})}{\pi(\mathcal{N}_K^{n,T})+\pi(\mathcal{N}_{NK}^{n,T})}$	$\frac{f_{[k]}^k \cdot \pi(n)+f_{[k]}^{k+1} \cdot \pi(NCN_1)+\alpha f_{[k]}^{k+1} \cdot \pi(CN)}{\pi(\mathcal{N}_K^{n,T})+\pi(\mathcal{N}_{NK}^{n,T})+\pi(NCN_2)}$

accordingly. Nonetheless, a carefully chosen C value will lead the nodes to share it with an overwhelming probability.

Remark III. Being the round leader should be more appealing than being an intermediary node, thus the round leader would try to fulfill the round block capacity to maximize his profit. The system may not work at full capacity if the nodes gain the same reward from propagating instead of validating (as the round leader) transactions. In Corollary 5, the propagation condition is given as $f_{[k]}^{k+1} \geq C \cdot f_{[k]}^k$. We fix the condition in favor of the round leader:

$$\forall\, k, \quad f_{[k]}^{k+1} = C \cdot f_{[k]}^k\,. \tag{2}$$

Permanence condition. In the simultaneous move analysis, we investigated one step at a time, i.e., what will happen immediately after the decision of propagation. However, all possible future actions should be taken into account. For example, the sender of a transaction should consider the possibility of the further propagation done by the receiver. From Lemma 3, capacities of the neighboring nodes do not have any influence on the sharing decision. Unless the processing fee share decreases, which is caused by some possible future actions like increased path length, the same lemma will be satisfied. If the share of a propagating node is non-decreasing with respect to the path length, then the ones who propagate will not suffer from any future actions. This can be formulated as

$$\forall\, i < k, \quad f_{[i]}^k \geq f_{[i]}^{k+1}\,. \tag{3}$$

C. Fee Sharing Function

With the equations obtained from the required conditions, we can uniquely determine the fee sharing function and conclude Theorem 1. First, using permanence condition (3), Sybil-proofness condition (1), can be reduced to $f_{[k]}^k \geq f_{[k+1]}^{k+1} + f_{[k]}^{k+1}$:

$$\begin{aligned}\forall\, k \geq 1,\ f_{[k]}^k &\geq f_{[k+1]}^{k+1} + f_{[k]}^{k+1} \geq f_{[k+2]}^{k+2} + f_{[k+1]}^{k+2} + f_{[k]}^{k+1} \\ &\geq f_{[k+3]}^{k+3} + f_{[k+2]}^{k+3} + f_{[k+1]}^{k+2} + f_{[k]}^{k+1} \geq \cdots \\ \forall\, s \geq 1, \qquad &\geq f_{[k+s]}^{k+s} + \sum_{i=0}^{s-1} f_{[k+i]}^{k+i+1} \geq f_{[k+s]}^{k+s} + \sum_{i=0}^{s-1} f_{[k+i]}^{k+s}.\end{aligned}$$

Therefore, we can update the Sybil-proofness condition as:

$$\forall\, k \geq 1, \quad f_{[k]}^k \geq f_{[k+1]}^{k+1} + f_{[k]}^{k+1}\,. \tag{4}$$

Then, we can obtain the following equations:

$$\begin{aligned}\text{Using (4)} \qquad &\sum_{i=1}^{k} f_{[i]}^i \geq \sum_{i=1}^{k} f_{[i+1]}^{i+1} + \sum_{i=1}^{k} f_{[i]}^{i+1} \\ &\implies F = f_{[1]}^1 \geq f_{[k+1]}^{k+1} + \sum_{i=1}^{k} f_{[i]}^{i+1} \\ \text{Using (3)} &\implies F \geq f_{[k+1]}^{k+1} + \sum_{i=1}^{k} f_{[i]}^{k+1} = F \\ &\implies f_{[i]}^k = f_{[i]}^{k+1} \text{ and } f_{[k]}^k = f_{[k+1]}^{k+1} + f_{[k]}^{k+1}. \end{aligned} \tag{5}$$

After all, we can finalize the fee sharing function which corresponds to Theorem 1. Using (2) and (5), the share of the round leader can be computed:

$$f_{[k]}^k = f_{[k-1]}^{k-1}(1-C) = \cdots = F \cdot (1-C)^{k-1}. \tag{6}$$

Using (5) and (6), the share of an intermediary node can be computed:

$$\forall\, i < k, \quad f_{[i]}^k = f_{[i]}^{i+1} = F \cdot C(1-C)^{i-1}\,.$$

D. Discussion

Integration. Implementation of the incentive mechanism should take into account the security and efficiency concerns. The propagation path should be immutable in a way that an adversary cannot add or subtract any node neither in the propagation process nor after the block generation. At the same time, storage efficiency is also essential since these path logs are needed to be stored in the ledger by every node. Both existing incentive-compatible blockchain solutions [16], [17] adopted a signature chaining mechanism where each propagated message includes the public key of the receiver and signature of the sender. This protocol prevents any manipulation over the path and thereby secures the shares of each contributor. It requires additional storage which is the signatures of the contributors. Although signature chaining solution requires the knowledge of the public key of the receiver and stores signatures of each sender, it is generic and can be applied to any blockchain. In Section VI, we present a novel and storage-efficient solution which is feasible for *FLTB* blockchains. It is embedded into routing mechanism and does not require the knowledge of the public keys of the neighboring nodes.

Determining C parameter. C value plays an important role to make sure that there will be incentive to propagate a transaction for some nodes until it reaches to the whole network. On

the one hand, as the choice for the C value increases, it will be easier to satisfy the propagation condition since there will be more chance to find nodes satisfying $\pi(n) < C \cdot \pi(\mathcal{N}_K^T)$. On the other hand, the higher C value, the lower fee remains for the rest of the propagation path. It significantly reduces the fee of the round leader, thereby the incentive. For these reasons, it is required to choose a moderate C value, e.g., a reasonable choice would be $C = \frac{2}{N_{con}}$ where N_{con} denotes default number of connections of a node. For example, in Bitcoin network where $N_{con} = 8$, nodes will propagate unless they assume that their mining power is greater than 25% of the ones having the transaction. Even at the very beginning, at least N_{con} nodes have the transaction, $C = \frac{2}{N_{con}}$ setting would provide overwhelming probability to have nodes willing to propagate according to Corollary 5.

Client ($0-$capacity) nodes. The main goal of the propagation incentive mechanism is to make sure that the transactions are received by the nodes who are capable of validating transactions as well as creating blocks. For that reason, we mainly focused on the nodes having a capacity greater than zero, i.e., $\pi(\cdot) > 0$. Nevertheless, a client node can be seen as a potential capacity node because of the possible propagation of the client. Regarding Lemma 3 and permanence condition (3), a rational node, who decided to propagate, would benefit from propagating to the client nodes as well. At the same time, a client node will always benefit from propagating any transaction since otherwise it will not have any chance to gain a fee.

Decentralization effect. In the conventional permissionless blockchains, all rewards including block reward and transaction fees are given to the block owner. In other words, nodes have only one incentive to participate in the network: being round leader. The less chance individual nodes have to be the round leader, the more they are motivated to join into centralized forms (e.g. mining pools) [13], [28]. Conversely, the transaction fee is shared with all propagators nodes. In addition, since many transactions are included in a single block, aiming processing fees of (some) transactions has significantly more chance than being the round leader. Thereby, it is reasonable to conclude that incentive mechanism would have a positive impact on the decentralization of the permissionless blockchains.

V. Routing Mechanism

As a non-hierarchical peer-to-peer network, the blockchain ledger is validated by all nodes (miners) individually. This requires broadcasting every data and blocks over the network since every node needs to keep a record of the chain to validate new blocks. In existing permissionless blockchains, every transaction is broadcast throughout the network by the client, then the new block including (some of) these is constructed and broadcast by the round leader. Hence, each transaction is broadcast at least twice. Even more (`inv`) messages are sent to check the awareness of the neighbors on the transaction.

In Nakamoto-like consensus protocols, the round leader is validated simultaneously with his proposed block where the redundant propagation of the client is inevitable. In *FLTB* protocols, on the other hand, it is possible to validate the round leader before the block is proposed. It enables to determine a direct route between each client and the round leader. Our routing mechanism in Algorithm 1 finds the shortest paths between clients and the round leader for each round. Instead of sending each transaction to all nodes in the network, it is relayed over the shortest path between the client and the leader. The distance between (almost) any two nodes in a connected graph is dramatically smaller than the size of the network [29]. This is equivalent to cost reduction from $O(N)$ to $O(\ln N)$ in a random network of size N [30], [31].

The treat model of routing mechanism we present in this section considers a malicious adversary rather than a rational one. In the routing mechanism, a malicious adversary may try to block or censor some of the transaction propagations.

Our protocol can be divided into two parts: *Recognition Phase* where the routes are determined and *Transaction Phase* where the transactions are propagated (see Figure 2). First, in the recognition phase, the round leader is recognized throughout the network and his credential is propagated with a standard gossip protocol. Each node n_i learns his closest node towards the round leader, *gradient node* (gn_i), who is the first node forwarding the credential. In the transaction phase, each client forwards his transaction to (some of) his neighbors. Then, each node, receiving a transaction for the first time, directly transmits to his gradient node. Here, the reason for clients to broadcast to more than one neighbor is that one path could yield a single point of failure. It could be caused by the nodes who fail or maliciously censor some of the transactions. As presented in the experimental results, forwarding transaction to a few of the neighbors (precisely N_{con}) is sufficient. Note that, the routing mechanism works under asynchronous network assumptions since a client does not have to wait for all nodes but N_{con} of his neighbors. Similarly, for an intermediary node, waiting for the first credential message is enough to propagate received transactions.

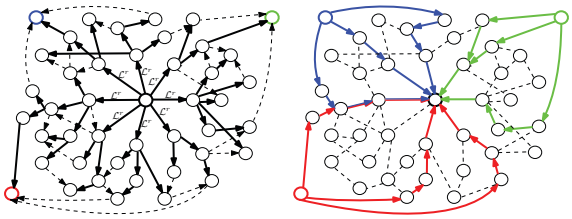

Fig. 2. The Routing Mechanism. The left one illustrates the Recognition Phase and connections to the gradient nodes are shown with bold solid lines. On the right, three clients and their transaction paths are presented.

Locational privacy. There have been several papers investigating anonymity in the permissionless blockchain networks, especially for the Bitcoin network [32]–[34]. It is found out that matching public keys and IP addresses can be done by eavesdropping. In this manner, *FLTB*-based blockchains may expose to DoS (denial-of-service) attacks against to the round

Algorithm 1 The Routing Algorithm

Recognition Phase
Leader provides his credential $\mathcal{L}^r$ to his neighbors.
for Node n_1 to n_N **do**
  if First time receiving $\mathcal{L}^r$ **then**
    Store ID of the sender (gradient) node n_j, i.e., $gn_i \leftarrow n_j$
    Propagate $\mathcal{L}^r$ to neighbors.
  end if
end for

Transaction Phase
Client provides transaction T to his neighbors.
for Each node n_i receiving T **do**
  if First time receiving T **then**
    Send it to the gn_i
  end if
end for

leader. We want to stress that our routing mechanism does not leak any more locational information about the position of the leader other than the original *FLTB* protocols do. It just takes advantage of the announcement of the leader which is done exactly in the same manner with the *FLTB* protocols. Therefore, our routing mechanism does not cause any additional vulnerabilities for DoS-like attacks against the round leader. Yet, it is possible to improve the locational privacy via anonymity phase where the message is first forwarded in a line of nodes, then diffused from there [35]. The extra cost of anonymity would be a few nodes on the line which is still proportional to the logarithmic size of the network.

A. Experimental Results

In this experiment, we use Barabási-Albert (BA) graph model [30] which simulates peer discovery in a peer-to-peer network. It starts with a well-connected small graph and each new node is connected to some of the previous nodes with a probability proportional to their degrees.

Barabási-Albert (BA) [30] and Erdős-Rényi (ER) [31] graph models have been used to simulate permissionless blockchains [36], [37]. In our setting, we combine both models where the network starts with a small ER graph and grows according to BA model. We start with 50 nodes in ER model [31] with edge probability of $1/2$, meaning that on average each node has 25 connections. Then, each new node is added by connecting with N_{con} nodes in the network. For each (N, N_{con}) pair analyzed, we generated various graphs using Python graph library [38].

Bandwidth gain. In [39], the average shortest path length between any two nodes, i.e., the average path length, of a BA graph is shown to be in the order of $\frac{\ln N}{\ln \ln N}$. Hence, our routing protocol reduces the communication cost of a message transaction from $O(N)$ to $O(N_{con} \cdot \frac{\ln N}{\ln \ln N})$. The communication gain is up to 99% for scaled networks (see Figure 3), which can be verified by counting the average number of nodes visited per transaction. Here, we assume that the first arriving credential is coming from the node which is closest to the leader with respect to the number of nodes in between. In other words, the delay between any two nodes is computed by the node-distance.

In Figure 3, we count only one redundant communication for each transaction. Even more redundancy is caused by the flooding of each transaction because the same transaction is received from different neighboring nodes. In other words, the total redundancy is not N, but on average $N_{con} \cdot N$. In the existing blockchains, this additional redundancy is reduced by the sending the hash of the transaction to check whether the neighbor has it or not. If storage size of the transaction is relative to the size of the hash, then the total number of relays of a transaction would be significantly more than double of the network size. For example, Statoshi info [40], a block explorer of Bitcoin, shows that average incoming bandwidth usage for the transactions (`tx`) is, 2.87 KBps, less than for the checking messages (`inv`), 4.12 KBps (measurements taken between 02:00 AM and 14:00 PM in 13 of Feb. 2018). To conclude, since our mechanism does not suffer from the flooding effect, the actual communication gain would be much higher than the result in Figure 3.

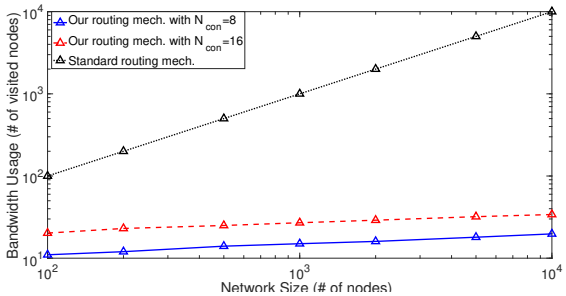

Fig. 3. Communication cost for advertisement of a transaction.

Failing transmissions. Since each transaction is propagated among a small set of nodes, we need to take into account the possibility of propagation failure which can be caused by the nodes who fail or censor the transaction. The failure probability of a transaction can be approximated by $\left(1-(1-h)^{\frac{\ln N}{\ln \ln N}-1}\right)^{N_{con}}$ where h denotes the probability of a node in the network who fails or censors the transaction. These failing nodes are the ones who were present at the recognition phase and failed just afterwards. Long-term offline nodes can be ignored since they will not be chosen as gradient nodes. Thus, Figure 4 demonstrates that our routing is robust against instant network fluctuations. For a blockchain network with $N = 10000$ and $N_{con} = 8$, similar to Bitcoin network, if 30% of the active nodes fail after the recognition phase, only 9% of the transactions will be affected.

VI. Combined Propagation Mechanism

In this section, we show how to deploy both of the incentive and routing mechanisms for any blockchain having a *FLTB* consensus protocol. At first glance, they seem to conflict

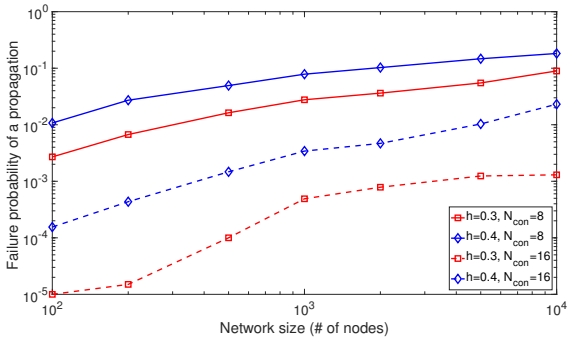

Fig. 4. Probability of a transaction failing to be received by the round leader where h is the probability of an intermediary node being a failing or censoring node.

with each other because the incentive mechanism is used to encourage propagation while the routing mechanism helps to reduce redundant propagation. We combine them in a way that rational nodes are encouraged to propagate only the transactions which are coming from the predefined paths of the routing mechanism. As demonstrated in Algorithm 2, we use the same infrastructure with the routing mechanism, and we include proofs of the intermediary nodes such that their contributions cannot be denied. Each transaction path is defined and secured by a path identifier which includes the public keys of the propagating nodes. Blocks consist of transactions as well as their path identifiers used to claim processing fee shares.

In the recognition phase, each intermediary node conveys the leader credential and the path identifier. Incoming and outgoing path identifiers of a node n are denoted by IN_n and OUT_n, which are used to validate and secure the propagation path. The round leader ℓ produces the initial identifier, $OUT_\ell = H(\mathcal{L}^r, PK_\ell)$, and propagates to his neighbors. Each node n updates the identifier coming from the gradient node by $OUT_n = H(IN_n, PK_n)$. This operation is done just for the gradient node (first one sending $\mathcal{L}^r$), then updated identifier and the credential are forwarded to the neighbors. Nodes may ignore the subsequent identifiers except a client who stores the first N_{con} ones for the transaction phase.

After the routing paths are determined, each client delivers the signed transaction and the incoming identifier to his N_{con} neighbors. The first receiving nodes, check the signature, then add their public keys to the transaction and forward it to their gradient nodes. From that point, each intermediary node in the path first checks the validity of the path via the public keys included and his own identifier, then forwards the transaction including his public key to the gradient node.

Once transactions are received by the round leader, he includes the valid ones into the block. The block consists of the credential, hash of the previous block and valid transactions with their paths. Then, the block is propagated throughout the network.

Incentive for block propagation. As a consequence of the incentive and routing mechanisms, intermediary nodes also have incentives to propagate the block since they share processing fees. Even more, the ones who are closer to the leader would have higher motivation since they probably gain from more transactions.

Algorithm 2 The Combined Propagation Algorithm

Recognition Phase
Leader l propagates $\mathcal{L}^r$
for Each node n_i **do**
  if First time receiving $\mathcal{L}^r$ and $IN_{n'}$ **then**
    if $\mathcal{L}^r$ is valid **then**
      Assign $IN_{n_i} \leftarrow IN_{n'}$ and gradient node as n'
      Compute $OUT_{n_i} = H(IN_{n_i}, PK_{n_i})$
      Propagate $\mathcal{L}^r$ and OUT_{n_i} to neighbors.
    end if
  end if
end for

Transaction Phase
Client c_T provides $Signed(T, IN_{c_T})$ (and $\mathcal{PK} = \emptyset$) to the first N_{con} gradient nodes.
for Each node n_i receiving $Signed(T, IN_{c_T})$ and $\mathcal{PK}$ **do**
  if First time receiving T **then**
    if Signature path holds **then**
      Update $\mathcal{PK} \leftarrow \mathcal{PK} \bigcup \{PK_{n_i}\}$
      Send $Signed(T, IN_{c_T})$ and $\mathcal{PK}$ to the gradient node.
    end if
  end if
end for

Storage efficiency. Any propagation incentive mechanism requires additional data storage than the data itself to keep track of the propagation path. Previous works having incentive [16], [17] utilize signature chains where each node signs the transaction and the public key of the receiver. Therefore, additional to the transaction, the signature package of each propagating node is included. On the other hand, our solution with the path identification benefits from the recognition phase of the routing protocol, and its additional storage requirement is only the public keys of propagating nodes and a signature of the client. Since the ability to claim propagation reward and the validation of the path need to be available, our propagation mechanism demands minimal storage components.

Privacy of the intermediary nodes. Signature chains and the proposed path identifier yield a direct connection between nodes network ID and their public keys. Unlike signature chains, our solution consists of two phases and the propagating nodes validate it by checking whether their input is preserved or not. This enables us to tackle the privacy issue by replacing plain public keys with commitments. Instead of directly including a public key, each node can obscure it in a simple commitment with a random number ($CT_i = H(PK_i, R_i)$). All verifications can be handled with the commitments while

claiming propagation reward requires to reveal it. The commitment version uses the same network structure without compromising the identities of the nodes except clients and the round leader. The location of the round leader and clients will be known to their neighbors. They may need to update their key pairs or replace their connections for the next rounds.

VII. Conclusion

In this work, we investigated two transaction propagation related problems of blockchains: incentive and bandwidth efficiency. We presented an incentive mechanism encouraging nodes to propagate messages, and a routing mechanism reducing the redundant communication cost.

We analyzed the necessary and sufficient conditions providing an incentive to propagate messages as well as to deviate participants (nodes) from introducing Sybil nodes. We studied different types of network topologies and we showed the impossibility result of the Sybil-proofness for the 1-connected model. We formulated the incentive-compatible propagation mechanism and proved that it obeys the rational behavior.

We presented a new aspect of the consensus algorithms, namely first-leader-then-block protocols. We proposed a smart routing mechanism for these protocols, which reduces the redundant transaction propagation from the size of the network to the scale of average shortest path length. Finally, we combined incentive and routing mechanisms in a compatible and memory-efficient way.

Future work and open questions. In Section IV-D, we mentioned the parameter choice and possible outcomes of the incentive mechanism. Detailed effect of incentive model and parameter choice are left as a future work. Another open question is the effect of the incentive mechanism on the topology of the network. Nodes would benefit from increasing their connection to contribute more transaction propagations, i.e., it would increase the connectivity of the network. Using that result, a rigorous analysis on the choice of the C parameter can be done. Finally, there are open problems regarding the economics of the transaction fee: analyzing the accuracy of the de facto formulas in the existing cryptocurrencies with respect to the cost of the propagation and validation and investigating the possible impacts of the sharing fee like decentralization effect.

VIII. Acknowledgment

This work was supported by NWO Grant 439.16.614 Blockchain and Logistics Innovation.

References

[1] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in *Banking Beyond Banks and Money*. Springer, 2016, pp. 239–278.

[2] Y. Sompolinsky and A. Zohar, "Bitcoin's underlying incentives," *Commun. ACM*, vol. 61, no. 3, pp. 46–53, Feb. 2018. [Online]. Available: http://doi.acm.org/10.1145/3152481

[3] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *Financial Cryptography and Data Security - 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers*, ser. Lecture Notes in Computer Science, N. Christin and R. Safavi-Naini, Eds., vol. 8437. Springer, 2014, pp. 436–454. [Online]. Available: https://doi.org/10.1007/978-3-662-45472-5_28

[4] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," in *Financial Cryptography and Data Security - 20th International Conference, FC 2016, Christ Church, Barbados, February 22-26, 2016, Revised Selected Papers*, ser. Lecture Notes in Computer Science, J. Grossklags and B. Preneel, Eds., vol. 9603. Springer, 2016, pp. 515–532. [Online]. Available: https://doi.org/10.1007/978-3-662-54970-4_30

[5] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," in *IEEE European Symposium on Security and Privacy, EuroS&P 2016, Saarbrücken, Germany, March 21-24, 2016*. IEEE, 2016, pp. 305–320. [Online]. Available: https://doi.org/10.1109/EuroSP.2016.32

[6] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi, Eds. ACM, 2016, pp. 3–16. [Online]. Available: http://doi.acm.org/10.1145/2976749.2978341

[7] M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," *CoRR*, vol. abs/1112.4980, 2011. [Online]. Available: http://arxiv.org/abs/1112.4980

[8] N. T. Courtois and L. Bahack, "On subversive miner strategies and block withholding attack in bitcoin digital currency," *CoRR*, vol. abs/1402.1718, 2014. [Online]. Available: http://arxiv.org/abs/1402.1718

[9] I. Eyal, "The miner's dilemma," in *2015 IEEE Symposium on Security and Privacy, SP 2015, San Jose, CA, USA, May 17-21, 2015*. IEEE Computer Society, 2015, pp. 89–103. [Online]. Available: https://doi.org/10.1109/SP.2015.13

[10] S. Bag, S. Ruj, and K. Sakurai, "Bitcoin block withholding attack: Analysis and mitigation," *IEEE Trans. Information Forensics and Security*, vol. 12, no. 8, pp. 1967–1978, 2017. [Online]. Available: https://doi.org/10.1109/TIFS.2016.2623588

[11] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[12] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, 2014.

[13] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, "Is bitcoin a decentralized currency?" *IEEE Security & Privacy*, vol. 12, no. 3, pp. 54–60, 2014. [Online]. Available: https://doi.org/10.1109/MSP.2014.49

[14] A. Miller, J. Litton, A. Pachulski, N. Gupta, D. Levin, N. Spring, and B. Bhattacharjee, "Discovering bitcoins public topology and influential nodes," May 2015.

[15] A. E. Gencer, S. Basu, I. Eyal, R. van Renesse, and E. G. Sirer, "Decentralization in bitcoin and ethereum networks," *CoRR*, vol. abs/1801.03998, 2018. [Online]. Available: http://arxiv.org/abs/1801.03998

[16] M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar, "On bitcoin and red balloons," in *ACM Conference on Electronic Commerce, EC '12, Valencia, Spain, June 4-8, 2012*, B. Faltings, K. Leyton-Brown, and P. Ipeirotis, Eds. ACM, 2012, pp. 56–73. [Online]. Available: http://doi.acm.org/10.1145/2229012.2229022

[17] I. Abraham, D. Malkhi, K. Nayak, L. Ren, and A. Spiegelman, "Solidus: An incentive-compatible cryptocurrency based on permissionless byzantine consensus," *CoRR*, vol. abs/1612.02916, 2016. [Online]. Available: http://arxiv.org/abs/1612.02916

[18] I. Eyal, A. E. Gencer, E. G. Sirer, and R. van Renesse, "Bitcoin-NG: A scalable blockchain protocol," in *13th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2016, Santa Clara, CA, USA, March 16-18, 2016*, K. J. Argyraki and R. Isaacs, Eds. USENIX Association, 2016, pp. 45–59. [Online]. Available: https://www.usenix.org/conference/nsdi16/technical-sessions/presentation/eyal

[19] I. Bentov, A. Gabizon, and A. Mizrahi, "Cryptocurrencies without proof of work," in *Financial Cryptography and Data Security - FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers*, ser. Lecture Notes in Computer Science, J. Clark, S. Meiklejohn,

P. Y. A. Ryan, D. S. Wallach, M. Brenner, and K. Rohloff, Eds., vol. 9604. Springer, 2016, pp. 142–157. [Online]. Available: https://doi.org/10.1007/978-3-662-53357-4_10

[20] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]," *SIGMETRICS Performance Evaluation Review*, vol. 42, no. 3, pp. 34–37, 2014. [Online]. Available: http://doi.acm.org/10.1145/2695533.2695545

[21] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, ser. Lecture Notes in Computer Science, J. Katz and H. Shacham, Eds., vol. 10401. Springer, 2017, pp. 357–388. [Online]. Available: https://doi.org/10.1007/978-3-319-63688-7_12

[22] F. Drucker and L. Fleischer, "Simpler sybil-proof mechanisms for multi-level marketing," in *ACM Conference on Electronic Commerce, EC '12, Valencia, Spain, June 4-8, 2012*, B. Faltings, K. Leyton-Brown, and P. Ipeirotis, Eds. ACM, 2012, pp. 441–458. [Online]. Available: http://doi.acm.org/10.1145/2229012.2229046

[23] Y. Emek, R. Karidi, M. Tennenholtz, and A. Zohar, "Mechanisms for multi-level marketing," in *Proceedings 12th ACM Conference on Electronic Commerce (EC-2011), San Jose, CA, USA, June 5-9, 2011*, Y. Shoham, Y. Chen, and T. Roughgarden, Eds. ACM, 2011, pp. 209–218. [Online]. Available: http://doi.acm.org/10.1145/1993574.1993606

[24] J. M. Kleinberg and P. Raghavan, "Query incentive networks," in *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2005), 23-25 October 2005, Pittsburgh, PA, USA, Proceedings*. IEEE Computer Society, 2005, pp. 132–141. [Online]. Available: https://doi.org/10.1109/SFCS.2005.63

[25] C. Li, B. Yu, and K. P. Sycara, "An incentive mechanism for message relaying in unstructured peer-to-peer systems," *Electronic Commerce Research and Applications*, vol. 8, no. 6, pp. 315–326, 2009. [Online]. Available: https://doi.org/10.1016/j.elerap.2009.04.007

[26] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on bitcoin's peer-to-peer network," in *24th USENIX Security Symposium, USENIX Security 15, Washington, D.C., USA, August 12-14, 2015.*, J. Jung and T. Holz, Eds. USENIX Association, 2015, pp. 129–144. [Online]. Available: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/heilman

[27] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies," in *2017 IEEE Symposium on Security and Privacy, SP 2017, San Jose, CA, USA, May 22-26, 2017*. IEEE Computer Society, 2017, pp. 375–392. [Online]. Available: https://doi.org/10.1109/SP.2017.29

[28] Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, and J. S. Rosenschein, "Bitcoin mining pools: A cooperative game theoretic analysis," in *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems, AAMAS 2015, Istanbul, Turkey, May 4-8, 2015*, G. Weiss, P. Yolum, R. H. Bordini, and E. Elkind, Eds. ACM, 2015, pp. 919–927. [Online]. Available: http://dl.acm.org/citation.cfm?id=2773270

[29] J. Travers and S. Milgram, "The small world problem," *Phychology Today*, vol. 1, pp. 61–67, 1967.

[30] R. Albert and A.-L. Barabási, "Statistical mechanics of complex networks," *Reviews of Modern Physics*, vol. 74, no. 1, p. 47, 2002.

[31] P. Erdös and A. Rényi, "On the evolution of random graphs," *Publ. Math. Inst. Hung. Acad. Sci*, vol. 5, no. 1, pp. 17–60, 1960.

[32] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin P2P network," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, November 3-7, 2014*, G. Ahn, M. Yung, and N. Li, Eds. ACM, 2014, pp. 15–29. [Online]. Available: http://doi.acm.org/10.1145/2660267.2660379

[33] G. C. Fanti and P. Viswanath, "Deanonymization in the bitcoin P2P network," in *Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017, 4-9 December 2017, Long Beach, CA, USA*, I. Guyon, U. von Luxburg, S. Bengio, H. M. Wallach, R. Fergus, S. V. N. Vishwanathan, and R. Garnett, Eds., 2017, pp. 1364–1373. [Online]. Available: http://papers.nips.cc/paper/6735-deanonymization-in-the-bitcoin-p2p-network

[34] P. Koshy, D. Koshy, and P. D. McDaniel, "An analysis of anonymity in bitcoin using P2P network traffic," in *Financial Cryptography and Data Security - 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers*, ser. Lecture Notes in Computer Science, N. Christin and R. Safavi-Naini, Eds., vol. 8437. Springer, 2014, pp. 469–485. [Online]. Available: https://doi.org/10.1007/978-3-662-45472-5_30

[35] S. B. Venkatakrishnan, G. C. Fanti, and P. Viswanath, "Dandelion: Redesigning the bitcoin network for anonymity," *POMACS*, vol. 1, no. 1, pp. 22:1–22:34, 2017. [Online]. Available: http://doi.acm.org/10.1145/3084459

[36] T. Neudecker, P. Andelfinger, and H. Hartenstein, "Timing analysis for inferring the topology of the bitcoin peer-to-peer network," in *2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), Toulouse, France, July 18-21, 2016*. IEEE Computer Society, 2016, pp. 358–367. [Online]. Available: https://doi.org/10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0070

[37] M. Berini Sarrias, "Bitcoin network simulator data explotation," Master's thesis, Universitat Oberta de Catalunya, 2015.

[38] T. Nepusz, "IGraph: High performance graph data structures and algorithms," 2006–. [Online]. Available: http://igraph.org/python/

[39] A. Fronczak, P. Fronczak, and J. A. Hołyst, "Average path length in random networks," *Physical Review E*, vol. 70, no. 5, p. 056110, 2004.

[40] Statoshi Team, retreived 13 Feb. 2018. [Online]. Available: http://statoshi.info

[41] B. Faltings, K. Leyton-Brown, and P. Ipeirotis, Eds., *ACM Conference on Electronic Commerce, EC '12, Valencia, Spain, June 4-8, 2012*. ACM, 2012. [Online]. Available: http://dl.acm.org/citation.cfm?id=2229012

[42] N. Christin and R. Safavi-Naini, Eds., *Financial Cryptography and Data Security - 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers*, ser. Lecture Notes in Computer Science, vol. 8437. Springer, 2014. [Online]. Available: https://doi.org/10.1007/978-3-662-45472-5