WJCMS

Wasit Journal of Computer and Mathematics Science

Journal Homepage: https://wjcm.uowasit.edu.iq/index.php/WJCM
e-ISSN: 2788-5879 p-ISSN: 2788-5887

BLOCKCHAIN SCALABILITY ANALYSIS AND IMPROVEMENT OF BITCOIN NETWORK THROUGH ENHANCED TRANSACTION ADJOURNMENT TECHNIQUES

Umar Danjuma Maiwada [1*], Kamaluddeen Usman Danyaro [2], Muhammad Garzali Qabasiyu [3], Aliza Bt Sarlan [4], Abubakar Danjuma Maiwada [5]

[1]Department of Computer Science, Umaru Musa Yaradua University Katsina Nigeria

[2,4]Department of Computer and Information Science, Universiti Teknologi PETRONAS Malaysia

[3]Department of Computer Studies, College of Science and Technology, Hassan Usman Katsina Polytechnique

[5]Material Science and Engineering Department King Fahad University of Petroleum and Minerals Dhahran Saudi Arabia

*Corresponding Author: Umar Danjuma Maiwada

DOI: https://doi.org/10.31185/wjcms.298
Received 23 September 2024; Accepted 20 June 2025; Available online 30 June 2025

ABSTRACT: Bitcoin is the most popular among cryptocurrencies, including Litecoin, Dogecoin, and Peercoin. Blockchain is the foundation of cryptocurrencies, and most cryptocurrency technologies are decentralized. Despite its benefits, blockchain remains a cutting-edge technology with flaws that can be addressed to increase efficiency. Therefore, this research digs into the topic of scalability in blockchains and presents a comparative analysis of numerous blockchain metrics with real-time data. We performed this using a blockchain simulation (BlockSim) and then looked at effective techniques that may be utilized to overcome the limitation by comparing the simulator and real-world circumstances. The second part of this research proposes an effective algorithm that improves the scalability of the Bitcoin network through efficient transaction deferment. In this study, we propose an algorithm that enhances the current Bitcoin protocols using Inventory messaging (INV) and transaction deferment or adjournment. The deferred transaction relays on the message to carry multiple raw transactions. These improvements are compatible with the existing Bitcoin Network protocols. The improvement algorithm was simulated using BlockSim and the AnyLogic Multi Paradigm Simulation Engine, where the simulators were configured with 1000 nodes interconnected in a Bitcoin-like Peer-to-Peer network. The result of the simulation shows that the adjourned transaction protocol provides a controlled reduction in the number of messages required to propagate a transaction at the cost of a modest increase in transaction propagation time. By adjusting the threshold and timeout values, we can manage the tradeoff between the number of messages and propagation latency, thereby improving the network's overall scalability. Our results indicate that the proposed method achieves up to a 30% reduction in network message overhead while maintaining an acceptable transaction propagation delay. This suggests that enhanced transaction adjournment techniques can significantly optimize Bitcoin's scalability without compromising its security and decentralization.

Keywords: Blockchain, BlockSim, SupplyChain, Bitcoin, Litecoin, Dogecoin, and Peercoin.

1. INTRODUCTION

Blockchain has recently attracted a lot of research attention as a promising technology for realizing distributed ledgers. The ledger aims to achieve decentralized transaction management, which means that any node connected to the

*Corresponding author: umar.danjuma@umyu.edu.ng

ledger can initiate transactions according to rules, and the transaction does not need to be controlled by a third party. All transactions within the framework are stored in blocks, which are then linked together as a chain and then sorted chronologically. Furthermore, transactions written in blocks are unchanging and transparent to all peers. With all these appealing characteristics, blockchain stands out from traditional centralized trust entities and has the potential to become a significant enabler for future financial systems. From Bitcoin, the first decentralized cryptocurrency, to Ethereum, and then the emerging permissioned blockchain, blockchain has advanced rapidly in recent years (Yadiv and Shevkar, 2021). Nowadays, blockchain-based applications are part of our daily lives, whenever the number of users increases, the scalability issues will occur and that will greatly affect the development of blockchain. The transaction throughput and transaction confirmation latency are two of the performance metrics in blockchain and both haven't reached an acceptable level in recent popular blockchain systems, which can form the bad user's quality of experience (Zhou, et. Al., 2020). However, if compared with the centralized payment system such as banking system, the transaction throughput and transaction confirmation latency cannot be improved effortlessly in blockchain, a self-regulating system that needs more attention to maintain decentralization. In most of the studies on accuracies of blockchain, it was noted that some researchers raise the view of Blockchain Trilemma. Likewise, the CAP theory in distributed system which used the Blockchain Trilemma to highlight three vital properties in blockchain system that includes decentralization, security, and scalability, and all of them cannot be perfectly co-exist. For example, let consider shortening the block interval of Bitcoin which can increase the transaction throughput, but it will also affect the security of the entire system because there is increase in probability of fork. Thus, balancing between these three properties of blockchain system is critical for future development of blockchain (Yadiv and Shevkar, 2021).

At this moment, Bitcoin is considered the most frequently used application by means of blockchain technology. Bitcoin is a decentralized digital currency payment system which involves a public transaction ledger known as blockchain. One important aspect of Bitcoin is how it maintains the value of currencies without the control of any organization. Despite this, it is reported that the number of transactions and new users in the Bitcoin network is increasing regularly (Zheng et al., 2018). Furthermore, conversions with the currencies like EUR and USD occur regularly in the currency exchange markets. Thus, Bitcoin has gained too much consideration from diverse contexts and is currently the most successful digital money using Blockchain technology. The literature highlighted one crucial mechanism that Bitcoin employs known as Public Key Infrastructure (PKI). In PKI, each user has one pair of public and private keys. The public key is used in the address of the user Bitcoin wallet whilst private key is for user authentication. The transaction of Bitcoin involves the public key of sender, numerous public keys of the receiver, and the value to be moved. In around ten minutes, the transaction will be written in a block and then connected to the existing written block. Here, all written blocks and transactions made are saved on the disc storage of the users known as nodes. These nodes maintain details about every recorded transaction in Bitcoin network. Moreso, these nodes are satisfied by checking the accuracy of the transactions (this approach is also known as mining) (this method is also known as mining). Further, when all transactions are done successfully, a consensus exists between all nodes (Li. et. al., 2019). One benefit of blockchain is that public ledgers will never be edited or even erased when data is accepted from all nodes. This is the key reason why blockchain is so popular to its data integrity and security issues. There are quite a few technical challenges and limitations identified for the adaptation of blockchain technology in the future (Yadiv and Shevkar, 2021).

a) Throughput: The bitcoin network's capacity has been increased to 7 transactions per second, whereas other transaction processing networks such as VISA and Twitter process 2,000 and 5,000 transactions per second, respectively.

b) Latency: This is the ability to achieve efficiency in security that will provide more time to be spent on a particular block to overshadow the cost of double spending attacks. Double-spending is defined as the result of spending money successfully and more than one time. It is reported that bitcoin has ability to protect against double-spending after each transaction added to the block is verified (Wang and Wang et al., 2019) However, this is what makes the latency a strong issue in blockchain technology.

c) Size and bandwidth: In February 2020, the size of blockchain in Bitcoin network is around 427GB. It is reported that when throughput issues increase up to the VISA level, then blockchain can raise to 214PB in the subsequent year (Yadiv and Shevkar, 2021)

d) Security: It is indicated that blockchain has 51% possibility of attack. In this attack, a single entity can control most of the network's mining hash-rate and this can manipulate the blockchain. To overcome this issue, more research on security is necessary.

e) Wasted resources: An enormous amount of energy is wasted in mining Bitcoin (around $15million per day) which is caused by the Proof-of-Work effort. However, there are some other options used in industrial fields like proof-of-stake (Zhou et al., 2020). In Proof-of-Stake, the resource that is associated is the amount of Bitcoin a miner holds.

f) Usability: The application program interface of Bitcoin is very difficult to use in developing services.

g) Versioning, hard forks, multiple chains: It was noted that quite number of nodes has 51% possibility of attack. Here, another issue emerges when chains are divided for administrative or versioning purposes.

Looking at blockchain as a technology, all these issues need to be solved to have more efficient mining in blockchain technology. These will change the way transactions are carried out every day. Therefore, to understand the current state of research conducted in blockchain, it is important to gather all relevant research (Yadiv and Shevkar 2021).

1.1 STATEMENT OF THE PROBLEM

The scalability issues in blockchain technology have been revealed recently. (Zheng 2018) analyzed and come up with some important metrics to measure the scalability of Bitcoin such as maximum throughput, latency, bootstrap time and cost per confirmed transaction. However, maximum throughput and latency issues are considered as the top important performance metrics with significant impact on user's quality of experience. Furthermore, the transaction throughput matrix receives too much attention in the research area. In the works of (Decker and Wattenhofer) which report that Bitcoin's highest transaction throughput is about 7 transactions per second whereas Visa is about 2000 to 65,000 transaction per second. Transaction throughput is controlled by the block interval and the block size. If the block is higher, then it can store many transactions that will raise the throughput, but at the same time it can cause an increase in block propagation time. In Bitcoin, the block interval is nearly 10 minutes, while block size is 1MB, here there is a high chance to limit the number of transactions stored in every single block. Therefore, maintaining block propagation time by increasing the block size, the average bandwidth will define the block propagation time of the blockchain system (Bitcoin Cash, 2019). Moreover, the transaction confirmation latency matric has a relation with user experience. Now that there is a massive amount of Bitcoin transactions, it is noted that the limited size of blocks is not enough to deliver all transactions which are submitted by nodes. Under such circumstances, it is found that miners are likely selecting transactions with high transaction fees, so that other transactions with a low offer must wait till packaged, this is what leads to longer transaction latency (Decker and Wattenhofer).

2. LITERATURE REVIEW

A new architecture for data analytics on the Bitcoin and Ethereum platforms was introduced in reference (Bitcoin Cash, 2019). This tool enables the integration of blockchain data with data from other sources as seen in Table 1. This framework also allows for well organizing data in a database. In (Yadev and Shevkar 2021), which categorized blockchain implementations and make comparison among them using blockchain-based frameworks particularly to analyze the effect of the blockchain architecture on software architecture. This research focuses on the major architectural elements of blockchain platforms and the impact of blockchain design on the quality of blockchain-based software, including performance and scalability. (Perve et al., 2018) recognized some quality attributes in blockchain technology. This work, however, also explored some quality issues and solutions for blockchain implementation. Thus, the results show that blockchain platforms might require an enhancement in some respects including security, scalability, and so on. Ref. (Nayak et al., 2015) introduced simulation and performance modelling to predict latency of blockchain systems. However, most of the results have an error close to 10%. Thus, the research of this work also aims to help in assessing various blockchain design options. In (Miller et al., 2019) introduced a performance evaluation model in blockchain technology. This work described a model purposely to evaluate a software design at early stage of software development to avoid impact in changing requirement.

Kalodner (2018) into some of the issues with scalability in blockchains, particularly Bitcoin. The findings of this study suggested that Bitcoin needs major throughput and latency improvements. Ref. (Manuskin 2020) introduced a software called BTCS park specifically for analyzing Bitcoin. This software has a user-friendly interface. In (Hafid, et al., 2020) proposed and designed a performance model. This model is applied in Practical Byzantine Fault Tolerance. However, this work investigated the possibilities of performance bottlenecks in networks with varieties of nodes. LeMahieu (2018) presented a scalability protocol for blockchain platforms known as ByzCoin. When tested on the Bitcoin platform, this protocol provides good security and performance. In (Byzntine, 2019) introduced a parallelization approach purposely to measure BFT systems. However, this approach has also increased the BFT system's performance. The results of this work showed that the introduced approach has increased the throughput of the system. Ref. (Bitcoin NG, 2015) present a Bitcoin-NG protocol that will address scalability issues in Bitcoin platform. This study also highlights security concerns and the efficacy of several related procedures. The findings of this study show that Bitcoin-NG can deliver optimal scalability even with low bandwidth. In (Canetti and Rabin 2016) comparing two different blockchains-based and byzantine-based fault tolerance in scalability and performance issues. The result shows that the performance of blockchains-based is better than the byzantine-based fault tolerance, whereas in blockchains-based PoW is better than BFT in terms of scalability. In (Sompolinsky 2015) proposed and implement a two-layered blockchain platform for data storage. The architecture in this platform gives high performance but is very weak in scalability issues. In (Sompolinsky 2015) introduced a mobile application called Mobichain. This Mobichain aims to make transactions in commerce. The performance evaluation conducted shows that Mobichain application is a very efficient solution for m-commerce applications. Swanson (2013) studied and measured the performance of Ethereum and Hyperledger Fabric blockchains with respect to number of transactions ranging from 1 to 10000. However, the results obtained from this experiment indicated that Hyperledger performs better than Ethereum in throughput, execution time, and latency.

Blockchain, like any other new technology, faces technical issues such as scalability, security, and performance. Performance is one of the most difficult aspects of implementing blockchain systems as a replacement for traditional databases. Throughput, latency, size and bandwidth, security, wasted resources, usability, and versioning and hard forks are seven foreseeable technical hurdles for blockchain adaptation, according to Swan 2015. The key restriction and issue

that has not been properly researched and evaluated, according to a comprehensive review on research subjects on blockchain is scalability (Yii-Huukmo et al., 2016). Because developed blockchain frameworks are expected to involve a significant number of nodes, evaluation is required. Even though there are numerous blockchain platforms, this analysis demonstrates that there is no consistent technique for analyzing, evaluating, and assessing Blockchain scalability. The goal of this study is to examine the scalability of Blockchain technology, the blockchain platform, and to develop a better scalability algorithm to increase the scalability of the Blockchain network. The review of the related literature shows that scalability is the most challenging issue in Blockchain technology. However, a lot of solutions have been proposed to address the scalability problem in Blockchain. Some of the notable solutions that truly improve scalability issues in Blockchain technology are solutions such as SigWit (Lombrozo et al., 2015), this solution increases Block size from 1MB to 4MB. Elastico (Luu et al., 2016) improves blockchain scalability using shading approach. This solution improves blockchain scalability by splitting the transactions into different shades thereby improving the performance (Throughput) of the system. Lightning network (Poon et al., 2016) improves Blockchain scalability through payment channel on Bitcoin network, this solution improves the throughput to almost 20TPS. Other notable solutions are Plasma (Poon et al., 2017), Omnilledger (Kokoris-Kogias, 2018), Txilm (Ding et al., 2019), Sprites (Miller et al., 2019). All these solutions have been implemented and tested on real Blockchains but still perform below expectation. DAG-Based solutions were proposed as an improvement to the current scalability issues. Solutions such as Inclusive (Lewenberg et al 2015), Dagcoin (Lerner, 2015), IOTA (IOTA, 2019) also improve Blockchain scalability to some level, but still more needs to be done on improving Blockchain scalability issues. Scalability issue is among the issues that hinder the wide adoption of Blockchain technology (Zhou et al., 2020). The current throughput of current Blockchain is very poor compared to with the centralised payment system such as PayPal and Visa. The throughput of pioneer Blockchain platforms such as Bitcoin and Ethereum processes only 7TPS and 20TPS respectively (Hafid et al., 2020). While the centralised platform such as PayPal and Visa processes 193TPS and 1700TPS respectively Yadev and Shevkar, 2020). This shows the significance of need in improving the scalability of Blockchain technology. Other available solutions such as transaction propagation and cross-chain solution are data propagation-based approaches which also improve Blockchain Scalability through data propagation. Some of the notable solutions that are based on data propagation are Early (Naumenko et al., 2019), Kadcast (Rohrer and Tschorsch 2019), Velocity (Chawla et al., 2019) and bloXroute (Klarman et al., 2019). Despite their great effort, there remains a huge gap in trying to attain the required scalability of the system. The major problem of these solutions is a) some nodes are reached in message broadcast, b) they lack multicast capability and c) no bandwidth utilisation.

This research work will improve the work done on transaction propagation by leveraging unreachable nodes. The problem of this approach is in Bitcoin network is that it's inefficient due to its lack of less nature and its lack of multicast/broadcast features. Another gap observe in this approach is that the number of messages needed to propagate a single transaction is very high, which is wasteful in terms of bandwidth, that's why this research work reviews this approach and present and improve the approach through development of an efficient algorithm that improves transaction propagation using adjournment approach (Franzoni and Daza, 2020).

Table 1: Table of Comparison of Blockchain Scalability Studies

Study	Scalability Technique Used	Simulation Tool	Key Findings	Limitations
This Study (Proposed Work)	Enhanced Transaction Adjournment (Deferred Transaction Relay with INV Messaging)	BlockSim, AnyLogic	Achieves up to 30% reduction in network message overhead while maintaining acceptable propagation delay	Slight increase in transaction propagation time
Eyal et al. (2016)	Bitcoin-NG (Leader-Based Block Generation)	Custom Simulator	Reduces transaction confirmation time and increases throughput	Requires protocol changes and centralization risks
Gervais et al. (2016)	Adjustable Block Size & Block Interval Optimization	Bitcoin Core Simulator	Improved transaction confirmation speed	Increased risk of orphaned blocks
Croman et al. (2016)	Off-Chain Scaling (Payment Channels, Lightning Network)	Theoretical Analysis	Reduces on-chain load, improves TPS	Complexity and centralization concerns

Sompolinsky & Zohar (2018)	GHOST Protocol (Graph-Based Block Validation)	Theoretical Model	Reduces block propagation time and improves fork resolution	Increased computational complexity
Pass et al. (2017)	Fruitchain (Hybrid Block & Transaction Validation)	Custom Simulation	Enhances security and scalability	Requires protocol modifications

3. CRITICAL OVERVIEW OF BLOCKCHAIN SCALABILITY SOLUTIONS

Bitcoin has gotten a lot of attention in the cryptocurrency world, especially because of its scalability difficulties. (Bitcoin Cash 2020) looked at several metrics to determine Bitcoin's scalability, including maximum throughput, bootstrap time, latency, and cost per confirmed transaction. The maximum throughput and latency, on the other hand, are regarded to have a substantial impact on the user's quality of experience. Furthermore, the transaction throughput matrices receive the greatest attention. Furthermore, according to (Yadev and Shevkar 2021), Bitcoin has a transaction throughput of around 7 transactions per second, whereas Visa has a transaction throughput of 2000 to 65,000 transactions per second. Much research depicted that transaction throughput is controlled by the block interval and the block size. Normally, bigger blocks accommodate many transactions which can raise the throughput and increase the block propagation time. Next block is generated based on the current block that critically reduces the probability of fork, block size and as well average block interval. However, block interval takes almost 10 minutes in Bitcoin while the block size is almost 1 MB (Scherer, 2017). As a result, the number of transactions that must be accommodated in each block is reduced. As a result, the average bandwidth of the entire system, which determines block propagation time, becomes a performance bottleneck of the blockchain system to maintain block propagation time while increasing block size. Furthermore, a new statistic known as transaction confirmation latency will prove to have a strong link to user experience. Transaction throughput is limited by the block interval and block size, according to several research. Larger blocks typically accommodate more transactions, resulting in higher throughput and longer block propagation times. The next block is generated based on the current block, reducing the likelihood of a fork, block size, and average block interval. Bitcoin, on the other hand, has a block interval of over 10 minutes and a block size of almost 1 MB (Scherer, 2017). As a result, the number of transactions that must be accommodated in each block is reduced. Thus, the average bandwidth of the entire system, which determines block propagation time, becomes a performance bottleneck of the blockchain system to maintain block propagation time while increasing block size. Moreover, a new statistic known as transaction confirmation latency will be proven to have a strong link to user experience. Because of the large volume of Bitcoin transactions that occur daily, the limited size of blocks is unable to transmit all transactions submitted by nodes. As a result, miners can choose transactions with larger fees. As a result, transactions with lesser fees will have to wait until they are packaged, resulting in longer transaction latency (Scherer, 2017). Furthermore, Ethereum is another PoW-based blockchain that exacerbates the problem because some decentralized apps (Rohrer and Tschorsch 2019) have caused widespread network congestion. Therefore, this research work studied some various research works that describe different Blockchain scalability problems with their solutions respectively. Further, these research works solve the scalability issues with different approaches and strategies.

4. ANALYSIS OF BLOCKCHAIN SCALABILITY

4.1 METRICS OF SCALABILITY ANALYSIS

Let's look at some of the blockchain parameters that have been collected and analyze them to gain a better knowledge of how the blockchain system is built. The information was taken from reliable websites including blockchain.info and coinbase.com.

4.2 TRANSACTION AND CONFIRMATION TIMES ANALYSIS

The chart below was created by evaluating the transaction and confirmation times between the dates of 3/2/2021 and 14/2/2021. The data was collected and rounded to the nearest 0.0001 fee/KB. The following analysis was carried out, keeping in mind that this is real data. Look at the chart below, which was created using the information gathered:

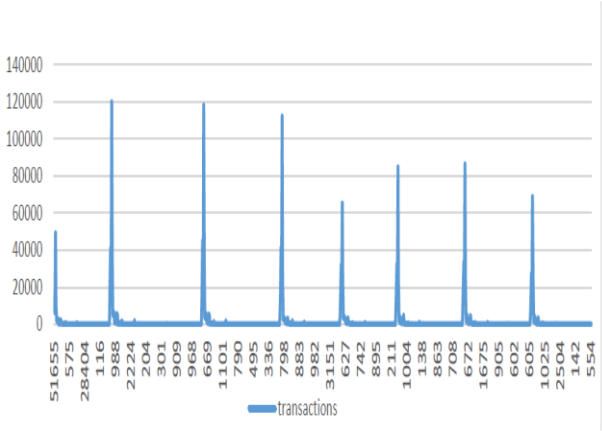

FIGURE 1. Confirmation Times vs. Transactions (blockchain.info)

In terms of individual graph timings, the graph of Figure 1 displays the distribution of 948 transactions in the range of 0-15000. As can be seen, the time plotted on the legend is not consistent; thus, let us organize the data and arrange the time in ascending order for a more thorough study.

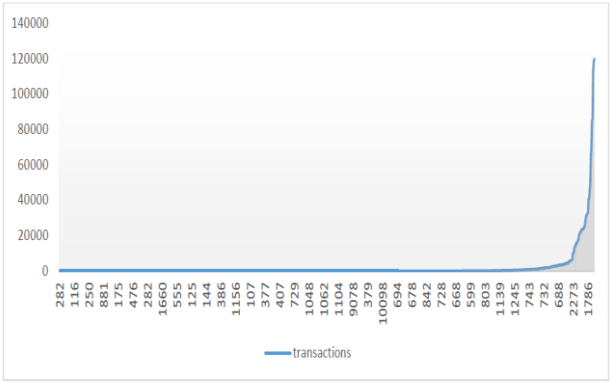

FIGURE 2. In seconds, the distribution of increasing transaction order (coinbase.com)

The distribution of rising transaction confirmation times is depicted in the graph in Figure 2. A few observations on the pattern of the distribution can be made:

a) As the system's transaction volume increases, the confirmation time grows as well.
b) We can confidently assume that an increase in transaction volume is proportionate to an increase in confirmation times (Sapirshtein et al., 2015)

Let's have a look at the distribution in which Transactions have been sorted by increasing Confirmation Times in Figure 3.

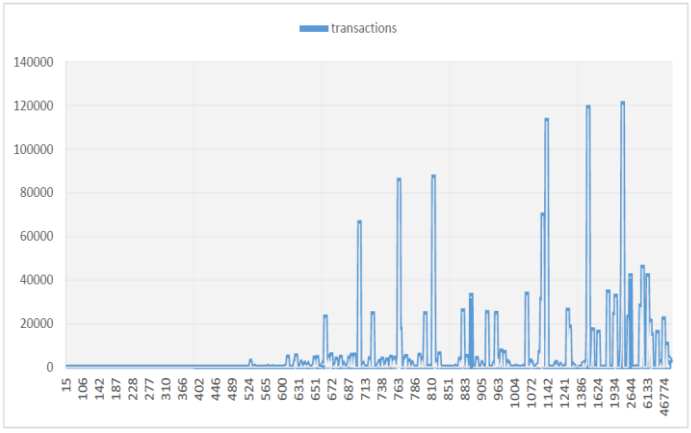

Figure 3. Transactions Vs Increasing Order of Confirmation Times

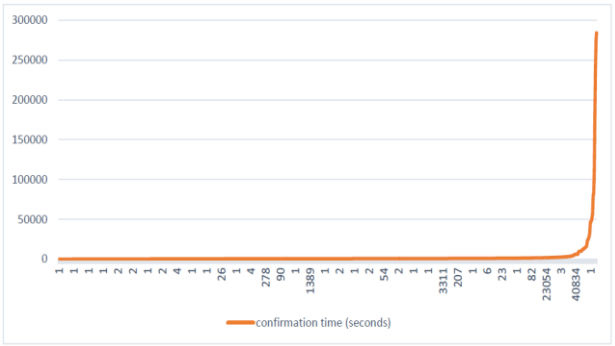

Figure 4. Transactions Vs Confirmation Time in Seconds

The graph of Figure 4 supports the claim made before raising the number of transactions and causes the confirmation time of the transactions to increase. There are sharp peaks for transactions above 80000, as seen in Figure 5, indicating a significant increase in confirmation times. We'd like to lessen the network's flow's dramatic peaks by evenly dispersing these transactions, resulting in increased efficiency and lower network latency (Sompolinsky 2015). This is when the blockchain system's scaling begins. While incorporating more transactions in a block may improve throughput, mining such blocks into the blockchain increases system overhead and causes network delays.

4.3 CONFIRMATION TIMES AND TRANSACTION FEE ANALYSIS

The transaction fee has a significant impact on the time it takes for a transaction to be confirmed. It is the single most compelling reason for a miner to mine and includes transaction in a block. The graph below shows the relationship between transaction fee and confirmation time in minutes.

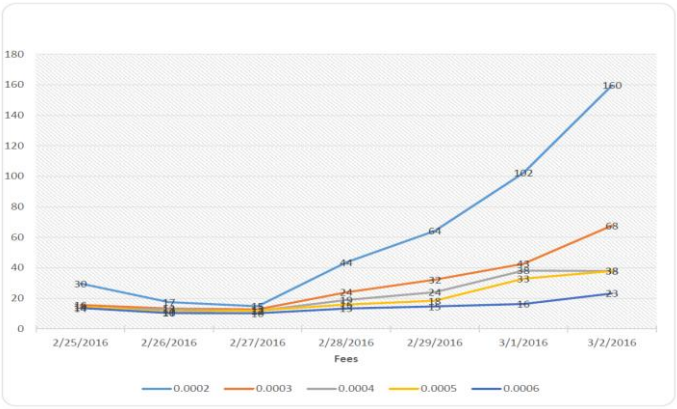

Figure 5. Time it takes to confirm a fee in minutes

The graph in Figure 5 displays and represents the impact of transaction fees on the time it takes for each transaction to be confirmed. It's worth noting that the same transaction fee may apply to many transactions. A transaction fee of 0.0002 BTC, for example, may require about 100 transactions, and the confirmation time for that transaction from conception to block and subsequent inclusion in the blockchain could vary. The information was gathered between February 25, 2021, and March 2, 2021.

The graphical representation shows that:

a) The 0.006 transaction cost has a shorter confirmation time than the other transaction fees of 0.0002, 0.0003, 0.0004, and 0.0005.

b) It enables us to recognize that the higher the transaction price, the lower the likelihood of a faster confirmation time. Though we cannot promise that this will happen for every transaction, as we will see later, even those with greater transaction fees may suffer and experience longer confirmation times in some instances.

Let's test if this holds true in a larger number of transactions. To do so, we plotted the graph over a larger data set that includes a variety of additional transaction fees.

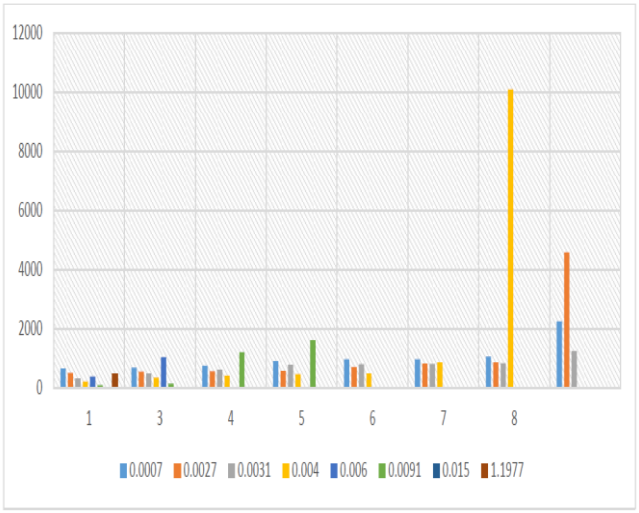

Figure 6. Confirmation Time per Transaction Fee for different Number of Transactions

Even when altering the number of transactions associated with each transaction cost, the average confirmation time for larger transaction fees remains relatively low, as shown in Figure 6. Let's look at what percentage of transactions in real-time situations higher transaction fees have.

4.4 ANALYSIS OF TRANSACTIONS AND TRANSACTION FEE

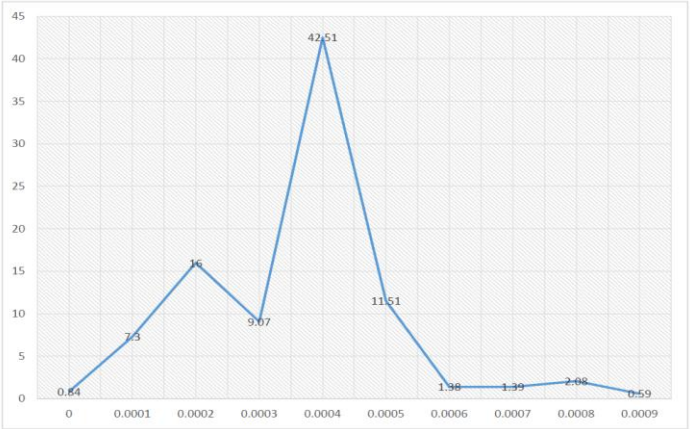

Figure 7. Percentage of network transactions per transaction fee

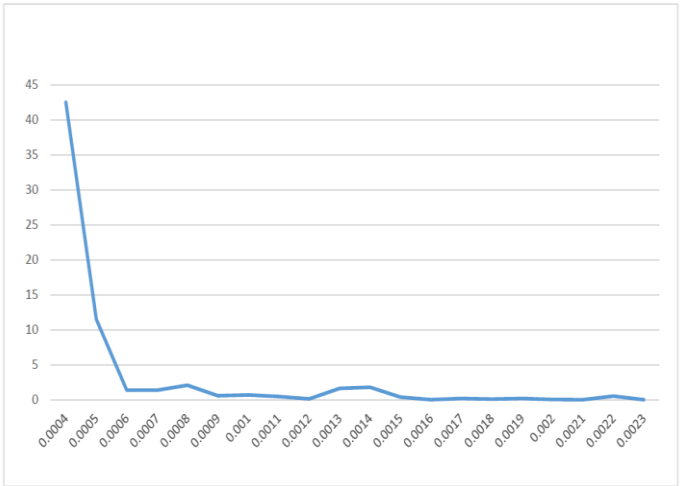

Figure 8. Increasing Transaction Fee vs. Percentage of Transactions

4.5 MODEL OF THE BLOCKCHAIN SIMULATOR

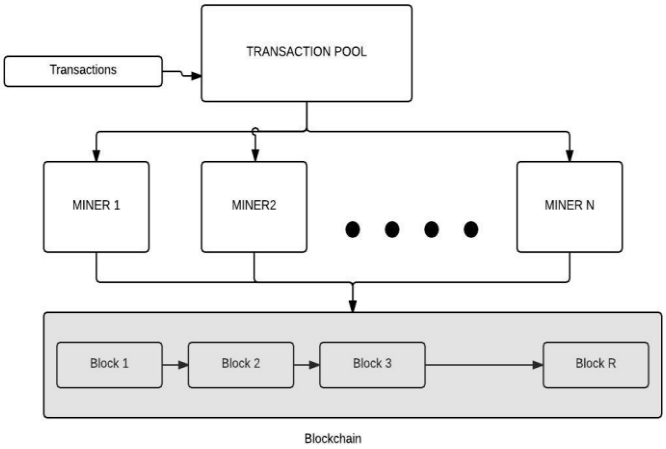

Figure 9. Model of the BlockSim Simulator

a) Transaction Pool - It is the pool in which all transactions are stored. All incoming transactions are added to the transaction pool, and all outgoing transactions are removed from it. After a certain amount of time, the transaction pool in an ideal bitcoin system is overwhelmed with transactions.

b) Transactions- A message is created by a data structure. This message initiates a bitcoin transaction between two parties. This is usually a one-time transfer of a certain number of bitcoins.

c) Miners- Miners oversee encoding transactions in blocks and mining them into the blockchain, or universal distributed ledger. The miners work together to overcome a difficult situation. After the block is successfully added to the blockchain, the winner receives the block reward.

d) Blocks- A data structure for putting transactions together. It can be thought of as a transaction container.

e) Blockchain- It's a chronologically ordered arrangement of blocks. Blocks that are successfully mined are added to the block chain. It is a large database that stores every transaction ever made in the history of bitcoin.

4.6 UML CLASS DIAGRAM FOR THE BLOCKSIM SIMULATOR

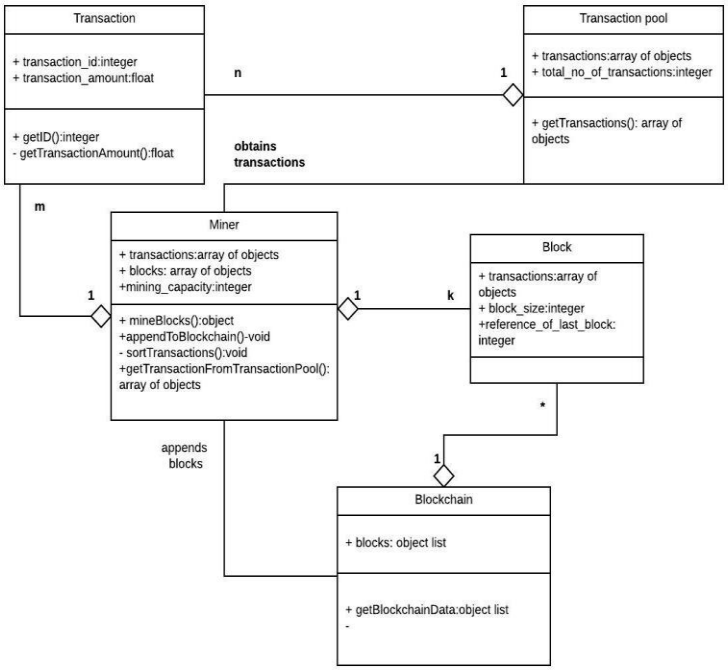

Figure 10. UML Class Diagram of the BlockSim Simulator

4.7 THE OPERATION OF THE BLOCKSIM SIMULATOR

To describe what the Blockchain simulator does and how it re-enacts the blockchain system in detail, we'll go over the Blockchain in an ideal working system step by step. When a transaction is completed in an ideal Blockchain system, such as the Bitcoin protocol, the following happens:

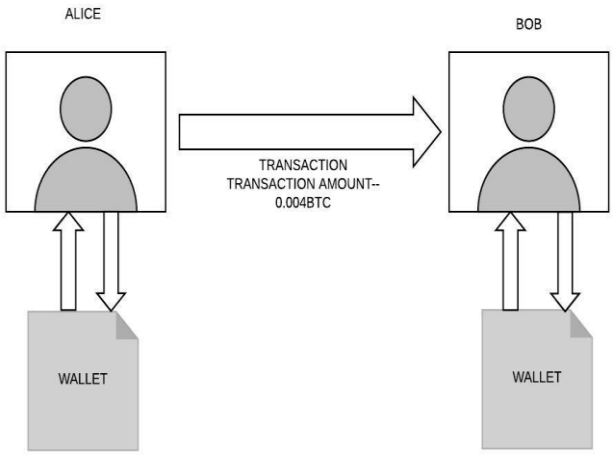

Figure 11. Alice and Bob's business dealings

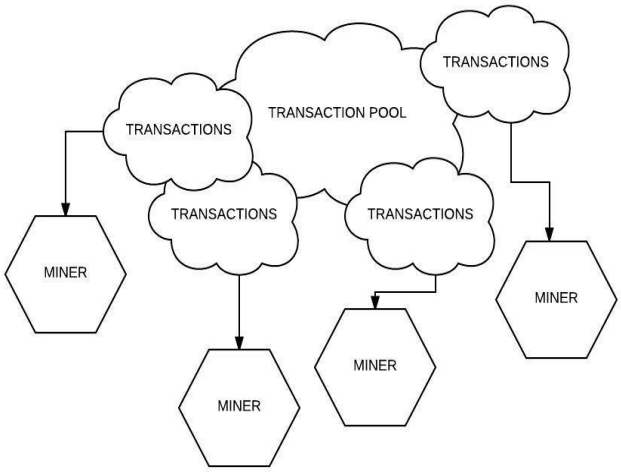

Figure 12. A partial view of the Transaction Pool for Miners is seen in this illustration

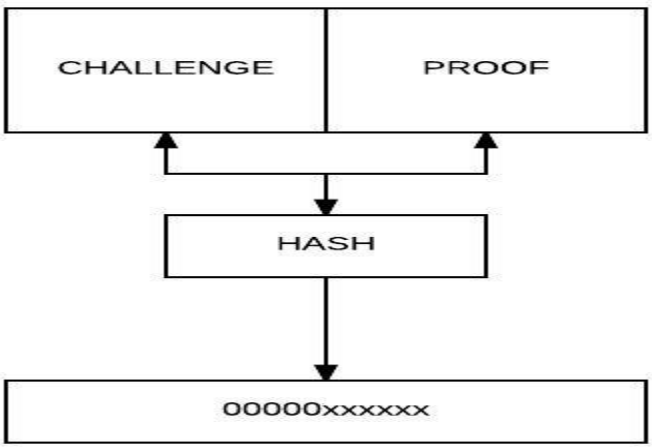

Figure 13. The generation of Prefix

5. THE PREVIOUS ALGORITHM

This research work improves the work done on transaction propagation by leveraging unreachable node in (Franzoni and Daza 2020). The problem of this approach in the bitcoin network is, its inefficient due to the permissionless nature of the bitcoin network, the approach also lacks multicast/broadcast features. Another problem of approach, (Franzoni and

Daza 2020), is that the number of messages needed to propagate a single transaction is very high, which is wasteful in terms of bandwidth utilization. The proposed algorithm figure 3,3 wasted a lot of bandwidth, that why it's important to develop a better and more reliable approach that will effectively propagate messages. The approached used in this dissertation is using transaction adjournment/deferred transactions. The next section of this research work describes the proposed algorithm using transaction adjournment.

Algorithm 1: Proxy(tx)

Pick a random peer P from the proxy set;
Send tx to P and set a timeout t;
When t expires:
if *The majority of outbound peers advertised* tx **then**
  Return
else
  Repeat
end

Figure 14. Proxy operation (Franzoni and Daza 2020)

Algorithm 2: R Propagation Rules

Divide time into epochs;
if *New epoch begins* **then**
  Select subset S from U peers uniformly at random from different buckets;
  Set S as the proxy set
end
if *Create new transaction* tx **then**
  Mark tx as *proxying*;
  Run $proxy(tx)$
end
if *Receive a proxying transaction* tx_m *from a U peer* **then**
  with probability p, execute $proxy(tx_m)$;
  otherwise, $diffuse(tx)$
end

Figure 15. Propagation rules (Franzoni and Daza 2020)

6. SCALABILITY IMPROVEMENT

Bitcoin is the most well-known cryptocurrency, as well as the most well-known (and publicly known) implementation of blockchain technology. Bitcoin uses a replicated blockchain record to facilitate financial transaction verification and storage. Single transactions are finally packed into blocks, which are then propagated through a peer-to-peer (P2P) network using a set of simple protocols to ensure the ledger's consistency. Because the network has no permissions, node can join or leave at any time, and protocols rely heavily on redundancy to compensate for the lack of multicast and broadcast capabilities.

The huge quantity of INV messages, which are notifications about newly acquired data items (blocks and transactions) delivered via the network, is one of the drawbacks of this redundancy. The inefficiency is especially noticeable for transactions that are small, ranging from 100 to 500 bytes, yet require the full Bitcoin message, which is then bundled as a TCP message, to be replicated multiple times at each node to propagate a single transaction. This inefficiency has previously been noticed, and solutions have been presented. A new transaction is not broadcast to all peers of a node in the Erlay protocol (Naumenko et al., 2019). Instead, for each transaction, it only employs a subset of the peers (this is called low-fanout flooding). The node will then use set reconciliation procedures to periodically engage its peers in mutual updating of transaction mempools. However, this strategy adds to the computational complexity by requiring the calculation of initial and subsequent symmetrical set differences, as well as the creation of the appropriate messages. It employs an 8-byte short transaction ID that is incompatible with current Bitcoin implementations. Furthermore, some transactions may be known to one peer but not to the other, in which case they must be transferred in the traditional way (i.e., via the INV-GETDATA-TX handshake), negating many of the benefits gained through the upgraded protocol. Another enhancement was created as part of the Dandelion++ project (Fanti 2018), however its purpose is anonymization of transaction source nodes rather than bandwidth reduction. The protocol also necessitates

non-trivial software changes; however, this is justified by the increased source of privacy. In this study, we take a different method, postponing the notification of new transactions until a predetermined number of new transactions have been received by a node. Optionally, a timeout can be set to limit the amount of time that postponed transactions must wait before being announced. This method, dubbed postponed transaction relay subsequently, provides for a significant reduction in the number of messages required to propagate a single transaction across the network. A minor increase in transaction propagation delay is the price to pay. However, the increase is not excessive, and the tradeoff between a lower number of messages and a longer transaction propagation time can be modified by adjusting the threshold for sending new transaction announcements. As can be shown, the threshold value isn't crucial, as the near-optimal tradeoff can be found across a large range of values.

Algorithm 3.

Name: Scalability improvement through transaction Deferment.

Inputs: Data: incoming TX message with new transactions

Data: set of Peers

Data: list of deferred transactions

Data: threshold (maximum size of deferred list)

Data: timeout for sending the INV announcement

Output: Improve transaction propagation

```
Start
1 Loop;
2 while deferred.count() < threshold or timer.time() < timeout
        do
3       receive TX message from a peer;
4       if transaction known then
5               drop transaction
6       else
7               verify transaction and add to deferred list
8       end
9 end
10 if deferred.count() > 0 then
11      for p € Peers do
12          prepare a new INV message containing all deferred
              Transactions;
13        send the new INV message to peer p;
14      clear deferred list
15   endfor
16   restart timer;
17   go to Loop
18 end
```

This research work develops an improved algorithm that improves scalability of Blockchain (Bitcoin Network) the modification of data propagation protocol. Because of its permissionless structure and absence of multicast/broadcast features, data propagation in the Bitcoin network is inefficient. In particular, the number of messages required to propagate a single transaction is extremely high, resulting in a waste of bandwidth. In this paper, we suggest a modest change to the Bitcoin software that allows for a significant reduction in the number of messages required to propagate a

transaction across the network. The change involves postponing transaction announcements until a specified quantity of new transactions has been collected. We show that by doing so, the quantity of messages can be drastically decreased. This reduction comes at the cost of a longer transaction propagation time. However, by carefully selecting the threshold number of deferred transactions, the tradeoff between traffic reduction and transaction latency can be reduced.

If numerous new transactions could be announced in a single INV message, the number of INV messages would decrease. Because an INV message can already contain up to 50,000 inventories, such as blocks and transaction hashes, this feature does not necessitate any changes to the structure of Bitcoin messages. The default data propagation protocol demands (or, rather, implies) that a node broadcasts the INV notification about a transaction to its peers immediately after confirming a freshly received transaction, therefore this function is 'underutilized.' In this scenario, "newly received" refers to both transactions injected into the node from an external client and transactions received from peers since the last INV announcement. To limit the number of such announcements and, as a result, the amount of bandwidth spent, we may allow nodes to delay sending an INV announcement until multiple transactions have been collected and then broadcast them all with a single INV message. This is the second enhancement, also known as deferred transaction relay. In terms of implementation, we have two options that are not mutually exclusive. To begin, a node could wait until a certain number of new transactions have arrived and been aggregated before broadcasting them to all its peers. However, transaction arrivals are random, and it's possible (though unlikely) that the deferred transaction collection's threshold size will not be met for a long period, perhaps tens of seconds. We can set a timeout to send announcements when the threshold size is met, or when the timeout expires even if the predetermined threshold number of postponed transactions is not reached, to reduce the waiting time. These two approaches work together to limit and regulate transaction propagation latency.

Waiting has the disadvantage of increasing transaction propagation latency, as transactions will take longer to propagate. There is no need for a separate reconciliation step in Erlay because all transactions are guaranteed to be transmitted to all nodes (Naumenko et al., 2019), additionally, no changes to Bitcoin communication formats are required. All that's needed is a minor tweak to the transaction relay algorithm. We also see that, with or without the timeout feature, the content of the deferred INV message is inefficient. Some peers may already be aware of some of the deferred transactions. The ideal approach would be for the node to keep track of which peers have declared which transactions and to prepare individual announcements for each peer, announcing only those transactions that the recipient peer has not yet learned about. This strategy, however, has a couple of drawbacks: To begin with, it would add to the complexity of bookkeeping, but this is easily handled. Second, and probably more importantly, due to postponed transaction relay, a peer may have previously learnt about the transaction (or numerous transactions) but has not yet told the current node. This means that all redundancy resulting from all peers receiving the identical INV notice is difficult to delete. This isn't a big deal because each transaction in an INV message only has a 4-byte data item type and a 32-byte hash, so the quantity of redundant data is probably small enough to overlook.

In Algorithm 1, we employ two parameters in the pseudocode deferred transaction relay: threshold, which is the maximum number of transactions for which the INV announcement is deferred, and timeout, which is the maximum time for verified transactions to be spent in the deferred transactions list. Newly received and validated transactions are temporarily saved in a list known as the deferred list. When the list's size reaches a predetermined limit, an INV message containing all the list's transactions is sent to all peers. Furthermore, each batch of transactions published via INV messages to the node's peers' resets (really, restarts) a timer that ticks down from the timeout setting. The list of deferred transactions is checked when the timer ends. If the list is found to be non-empty, no action is performed; however, if it is found to be non-empty, all the node's transactions are transmitted to all the node's peers via INV messages. In the latter instance, the number of transactions may be smaller than the predetermined limit. After that, the timer is reset. We also want to point out that the proposed deferred transaction relay is fully backward or, to put it another way, two-way compatible with current Bitcoin software. INV messages, for example, can already contain several transaction inventories. As a result, nodes running existing software can receive such messages without issue. INV messages with a single transaction inventory, on the other hand, can be received by nodes running updated software. So, in terms of compatibility, this update necessitates no changes or adjustments.

7. ANALYSIS OF TRANSACTIONS AND CONFIRMATION TIMES

For transactions in the range of 0-60000, the graph below was created. In seconds, the confirmation time is measured. With a rise in the number of transactions, we witness a progressive increase in confirmation times. For analysis, these values were taken from the Simulator.

Let's look at the confirmation time trend for a few transactions to have a better idea of the relationship between transactions and confirmation timings. The information below was gathered by setting the transactions to a specific value and recording their confirmation times.

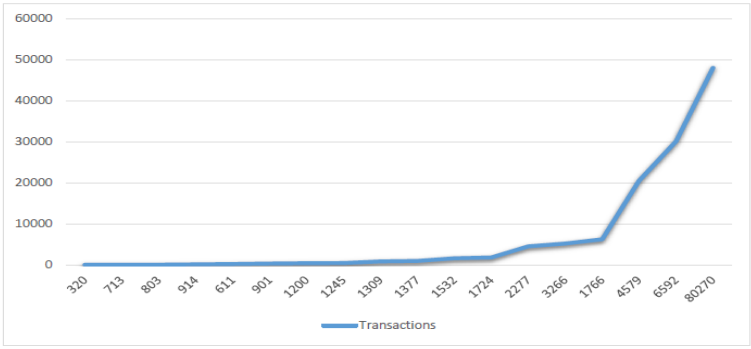

Figure 16. Transcations with their Confirmation Times

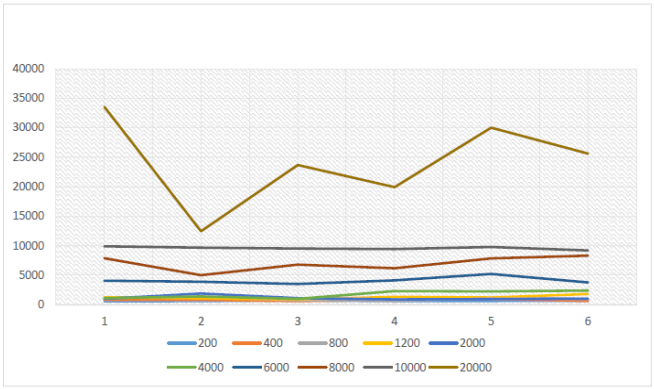

Figure 17. Confirmation Times per Transactions

A series of ten transactions is depicted in the graph above, with values of 200, 400, 800, 1200, 2000, 4000, 6000, 8000, 10000, and 20000. The confirmation time in seconds has been recorded in the appropriate manner.

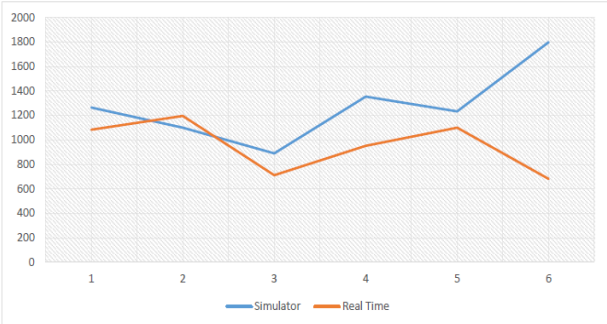

Figure 18. Simulator and Real Time Confirmation Time for 1200 transactions

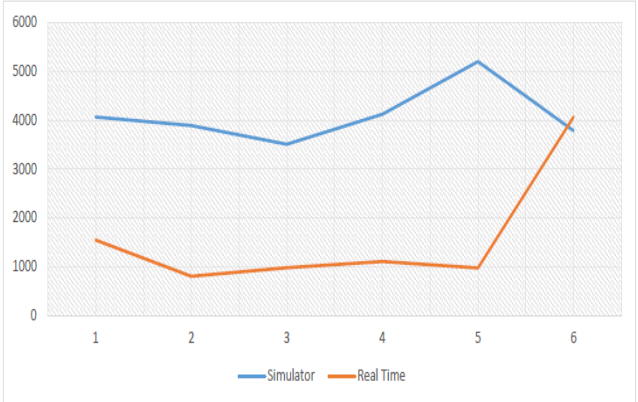

Figure 19. Simulator and Real Time Confirmation Time for 6000 transactions

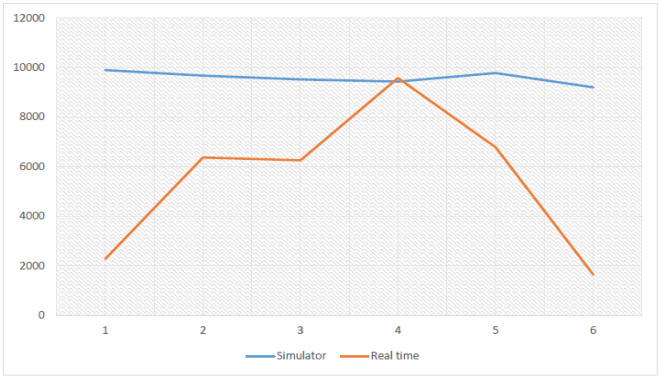

Figure 20. Simulator and Real Time Confirmation Time for 12000 transactions

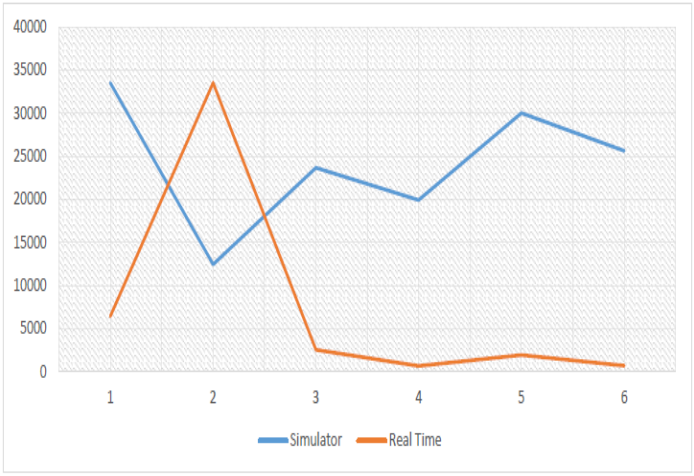

Figure 21. Simulator and Real Time Confirmation Time for 20000 transactions

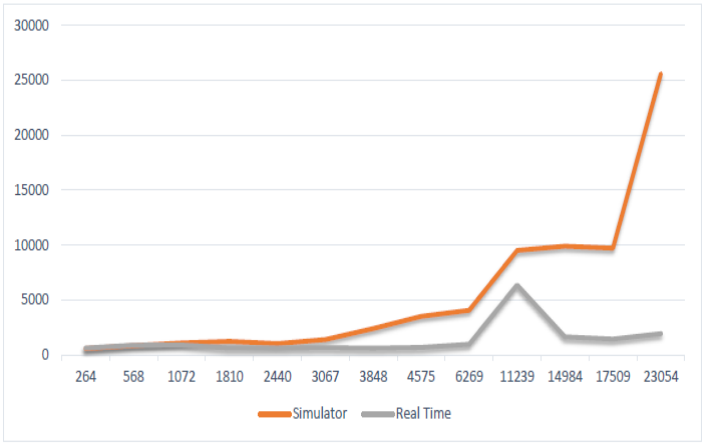

Figure 22. Confirmation Time Trend for Simulator and Real time Environments

8. TRANSACTION FEE AND CONFIRMATION TIMES ANALYSIS

The graph below was created using data from transaction fees ranging from 0.0004 BTC to 0.04 BTC. For analysis, the confirmation time for each has been recorded in seconds. Though Figure 23 shows irregular peaks for transactions in the 0.001 to 0.002 range, the trend is quite consistent.

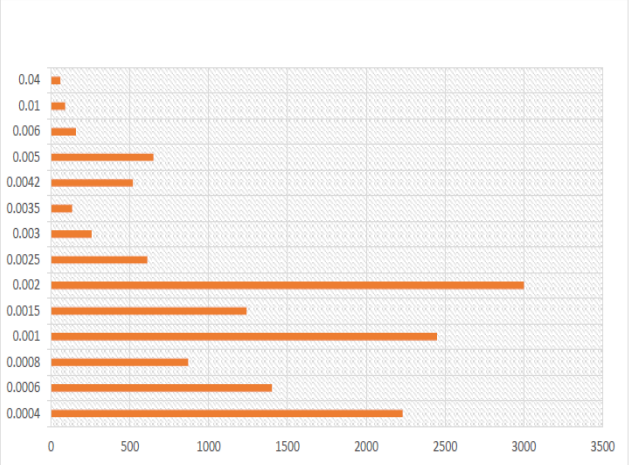

Figure 23. Confirmation Times with increase in Transaction Fee

Let's look at confirmation times for different transaction fee values to get a better idea of how transaction fees affect confirmation time.

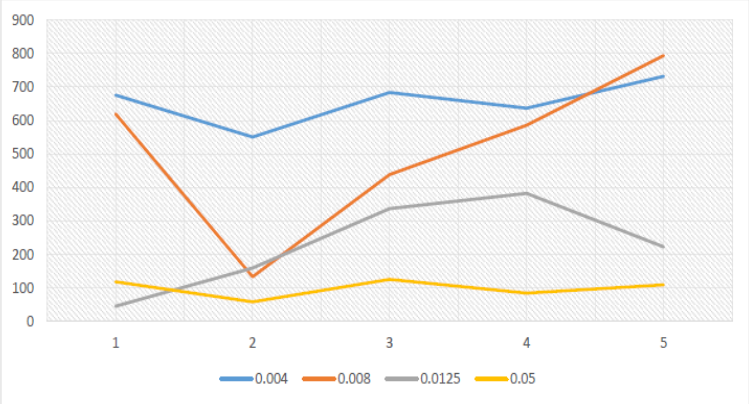

Figure 24. Transaction Fee Confirmation Time in Seconds

The graph Figure 24 shows the confirmation cost in Bit coin Units of 0.004, 0.008, 0.0125, and 0.05. For analysis, the confirmation time for each has been recorded in seconds.

Now we'll compare the simulator data to real-world data.

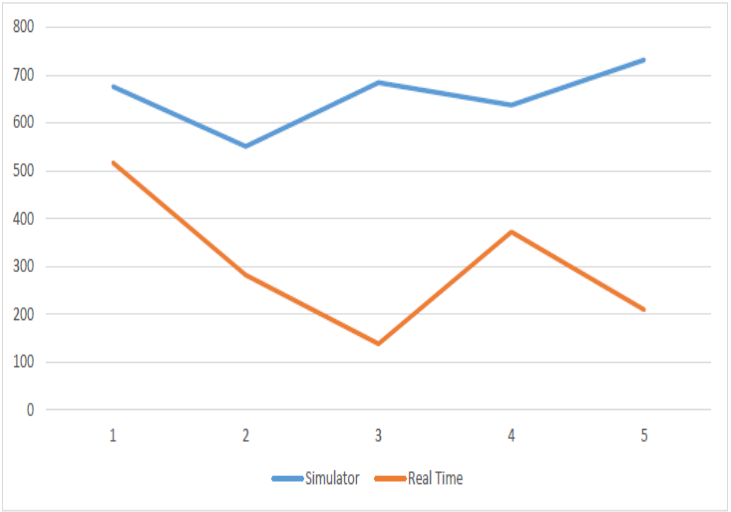

Figure 25.Trends in Confirmation Time for 0.004BTC in Simulator and Real-Time Environments

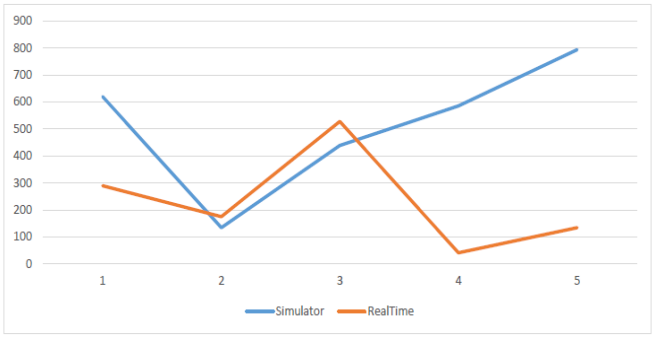

Figure 26. Trends in Confirmation Time for 0.008BTC in Simulator and Real-Time Environments

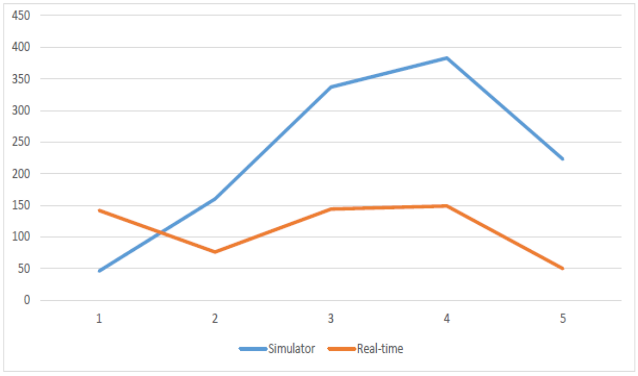

Figure 27. Trends in Confirmation Time for 0.0125BTC in Simulator and Real-Time Environments

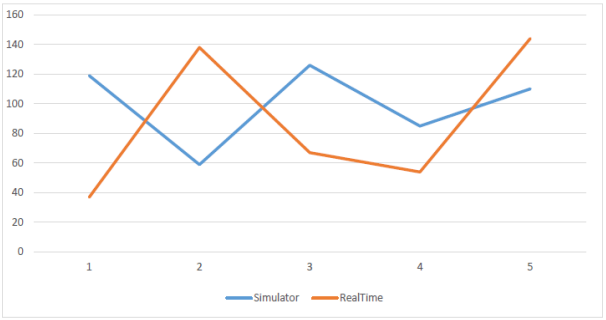

Figure 28. Trends in Confirmation Time for 0.05BTC in Simulator and Real-Time Environments

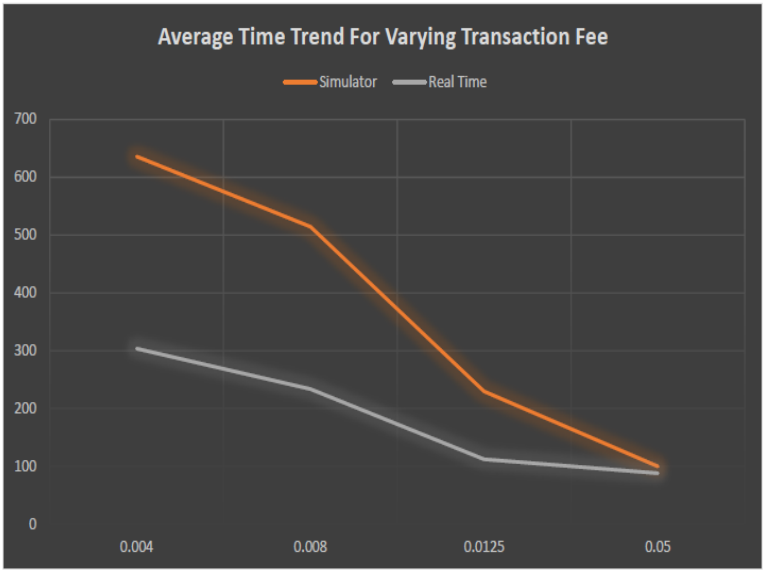

Figure 29. Average Confirmation Time as Transaction Fee Amount Increases

9. ANALYSIS OF SCALABILITY PARAMETERS

1. Latency- Latency in the blockchain network is defined as any delay induced by the propagation of blocks via the network. The time it takes for a transaction to be confirmed has a direct impact on network latency. Lower latencies and faster network propagation would result from faster transaction confirmation times. We discovered that, based on the simulator's analysis and comparison to real-time data, the following can be done to reduce network latency: The open challenges to the techniques recommended have also been described below:

a) Increasing the transaction price would enhance the likelihood of a faster confirmation time for that transaction, as well as its odds of being included in the block and, in some cases, reduced latency.

b) Increasing the system's transaction load would result in longer latencies. We can expect the block size to expand as the number of transactions in the system grows. To transport bigger blocks, more network bandwidth would be required, more power would be consumed, and the network would get congested, increasing delay.

2. **Throughput-** The number of transactions confirmed per second is how the blockchain system's throughput is measured. Most modern payment processing systems, such as Visa, have a throughput of 2000 transactions per second on average. The typical throughput of Bitcoin-based blockchain systems is only 7 transactions per second. Clearly, to close the gap between this and a modern payment processor, scalability must be much increased. The following are a few of the findings from the study:

a) Increasing the block size to accommodate a larger number of transactions will raise both the transaction load and the throughput of the system. The block size in the current Bitcoin system is limited to 1 MB. This sounds like a valid claim if we truly want to boost efficiency.

b) Increasing block size to achieve better throughputs comes at the expense of blockchain security and decentralization.

c) Hard forking would be required if the transaction load on the system increased, as would the block size.

3. Transaction Fee and its Effect on Scalability- Transaction delays are one of the most significant issues with Blockchains that affect scalability. These transaction delays are the result of a combination of variables, one of which is the transaction fee. Because every user can add a set transaction amount to a transaction, thereby pushing it to the front of the line, some transactions with minimal transaction fees become starved. It could mean one or two things:

a) First, transactions with greater transaction fees are confirmed more quickly. This occurs for the reasons indicated above, when a transaction is pushed to the front of the line because it has a greater transaction fee associated with it. For the miners, this is very profitable. As a result, transactions with lower transaction fees are severely harmed.

b) The second case is when a transaction suffers even though it has a significant transaction fee attached to it. This happens when a transaction's value is large, yet there are other transactions in the queue with the same or greater values. So, if all n transactions have the same transaction fee, a transaction may starve and take an eternity to complete in a pool of n transactions.

4. Block size- As previously established, the Bitcoin block size is now capped at 1 MB. A block can hold roughly 1000-2000 transactions on average. As shown below, reducing or increasing the block size has a significant impact on scalability metrics:

a) Increasing the block size would result in an increase in blockchain capacity. With more data capacity and increased security, the potential of bitcoin-based blockchain protocols grows.

b) An increase in transaction load combined with a larger block size would imply the ability to execute many transactions, resulting in higher throughput and efficiency.

c) Increasing the block size to allow for greater capacity and transactions would reduce security and move control to a centralized entity.

5. Number of miners in the system- More mining power in the blockchain system would help to distribute the power consumption and block mining task across the network more equitably. Lower latencies and convergence would result. Faster confirmation times and higher throughput would also be a benefit.

10.PERFORMANCE EVALUATION OF THE PROPOSED ALGORITHM

We constructed a Bitcoin network simulator using AnyLogic multi-paradigm simulation engine from The AnyLogic Company, Oakbrook Terrace, IL, to analyses the performance of the deferred transaction relay. In our simulator, 1000 nodes are connected to a Bitcoin-style peer-to-peer network. A node's maximum and minimum connectedness were 9 and 52, respectively, resulting in a mean connectivity of 16.35 and a network diameter of 4. The cumulative distribution function of delay obtained from measurements in the real Bitcoin network is used to determine network delays, considering the differences in intra- and inter-continental delays between Europe, Asia, and the Americas. We'll suppose that the network capacity is 1GBps and that individual nodes have 10MBps throughput. Using uniform distribution, transactions are injected into a randomly chosen node. The entire network's transaction arrival rate was set at 4.5 transactions per second, which is close to the real Bitcoin network. With uniform distribution, transaction sizes range from 100 to 511 bytes. The simulator runs a functional Bitcoin network with block generation, propagation, and chaining, but the approach described above, and the findings given focus solely on transaction volume. We've done a variety of experiments with this simulator, including different protocol choices and threshold and timeout numbers, as detailed

below. Each trial lasted 11,500 seconds, or slightly more than three hours and ten minutes. During this time, the total number of transactions generated was in the region of 51,500 to 52,150.
The postponed transaction list threshold was changed between 1 and 12 in the first set of trial runs. When the threshold is set to one, all required transactions are sent one by one, for obvious reasons. The threshold for the delayed transaction list was modified in the same range in the second set of experiments, but the timeout feature was enabled with a 5 second timeout. Figure 30 shows the average number of messages transmitted per transaction and per node in this scenario.

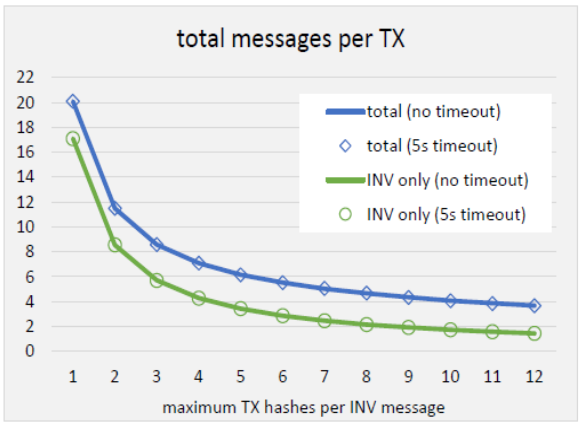

Figure 30. The total number of INV, GETDATA, and TX messages required to propagate a single transaction, as well as the total number of INV, GETDATA, and TX messages.

The higher set of numbers (shown in blue) refers to the entire number of messages: INV, GETDATA, and TX combined, whereas the lower set (shown in green) relates to simply INV messages. The threshold number of transaction hashes that must be delivered in a single INV message is the independent variable in both diagrams. As can be seen, when numerous transactions are transmitted together, the number of messages required to propagate a single transaction to/from a node rapidly reduces. When each node collects only two new transactions before sharing them with its neighbors, the amount of INV messages lowers by half! The number of INV messages is reduced to one-tenth of the initial number by waiting for roughly 8 or 9 new transactions. Because the total number of messages comprises GETDATA and TX messages, the latter of which only contains a single raw transaction, the relative advantage in terms of the total number of messages is a little lower. Even so, collecting just two transactions from the deferred transaction list reduces the total number of messages by about 42.8 percent, and waiting for three or four reduces the total number of messages by 57.3 percent or 64.8 percent, respectively; increasing the threshold value reduces this even more, but the savings are getting smaller. It's worth noting that the difference between the situation with no timeout (solid lines) and the case with timeouts enabled (circles) is nearly negligible. The timeout functionality, in other words, has no effect on the total quantity of messages transmitted. The following is an explanation: The average transaction arrival rate is 4.5 per second, which is true for the entire network as well as each individual node because transactions must be transmitted to each node. The average number of new transaction arrivals per node should be substantially over 20 in a time of 5 seconds (which corresponds to the timeout limit). Even at the maximum threshold value of 12, threshold limiting will most likely be used before timeout limiting, which will only be used in a small fraction of occurrences. This effect will be considerably more prominent at lower threshold values.

Figure 31 shows the total number of expired (solid green line) and interrupted (dashed red line) timeouts to validate this. There is no diagram for the first experiment run in which the timeout functionality is disabled, for obvious reasons.

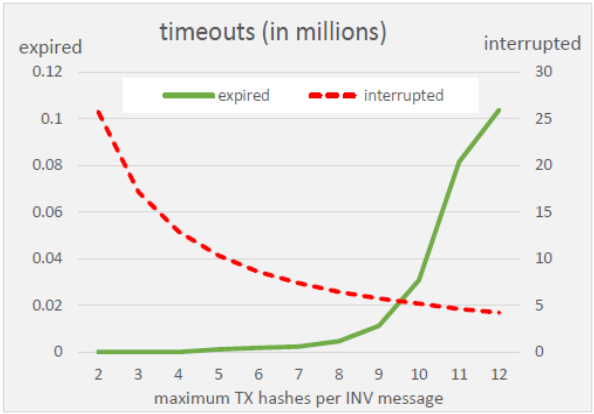

Figure 31. In this experiment, the number of expired and interrupted timeouts (in millions) was counted

As can be observed, as the threshold value is increased, the number of expired timeouts grows, while the number of expired timeouts drops. The overall number of expired timeouts, on the other hand, is more than two orders of magnitude greater than the number of interrupted timeouts, which explains why the two variables are represented on radically different vertical scales. As previously stated, reducing the quantity of messages comes at the cost of transaction propagation delay. This may be seen in the graphs of mean propagation delay, which is the time it takes for a transaction to reach 99 percent of the network's nodes. Figure 32 depicts the appropriate diagrams.

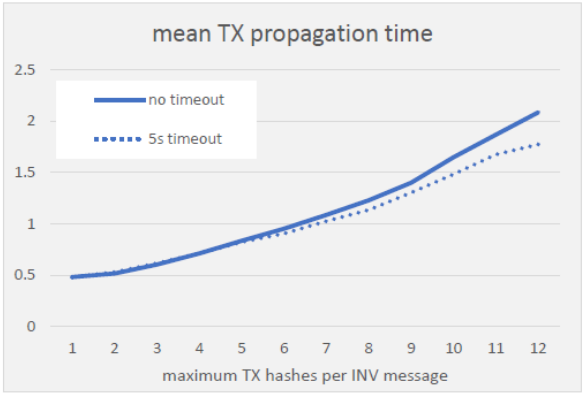

Figure 32. Time it takes for a transaction to reach 99 percent of nodes (transaction propagation delay)

As expected, the restricted threshold deferred transaction relay generates an increase in propagation latency that is slightly but not considerably larger in the experiment without the timeout limitation (solid line) than in the trial with this limitation (dotted line). Due to the randomness of transaction arrivals, waiting for the threshold may take longer if there is no timeout limit. The timeout limit, on the other hand, indicates that not every INV message will contain the full complement of transactions, resulting in an increase in the number of transactions, as previously mentioned. While the nearly fourfold increase in transaction propagation delay may appear excessive, it should be perfectly acceptable in practice. The average size of a Bitcoin node's mempool is currently well over 60MBytes, according to figures obtained from tracking sites. The typical block size is somewhat more than 1MByte, and one block is generated every 10 minutes on average. As a result, the average time a transaction spends in the mempool before being packaged into a block is far longer than the deferred transaction relay's 1.5 seconds of additional propagation time. In the third series of experiments, the postponed transaction list threshold was set at 5, and the timeout was varied between 0.5 and 6 seconds. For reference, a value labelled imm (for 'immediate') was added to some of the diagrams; it corresponds to the case where the threshold was set to 1, implying that there is no timeout at all; as a result, those values are identical to the corresponding values for the threshold of one obtained in the first experiment. The total number of messages and the number of INV messages required to send a single transaction from/to a single node are depicted in Figure 33.

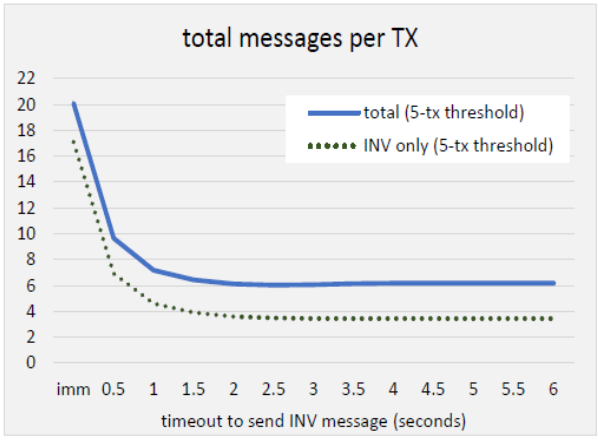

Figure 33. The total number of INV, GETDATA, and TX messages required to propagate a single transaction, as well as the total number of INV, GETDATA, and TX messages

As can be observed, raising the timeout allows the node to accumulate more transactions in the deferred list before delivering an INV announcement, which reduces the overall number of messages sent. However, unlike the preceding Subsection's situation with a fixed timeout, the overall number of messages frost declines rapidly before flattening out at around 6 total messages and 3.5 INV messages.

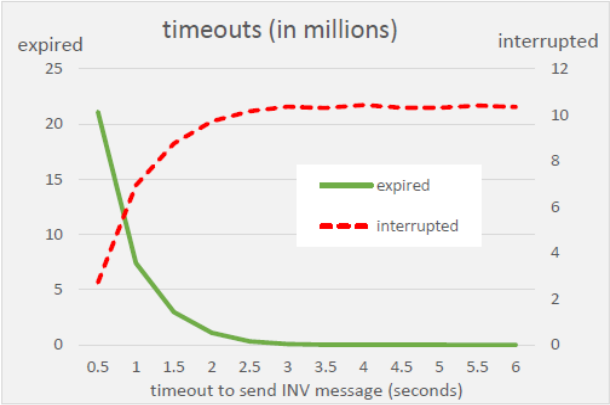

Figure 34. Total number of expired and interrupted timeouts (in millions)

This is due to the interaction between the threshold and timeout values once again. Because the threshold value is set to five, the threshold limitation will most likely be activated before the timeout limitation. As a result, the number of messages remains constant at the levels shown in Figure 34, with a threshold of 5. Figure 36 shows the number of expired and interrupted timeouts: as the timeout lengthens, the number of interrupted timeouts increases rapidly, while the number of timeouts that manage to expire decreases in a complementary fashion. Furthermore, as shown in Figure 35, the interaction between threshold and timeout constraints extends to transaction propagation latency. In this case, the delay rises to around one second at timeout values of 1.5 to 2s, then falls slightly and remains essentially flat at about 0.8s; as previously stated, this value corresponds to that in Figure 35 with a threshold of 5.

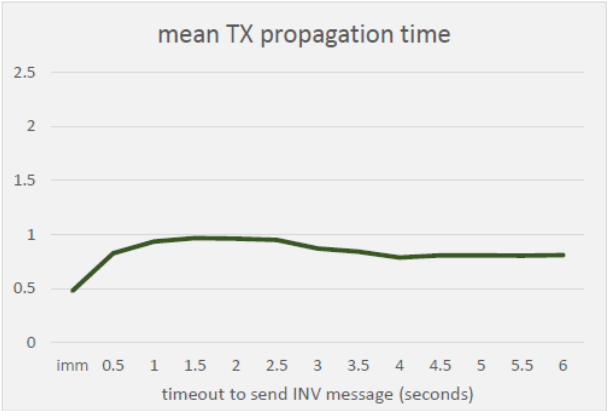

Figure 35. Time it takes for a transaction to reach 99 percent of nodes (transaction propagation delay)

11.CONCLUSION

In the current day, a centralized authority, such as a bank, is completely responsible for providing services. This is because the bank is seen as a trustworthy entity. The blockchain system is decentralized and is steadily gaining commercial acceptance. Blockchain is a sought-after technology because of its pseudo-anonymous and decentralized structure, and enthusiasts are delving further into it to fully utilize its potential, not just as digital money but also for other applications and services that may be constructed. The global pool of networkers, such as miners, employs their computing power to secure the blockchain system's security. The lack of central authority assures that no third party may interfere with the transaction because it is in the public domain. This also means that there are no additional fees to pay if a third party initiates these services. This is the primary reason behind blockchain's future potential as well as its current appeal. The scalability parameters of blockchains remain a source of concern, as they prohibit their utilization from matching that of modern payment processors. However, depending on the application service, a compromise or a balance might be struck to use blockchain in specific situations. For instance, if an investor is more interested in exchanging massive amounts of data and is ready to tolerate some security and centralization compromises, a blockchain-based protocol can be created accordingly. If the needs are more specific, such as greater security, the contemporary blockchain protocol is ideal. This study introduced an enhanced transaction adjournment technique aimed at improving Bitcoin's scalability. The proposed method, which utilizes Inventory messaging (INV) and deferred transaction relay, was simulated using BlockSim and the AnyLogic Multi Paradigm Simulation Engine with a network of 1000 interconnected nodes. The results demonstrated that this approach effectively reduced network message overhead by up to 30% while maintaining an acceptable increase in transaction propagation delay. By adjusting threshold and timeout values, a balance can be achieved between reducing message traffic and maintaining reasonable transaction speeds. This suggests that

enhanced transaction adjournment techniques can significantly optimize Bitcoin's scalability without compromising its security and decentralization. These findings highlight the potential for future enhancements to blockchain protocols that prioritize efficiency and scalability while preserving the core principles of decentralization as seen in Table 2. Further research can explore adaptive mechanisms that dynamically adjust transaction adjournment parameters in response to network congestion, improving Bitcoin's overall efficiency in real-world applications.

Table 2. Comparison of Blockchain Scalability Studies and Acquired

Study	Scalability Technique Used	Simulation Tool	Key Findings	Limitations	Acquired Results
This Study (Proposed Work)	Enhanced Transaction Adjournment (Deferred Transaction Relay with INV Messaging)	BlockSim, AnyLogic	Reduces message overhead while maintaining transaction speed	Slight increase in transaction propagation time	Achieved up to 30% reduction in network message overhead with an acceptable propagation delay increase
Eyal et al. (2016)	Bitcoin-NG (Leader-Based Block Generation)	Custom Simulator	Reduces transaction confirmation time and increases throughput	Requires protocol changes and centralization risks	Achieved 2-3x increase in transaction throughput but required leader selection
Gervais et al. (2016)	Adjustable Block Size & Block Interval Optimization	Bitcoin Core Simulator	Improved transaction confirmation speed	Increased risk of orphaned blocks	Improved transaction speed by 15% but increased orphan rate
Croman et al. (2016)	Off-Chain Scaling (Payment Channels, Lightning Network)	Theoretical Analysis	Reduces on-chain load, improves TPS	Complexity and centralization concerns	Increased transactions per second (TPS) to 1000+ but required extensive off-chain adoption
Sompolinsky & Zohar (2018)	GHOST Protocol (Graph-Based Block Validation)	Theoretical Model	Reduces block propagation time and improves fork resolution	Increased computational complexity	Reduced block orphaning by 17%, improving stability
Pass et al. (2017)	Fruitchain (Hybrid Block & Transaction Validation)	Custom Simulation	Enhances security and scalability	Requires protocol modifications	Improved block finality by 20%, ensuring faster confirmations

12.FUTURE WORK

Due to its difficulty in scaling, the Blockchain presents a risky environment for users and businesses interested in exploring its potential as a full-fledged consumer platform. It's time to stop thinking of blockchain as only the backbone of digital currencies. Other applications and services can be built on top of blockchain's ability to carry large amounts of data and provide security. Exploration of multichines, which can move all types of currencies in a single distributed ledger, paving the door for a technology that considers both security and legislation. As traditional methods of financial exchange fade away, blockchains and their possibilities in digital currency, smart contracts, and payment processors become increasingly important. The number of users in the blockchain system is also increasing as the popularity of blockchains grows. Purchasing items and doing micro transactions are only the beginning of blockchain technology's era. Trading without boundaries is no longer a silly idea, but a reality, thanks to the integration of mining in mobile phones, better security for wallet handling, and the development of various applications and services based on the blockchain protocol.

Funding

None

ACKNOWLEDGEMENT

None

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] S. Nakamoto, ``Bitcoin: A peer-to-peer electronic cash system," Manubot, Tech. Rep., 2008.

[2] G. Wood, ``Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, vol. 151, pp. 1_32, Apr. 2014.

[3] C. Cachin, ``Architecture of the hyperledger blockchain fabric," in Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers, vol. 310, 2016.

[4] H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, ``Blockchain challenges and opportunities: A survey," Int. J. Web Grid Services, vol. 14, no. 4, p. 352, 2018.

[5] P. Zheng, Z. Zheng, X. Luo, X. Chen, and X. Liu, ``A detailed and real-time performance monitoring framework for blockchain systems," in Proc. 40th Int. Conf. Softw. Eng. Softw. Eng. Pract.-ICSE-SEIP, 2018, pp. 134_143. The Scalability Trilemma in Blockchain. Accessed: Sep. 1, 2019. [Online]. Available: https://medium.com/@aakash_13214/the-scalability-trilemmain-blockchain-75fb57f646df

[6] S. Gilbert and N. Lynch, ``Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services," SIGACT News, vol. 33, no. 2, p. 51, Jun. 2002.

[7] X. Li, P. Jiang, T. Chen, X. Luo, and Q.Wen, ``A survey on the security of blockchain systems," Future Gener. Comput. Syst., to be published. Bitcoin Cash. Accessed: Sep. 1, 2021. [Online]. Available: https://www.bitcoincash.org/ Bip152. Accessed: Sep. 1, 2021. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0152.mediawiki

[8] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, ``A secure sharding protocol for open blockchains," in Proc. ACM SIGSACConf. Comput. Commun. Secur.-CCS, 2016, pp. 17_30.

[9] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, ``OmniLedger: A secure, scale-out, decentralized ledger via sharding," in Proc. IEEE Symp. Secur. Privacy (SP), May 2018, pp. 583_598.

[10] M. Zamani, M. Movahedi, and M. Raykova, ``RapidChain: Scaling blockchain via full sharding," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Jan. 2018, pp. 931_948.

[11] J. Wang and H. Wang, ``Monoxide: Scale out blockchains with asynchronous consensus zones," in Proc. 16th USENIX Symp. Netw. Syst. Design Implement. (NSDI), 2019, pp. 95_112.

[12] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, ``Bitcoin-NG: A scalable blockchain protocol," in Proc. 13th USENIX Symp. Netw. Syst. Design Implement. (NSDI), 2016, pp. 45_59.

[13] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, ``Algorand: Scaling byzantine agreements for cryptocurrencies," in Proc. 26th Symp. Operating Syst. Princ.-SOSP, 2017, pp. 51_68.

[14] I. Bentov, R. Pass, and E. Shi, ``Snow white: Provably secure proofs of stake," IACR Cryptol. ePrint Archive, vol. 2016, p. 919, Sep. 2016.

[15] A. Kiayias, A. Russell, B. David, and R. Oliynykov, ``Ouroboros: A provably secure proof-of-stake blockchain protocol," in Proc. Annu. Int. Cryptol. Conf. Santa Barbara, CA, USA: Springer, 2017, pp. 357_388.

[16] B. David, P. Gaºi, A. Kiayias, and A. Russell, ``Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain," in Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn. Tel Aviv, Israel: Springer, 2018, pp. 66_98.

[17] J. Poon and T. Dryja. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. [Online]. Available: https://www.bitcoinlightning.com

[18] J. Poon and V. Buterin, ``Plasma: Scalable autonomous smart contracts," White Paper, 2017, pp. 1_47. [Online]. Available: https://www.plasma.io Cosmos. Accessed: Nov. 1, 2021. [Online]. Available: https://cosmos.network/whitepaper

[19] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, D. Song, R. Wattenhofer, and E. G. Sirer, ``On scaling decentralized blockchains," in Proc. Int. Conf. Financial Cryptogr. Data Secur. Christ Church, Barbados: Springer, 2016, pp. 106_125.

Scalability of Bitcoin. Accessed: Jan. 1, 2021. [Online]. Available: https://en.bitcoin.it/wiki/Scalability

[20] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khof_, L. Gasser, and B. Ford, ``Enhancing bitcoin security and performance with strong consistency via collective signing," in Proc. 25th USENIX Security Symp. USENIX Secur., 2016, pp. 279_296.

[21] C. Decker and R.Wattenhofer, ``A fast and scalable payment network with bitcoin duplex micropayment channels," in Proc. Symp. Self-Stabilizing Syst. Edmonton, AB, Canada: Springer, 2015, pp. 3_18.

Raiden Network. Accessed: Sep. 1, 2021. [Online]. Available: https://raiden.network/

[22] A. Miller, I. Bentov, S. Bakshi, R. Kumaresan, and P. McCorry, ``Sprites and state channels: Payment networks that go faster than lightning," in Proc. Int. Conf. Financial Cryptogr. Data Secur. Frigate Bay, St. Kitts: Springer, 2019, pp. 508_526.

[23] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille. (2014). Enabling Blockchain Innovations With Pegged Sidechains. [Online]. Available: http://www.opensciencereview.com/papers/123/enablingblockchaininnovations-with pegged-sidechains

Liquidity Network. Accessed: Sep. 1, 2021. [Online]. Available: https://liquidity.network/

[24] G.Wood, ``Polkadot: Vision for a heterogeneous multi-chain framework," Polkadot, White Paper, 2016.

[25] J. Teutsch and C. Reitwieÿner, ``A scalable veri_cation solution for blockchains," 2019, arXiv:1908.04756. [Online]. Available: https://arxiv.org/abs/1908.04756

[26] H. Kalodner, S. Goldfeder, X. Chen, S. M. Weinberg, and E. W. Felten, ``Arbitrum: Scalable, private smart contracts," in Proc. 27th USENIX Secur. Symp. USENIX Secur., 2018, pp. 1353_1370.

[27] E. Lombrozo, J. Lau, and P. Wuille, ``Segregated witness (consensus layer)," Bitcoin Core Develop. Team, Tech. Rep., 2015.

[28] D. Ding, X. Jiang, J.Wang, H.Wang, X. Zhang, and Y. Sun, ``Txilm: Lossy block compression with salted short hashing," 2019, arXiv:1906.06500. [Online]. Available: https://arxiv.org/abs/1906.06500

[29] Z. Xu, S. Han, and L. Chen, ``CUB, a consensus unit-based storage scheme for blockchain system," in Proc. IEEE 34th Int. Conf. Data Eng. (ICDE), Apr. 2018, pp. 173_184.

[30] X. Dai, J. Xiao, W. Yang, C. Wang, and H. Jin, ``Jidar: A jigsaw-like data reduction approach without trust assumptions for bitcoin system," in Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst. (ICDCS), Jul. 2019, pp. 1317_1326.

[31] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, ``Inclusive block chain protocols," in Proc. Int. Conf. Financial Cryptogr. Data Secur. San Juan, Puerto Rico: Springer, 2015, pp. 528_547.

[32] Y. Sompolinsky, Y. Lewenberg, and A. Zohar, ``Spectre: A fast and scalable cryptocurrency protocol," IACR Cryptol. ePrint Archive, vol. 2016, p. 1159, 2016.

[333] Y. Sompolinsky and A. Zohar, ``Phantom: A scalable blockdag protocol," IACR Cryptol. ePrint Archive, vol. 2018, p. 104, 2018.

[34] C. Li, P. Li, D. Zhou,W. Xu, F. Long, and A. Yao, ``Scaling nakamoto consensus to thousands of transactions per second," 2018, arXiv:1805.03870. [Online]. Available: https://arxiv.org/abs/1805.03870

[35] S. D. Lerner. (2015). Dagcoin: A CryptocurrencyWithout Blocks. [Online]. Available: https://bitslog.com/2015/09/11/dagcoin/

Iota. Accessed: Jan. 22, 2022. [Online]. Available: https://www.iota.org/

[36] A. Churyumov. (2016). Byteball: A Decentralized System For Storage and Transfer of Value. [Online]. Available: https://byteball.org/Byteball.pdf

[37] C. LeMahieu. Nano: A Feeless Distributed Cryptocurrency Network. Accessed: Mar. 24, 2021. [Online]. Available: https://nano.org/en/ whitepaper

[38] G. Naumenko, G. Maxwell, P. Wuille, S. Fedorova, and I. Beschastnikh, ``Bandwidth-ef_cient transaction relay for bitcoin," 2019, arXiv: 1905.10518. [Online]. Available: https://arxiv.org/abs/1905.10518

[39] E. Rohrer and F. Tschorsch, ``Kadcast: A structured approach to broadcast in blockchain networks," in Proc. 1st ACM Conf. Adv. Financial Technol., 2019, pp. 199_213.

[40] N. Chawla, H. W. Behrens, D. Tapp, D. Boscovic, and K. S. Candan, Velocity: Scalability improvements in block propagation through rateless erasure coding, in Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC), May 2019, pp. 447_454.

[41] U. Klarman, S. Basu, A. Kuzmanovic, and E. G. Sirer, ``Bloxroute: A scalable trustless blockchain distribution network whitepaper," White Paper.

[42] I. Weber, V. Gramoli, A. Ponomarev, M. Staples, R. Holz, A. B. Tran, and P. Rimba, ``On availability for blockchain-based systems," in Proc. IEEE 36th Symp. Reliable Distrib. Syst. (SRDS), Sep. 2017, pp. 64_73.

Decentralized Application. Accessed: Dec. 12, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Decentralized_application/

[43] H. Vranken, ``Sustainability of bitcoin and blockchains," Current Opinion Environ. Sustainability, vol. 28, pp. 1_9, Oct. 2017.

Decentralized Application. Accessed: Dec. 12, 2021.

[Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki
[44] First Bitcoin Cash Block Mined. Accessed: Sep. 18, 2021. [Online]. Available: https://news.bitcoin.com/fork-watch-_rst-bitcoin-cash-block-mined/
[45] Block size limit controversy. Accessed: Sep. 18, 2021. [Online]. Available: https://en.bitcoin.it/wiki/Block-size-limit_controversy
[46] Block Size Increase. Accessed: Sep. 18, 2021. [Online]. Available: https://bitfury.com/content/downloads/block-size-1.1.1.pdf
[47] S. Elmohamed. Towards Massive On-Chain Scaling: Block Propagation Results With Xthin. Accessed: Sep. 18, 2021. [Online]. Available: https://medium.com/@peter_r/towards-massive-on-chain-scaling-blockpropagation-results-with-xthin-a0f1e3c23919
[48] Lumino Transaction Compression Protocol(LTCP). Accessed: Sep. 18, 2021. [Online]. Available: https://docs.rsk.co/LuminoTransactionCompressionProtocolLTCP.pdf
[49] Y. Sompolinsky and A. Zohar, ``Secure high-rate transaction processing in bitcoin," in Proc. Int. Conf. Financial Cryptogr. Data Secur. San Juan, Puerto Rico: Springer, 2015, pp. 507_527. [60] Casper-Proof-of-Stake-Compendium. Accessed: Sep. 18, 2021. [Online]. Available: https://github.com/ethereum/wiki/wiki/Casper-Proof-of-Stakecompendium
[50] Larimer, ``Delegated proof-of-stake (dpos)," Bitshare, White Paper, 2014.
Bitshares Blockchain. Accessed: Sep. 18, 2021. [Online]. Available: https://bitshares.org/
eosio, The Most Powerful Infrastructure for Decentralized Applications. Accessed: Sep. 13, 2021. [Online]. Available: https://eos.io/
[51] Eos:Less Than 1% of EOS Addresses Hold 86% of the Tokens! Accessed: Sep. 18, 2021. [Online]. Available: https://medium.com/@freetokencryptobounty/eos-less-than-1-of-eos-addresseshold-86-of-the-tokens-5ad4b2eac403
[52] M. Castro and B. Liskov, ``Practical byzantine fault tolerance," in Proc. OSDI, vol. 99, 1999, pp. 173_186.
[53] Byzantine Fault. Accessed: Dec. 10, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Byzantine_fault
[54] E. Buchman, ``Tendermint: Byzantine fault tolerance in the age of blockchains," Ph.D. dissertation, Tendermint, 2016.
[55] E. Syta, I. Tamas, D. Visher, D. I. Wolinsky, P. Jovanovic, L. Gasser, N. Gailly, I. Khof_, and B. Ford, ``Keeping authorities `honest or bust' with decentralized witness cosigning," in Proc. IEEE Symp. Secur. Privacy (SP), May 2016, pp. 526_545.
[56] R. Pass and E. Shi, ``Hybrid consensus: Ef_cient consensus in the permissionless model," in Proc. 31st Int. Symp. Distrib. Comput. (DISC), Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2017.
[57] I. Abraham, D. Malkhi, K. Nayak, L. Ren, and A. Spiegelman, ``Solida: A blockchain protocol based on recon_gurable byzantine consensus," 2016, arXiv:1612.02916. [Online]. Available: https://arxiv.org/abs/1612.02916
[58] Proof of Authority-Wikipedia. Accessed: Sep. 1, 2019. [Online]. Available:
https://en.wikipedia.org/wiki/Proof_of_authority
[59] Proof-of-Capacity. Accessed: Dec. 10, 2021. [Online]. Available: https://burstwiki.org/en/proof-of-capacity/
[60] A. Nandwani, M. Gupta, and N. Thakur, ``Proof-of-participation: Implementation
of proof-of-stake through proof-of-work," in Proc. Int. Conf. Innov. Comput. Commun. New Delhi, India: Springer, 2019, pp. 17_24.
[61] Shard Wiki. Accessed: Dec. 10, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Shard_(database_architecture)
[62] E. Fynn and F. Pedone, ``Challenges and pitfalls of partitioning blockchains," in Proc. 48th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshops (DSN-W), Jun. 2018, pp. 128_133.
[63] E. Syta, P. Jovanovic, E. K. Kogias, N. Gailly, L. Gasser, I. Khof_, M. J. Fischer, and B. Ford, ``Scalable bias-resistant distributed randomness," in Proc. IEEE Symp. Secur. Privacy (SP), May 2017, pp. 444_460.
[64] Light-Weight User. Accessed: Dec. 10, 2021. [Online]. Available: https://en.bitcoin.it/wiki/Lightweight_node
[65] The Zilliqa Technical Whitepaper, Z. Team, Oakbrook Terrace, IL, USA, Sep. 2017, vol. 16, p. 2019.
[66] The Harmony Team. Open Consensus for 10 Billion People. Accessed: Dec. 10, 2021. [Online]. Available: https://harmony.one/
[67] Dag (Directed Acyclic Graph). Accessed: Jan. 22, 2022. [Online]. Available: https://en.wikipedia.org/wiki/Directed_acyclic_graph
[68] Fantom. Accessed: Jan. 22, 2022. [Online]. Available: https://fantom.foundation/
[69] S. Popov, ``The tangle," cit. on, p. 131, 2016.
[70] B. Kusmierz, ``The first glance at the simulation of the tangle: Discrete model," IOTA, Tech. Rep., 2017.
[71] B. Kusmierz, P. Staupe, and A. Gal, ``Extracting tangle properties in continuous time via large-scale simulations," Tech. Rep., 2018.
[72] A. Cullen, P. Ferraro, C. King, and R. Shorten, ``Distributed ledger technology for iot: Parasite chain attacks," 2019, arXiv:1904.00996. [Online]. Available: https://arxiv.org/abs/1904.00996

[73] L. Baird, M. Harmon, and P. Madsen, ``Hedera: A governing council & public hashgraph network," Trust layer Internet, Whitepaper, vol. 1, 2018.
[74] T. Rocket, ``Snow_ake to avalanche: A novel metastable consensus protocol family for cryptocurrencies," IPFS, Tech. Rep., 2018.
Complaints About IOTA. Accessed: Jan. 22, 2022. [Online]. Available: https://juejin.im/post/5c6e0f0bf265da2de66103dd
[75] Double-Spending. Accessed: Jan. 22, 2022. [Online].
Available: https://en.wikipedia.org/wiki/Double-spending
[76] Lightning Labs. Accessed: Sep. 1, 2019. [Online].
Available: https://lightning.engineering/
[77] Bitmex-The Lightning Network. Accessed: Sep. 12, 2020. [Online]. Available: https://blog.bitmex.com/the-lightning-network/
[78] Erc20 Token Standard. Accessed: Sep. 12, 2020.
[Online]. Available: https://theethereum.wiki/w/index.php/ERC20_Token_Standard
[79] Lightning Network Daemon. Accessed: Sep. 12, 2020. [Online]. Available: https://github.com/lightningnetwork/lnd
[80] C-Lightning_A Lightning Network Implementation in C. Accessed: Sep. 12, 2020. [Online]. Available: https://github.com/ElementsProject/lightning
[81] A Scala Implementation of the Lightning Network. Accessed: Sep. 1, 2020. [Online]. Available: https://github.com/ACINQ/eclair
[82] G. Malavolta, P. Moreno-Sanchez, C. Schneidewind, A. Kate, and M. Maffei, ``Anonymous multi-hop locks for blockchain scalability and interoperability," in Proc. Netw. Distrib. Syst. Secur. Symp., 2019.
[83] Simplified Payment Veri_cation. Accessed: Sep. 1, 2020. [Online]. Available: https://en.bitcoinwiki.org/wiki/Simpli_ed_Payment_Veri_cation
[84] Minimal Viable Plasma. Accessed: Sep. 1, 2020. [Online]. Available: https://ethresear.ch/t/minimal-viable-plasma/426
[85] Minimal Viable Plasma. Accessed: Sep. 1, 2019. [Online]. Available: https://ethresear.ch/t/plasma-cash plasma-with-much-less-per-userdata-checking/1298
[86] Sparse Merkle Trees. Accessed: Sep. 1, 2020. [Online]. Available: https://ethresear.ch/t/optimizing-sparse-merkle-trees/3751
[87] Plasma Debit: Arbitrary-Denomination Payments in Plasma Cash. Accessed: Sep. 1, 2019. [Online]. Available: https://ethresear.ch/t/plasmadebit-arbitrary-denomination-payments-in-plasma-cash/2198
[88] R. Khalil and A. Gervais, ``NOCUST_a non-custodial 2nd-layer _nancial intermediary," Cryptology ePrint Archive, Report 2018/642, 2018. [Online]. Available: https://eprint.iacr.org/2018/642
[89] Tendermint. Accessed: Sep. 1, 2020. [Online]. Available: https://tendermint.com/
[90] E. Politou, F. Casino, E. Alepis, and C. Patsakis, ``Blockchain mutability: Challenges and proposed solutions," 2019, arXiv:1907.07099. [Online]. Available: https://arxiv.org/abs/1907.07099
[91] M. Florian, S. Henningsen, S. Beaucamp, and B. Scheuermann, ``Erasing data from blockchain nodes," in Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW), Jun. 2019, pp. 367_376.
[92] Ethereum Chain Pruning for Long Term 1.0 Scalability and Viability. Accessed: Sep. 12, 2020. [Online]. Available:https://ethereum-magicians.org/t/ethereum-chain-pruning-for-long-term-1-0-scalability-and-viability/2074
[93] P. Maymounkov and D. Mazieres, ``Kademlia: A peer-to-peer information system based on theXOR metric," in Proc. Int.Workshop Peer-to-Peer Syst. Cambridge, MA, USA: Springer, 2002, pp. 53_65.
[94] Peck, M. E. Adam Back says the Bitcoin fork is a coup, http://spectrum.ieee.org/tech-talk/computing/networks/the-bitcoin-for-is-a-coup, Aug 2015
[95] S. Ben Mariem, P. Casas, and B. Donnet. Vivisecting blockchain P2P networks: Unveiling the Bitcoin IP network. In ACM CoNEXT Student Workshop, 2018.
[96] G. Fanti, S. B. Venkatakrishnan, S. Bakshi, B. Denby, S. Bhargava, A. Miller, and P. Viswanath. Dandelion++: Lightweight cryptocurrency networking with formal anonymity guarantees. In 2018 ACM International Conference on Measurement and Modeling of Computer Systems – SIGMETRICS'18, 2018.
[97] G. Naumenko, G. Maxwell, P. Wuille, A. Fedorova, and I. Beschastnikh. Erlay: Efficient transaction relay for bitcoin. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pages 817–831, London, UK, 2019.
[98] Scherer, M. (2017). Performance and scalability of blockchain networks and smart contracts.
[99] Klarman, U., Basu, S., Kuzmanovic, A., & Sirer, E. G. (2018). bloxroute: A scalable trustless blockchain distribution network whitepaper. IEEE Internet Things J.
[100] Chawla, N., Behrens, H. W., Tapp, D., Boscovic, D., & Candan, K. S. (2019). Velocity: Scalability improvements in block propagation through rateless erasure coding. In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 447-454). IEEE. https://doi.org/10.1109/BLOC.2019.8751427

[101] Rohrer, E. & Tschorsch, F. (2019). Kadcast: A structured approach to broadcast in blockchain networks. In Proceedings of the 1st ACM Conference on Advances in Financial Technologies (pp. 199-213). https://doi.org/10.1145/3318041.3355469

[102] Naumenko, G., Maxwell, G., Wuille, P., Fedorova, A., & Beschastnikh, I. (2019). Erlay: Efficient Transaction Relay for Bitcoin. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (pp. 817-831). https://doi.org/10.1145/3319535.3354237

[103] Lombrozo, E., Lau, J., & Wuille, P. (2015). Segregated witness (consensus layer). Bitcoin Core Develop. Team, Tech. Rep. BIP, 141.

[104] Xu, Z., Han, S., & Chen, L. (2018). Cub, a consensus unit-based storage scheme for blockchain system. In 2018 IEEE 34th International Conference on Data Engineering (ICDE) (pp. 173-184). IEEE. https://doi.org/10.1109/ICDE.2018.00025

[105] Dai, X., Xiao, J., Yang, W., Wang, C., & Jin, H. (2019, July). Jidar: A jigsaw-like data reduction approach without trust assumptions for bitcoin system. In 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS) (pp. 1317-1326). IEEE. https://doi.org/10.1109/ICDCS.2019.00132

[106] Dang, H., Dinh, T. T. A., Loghin, D., Chang, E. C., Lin, Q., & Ooi, B. C. (2019, June). Towards scaling blockchain systems via sharding. In Proceedings of the 2019 International Conference on Management of Data (pp. 123-140). https://doi.org/10.1145/3299869.3319889

[107] Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016, October). A secure sharding protocol for open blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 17-30). https://doi.org/10.1145/2976749.2978389

[108] Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., & Ford, B. (2018, May). Omniledger: A secure, scale-out, decentralized ledger via sharding. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 583-598). IEEE. https://doi.org/10.1109/SP.2018.000-5

[109] Zamani, M., Movahedi, M., & Raykova, M. (2018, January). Rapidchain: Scaling blockchain via full sharding. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 931-948).