Propagation Delay in Bitcoin Networks: Issues and Countermeasures

Khaled Tarmissi
Umm al-Qura University
Atef Shalan (amohamed@georgiasouthern.edu)
Georgia Southern University
Abdullah Al Shahrani
Umm al-Qura University
Rayan Alsulamy
Umm al-Qura University
Saud S. Alotaibi
Umm al-Qura University
Sarah Al-Shareef
Umm al-Qura University

Research Article

Keywords: Bitcoin network, blockchain, cryptocurrency, propagation delay.

Posted Date: June 10th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1735532/v1

Propagation Delay in Bitcoin Networks: Issues and Countermeasures

Khaled Tarmissi[a,**], Atef Shalan[b,**], Abdullah Al Shahrani[a], Rayan Alsulamy[a], Saud S. Alotaibi[a], Sarah Al-Shareef[a]

[a] *College of Computer and Information Systems, Umm A-Qura University, Makkah, KSA*
[b] *College of Engineering and Computing, Georgia Southern University, GA, USA*

Abstract

Bitcoin (₿) synchronizes a public ledger over a large decentralized blockchain network as underlying infrastructure. Propagation delay among long chains of network nodes is a major threat to message dissemination and integrity of digital currency transactions. In this paper, a comprehensive survey presents state-of-the-art analytical studies on the bitcoin network. The survey describes the problems caused by the delay of dissemination and discusses the solutions proposed to enhance the propagation delay in the current literature. First, an overview of propagation algorithms is discussed by focusing on the bitcoin network. Then, the factors that have impacts on the delay and their issues are introduced. Improvement of the delay and some countermeasures are presented next. Finally, our conclusion and future research recommendations are also discussed.

Keywords: Bitcoin network, blockchain, cryptocurrency, propagation delay.

*Corresponding author 1
**Corresponding author 2
Email addresses: kstarmissi@uqu.edu.sa (Khaled Tarmissi), amohamed@georgiasouthern.edu (Atef Shalan), s43780409@st.uqu.edu.sa (Abdullah Al Shahrani), rooni.1413@gmail.com (Rayan Alsulamy), ssotaibi@uqu.edu.sa (Saud S. Alotaibi), saashareef@uqu.edu.sa (Sarah Al-Shareef)

1. Introduction

Blockchain technology emerged as part of the continuous innovation of the Internet. In this technology, computers follow some protocols that allow communicating with each other [1]. In 2008, Bitcoin was conducted by one or a group of researchers as the first cryptocurrency that applies Blockchain technology [2]. The bitcoin network is defined as an open ledger of a database synchronized between all nodes in the distributed and immutable environment. The main purpose beyond the underlying structure of the Bitcoin network is to eliminate a centralized environment in which no intermediaries can manage data and transactions[1] [3]. Despite being highly secure due to the cryptographic Public Key Infrastructure (PKI) principle, the bitcoin network suffers from some issues which need to be addressed and solved in future research on this domain. One of these issues is the challenge of the network's ability to reach a consensus among parties who do not trust each other across vast distances without any control or authority.

Since blockchain inception, researchers have studied most issues and proposed solutions to the adversarial strategies and security vulnerabilities [4]. Information propagation (transmission time plus verification time) is responsible for disseminating transactions and blockchain records (or blocks) on the bitcoin network. Data propagation is in charge of most of the security issues in anonymity and decentralized network such as bitcoin. As a result, data propagation has been gaining more attention in the blockchain research field. This research includes various types of attacks from double-spending attacks to inconsistencies in the replicas of the ledger, in addition to other attacks like partition attack and eclipse attack, which take advantage of the propagation delay.

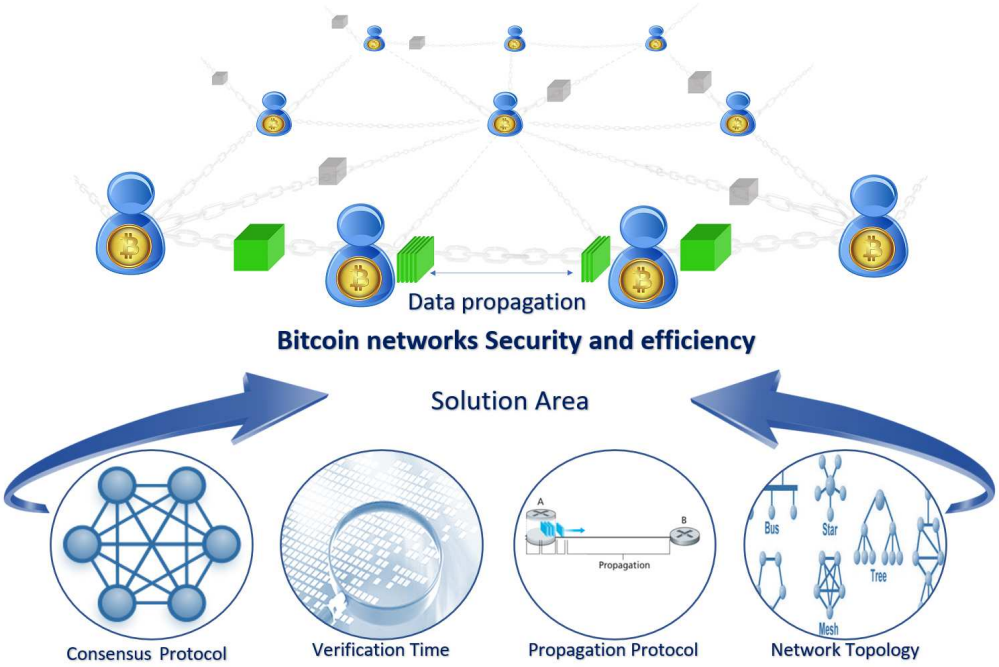

Figure 1: Message exchange using the pipelining technique.

1.1. Contributions

Our research in this paper aims to investigate the impacts of information propagation delay on the security of the bitcoin network and its efficiency. We survey the cutting-edge research on information propagation delay and study their effectiveness as countermeasures against the propagation delay impacts. Based on our study, we classify the existing solutions that enhance propagation delay into four categories as shown in Fig.1. These categories are also listed below:

1. Change consensus protocol
2. Minimize verification time
3. Propagation protocol
4. Network topology

[1] A bitcoin transaction (or simply transaction) means the network information representing the operation of sending bitcoins between network addresses.

In that way, we can identify countermeasures based on these four categories and demonstrate a research plan for those enthusiastic about this topic.

1.2. Organization

This paper is organized as follows: Section 2 provides an overview of information propagation mechanisms. Section III introduces analytical studies which tackle propagation and its implications. Section IV details the current research for improving dissemination over the bitcoin networks. Section V lists recommendations for future researchers. Finally, Section VI concludes this work.

2. Overview of Propagation Mechanisms

A propagation mechanism describes how a bitcoin transaction or a block spreads through the network to all nodes, where all the information is expected to be received completely. Unfortunately, that does not happen due to some network scalability and security issues, e.g., partitioning of the network [5]. The propagation mechanisms used in blockchain are described below.

Advertisement-based information dissemination

This is an information dissemination protocol (a Gossip-like protocol) in which a network node advertises the information to its peers as it receives it. This protocol is used in the bitcoin network essentially. When node A receives a message, it announces it to its peer using inv-message. A node B, a peer of node A, responds using getdata-message if the message has not been received yet. Otherwise, no action will be taken [6][7].

Send headers

This is an updated form of the previous mechanism. Here, nodes can send block headers directly to their peers without sending an inv-message to reduce the latency and decrease bandwidth overhead [7].

Unsolicited block push

When the miner mines a block, then there is no need for the block to be advertised because it has not been known yet among the other nodes. This reduces the overhead bandwidth and time latency [6].

Relay networks

This mechanism allows miners to share a mining pool using transaction ID since it has less size than the transaction itself. Consequently, the transaction is replaced by its ID in the block during broadcasting to minimize the delay [7].

Hybrid push/advertisement systems

In this mechanism, when node A has n peer, it will announce the block to the $\sqrt{n}$ and push the block to $n - \sqrt{n}$. This protocol is used in Ethereum [7].

3. ANALYTICAL STUDIES ON PROPAGATION DELAY

According to the decentralization of the bitcoin network, the information, as transactions or blocks, has to reach a consensus for verification and validation. There are common factors that have a direct impact on the propagation and that are causing inconsistencies in the replica. This section describes these negative factors followed by a description of the inconsistencies resulting from the propagation delay.

3.1. Negative Factors on Propagation Delay

Analysis of information propagation in the bitcoin network, presented by [8],[9],[6],[10], and [11], concentrated on the following factors:

NETWORK SCALABILITY

While the bitcoin network relies on participating nodes with no central authority, a transaction has to be transmitted through all of them. When the number of nodes increases, the transmission speed will be slower.

BANDWIDTH OVERHEAD

Taking bandwidth into account, the number of exchanged messages affects propagation delay. That means increasing the bandwidth overhead delays the propagation.

BLOCK SIZE

Since the inception of bitcoin, the number of transactions has been limited and still increasing gradually. As presented in www.blockchain.com, in Aug 2021, the average number of transactions per block is 2000 [12]. When the number of transactions increases, the size of the block becomes more extensive, which will affect the speed of the block propagation over the network.

LINK LATENCY

When the node creates a transaction and broadcasts it to the peers, the transmission time processing is the link latency between the origin node and its peer. When the origin node is far away from the peer, the link latency will be lower.

CLIENT BEHAVIOR

Node session length refers to client behavior and how long the client is connected to the network. When the node connects for a while and then gets disconnected, this will affect the links between the peers and thereby the network topology which is in charge of affecting the propagation processing.

NETWORK TOPOLOGY

As the nodes connected randomly to each other based on network protocols, every node maintains a list of Domain Name Services (DNSs) returning IP addresses of peers. Such a random connection provides non-compulsory hops that will affect the propagation by wasting time to disseminate over them.

3.2. Threats and obstacles due to propagation delay

As we mentioned, the propagation delay causes some security issues and affect the performance. Below, we describe each of them briefly.

REPLICA INCONSISTENCY

When the transmission of a message becomes slow during dissemination, the synchronizing of the ledger will be a challenge, thereby leading to many potential risks like double-spending, partitions, and eclipse attacks.

double-spending ATTACK

From an information propagation perspective, several research efforts have studied and analyzed this problem. Because of the inconsistency in the replicas, double-spending might occur and abuse the public ledger [13]. The adversary may spend the same coin twice. When the attacker creates two transactions (t_a, t_m) with the same input and different recipients. In such a case, t_a will be sent to the majority and t_m will be sent to the merchant. If t_a was accepted by the majority, then t_m will not be valid and got rejected by them. In this situation, we consider double-spending as a successful attack. The risk of double-spending will increase with slower transaction propagation.

PARTITION ATTACK

The blockchain fork is addressed by [8] and [9]. In this case, we can say, a partition occurs when there is more than one head in the Blockchain and the nodes do not agree on which block is the head of the chain [14]. By that time, the longer chain will become adopted as the main chain and the shorter one will be removed by the nodes. That forms so-called stale blocks or orphan blocks, in which those blocks increase the advantage of double-spending and eclipse attacks. Most of the advisories exploit these blocks to do their malicious

activities. The propagation delay pertained to the occurrence of partitions on the network by delaying the ledger synchronization.

3.3. COUNTERMEASURES

In this section, most of the countermeasures that were proposed to improve propagation delay in the bitcoin network are introduced.

Karame et al. [15] proposed a set of countermeasures that enable detecting the double-spending attack on the bitcoin fast payment. The first method is performed by waiting for a few periods of time after receiving a transaction from a node and before sending a service back to it. These waiting periods are considered to check whether there is a conflict with another transaction that has the same input. Another solution to detect double-spending is to set an observer as a node that directly relays all transactions to the vendor to be aware of double-spending. The third solution is to adopt a bitcoin peer which alerts to conflict transactions.

Bamert et al., [16] minimized the double-spending problem chance in fast payment scenarios by proposing some strategies that improve the payment processing time. They suggested that the merchant should not accept a direct transaction from the sender itself. Additionally, the merchant has to be connected to random nodes as large as possible to avoid any possibility of fault transaction injection.

Decker et al., [8] proposed three methods to speed up and improve the propagation information in the network. The time it takes to verify the block is the major contributor to the propagation delay, and there is a correlation between block size and the time spent to be verified.

The second method is pipelining block propagation. Fig.2 shows this technique, which can be done immediately by forwarding inv messages to neighbor nodes utilizing the round-trip times between nodes and its neighbors by an-

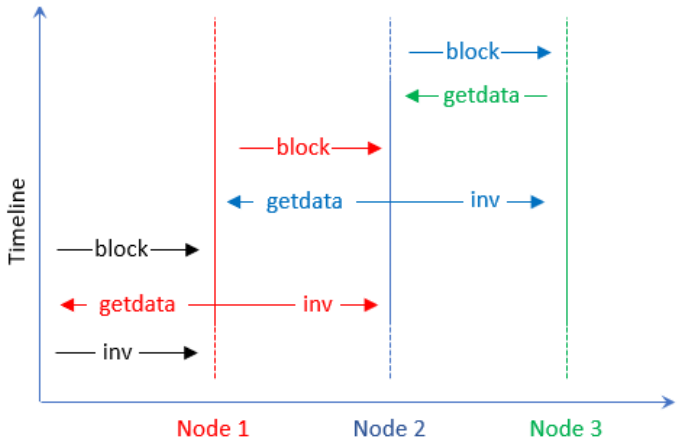

Figure 2: Message exchange using the pipelining technique.

nouncing block availability earlier before getting it.

One of the limitations is the advisory may announce a number of fake blocks in which he cannot provide them when asked for it. The third method works by shortening the distance between the nodes using a star-sub graph network. Hence, the hub between every two nodes became near to 2 hubs. However, this method can work efficiently on a small network, but it can cost vast bandwidth in the larger network.

An analysis of the feasibility of partitioning attack on the bitcoin network was presented by Neudecker et al., [9]. They proposed a simulation model that studied a feasible attack on the bitcoin network topology. The model was parameterized based on some measurements like peer's session length and link latencies between them which were performed by using the bitnodes.io project that provide a crawler for a reachable node on the bitcoin network. As a result, validating the model displayed correspondence with information propagation on a real bitcoin network. The analysis that revealed the control of 6000 of the peers makes less chance for the attacker to be exploiting the partitions on the network.

Gervais et al., [6] Studied and devised various optimal strategies for double-spending and selfish mining PoW blockchain. They presented a novel quantitative model that analyzes different implications on PoW blockchain. They simulated a model of PoW-Blockchain and network layer, which mimics aspects of real-world network and Blockchain parameters, which were modeled based on Markov Decision Process (MDP). They presented crawler nodes for different PoW Blockchain-based instances, which in turn measured stale blocks rate (Table.1). They fed their model as input to quantify the optimal attacker strategies for double-spending and selfish mining. The result showed the impacts of network parameters on the security of PoW Blockchain for stale blocks on double-spending and selfish mining.

Bitcoin network measurement was presented by [10] for simulating and validating transaction propagation. They discussed the effect of delay on the security due to inconsistencies in the replicas that lead to the opportunity of double-spending and then abuse the public ledger. They run a real bitcoin client that works as a crawler for learning the number of reachable connected nodes and their session lengths precisely.

In addition, they implemented a measuring node that has the same behavior as the real bitcoin node, such a node is connected to peers, and therefore, it can create and propagate transactions. The measuring node was able to track

Table 1: Comparison of different bitcoin forks. Stale block rate (r_s), average block size (s_B), t_{MBP} stands for median block propagation time [9]

	Bitcoin	**Litecoin**	**Dogecoin**	**Ethereum**
Block interval	10 min	2.5 min	1 min	10-20 seconds
Public nodes	6000	800	600	4000
Mining pools	16	12	12	13
t_{MBP}	8.7 s	1.02 s	0.85 s	0.5-0.75 s
r_s	0.41%	0.273%	0.619%	6.8%
s_B	534.8KB	6.11KB	8KB	1.5KB

that transaction over the dissemination on the network, thereby calculating the propagation delay differences between sending time and the received time by each node. Fig.3 shows the distribution of propagation in a real network compared to the simulation. The result revealed that increasing the number of nodes has a direct impact on propagation delay and not all the nodes except rare cases receive the transaction while dissemination.

Three different bitcoin models were presented by Sallal et al., [17] to enhance the propagation delay on the bitcoin network. The first method is called Bitcoin Clustering-Based Super Node (BCBSN) that parametrized based on a real bitcoin network. Here, they created a bitcoin client that crawls the network and gathers the required data, i.e. number of reachable nodes, peers' session length, and link latencies between them.

The main idea of the BCBSN model is to reduce the non-compulsory hops thereby enhancing the propagation delay by building a bitcoin network using clustering peers in which each cluster is maintained by a node called a super node. This super node is known for other super nodes and other nodes which are connected to super nodes. Both super nodes and other nodes are structured

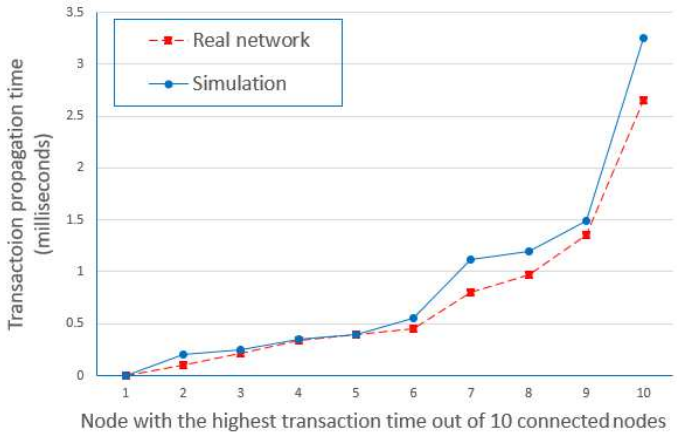

Figure 3: Distribution of propagation in the real network compared to the simulation [10].

based on some features like higher weighted, node reputation and geographical algorithms. Fig.4, from [18], shows a significant decrease of propagation delay for the BCBSN protocol in comparison to the existing bitcoin protocol.

In addition to BCBSN, Fadhil et al., [19] presented Locality-Based Clustering (LBC) protocol to form peers' connections with an aim of reducing the non-compulsory hops and improving propagation delay. Based on a threshold distance, the node measures the distance to the discovered node and send a JOIN request to it. Once the connection it is established, it learns the IP's of the nodes which belong to the same cluster. By evaluating this method, the result showed a decrease in the propagation delay compared to both the real and BCBSN protocols as depicted by Fig.5.

Finally, Fadhil et al., [19] presented a proximity-based clustering approach (BCBPT) using time latency to structure peer nodes of the bitcoin network. The key reason behind this is to decrease the links between nodes and hence reduced latencies between them. The results of all the three proposed methods by Fadhil et al., [10] are displayed in Fig.6 which demonstrates the decrease of propagation delay distribution. Unfortunately, LBC protocol is susceptible

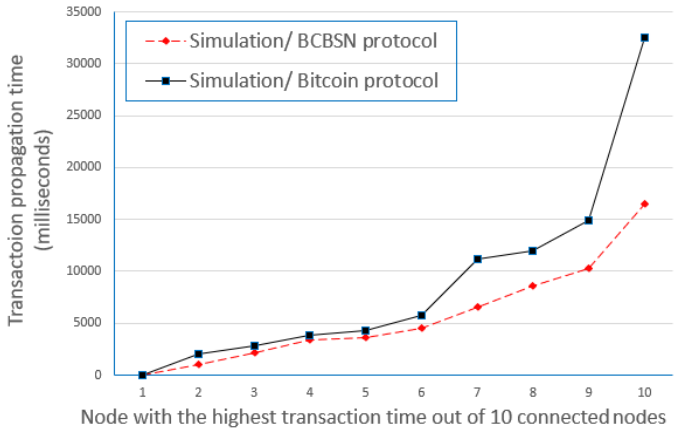

Figure 4: Comparison of the distribution of the transactions of connected nodes as measured in the simulated bitcoin protocol with BCBSN protocol simulation results [18].

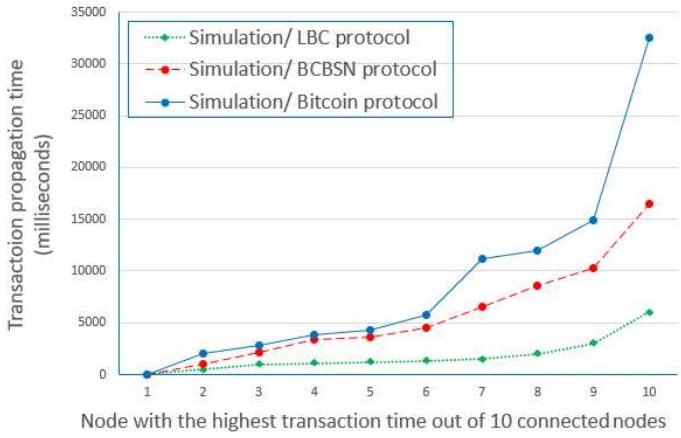

Figure 5: Propagation delay distribution as measured in real bitcoin, BCBSN, and LBC [19].

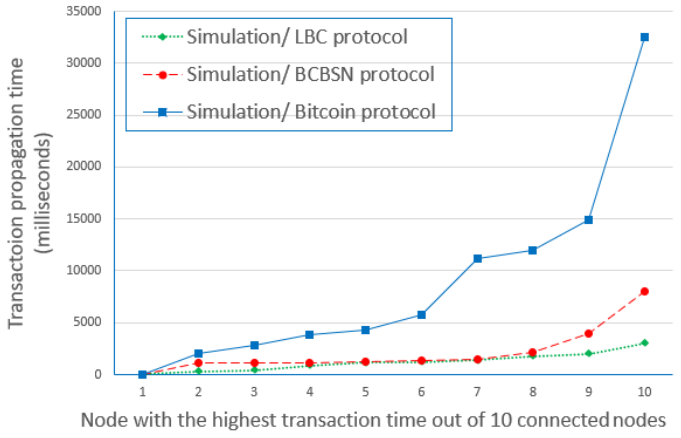

Figure 6: Propagation delay distribution as measured in real bitcoin, LBC, and BCBPT [20].

to adversarial activities like partitioning and eclipse attacks which reduces the randomness for peer selection and thereby decreases the security of the network. As the node's behavior is unstable, all the proposed methods will suffer from clients joining and disjoining while looking for an optimal peer every time. Furthermore, the researchers above conducted an improvement of their previous protocol (BCBSN) called Master Node Based Clustering (MNBC). In MNBC protocol, the master nodes are fully connected based on proximity and informa-

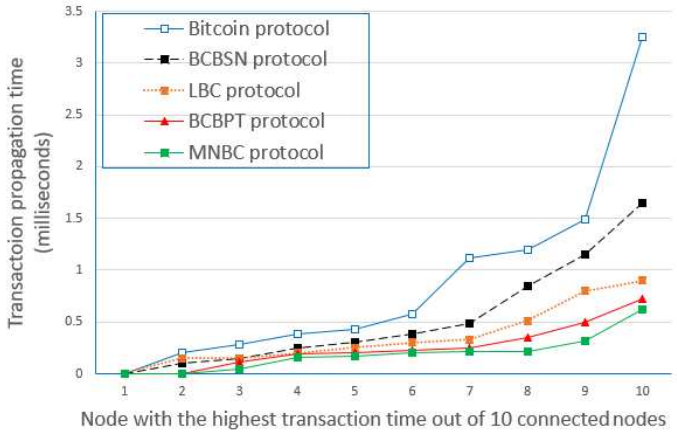

Figure 7: Comparison of different proposed method with the real protocol [10].

tion can be transferred between master nodes as well as the normal nodes. The main idea for this is to reduce occurrence of partition attacks. Fig.7 shows the result of evaluating all of the aforementioned protocols.

Stathakopoulou et al., [21] conducted a dissertation that tries to address the problem of consensus on transaction history by minimizing propagation delay by using pipelining messages. Here, inv message sent directly to peers as soon as it arrives and while the node waiting for getting the data without verifying that message to be spread rapidly over the network. In addition, they tried to increase connectivity of the geographically closest nodes to speed up information propagation. Implementing this method showed that when increasing connectivity to the closest peers, the average of requesting data of inv message was decreases from 0.86 to 1.14, and when pipelining mechanism applied to the broadcasting transactions, the average time a transaction has to be propagated was decreased to 0.2943 sec whereas without pipelining was 0.7474 sec. By combination of the two proposed solutions, the average percentage of announced transactions was 71%. Despite of the effectiveness of that solution, their suggestions signify compromises on security. This allows the advisory to

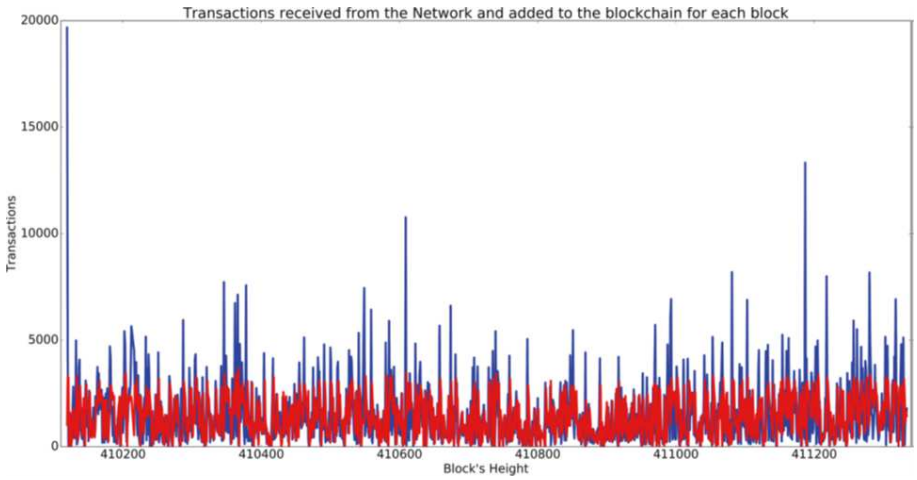

Figure 8: Comparison of observed transactions in a period of time and the transactions included in blocks in the same time [22].

flood the network by fake transactions. Additionally, connecting to the closest peers using selection method is vulnerable to an eclipse attack.

Fig.8 shows the comparison of observed transactions in a period of time and the transactions included in blocks within the same time-frame. The authors recommended setting enough transaction fees as a countermeasure to timely incentive the miners to process and to guarantee their inclusion to the blockchain. Analysis of the bitcoin network and observation of the transaction and block dissemination was presented by Pappalardo et al., [22]. They used a bitcoin client that can establish connections with peers and able to monitor the network activities for a period of time to identify transaction appearance in the Blockchain network. In addition, they measured the propagation mechanism and the time of including the transaction or block to the blockchain. By observing the network, the result revealed that 42% of the low values transactions were not included in the ledger of the chain after 1 h from their appearance and 20% were not included after 1 month. This was not because of the block size but because of the lower fees that did not motivate the miners to mine those

transactions.

Marçal et al., in [11] studied the problem of minimizing exchange messages between nodes which allows saving the bandwidth without affecting the current approach. The main goal is to decrease the number of duplicated advertisements over the network and ensure that the transaction get to miners. Some algorithms were applied to predict miners or peer nodes connected to the miners based on some priorities. Every node maintains a list of transactions sent by the peers and time taken to be bunched in a block. By implementing the method and analyzing the result, the results showed a bandwidth reduction of 10.2% and the number of exchanged messages were reduced by 41.5%. However, they implemented the method in a stable network. If we take a client behavior into consideration, this method might be useless as the client's behavior changed every time because of the session's length. Sudhan et al., [23] studied the ledger inconsistencies which is caused by transaction propagation delay in the network. These inconsistencies help to double-spending twice. They proposed a peer selection technique to find the best combination of the number of outgoing connections, randomly or a proximity based, to reduce propagation delay. This method has two characteristics: the number of outgoing connections is

Table 2: Propagation delay varying proximity (NP) and randomly (NR) order of time and based on threshold distance (DT)[23]. NP: Nodes selected based on threshold (proximity), NR: Nodes selected randomly outside proximity parameter, DT: Threshold Distance

NP	**NR**	**DT**
6	2	1500
6	2	3000
4	4	1500
2	6	1500
4	4	3000
6	2	5000
Random Selection. (default in bitcoin protocol)		
4	4	5000
2	6	3000
2	6	5000

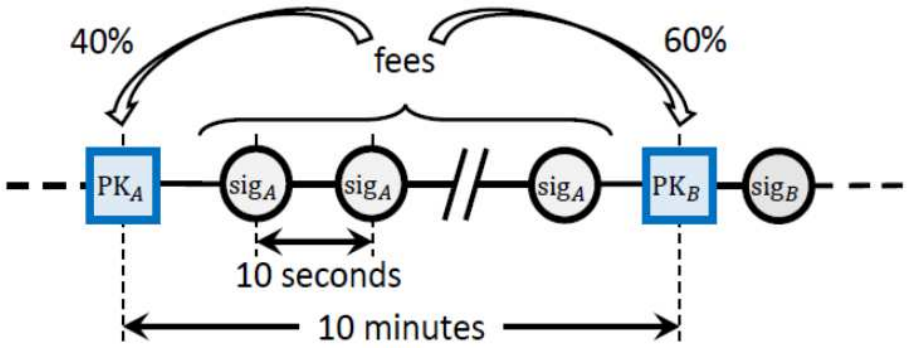

Figure 9: Design of the bitcoin-NG protocol. Microblocks are denoted by circles and Key blocks by squres. in which microblocks signed by the current leder and the fees shared between the current leder (40%) and the next one(60%). [24].

changeable and selection technique is based on both proximity and randomness.

The evaluation of the results is shown in Table.2. As it shows, the optimal number of outgoing connections was 6 outgoing connections based on proximity and 2 outgoing connections randomly in the distance of 1500. By applying the peer selection algorithm, the propagation delay decreased when the outgoing connection has a high number of connections. However, this method has the potential of eclipse attack.

Bitcoin NG is a new Blockchain protocol proposed by Eyal et al., [24] to tackle the problem of scalability, which is one of the issues that causing propagation delay in the bitcoin network. It decouples the block into two types: one for electing a leader called block key and the other for recording the transactions called microblock. Miners are competing to become a leader, in which the winner will be responsible for serializing the transactions till a new leader appears. Time is divided into epochs, in which each epoch has a single leader. By applying this method, the leaders will be in charge of recording transactions and generating the block in that epoch, and other nodes are responsible for exchanging the messages between the peers. Fig.9 shows the structure of this protocol, which accelerates transaction confirmation and improve the latency.

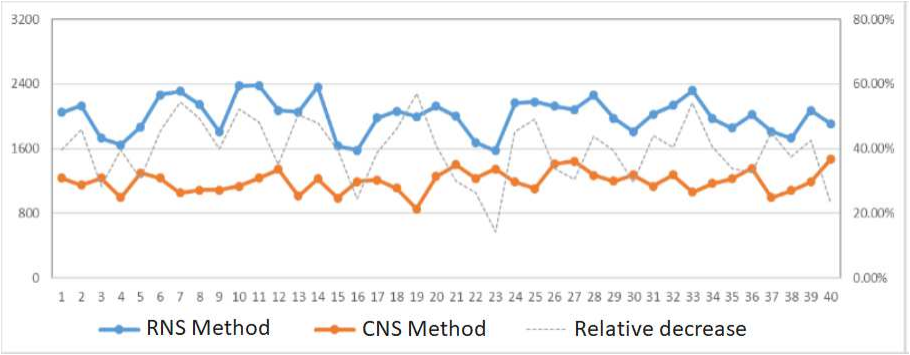

Figure 10: Comparison of Random Neighbor Selection (RNS) and CNS with average latency. [25].

However, this method is vulnerable to selfish mining attack. This introduces a tradeoff between security and bitcoin network where the leaders, who control most of the processes in the network, pose a threat to the community and the protocol.

Bi et al., [25] proposed a method called Closest Neighbor Selecting (CNS) for selecting closest peers based on Round Trip Time (RTT). RTT is used to measure the distance between connected peers. The smaller the distance, the closer the node. They claim that the method accelerates the propagation process and gives a better performance as shown in Fig.10. However, the CNS method has some limitations. For this, the authors had implemented it on a network with a small number of nodes (max experiment nodes were 40). Which increasing the number of the nodes, CNS did not produce an accurate result. Furthermore, the ability to select the peers increases the advantages of eclipse attack and decreases the randomness thereby compromising the security of the Blockchain network.

Compact block was presented by Corallo [27], [26] that used Bloom filter idea to reduce the bandwidth overhead of a new block propagation to full nodes. Rather than sending a whole block, the node sent a sketch to the peer which

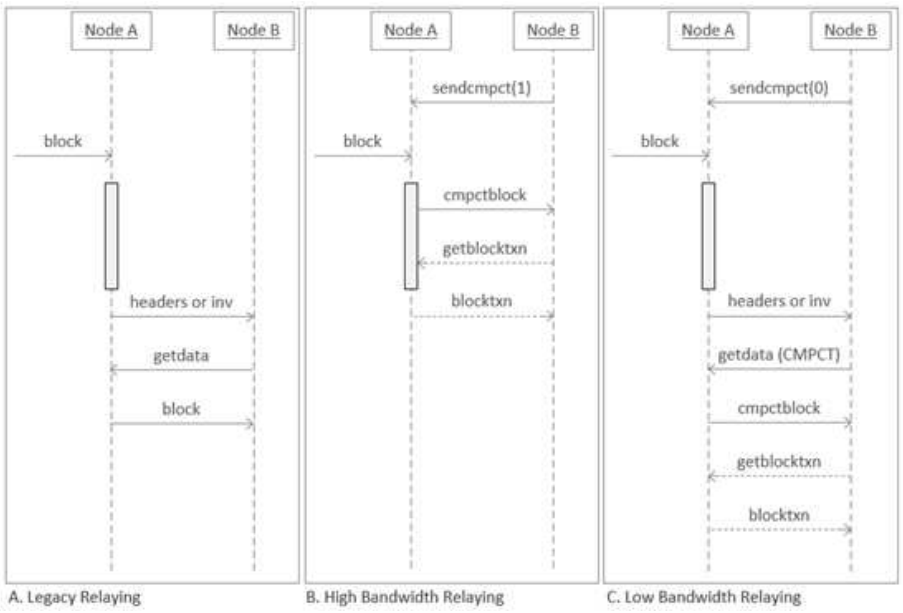

Figure 11: Classic block relaying compared to Compact Block with high and low bandwidths relaying [26].

contains only the block header, transactions IDs and the full transactions which are not expected to be received by the peer before. Once the peer receives that sketch, it tries to reconstruct the block based on the information in the header and the transactions which in its memory pool. If there is a need for some transaction, it will send a request for that missing transaction from the block sender. This approach has the advantages of sending the transaction once in the best case which reduces the amount of bandwidth and improves the propagation delay. Fig.11 shows the standard block relaying compared to compact block with high and low bandwidths relaying.

Tschipper [28] presented an update model of compact block protocol called Xtreme Thinblock by adding Bloom Filter to the compact block. Precisely, as shown in Fig.12, when an inv message sent to get a missing block, it sends a Bloom filter of its transactions along with the request. This method reduces the

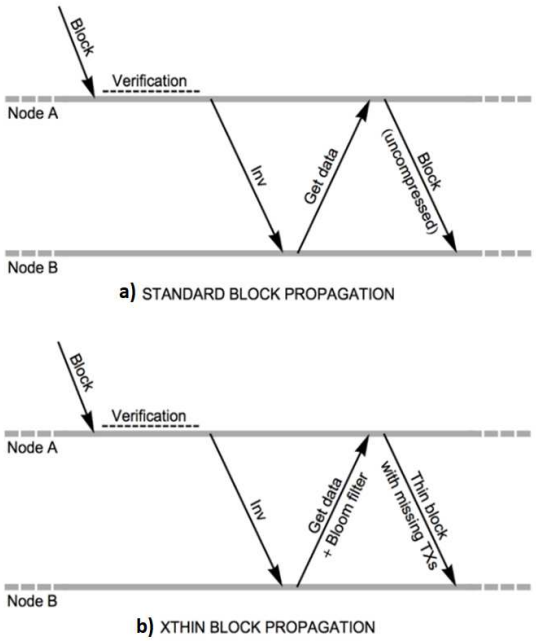

Figure 12: Classic block relaying compared to Compact Block with high and low bandwidths relaying [28].

message exchange into 2 but with a larger size compared to a compact block. However, taking the Bloom filter into account, it produces positive false values which in its turn affects missing of transactions. Researchers in [29] and [30] discussed the use of Invertible Bloom Lookup Table (IBLT) to reduce block propagation. The block to be sent computes the IBLT and sends to the peer to be compared with the IBLT mempool. The symmetric difference between them is the missing transactions where the largest IBLT will returned. However, this method has to be addressed and evaluated formally.

Ozisik et al., [31] proposed a protocol called Graphene, which merge the two previous methods: Bloom filter and IBLT to efficient block propagation. The solution uses Bloom filter to compute the symmetric difference between mempool and the block, and then applies ILBT to recover from Bloom filter errors.

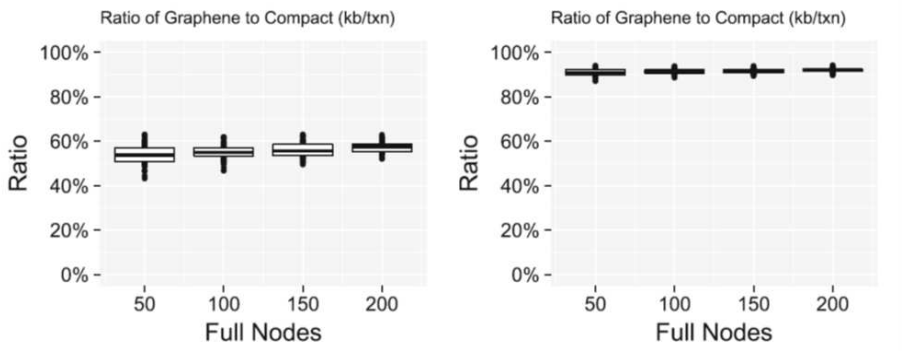

Figure 13: Graphene reduces traffic to 60% of the cost of Compact Blocks (or to 10% for total traffic, which includes transaction data) [31].

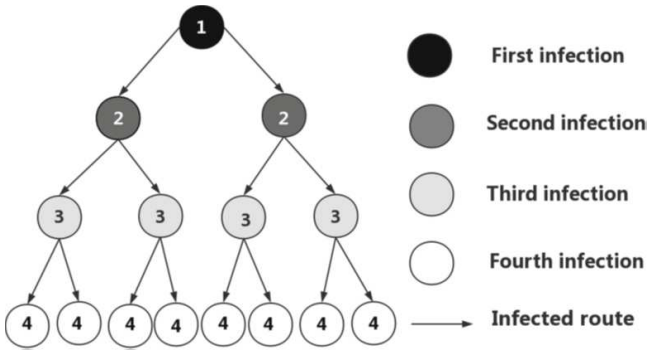

Figure 14: Structure of network broadcasting [32].

In details, the sender sends the header, ILBT, I, and Bloom filter of block transactions IDs, S. The receiver uses S to find out the transactions found in S, m', then recovers from error by computing I'="ILBT"(m') to decode it with I. If I-I' is decoded, then the transaction IDs included on the block. They claimed that their solution reduces the bandwidth overhead to about 60% in comparison to Compact Blocks as shown in Fig.13.

A Tree Based Network routing protocol presented by Kan et al., [32]. The concept of this protocol is to disseminate the messages based on the tree structure as shown in Fig.14. As a result, they claimed that their protocol can speed up

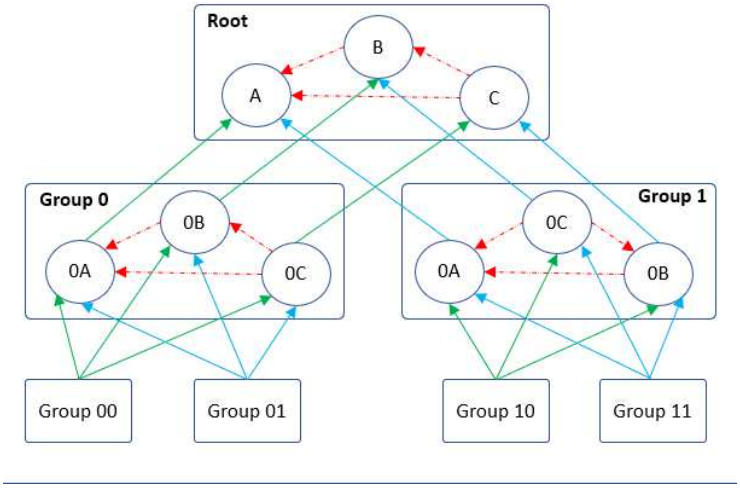

Figure 15: Broadcasting tree based with clusters [32].

the broadcast process and minimizes path duplication. When a node joins the network, it is connected as a leaf node. In case of exchanging the message, the originator node propagates the message to its parent and two children. Then, the message will be forwarded to others except the sender node.

However, because the message was sent in one way, the protocol is vulnerable to a single point failure. They overcame this problem by using cluster group. Here, each group will have 3 nodes, which are connected to each other. Each node is connected to its parent and children on other cluster groups. In case of node failure, the cluster still connected by buddies or children on another cluster group (Fig. 15).

Table.3 shows a comparison of the aforementioned countermeasures.

4. FUTURE RESEARCH RECOMMENDATIONS

Through our study of various proposed solutions to propagation delay problem, we are going to introduce some important findings to researchers in this

Table 3: Comparison of different countermeasures

Research	Methods	Features	Limitations
Decker et al., [8]	Minimize verification	Speedup transaction propagation	allow fake transactions to be flooded the network
	Pipelining block propagation	resistant to partitioning attack	Bandwidth overhead
	Connectivity increase		
Neudecker et al.[9]	Bitcoin Simulation Model to find partitioning attack on the bitcoin network	controlling of 6000 of the peers make less chance to attacker to be exploiting the partitions on the network	
Karame et al. [15]	waiting a few periods of time after receiving transaction to detect conflicting	Detect double-spending attack bitcoin fast payment	Still double-spending can occur in which the basic problem not solved
	Set observer node to relay all transitions to vender		
	Adopt node to alert about conflicting		
Bamert et al., [16]	merchant should not accept a direct incoming connection from the sender directly	minimized double-spending problem chance in fast payment	attacker could still be propagated to the majority
	merchant has to be connected to as large random nodes		
Gervais et al., [6]	Studying and devising various optimal strategies for double-spending and selfish mining PoW blockchain	presented a novel quantitative model that analyzing different implication on PoW blockchain	
Fadhil et al., [10]	Measurements for simulating bitcoin network	Transaction propagation measurements 2. Bitcoin network measurements	
Statha et al., [21]	pipelining messages	enhance information propagation delay	Allow non-exist transactions to be exchanged
	increase connectivity of the geographically closest nodes		

Sallal et al., [17]	Clustering based on super node Clustering based on locality Clustering-based ping time protocol Master node based clustering	Improve the propagation delay significantly	Vulnerable to portioning and eclipse attacks
Pappalardo et al., [22]	Analysis of the bitcoin network and observation of the transaction and block dissemination	incentive miners with enough fees	
Marçal [11]	Algorithm to predict miners or peer nodes connected to them	decrease the number of duplicated advertisements over the network	implemented the method in a stable network
Sudhan et al., [23]	peer selection technique to find the best combination of the number of outgoing connections either randomly or a proximity-based	to reduce propagation delay	potentially of eclipse attack
Eyal et al., [24], [33]	decouples the block into two types: block key for leader and microblock for recording the transactions	accelerate transaction confirmation and improve the latency	is vulnerable to selfish mining attack
Bi et al., [25]	selecting closest peers based on Round Trip Time	accelerated the propagation process and give a better performance	implemented the method on the small size of nodes, it also decreases the randomness of connecting to a peer
Corallo [27], [26]	Send compressed block rather than the whole block	sending the transaction once in the best case reducing the amount of bandwidth	Node has to receive the transaction initially before the block exchanged
Tschipper [28]	adding Bloom Filter to the compact block	reduced the message exchange into 2 but with a big size compared to compact block	Positive false of bloom filter values

Andresen [29] and Russel [30]	using Invertible Bloom Lookup Table (IBLT)	to reduce block propagation	Need to be evaluated formally
Ozisik et al., [31]	Bloom filter and IBLT (Graphene protocol)	efficient block propagation	A node must have 15% or more in mempool of the propagated block
Kan, Jia et al.[32]	Tree Based Network routing protocol	speed up broadcast process and minimize duplication	vulnerable to single point failure

area.

- Most of the researchers who addressed the propagation delay and evaluated the different proposed countermeasures are concentrated on the four categories we mentioned above: working with consensus protocol, minimizing verification time, changing propagation protocol, and working with the network topology.

- Because of decentralization of the bitcoin network and the information has to be transmit between the nodes, we found that the propagation delay is the fundamental originator for most security issues in the bitcoin network like replica inconsistencies, double-spending attack, partitioning attack, Blockchain forks, eclipse attack.

- The choice of selecting a peer either by using clustering or organizing the network based on some graph reduces randomness, and thereby exposing to various security threats, for instance selfish mining attack and eclipse attack.

- Bloom filter and Invertible Bloom Lookup Table (IBLT) data structures are effective mechanisms to minimize block size while propagation; however, they have to be addressed and evaluated further.

- Many tools might help to reduce information dissemination. Minimum Spanning Tree (MST) is one of them that may facilitate block broadcasting by selecting the best weighted hop among miners.

5. Conclusion

Bitcoin network is vulnerable to security risks due to delay of information propagation. In this paper, initially, we highlighted different studies and countermeasures of the propagation delay in the bitcoin network. We started by defining this problem. Next, an overview of the basic propagation mechanisms was introduced. Analytical studies that tackle propagation and its implications after that were presented. Most of the proposed countermeasures have been displayed subsequently. Finally, some important findings to researchers then were suggested.

References

References

[1] A. M. Antonopoulos, Mastering Bitcoin: Programming the open blockchain, " O'Reilly Media, Inc.", 2017.

[2] S. Nakamoto, A. Bitcoin, A peer-to-peer electronic cash system, Bitcoin.–URL: https://bitcoin.org/bitcoin.pdf 4 (2008).

[3] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, Where is current research on blockchain technology?—a systematic review, PloS one 11 (10) (2016) e0163477.

[4] K. Oosthoek, C. Doerr, Cyber security threats to bitcoin exchanges: Adversary exploitation and laundering techniques, in: IEEE Transactions on Network and Service Management, IEEE, 2021, pp. 1616–1628.

[5] Y. M. X. L. X. Feng, J. Ma, K. K. R. Choo, Social characteristic-based propagation-efficient pbft protocol to broadcast in unstructured overlay networks, in: IEEE Transactions on Dependable and Secure Computing, IEEE, 2021, pp. 1–1.

[6] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, 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, 2016, pp. 3–16.

[7] K. Wüst, Security of blockchain technologies, Master's thesis, ETH Zürich (2016).

[8] C. Decker, R. Wattenhofer, Information propagation in the bitcoin network, in: IEEE P2P 2013 Proceedings, IEEE, 2013, pp. 1–10.

[9] T. Neudecker, P. Andelfinger, H. Hartenstein, A simulation model for analysis of attacks on the bitcoin peer-to-peer network, in: 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), IEEE, 2015, pp. 1327–1332.

[10] M. Fadhil, G. Owen, M. Adda, Bitcoin network measurements for simulation validation and parameterisation, in: 11th International Network Conference, University of Plymouth, 2016, pp. 109–114.

[11] J. Marçal, L. Rodrigues, M. Matos, Adaptive information dissemination in the bitcoin network, in: Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, 2019, pp. 276–283.

[12] Average transactions per block, blockchain, https://www.blockchain.com/charts/n-transactions-per-block (Aug 2021). URL `https://www.blockchain.com/charts/n-transactions-per-block`

[13] Z. Xing, Z. Chen, A protecting mechanism against double spending attack in blockchain systems, in: 2021 IEEE World AI IoT Congress (AIIoT), IEEE, 2021, pp. 0391–0396.

[14] G. J. M. A. V. V. M. Tran, I. Choi, M. S. Kang, A stealthier partitioning attack against bitcoin peer-to-peer network, in: 2020 IEEE Symposium on Security and Privacy (SP), IEEE, 2020, pp. 894–909.

[15] G. Karame, E. Androulaki, S. Capkun, Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin., IACR Cryptol. ePrint Arch. 2012 (248) (2012).

[16] T. Bamert, C. Decker, L. Elsen, R. Wattenhofer, S. Welten, Have a snack, pay with bitcoins, in: IEEE P2P 2013 Proceedings, IEEE, 2013, pp. 1–5.

[17] M. F. Sallal, Evaluation of security and performance of clustering in the bitcoin network, with the aim of improving the consistency of the blockchain, Ph.D. thesis, University of Portsmouth (2018).

[18] M. Fadhil, G. Owenson, M. Adda, A bitcoin model for evaluation of clustering to improve propagation delay in bitcoin network, in: 2016 IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES), IEEE, 2016, pp. 468–475.

[19] M. Fadhil, G. Owenson, M. Adda, Locality based approach to improve propagation delay on the bitcoin peer-to-peer network, in: 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), IEEE, 2017, pp. 556–559.

[20] G. Owenson, M. Adda, et al., Proximity awareness approach to enhance propagation delay on the bitcoin peer-to-peer network, in: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), IEEE, 2017, pp. 2411–2416.

[21] C. Stathakopoulou, C. Decker, R. Wattenhofer, A faster bitcoin network, Tech. rep., ETH, Zurich,. Semester Thesis (2015).

[22] G. Pappalardo, T. Di Matteo, G. Caldarelli, T. Aste, Blockchain inefficiency in the bitcoin peers network, EPJ Data Science 7 (1) (2018) 30.

[23] A. Sudhan, M. J. Nene, Peer selection techniques for enhanced transaction propagation in bitcoin peer-to-peer network, in: 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), IEEE, 2018, pp. 679–684.

[24] I. Eyal, A. E. Gencer, E. G. Sirer, R. Van Renesse, Bitcoin-ng: A scalable blockchain protocol, in: 13th {USENIX} symposium on networked systems design and implementation ({NSDI} 16), 2016, pp. 45–59.

[25] W. Bi, H. Yang, M. Zheng, An accelerated method for message propagation in blockchain networks, arXiv preprint arXiv:1809.00455 (2018).

[26] Compact blocks faq, Bitcoin Core, https://bitcoincore.org/en/2016/06/07/compact-blocks-faq/ (Jun 2016).
URL `https://bitcoincore.org/en/2016/06/07/compact-blocks-faq/`

[27] M. Corallo, Compact block relay - bip: 152, GitHub, https://github.com/bitcoin/bips/blob/master/bip-0152.mediawiki (Apr 2016).
URL `https://github.com/bitcoin/bips/blob/master/bip-0152.mediawiki`

[28] P. Tschipper, Buip010: Xtreme thinblocks, Bitcoin Forum, https://bitco.in/forum/threads/buip.010-passed-xtreme-thinblocks.774 (Jan 2016).
URL `https://bitco.in/forum/threads/buip.010-passed-xtreme-thinblocks.774`

[29] G. Andresen, O(1) block propagation, GitHub, https://gist.github.com/gavinandresen/e20c3b5a1d4b97f79ac2 (Aug 2014).
URL https://gist.github.com/gavinandresen/e20c3b5a1d4b97f79ac2

[30] R. Russel, Playing with invertible bloom lookup tables and bitcoin transactions, Pettycoin, https://rustyrussell.github.io/pettycoin/2014/11/05/Playing-with-invertible-bloom-lookup-tables-and-bitcoin-transactions.html (Nov 2014).
URL https://rustyrussell.github.io/pettycoin/2014/11/05/Playing-with-invertible-bloom-lookup-tables-and-bitcoin-transactions.html

[31] A. P. Ozisik, G. Andresen, G. Bissias, A. Houmansadr, B. Levine, Graphene: A new protocol for block propagation using set reconciliation, in: Data Privacy Management, Cryptocurrencies and Blockchain Technology, Springer, 2017, pp. 420–428.

[32] J. Kan, L. Zou, B. Liu, X. Huang, Boost blockchain broadcast propagation with tree routing, in: International Conference on Smart Blockchain, Springer, 2018, pp. 77–85.

[33] M. M. A. Manuskin, I. Eyal, Ostraka: Secure blockchain scaling by node sharding, in: IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2020, pp. 397–406.