May 2017

Scalability Analysis of Blockchains Through Blockchain Simulation

Sneha Goswami
University of Nevada, Las Vegas, snehagoswami1992@gmail.com

SCALABILITY ANALYSIS OF BLOCKCHAINS THROUGH BLOCKCHAIN SIMULATION

By

Sneha Goswami

Bachelor of Technology-Computer Science
St.Thomas' College
of Engineering and Techology
2010

A thesis submitted in partial fulfillment
of the requirements for the

Master of Science in Computer Science

Department of Computer Science
Howard R. Hughes College of Engineering
The Graduate College

University of Nevada, Las Vegas
May 2017

UNLV | GRADUATE COLLEGE

Thesis Approval

The Graduate College
The University of Nevada, Las Vegas

March 17, 2017

This thesis prepared by

Sneha Goswami

entitled

Scalability Analysis of Blockchains Through Blockchain Simulation

is approved in partial fulfillment of the requirements for the degree of

Master of Science in Computer Science
Department of Computer Science

Yoohwan Kim, Ph.D.
Examination Committee Chair

Kathryn Hausbeck Korgan, Ph.D.
Graduate College Interim Dean

Ajoy K. Datta, Ph.D.
Examination Committee Member

Ju-Yeon Jo, Ph.D.
Examination Committee Member

V. Muthukumar, Ph.D.
Graduate College Faculty Representative

ABSTRACT

SCALABILITY ANALYSIS OF BLOCKCHAINS THROUGH BLOCKCHAIN SIMULATION

By

Sneha Goswami

Dr. Yoohwan Kim, Examination Committee Chair

Associate Professor, Department of Computer Science

University of Nevada, Las Vegas

The past decade has witnessed a surge of cryptocurrencies such as bitcoins, litecoin, dogecoin, peercoin, bitcoin being the most popular amongst them. Enthusiasts and skeptics have debated and come up with disparate opinions to contest both the success and failures of such currencies. However, the veracity of such opinions can only be derived after true analysis of the technological breakthroughs that have occurred in this domain. Blockchains being the backbone of such currencies is a broad subject that encompasses economics, law, cryptography and software engineering. Most of these technologies are decentralized and are open source algorithms. Blockchains popularity is largely based on its tremendous potential of carrying huge amount of data securely over a peer to peer network. This feature of blockchains has leveraged its value in the market for many companies who want to use blockchains for enterprise goals and profit making. For a more comprehensive understanding of blockchains and how the block generation algorithm works , how transactions are included in a block we must understand the genesis of the blockchain technology, what exactly it represents and its relevance to the real world**.** Despite its advantages, blockchains still remain a novel technology and their remains areas of concerns that can be bettered for attaining ideal efficiency. This research delves into the scalability issue of blockchains and provides a comparative analysis of several blockchain parameters with real time data . It delves into the factors that make block chains largely non-scalable. This is done by the simulation of blockchain. It then addresses the various mechanisms that can be employed to resolve this limitation through measuring the differences between the simulator and real time scenarios.

ACKNOWLEDGEMENTS

I would like to thank Dr. Yoohwan Kim, my research advisor for all the support and guidance he has offered me during the course of my graduate studies at University of Nevada, Las Vegas. His encouragement and valuable suggestions have helped me immensely in moving in the right direction for this thesis. He has helped me by providing all required resources for useful research with good hands on experience.

I would also like to thank Dr. Ajoy K. Datta, Dr. Ju-Yeon Jo and Dr. Venkatesan Muthukumar for serving my committee and reviewing my thesis. The research work I did behind this thesis has been a challenging experience to me and was accomplished through help of many people. I would like to heartily thank my parents Anilabha Goswami and Susmita Goswami who have given me the motivation to learn and the opportunitie to grow, my director Gautam Banerjea for his guidance and enthusiasm to always motivate me in the right direction and my grandmother Ms. Rekha Bhattachharya for her unconditional love and support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

CRYPTOCURRENCIES

Digital currencies have gained a lot of popularity over recent years. Cryptography is the science of communicating securely in the presence of an adversary who can listen in and even control the communication channel [1]. The underlying protocol behind these digital currencies is blockchain which forms the back bone of such cryptocurrencies. This chapter explores in detail the types of cryptocurrencies, by elucidating on the most popular digital currencies in recent time and era. It also explains in brief about the algorithms behind these protocols and presents a comparative analysis on these digital currencies. In order to understand blockchain from its inception to its popularity, we must understand what cryptocurrencies are and how blockchain plays an important role in their working.

1.1 Bitcoin

Bitcoin, the most popular digital cryptocurrency, was originally created by Satoshi Nakamoto. The Bitcoin paper was published in 2008 and the Bitcoin source code was released in early 2009. The mining on Bitcoin started as early as January 3, 2009. Currently Bitcoin occupies the largest market share among all other digital currencies.

Bitcoin is a cryptocurrency. The motto behind the development of any encryption algorithm is to make it difficult to break. Kerchoff's principle in cryptography provides a mechanism to achieve this. It recommends cryptographers to make the encryption algorithm public and the encryption key secret [2][17][58].

- *The Bitcoin Protocol*: The Bitcoin protocol uses digital signatures which is an application of public key cryptography. Digital signatures, like any normal form of signatures are utilized to validate the source and the integrity of the message generated. It also ensures non-repudiation that is the ability to ensure that the party who has signed the message is not able to deny the authenticity of their signature on the document they originated.

Bitcoin addresses are essentially public keys and there is a private key associated to each bitcoin address. These private keys are utilized to unlock the public keys. To make a transaction using the bitcoins in an address, that transaction must be signed or authorized using the private key associated to that address [1][3][4]. Public key cryptography ensures secure binding of digital signatures. In order to verify the source of a document, the receiver just needs to provide the public key, the document and the signature associated to that document.

- *Cryptography Algorithm in Bitcoins*: Bitcoin uses elliptic curve cryptography. A cryptographic eliptic curve can be seen as an extremely large succession of points. The generator which is a known point, marks the beginning of the eliptic curve protocol [5][7][12][45][58]. What makes this algorithm simple to use and difficult to break is the underlying computational complexity. It is extremely easy and fast to compute the public key for the protocol given a private key. This is done using a double and multiply algorithm. However, it is extremely difficult to compute the private key given the public key. This problem is a typical example of a discrete logarithmic problem [1][2][6][10][24]. The typical brute force method can be employed to solve this problem but in reality this might take several years making this solution computationally infeasible.

  Prior to using an elliptic curve algorithm, the parameters for the eliptic curve must be set. These parameters include the coefficients of the curve a and b, the order of the prime field p and the generator A which indicates the starting point of the curve. Several parameters based on the security level are available to help decide and set the arguments for this protocol. Satoshi chose the parameters of the standard secp256k1 for Bitcoin [3][4][7][8][11][13][17][21][27][58].

  The elliptic curve digital signature algorithm ECDSA which is the combination of the elliptic curve protocol and the DSA algorithm is the actual signature schema that is implemented in Bitcoins.

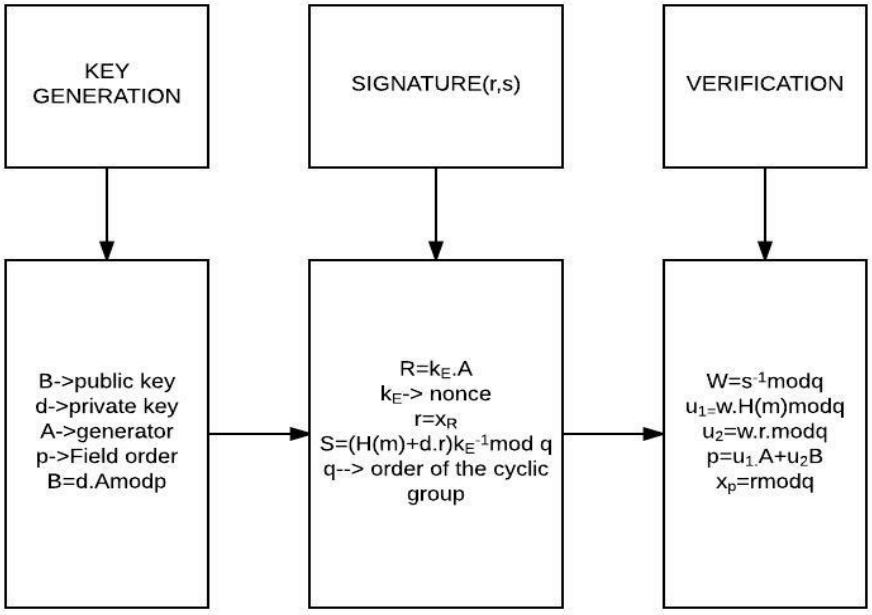

Figure 1: Elliptic Curve Digital Signature Algorithm Process [58]

As given in Figure 1, the ECDSA algorithm is divided into three sections:

a) As is evident from the figure, the public key B is computed from the private key d using the formulae B= d.A mod p where A is the generator.

b) To sign a message:

- A random number k_E is generated.
- k_E is used only once. It is typically called a nonce.
- Signature consists of the pair of two integers (r,s).
- The first number in the signature r is computed as the first coordinate of the point in the elliptic curve $R=k_E.A$.
- s is computed as $s=((H(m)+d.r)/k_E) \bmod q$.

c) The verification consists of a few steps and has been elucidated below:

- $w= s^{-1} \bmod q$ (Equation 1)
- $u1=w.H(m) \bmod q$ (Equation2)

- $u2=w.r \bmod q$ (Equation3)
- $(xp,yp)=u^1.A+u^2.B$ (Equation4)
- $Xp=r \bmod q$ (Equation5)

Further, Bitcoin utilizes OpenSSL for elliptic public key cryptography. OpenSSL is used to represent the points in elliptic curve using 65 bytes [1][2][3][14][15][20][26]. Further, hashing is done on the coordinates obtained using SHA256 and RIPEMD160. The second hashing is chosen to reduce the size of the transactions and to reduce the chances of collisions. The final step involves encoding with Base58. Base58 is basically an encoding algorithm that is involved in the translation of binary data to text format.

1.2 Litecoin

Litecoin was released in 2011. When it was written, it depicted a market capitalization of nearly 5 per cent.

Litecoin uses scrypt which is a memory hard key derivative function. The seminal idea behind scrypt is that it generates a huge chunk of pseudorandom numbers that it stores in the RAM. The reason behind storing these numbers in the RAM is access on demand that is these numbers can be accessed faster at a low computational cost. Also, the block generation in litecoin using scrypt is targeted at a mere 2.5 minutes which makes it computationally faster to include blocks in the transactions. A lower block generation time would essentially lower the mining difficulty at a constant network hash rate [22][25][28][37][40][45].

Litecoin mining in ASICs has been made possible with the parametrization of scrypt. The disadvantage is that Litecoin suffers by a factor of atleast 10 compared to Bitcoin as far as the ASIC implementation is concerned [32][41][43][58]. Scrypt has also not been scrutinized like other cryptographic algorithms such as SHA26 which makes it a bit risky to be used in real time scenarios as they may be more vulnerable to attacks.

1.3 Peercoin

Peercoin was introduce d in 2012.Peercoin uses hybrid proof of stake/proof of work system. In a proof of stake system new blocks are minted by coin holders in proportion to the amount of coins they control. In

the proof of work system blocks are generated analogous to the bitcoin system [31][32][33][43][54][57]. Block reward typically halves every time the difficulty level increases. Peercoin operates as given in the following stages:

- A transaction named coinstake is created.
- Coinstake spends the funds in the transaction output.
- Coinstake destroys the coin age.
- Hash of the header is computed.
- The header contains the transaction and the time.
- The hash generated is then checked against the proof of work requirement
- If the hash matches, the user in control is able to mint a new hash block.

1.4 Dogecoin

Dogecoin was introduced in 2013 by programmer Billy Markus who belonged to Portland, Oregon (Wikipedia).Dogecoin was introduced by forking litecoin. Dogecoin has a block generation time of 1 minute. Like litecoin, dogecoin also utilizes scrypt, a memory hard key derivative function [28][29][33][34][37][43][53]. Around 98 billion dogecoins were initially frontloaded for circulation, with a fixed increase of 5.2 billion dogecoins each year. According to Pedro Franco, as justified in his book , " Understanding Bitcoin – Cryptography, Engineering and Economics" , dogecoin can have huge applications in the future due to the inflationary nature of dogecoin (the rate of inflation for dogecoin decreases over time). Also since the supply of dogecoins is huge, it has gained accolade in the Internet tipping system. Dogecoins has found applications and uses in several fields. Some of them have been enlisted below:

- Dogecoin has gained accolade in Internet tipping system
- It has been used in several exchanges such as Mengmengbi, Bter and BTC38(Wikipedia)
- Physical goods and items can be traded with the use of Dogecoin in many online communities.

- Several ATMs supporting dogecoins are coming up in recent years to maintain the supply and demand of dogecoin.
- It has also been used in the past in the real estate business to buy or sell properties.

1.5 Comparitive Analysis

The table given below elucidates different metrics or properties that are inherent to all cryptocurrencies and presents a comparative analysis of some digital currencies like bitcoin, litecoin, Dogecoin and peercoin [35][44][47][58].

Properties	***Bitcoin***	***Litecoin***	***Dogecoin***	***Peercoin***
Release year	2008	2011	2013	2012
Block Generation Time	9.7 minutes	2.5 minutes	1 minute	10 minutes
Ha sh Rate	899.624 Thash/s	1.307 Thash/s	1.4 Thash/s	693.098 Thash/s
Cryptographic Algorithm	ECDSA	Scrypt	Scrypt	Hybrid
Mining Difficulty	High (Around 165,496,835,118)	Low 55,067	Low 21,462	Moderate(476,560,083)
Reward per Block	25 BTC	25 LTC	10,000 Doge	67.12 PPC
Power Consumption	Very high	Moderate	Low	Low
Total money in circulation	15,366,077 BTC	45,157,139 LTC	103,678,515,952 DOGE	23,076,620 PPC
Price	1 BTC = $ 415.92 USD	1 LTC = $ 3.25 USD	1 DOGE = $0.00023 USD	1 PPC = $ 0.45 USD

Table 1: Comparison of Different Metrics Associated with Digital Currencies

1.6 Vulnerability Attacks

A. **Packet Sniffing**- Digital cryptocurrency systems might be exposed to attackers who are just passively observing the transactions to and from the system [46][47][49]. The attacker might just monitor the Internet traffic and sniff the packets that the user generates. The attacker may make use of a packet analyzer to intercept the traffic and the packets transferred between the two parties.

B. **Sybil attack**- An attacker might be in control of the clients in a network. This situation would lead to a network that is only connected to attacker nodes [bitcoin wiki]. The attacker might exploit this sytstem composition for his own gain. He might refuse some transactions and allow others. He

might also make the users on the system vulnerable to double-spending by relaying only certain blocks or self created blocks [55][56][59].

C. **Timejacking**- An attacker might slow or speed up a network if he gains control over the network's time counter. He can use this to manipulate a node's timestamp and record inaccurate timestamps. By doing this he might be able to gain control over the system's mining resources and exploit it accordingly for both active and passive attacks

Timejacking can be used for the following purposes:

- *"Poison-pill" block*- The attacker might relay a novel block that is ahead of the real time. This will lead to a block that is rejected by the target node but accepted by the miners. The target node will reject the new relayed block as its timestamp would be greater than its own slowed-down network time[51][52][53][54]. The miners will keep on mining invalid blocks that will be continuously rejected by the target node and would eventually affect intervening operations and transactions.
- *Double-Spending*- The attacker might keep on generating poison blocks and feed it into the target along with confirmations in the invalid chain. These confirmations will be declined by the global chain once the network stabilizes [33][34][39][41]. However, during the period of the attack, the target will be flooded with such confirmations without the intervention of honest nodes. Succeeding the flooding of such confirmations, if the number of confirmation exceeds the threshold number set to verify a transaction, the invalid transaction will be confirmed and will lead to double spending.
- *Increasing attack window*- Modifying timestamps of nodes can be manipulated to increase transaction system.
- *Miners*- If the target of the attack are miners, timejacking will effectively reduce the mining power of the miners as more and more miners mine invalid blocks and add it to the

blockchain. This would eventually cause a network split and increase the network latency[42][43][44][45].

D. **Denial of Service**- Spamming a node with excess data may disable a node from making progress. It might reduce its ability or even stop it from processing cryptocurrency transactions.

E. **Energy consumption**- Cost of mining is severely dependent upon electricity price. Most mining techniques does not reduce energy consumption[17][19][23][25][27]. It just increases the network difficulty. This is one of the main bottlenecks of the bitcoin network. Cryptocurrencies such as peer coin has attempted to improve the energy consumption by employing alternative proof of work systems.

F. **Malicious client code** - The clients in any cryptocurrency community should follow the rules and regulations as imposed by the system [16][18]. Any aberration might lead to other clients adopting the same and eventual propagation of erroneous or malicious code. This will result in much reduced levels of safety for the traders and merchants making transactions in the network.

G. **Hash rate**- The chances of winning are largely dependent at the rate at which blocks are hashed. Starting with identical blocks, and nonce being incremented simultaneously would result in the fastest machine bagging the opportunity to win. In such a case, randomness needs to be ensured to provide each chain an equal chance of winning [32][33][35].

H. **False chaining**- An attacker can mine a block chain with much reduced level of complexity. This would lead to a false segmentation of the network and would make it impossible to combine the two networks. The network would automatically detect the false chain and would abort the legitimate transaction [40][42][43][49][50][53].

I. **Reduced block size**- The size of a bitcoin block is 1 MB and blocks larger than the size mentioned are considered invalid. This poses serious problems for the scalability of the bitcoin network. If block size is increased the rate of transactions made will rise and the currency can be extended to Mastercoins. Although the blocksize limit for dogecoin is the same as that of bitcoin, it is much faster than that of bitcoin as the number of coins for dogecoin is much higher.

J. **Tracing coin histories**- Coin histories in several cryptocurrencies can be traced back in order to align the transaction with the transactor. Addresses can be used to identify the source of the transaction and this information can then be utilized for malicious purposes.

K. **Hash Collision**- For several cryptocurrencies, generation of addresses involve hashing. Since hashing is done, there also arises the problem of collision. Collisions are less likely with addresses of greater range and key of larger sizes.

L. **Botnet**- Botnet is typically defined as a nexus of infected hosts under the command of a common master, called the BotMaster. Botnets poses severe threat to cyber security. Its presence is ever-growing. It can be exploited to attack the bitcoin network and propagate Distributed Denial of Service attacks, phishing, spamming and click fraud.

CHAPTER 2

BLOCKCHAINS AND RELATED TERMINOLOGIES

2.1 Introduction

There has been a lot of hype concerning blockchains as it forms the backbone of every modern cryptocurrency that exists such as bitcoin, litecoin, dodgecoin etc. In order for a more comprehensive understanding of blockchains and how the block generation algorithm works , how transactions are included in a block we must understand the genesis of the blockchain technology, what exactly it represents and its relevance to the real world [35][37]**.** Despite its advantages, blockchains still remain a novel technology and their remains areas of concerns that can be bettered for attaining ideal efficiency. This research delves into the scalability issue of blockchains and provides a comparative analysis of several blockchain parameters such as mining time, block generation time with real time data representing why block chains are largely non-scalable [45][46][51][52].

Given the incessant adoption and the increase of cryptocurrency transactions due to its use in digital transfer, smart contracts, cheap remittance, it is inevitable that the succeeding years would witness a splurge of transactions which would necessitate the use of bitcoin like blockchain protocols . For such a digital system to work, correct operation of these systems should be ensured and subsequently maintained [56][57][59]. These cryptocurrency systems hence implement a number of measures for correct operation and distribution of the digital currency. It should also be ensured that the adversaries and the perpetrators do not misuse loopholes in the devised system for malicious purposes.

The fundamental deficiencies and bottlenecks in the Bitcoin network prevent higher throughput and lower network latencies. Scalability is not a well-defined term or a singular attribute of the blockchain system. It involves different metrics or can be called as a cumulation of several metrics. It is hence imperative to quantify the scalability of the current bitcoin system, assess its limits and therefore address the open challenges existing in the current model. The goal is to have a better understanding of the bitcoin scalability

bottlenecks such that paving way for the innovation and understanding of other scalable protocols becomes lucid in the future. It is also seminal to understand the limit to which parameters can be pushed without compromising security and other factors inorder to achieve larger scalability and efficiency.

2.2 Previous Work

There have been several research papers in the area of cryptocurrencies and blockchains. Some of the most recent and popular works in this domain involve those of Pedro Franco, Till Neudecker. Malte Moser, Rainer Bohme, Dominic Breuker. The aforementioned individuals have done exceptional work in performing in depth analysis of Laundering Tools in the Bitcoin system. Florian Tschorsch and Bjorn Scheuermann in their paper "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies" have explored several terminologies in the bitcoin domain that have baffled experts and have provided a systematic approach to coin and define these terms.

Ittay Eyal, Adem Efe Gencer, Emin Gun Sirer, Robert Van Resse from the Cornell University in their paper published in 2015 developed a new Bitcoin protocol called Bitcoin-NG that addresses the scalability issue in blockchains. They devised a blockchain protocol that could scale better and showed better fault tolerance and robustness. In addition to this, other simulation models have been developed such as those based on Décor and Hop to simulate the Blockchain protocol employed in Bitcoins. All of these novel models aim to improvise and address the current issues associated with blockchains and are based on the same trust model as that of bitcoins. Many others such as Rhett Creighton have incorporated Big Data into this cryptographic system to propose higher ingestion of transactions into the blockchain inorder to address the current performance issues in current Blockchain systems by achieving higher efficiency and throughput.

Other factors apart from efficiency and throughput that form the baseline of the debate whether bitcoin transactions through blockchains would be scalable keeping in mind the ever increasing popularity of this technology are bandwidth and network delay. These have been explored in detail by Yonatan Sompolinsky

and Aviv Zohar. They further proposed a slightly modified Bitcoin system that shows increased speedup, lower block generation time and considerably less network propagation delay.

Apart from this several other methodologies exists such as transaction splitting that exploits blockchain state to propose a scalable mechanism in a larger validator pool. Such a technique has been put forward by Matthew Wamper Doty and John Cohn of IBM. They in their work have come up with solutions that evidently achieves arbitrary scaling for a particular transactional load.

2.3 Terminologies

Let us look at the some of the most important terms for a better understanding of the subject.

A. **Blockchain**- A public ledger, in other words a blockchain is a database of all Bitcoin transactions that have ever been executed. It is a constantly growing database and has in it all completed or mined blocks. It is ever increasing as blocks are mined every day and are added to this universal ledger in a linear, chronological order [38][56][57].

B. **Transactions**- Inorder to understand how the block generation algorithm works and how transactions are included in a block we must understand the genesis of a transaction, what exactly it represents and its relevance to the real world**.** A transaction is probably the most important component in a bitcoin system**.** It refers to an exchange between two users without the interference of a third intermediary. It can be visualized as a data structure that creates a message (encodes) initiating a transfer of value (an amount signifying the number of bitcoins) between members taking part in the bitcoin system [33][36][37][39][56][58].

   Each transaction is recorded in the bitcoin's block chain. In other words, a transaction can be seen as a public entry in the global ledger (the universal database of all bitcoin transactions) referred

to as the block chain.

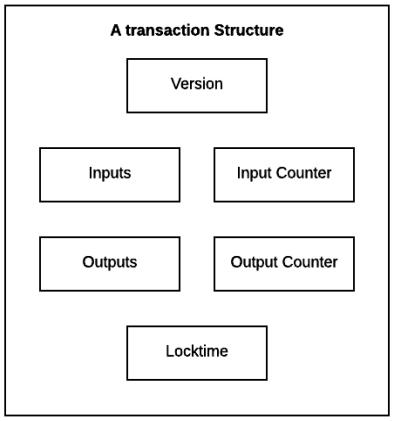

Figure 2: Structure of a transaction [58]

C. **Transaction Fee-** The priority of a transaction to be included in a block depends on a number of factors, transaction fee being one of the most important incentive for a miner to include a particular transaction into the next block [24][26][27][31][47]. It is a fee that is associated with each transaction. Transaction fees depend upon the size of the transaction and not on the transaction amount (unspent UTXO). Transaction fee may be influenced by market forces, network capacity and transaction volume

D. **Block-** A block can be visualized as a data structure that assimilates transactions to be put into the blockchain. Average block contains more than 500 transactions. A block in the blockchain contains a summary of all the aggregated transactions in the form of a merkle tree. A merkle tree is a binary hash tree that can be used to trace back to individual transactions. The algorithm used for constructing a merkle tree is double SHA-256 [55][57].

Let, number of transactions = N, Complexity of one transaction to be included in the merkle tree can be checked in 2* log2(N) calculations.

Let us consider a transaction A,

Then, H(A)=SHA256(SHA256(Transaction A)), H(AB)= SHA256(SHA256(H(A)+H(B))

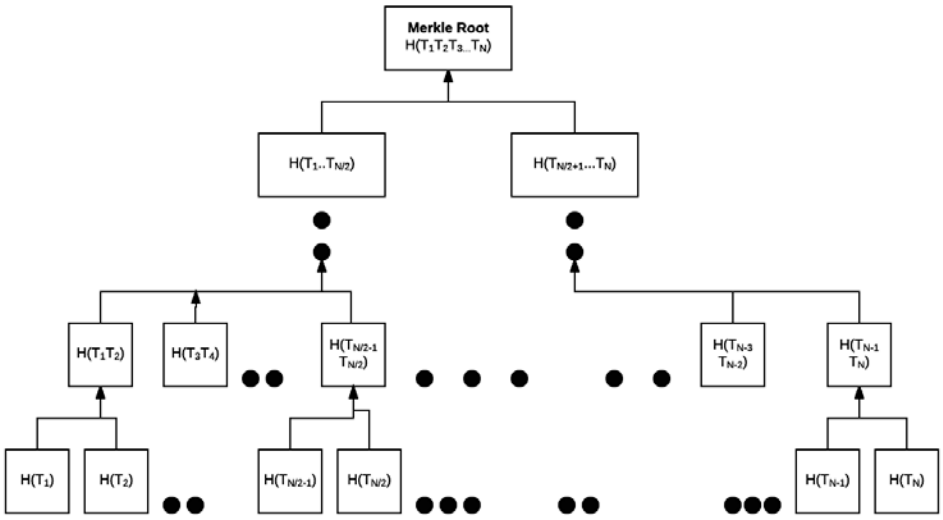

Figure 3: Merkle Tree Depicting Transactions

Transactions is contained in the body of a block. These are indirectly hashed. The Merkle root is responsible for hashing these transactions. Block hashing of 1 transaction takes equivalent effort as that with 10,000 transactions.

E. **Miners**- Miners are largely responsible for blockchain securing. They create or hash blocks that are added to the blockchain. A miner who has been successful at appending a particular block to the block chain is granted a block reward [1][16][26][37].

F. **Mining time**- Mining time is the time taken by a miner to append a block or successfully confirming that a block has been appended to the blockchain. This block contains a number of transactions. In other words, it can be defined as adding the record of transactions to the blockchain and the verification that the block has been added by other miners (proof of work).

G. **Block generation time**- Block generation time is the time taken to include transactions in a block. Bitcoin's proof of work has an average block generation time of 10 minutes whereas for litecoin it has a target of 2.5 minutes [24][37][38][47].

H. **Transaction pool**- Transaction pool is the universal pool containing all transactions. These transactions are made available to the miners for block generation and subsequent mining.

I. **Average mining time**- Average mining time for name coins differ with respect to which cryptocurrency is being used. For Bitcoins the average mining time for confirming a block in the blockchain is 10 minutes, for litecoin it is 2.5 minutes. It has been discussed in detail in further chapters [22][54].

J. **Block size-** Block size is the reserved space in each block that is used to store transactions that have been confirmed in the block. Block size may vary depending upon the number of transactions that has been fed into it. Generally, there is a limit of 1MB[32] on the block size, that is block size cannot be greater than the prescribed limit computed in the bitcoin core.

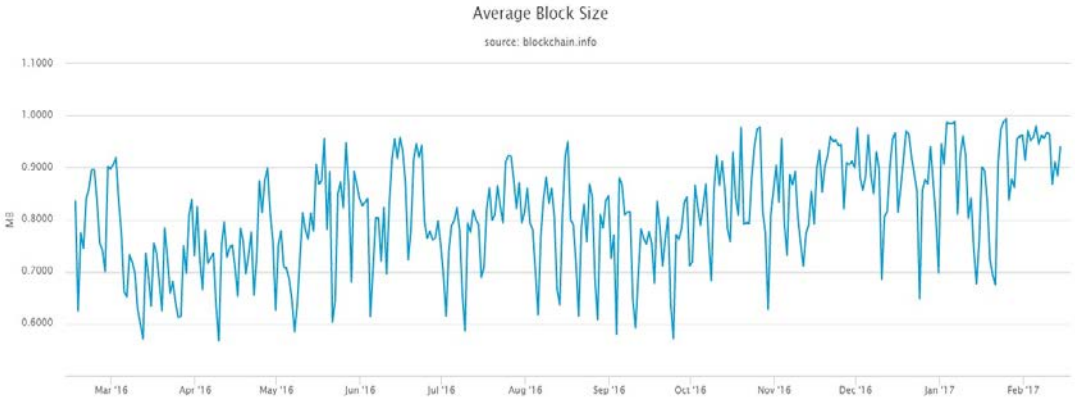

Figure 4: Chart Showing Average Block Size in MB over a period of 1 year [55]

K. Confirmation- When a transaction is verified by the peer to peer network that is the proof of work system employed in bitcoin's blockchain, the block is appended to the blockchain and the transaction is said to be confirmed. Once it is confirmed, a double spending cannot occur and any reversing of the transaction is not plausible [3][4][19].

L. Cryptocurrency- It is a digital currency in which techniques of encryption are utilized to generate units and regulate its generation. There is no centralized authority that governs the use and

distribution of cryptocurrencies. Cryptocurrencies are mostly decentralized and several security measures are used for its handling and transfer [23][29].

M. **Difficulty-** It is the hardness or the complexity that is involved in solving a block to be included in the blockchain.

N. **Genesis block-** It is defined as the very first block in the distributed ledger.

O. **Hashrate-** Miners perform hashes. It is the number of hashes that a miner can mine per second.

P. **Peer to Peer Network-** A network in which participants engage directly over decentralized interactions [34][39][41].

Q. **Proof of Stake-** Minting of blocks take place and computational power is zero in block minting. It is environmental friendly and faster.

R. **Proof of Work-** It depends on the mining ability of the miner and is easier for others in the peer to peer network to verify. High computational power is involved in such a system.

CHAPTER 3

THE SCALABILITY ISSUE

3.1 Introduction

Being widely deployed, Bitcoin based blockchain protocols are gaining momentum in the present age and era due to its decentralized nature and its huge capacity. Its popularity in finance, technical sectors and academics is rooted in its potential to transfer and delegate without a central governing body in presence of high security. The current Blockchain system offers a highly fault-tolerant system for transactions. Researchers, enthusiasts debate on the extension of this infrastructure for the enforcement of smart contracts, maintenance of anonymity for transactions paving way for a new generation in the era of Internet. Bitcoin approximately takes around 10 minutes to confirm a transaction and has an effective throughput of 7 transactions per second [4][6][52]. Today's modern transaction processor like Visa processes around 2000 transactions per second. Clearly, the gap in efficiency and throughput puts forward a dilemma for enthusiasts who debate on the potential of Blockchain based technology. In such a scenario, the need to scale blockchains becomes an issue of concern to exploit the full potential of blockchain. This chapter provides a design blueprint by analyzing the factors that make blockchains largely unscalable and then proposing mechanisms that have been identified to resolve these bottlenecks.

3.2 Scalability Bottlenecks

Before defining and elucidating on the bottleneck factors affecting scalability, let us try to understand that scalability is not a singular term. It is a cohesion of several parameters and several metrics. It is difficult to relate one factor to the huge array of factors that might affect performance and scalability cohesively. Let us now analyze the several metrics involved in measuring scalability.

3.2.1 Block Size- Currently in the Bitcoin Blockchain protocol, the block size is fixated to a maximum of 1MB. The Visa payment processor reaches a peak of around 48000 transactions per second. In order for the Bitcoin – Blockchain protocol to match up to that of the modern payment processing

systems, several bottlenecks such as the limited block size of Blockchain needs to be addressed. The simplest way to achieve this is by increasing the block cap on bitcoin block size. In order to match up to the current payment processors , researchers predict a block size of around 8 GB as opposed to the 1MB block size fixated. This would entail data of around 400 terabytes.

Let us see, how increasing the block-size would affect the scalability metrics in the Bitcoin based Blockchain protocol system [55][56].

1. *Throughput* – If the block size of the block is increased, the number of transactions processed per second would rise up. This would increase the throughput of the entire bitcoin based blockchain protocol system.
2. *Huge capacity*- Rendering the block size in the blockchain protocol will make way to transfer and handle huge amount of data. Researchers predict that an increase in blocksize to 8GB would pave way for handling around 400 terabytes of data.
3. *Lower transaction fees*- Increasing the block-size would also leave a huge space for more transactions to be included in the block. All Bitcoin competitors will be forced to lower their transaction fees [59].
4. *Increased scalability*- Increase in block size would dramatically increase the scalability of the Bitcoin based Blockchain network due to increased throughput and efficiency solely because of the increase in the number of transactions in the network.

Now, let us see the open challenges and the practical difficulties in increasing the block- size in the Bitcoin based Blockchain protocol system.

1. *Hard-forking*- Consensus is difficult to achieve.
2. *High power usage*- Increasing the block- size would requisite a huge amount of resources to handle the bulk amount of transactions and consequently mine them [43][47][49].

3. *Slower network propagation*- Increasing the block size would lead to heavier blocks being transmitted over the same network bandwidth as before. This would increase the network propagation time and lower speeds.
4. *High network Congestion*- An increase in the block size would lead to increase in congestion rates. Congestion eviction algorithms need to be then integrated with the system in order to handle the bulk traffic of transactions.
5. *Compromise on security*- Block size increase would lead to an effective compromise on the proof of work security associated with miners in the blockchain. Increasing the effective block size leads to an increase in the probability of the blocks being orphaned. Blocks with higher size are more likely to be orphaned. Apart from that the proof of work security employed by miners such as bandwidth cost, CPU validation cost also increases. With increased block size, huge transaction load, decreased transaction fee, the effective expenditure on security by miners will go down [41][51].
6. *Compromise on decentralization*- Increasing the block size would lead to a destabilization of the current decentralized system. Large block size would lead to increasing the cost associated with a full node. This would eventually lead to centralized parties having more power. Since Bitcoin is trustless, the larger the rate of hash that is controlled by a miner, more restricted and centralized it becomes.
7. *Sensitivity to demand*- With increase in block size, huge amount of transaction handling , the sensitivity to market forces for Bitcoin would likely increase. Price fluctuations with an increase or decrease in demand will be inevitable.

3.2.2 Block Interval - In order to make full utilization of the network bandwidth, to achieve higher throughput , greater efficiency, the block interval should be made as less as possible. Researchers have found out that the block interval for Bitcoin based Blockchain protocol should not be less than 12s. This would ensure faster propagation and low latency [2][17][29][34][44].

3.2.3 Network latency- It is defined as the time required to confirm a transaction. As stated earlier, the Bitcoin protocol takes an average confirmation time of 10 minutes for transaction confirmation. In order to achieve higher scalability, network latency should be low, that is the time taken for the protocol to confirm a transaction should be effectively decreased.

3.2.4 **Transaction Cost-** Transaction cost is the amount associated with bandwidth, storage and mining involved in the Bitcoin's blockchain network. The transaction fee plays a huge role in determining which transactions will be chosen and has a direct impact on the confirmation times affecting latency and other scalability metrics. Some transactions might starve, due to a mid range transaction fee while others might make progress. Hence, the cost associated with mining, bandwidth, energy consumption plays a direct role [32][33].

CHAPTER 4

BLOCKCHAIN REGULATIONS

4.1 Introduction

Even after introduction of Bitcoin based blockchain protocols in the popular realm, its operations did not undergo legal or regulatory scrutiny and serviced effectively outside the traditional monetary systems. However, Blockchain's popularity for all the wrong reasons, it bolstered the regulators to recognize and act upon the increasing popularity of a decentralized currency. Still regulators struggled to center on adequate legal structure and the inability to weigh the impediments laid before regulators in comprehending the risks and enormity of stakes compounded the difficulty of effectively tracking such transactions both internationally and domestically [1][6][30].

Blockchain raises legitimate regulatory and legal issues, concerning potential for facilitation to money laundering, affecting federal securities law and impacting the regulation of foreign exchange trading. The criminal anti-money laundering laws prohibits engagement of financial transaction that involve proceeds terrorist or felonious activities or that are functioned to finance such interests. Bank Secrecy Act (BSA) imposes various recordkeeping guidelines on banks and other financial institutions to deter and check these institutions from processing money laundering transactions. The Currency and Foreign Transaction Reporting Act, an ancillary law to the BSA, instructs financial institutions to file reports of cash transactions exceeding regulations amounts determined by the Secretary of the Treasury and file suspicious activity (SARs) over transaction breaching certain amount [54][55][58]

4.2 18 U.S.Code 1956

FinCEN guidance to money laundering jurisprudence hinges on Section a Clause 2 of 18 U.S.Code 1956 that states requirement of knowledge regarding illegal actions for determining offence. Thus dealers of Bitcoins can essentially repudiate any such knowledge of proceeds flowing consequent to their alleged illicit activities. Bitcoin's inherent pseudonymity makes it difficult to prove knowledge requirement. First,

the law enforcement needs to decipher the owner of the public key. Second, they would need to prove knowledge of Bitcoin usage to finance an unlawful activity. Such a process may seem difficult, as the law enforcement have to identify evidences of intent in reference to Bitcoin transfers.

Additionally, according to the law enforcements Bitcoin fails conveniently fit in the traditional definition of 'monetary instrument' as mentioned under Section c Clause 5 18 U.S.Code 1956. The difficulty of defining Bitcoin and establishing Bitcoin stakeholders has imposed legitimate concern to U.S lawmakers. On August 2013 the Federal regulators incorporated few approaches to define virtual currency. The regulators came to the conclusion that as virtual currency affects the security as understood in the federal securities laws, therefore, is deemed to be governed under federal regulations conditioned to specific facts and circumstance of the case. The Federal Bureau of Investigations maintains a default approach that virtual currency payment systems both decentralized and centralized extend an authorized and legal monetary remittance service. As FinCEN described that a decentralized virtual currency without any central repository and devoid of a single administrator makes Bitcoin a deficient legal tender stakeholder in most jurisdictions and an exchange medium deficient to attributes similar to real currencies [45][55].

4.3 Definition

There is a growing discrepancy over a carefully articulated definition of Bitcoin. Currently, in May 2013 Financial Crimes Enforcement Network (FinCEN) authored guidance memo defining virtual currency being a exchange medium operating like currencies in some environments, however do qualify or posses all attributes of a real currency.

It can be speculated how regulations on minors can deter them from being money transmitters in the interest of consumer protection or for the detering money laundering on a wider scale. However, there is difficulty in creating a consumer in protection from potential criminal intention to convert so-called dirty money into legal money. The FinCEN regulation's definition of the state of currency as being "real currency" and Bitcoin being called as "virtual Currency" creates a predicament of exchange medium being operative as

currency in few environments, however, there lays the shortcoming of Bitcoins failing to imbibe all attributes of a “real currency”. It lead an interpretation of virtual currency being a different kind and according to the current guidance it only extends as convertible virtual currency, defined either as value equivalent to real currency or otherwise substitute to real currency [34][45][55][57].

Definition of real currency got its recognition through rulemaking, whereas other substantive and relatively new concepts of virtual and convertible virtual currency obtained its existence from the guidance. Therefore, it resulted in the guidance probably seems as an overarching new law for Blockchain’s but in essence a vaguely similar interpretation of previous existing laws and rules. This calls for a new approach for definition and necessitates contemporary rulemaking for Bitcoins.

4.4 Policy Recommendations

Decentralized nature of structuring the Blockchain network makes it difficult to render essential impervious single point regulation system. Instead of endeavouring to monitor & control every aspect of Blockchain network, the effective method should be to analyse each Blockchain transaction individually. The potential problems can probably lead to some policy recommendations by the federal government such as a three-pronged approach, which may prove more effective implementation of Bitcoin regulation.

As Blockchain enjoys no conventional governmental safeguards as is afforded to long-established currencies. Therefore, to offer protection to Bitcoin consumers and for the purposes of bringing these virtual currencies within the umbrella of real currency regulatory structure the government should primarily promote cooperation between Blockchain exchangers and regulators. Alongside should deploy further resources to enforcement of non-compliant exchanges. And subsequently encourage institutionalization of Suspicious Activity Reports (SARs) to alert legal enforcement of probable illicit or criminal activity.

The regulators and government should work together for sustained growth of regulations assisting private financial institutions. The Director of FinCEN believes that legitimate Blockchain users will traffic the virtual currency, administrator or exchanger when they observe their money is being handled safely besides trusting the integrity and reputation of the company [38][40]. The lawful Blockchain business operators require a balanced approach to government regulation that brings legitimacy to virtual currencies without undue burden over new and developing companies.

A resilient position on non-compliant virtual currency exchanges will strengthen certainty as well as credibility in the Blockchainn marketplace. FinCEN should impose compliance standards for every Bitcoin exchange qualifying as money services businesses. The qualification criterion of Bitcoin exchanges has to fit within either one of the definitions of a money transmitter mentioned under 31 Code of Federal Regulations (C.F.R) 1010.100 [23][26][27][31][35].

FinCEN should also issue consistent and clear guidance and follow precedent to ensure certainty of punishment for those who are intentional evaders of regulatory control. Director of Calvery highlighted that it is pertinent for establishments to put checks and balances in order to cope with hazards of money laundering and meet their guidelines of reporting commitments [36][37]. In addition, good cooperate citizenship and compliance to regulatory responsibilities benefits the company's balance sheet too. Bitcoin exchangers also possess a stake in compliance to regulations, which in turn contributes regulators knowledge of who exchanges traditional real currency into virtual currency prior to users gaining pseudonymity in the Bitcoin based blockchain protocol's marketplace. Thus FinCEN's enforcement action has the potential to ensure Bitcoin exchange registry to money service businesses and compliance to all prevailing regulations.

CHAPTER 5

AN ANALYSIS OF BLOCKCHAIN SCALABILITY PARAMETERS IN REAL TIME SCENARIOS

5.1 Analysis of Scalability Metrics

Let us look at some blockchain parameters which have been acquired and perform an analysis on them for better understanding of what constitutes the making of the blockchain system. The data has been gathered from reliable sources such as blockchain.info, coinbase.com.

5.1.1 Analysis of transactions and Confirmation Times

Given below is a chart that has been obtained by analyzing the transaction and the confirmation times over the date range 3/2/2016 and 14/2/2016. Data has been grouped and rounded off to 0.0001 fee/KB. Keeping in mind this is real data, the following analysis has been performed.

Let us have a look at the chart below that has been plotted given the gathered data:

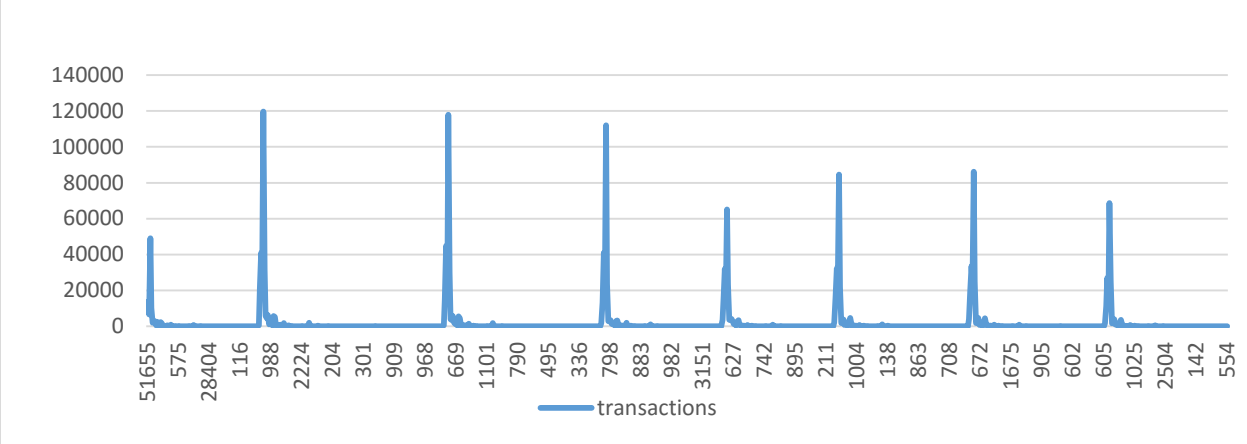

Figure 5: Graph illustrating Transactions vs their Confirmation Times

The above graph depicts the distribution of approximately 948 transactions in the range 0-15000 with respect to their individual graph times. As we see, the time plotted on the legend is un-uniform, for a closer look let us organize the data and arrange the time in ascending order for a concrete analysis.

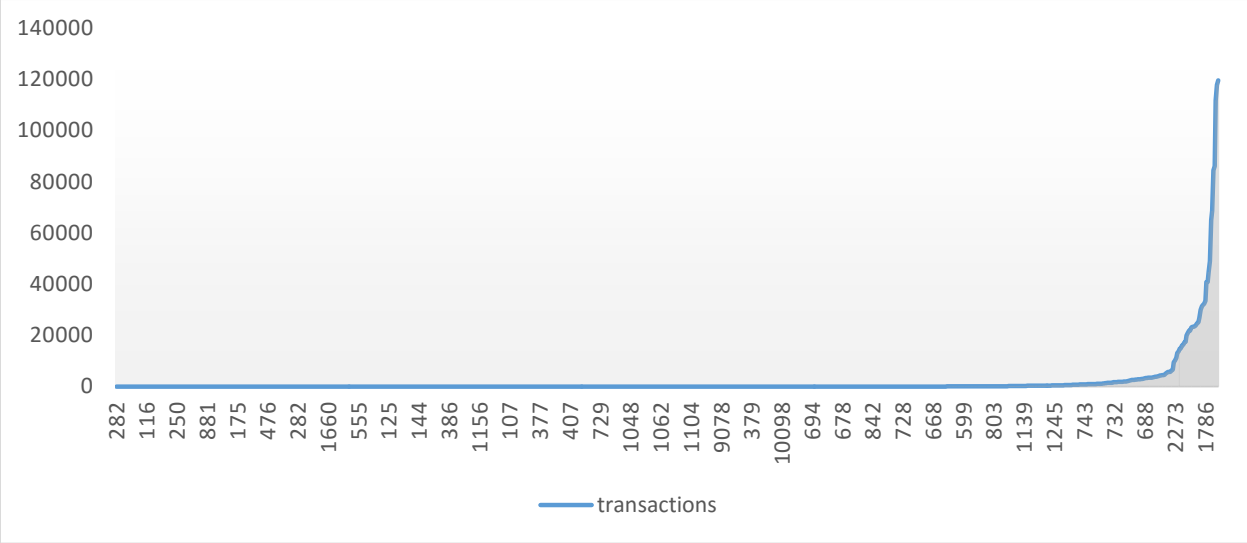

Figure 6: Graph depicting the distribution of Increasing order of transactions With Respect to Time in seconds

The above graph depicts the distribution of increasing transactions with respect to their confirmation times. A few observation can be made regarding the pattern of the distribution:

- The confirmation time increases as the number of transactions in the system is increased.
- We can safely conclude that the increase in amount of transactions is directly proportional to the increase in confirmation times [41][43].

$$n_T \propto C_T$$

$$where,$$

$$n_T represents\ the\ number\ of\ transactions,$$

$$C_T\ represents\ the\ Confirmation\ times$$

Let us now have a look at the distribution where Transactions have been ordered with respect to increasing Confirmation Times

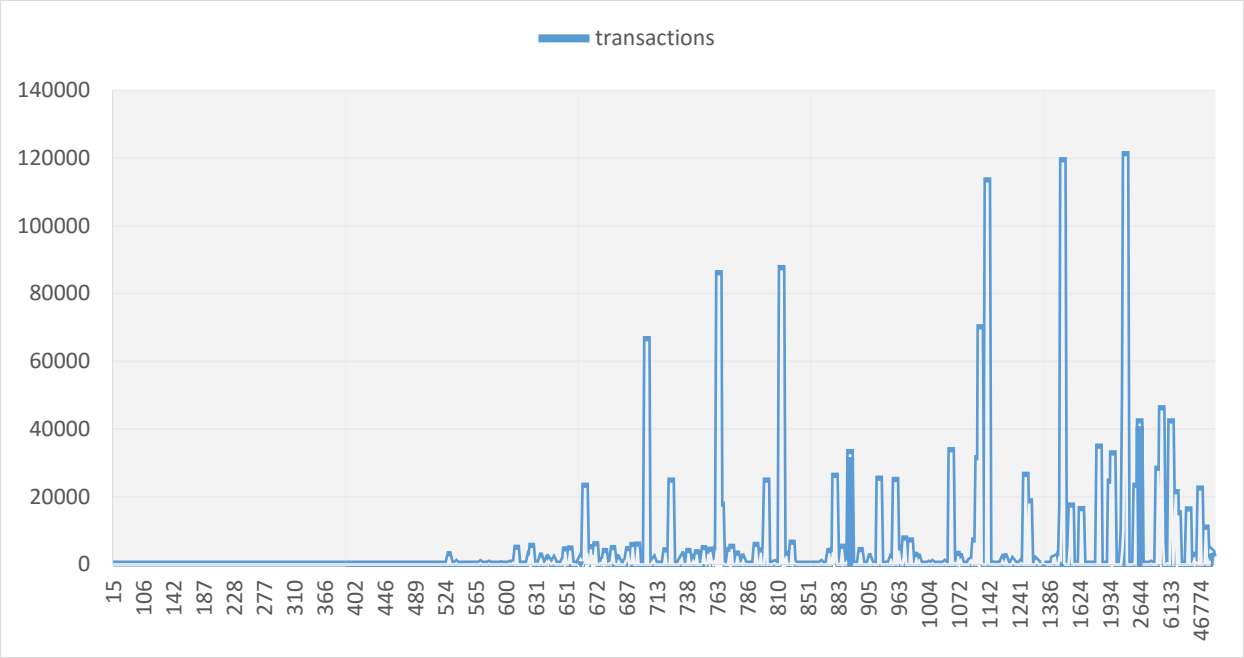

Figure 6: Transactions Vs Increasing Order of Confirmation Times

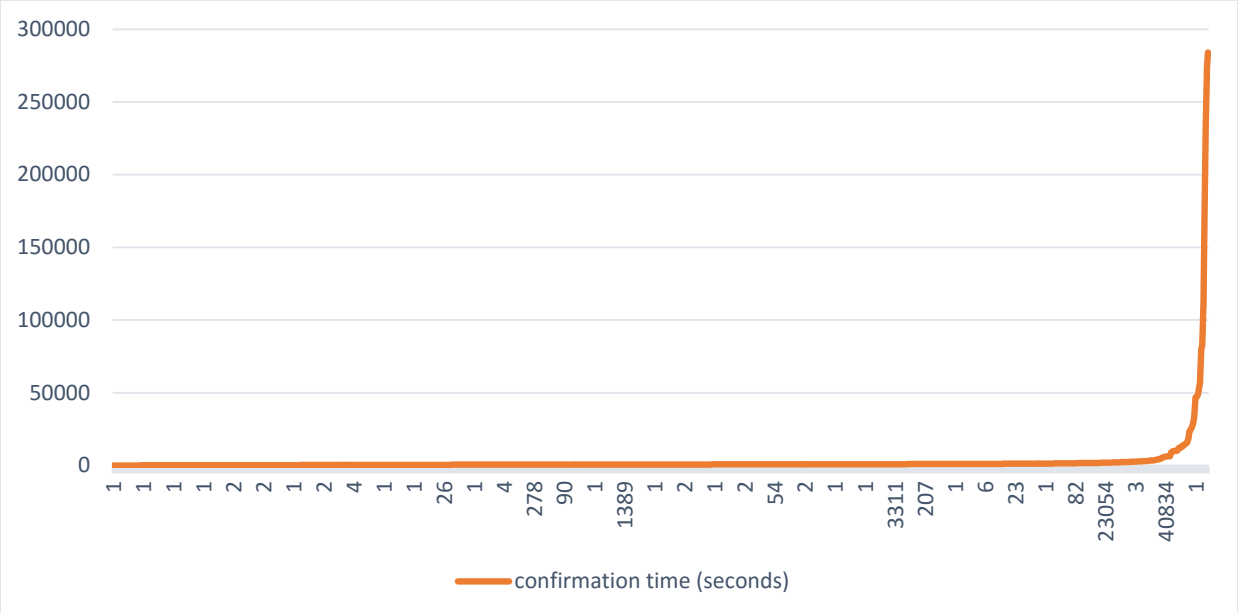

Figure 7: Confirmation Time In Seconds Vs Transactions

The above graph offers proof to the contention made earlier that increasing the amount or the number of transactions leads to an increase in the confirmation time of the transactions. As can be seen in Fig __ , there are sharp peaks for transactions above 80000 signifying a sharp increase in confirmation times. For smooth flow in the network, we would want to minimize such sharp peaks by evenly distributing these transactions and achieving higher efficiency and lower network latency [45][47][48]. This is the basis of making the blockchain system scalable. Ingesting of more transactions into a block might increase throughput but mining such blocks into the blockchain increases the overhead in the system and causes network delay.

Key Observations

- Increase in the amount of transactions leads to increase in the confirmation times.
- Increase in the number of transactions increases system and network overhead.
- Increase in the amount of transactions increases the throughput of the network.
- Increase in the amount of transactions leads to network delay and increased network latency.
- From Fig 4.3, it is apparent that sometimes in a system, higher amount of transactions can lead to lower confirmation times. As scalability depends not on one parameter but a cumulation of parameters, other factors, like network overhead, number of miners and transaction fee play an important role in deciding the confirmation time of a transaction.

5.1.2 Analysis of Confirmation Times And Transaction Fee

Transaction fee pays an important role in deciding the confirmation times of a transaction. It is the single most incentive for a miner to mine a particular transaction and include it in a block. The graph below depicts an illustration of transaction fee vs confirmation time in minutes.

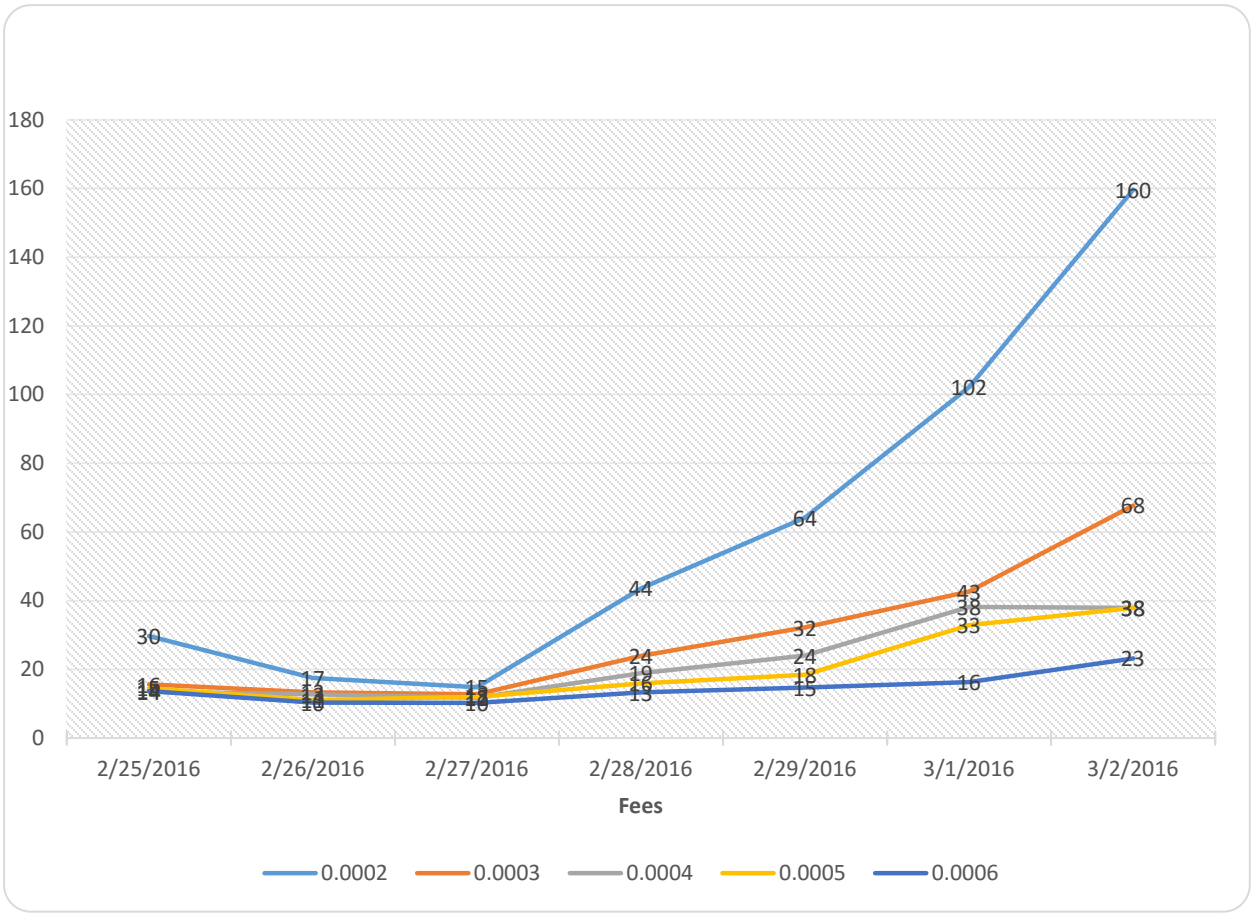

Figure 8 : Graph representing confirmation time per fee in minutes

The graph above depicts and represents the effect transaction fee has on determining the confirmation time associated with each transaction. Note there might be several transactions associated with the same transaction fee. For example, a transaction fee of 0.0002 BTC might entail around 100 transactions, and the confirmation time for that transaction from its inception to the block and the subsequent inclusion of the

block in the blockchain might vary. The data has been gathered on the date range of February 25, 2016 and March 2, 2016.

We notice from the graphical illustration that:

- Confirmation time for 0.006 transaction fee is comparatively lower from the other transaction fees such as 0.0002, 0.0003, 0.0004 and 0.0005.
- It helps us realize the fact that, higher the transaction fee more is the probability of it to have less confirmation time. Though, we cannot guarantee that this will occur for every transaction, as we see later, even some transactions with higher transaction fee might suffer and might incur higher confirmation time in certain scenarios.

Let us see if this hold true for more transactions. In order to do so, we have plotted the graph on a wider data range that encompasses several other transaction fees.

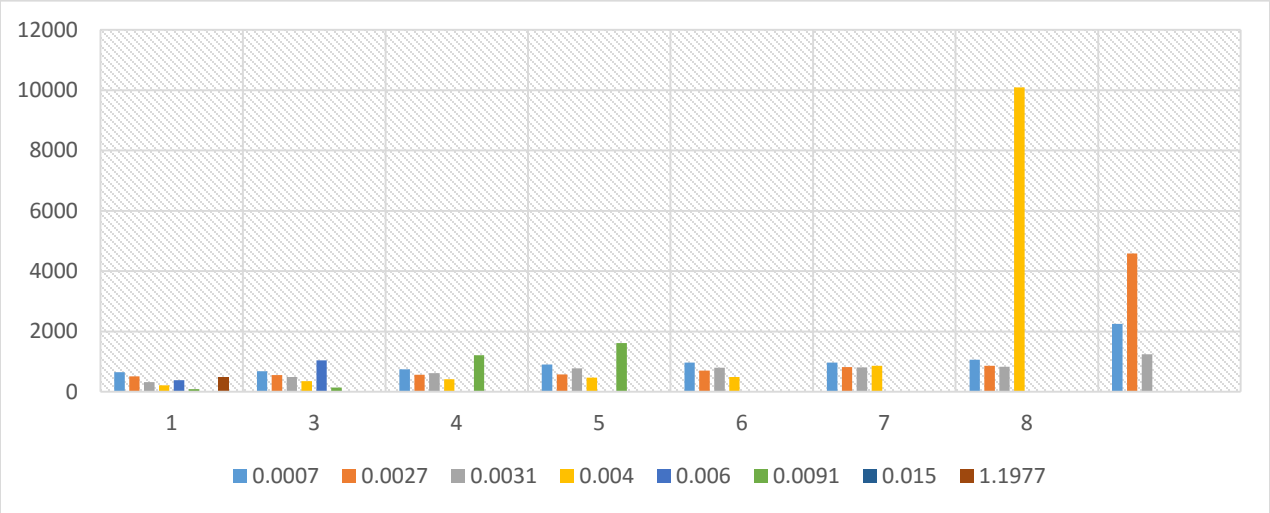

Figure 9: Confirmation Time per Transaction Fee for Varying Number of Transactions

We observe In Fig 9, that, the average confirmation time for higher transaction fee remains fairly low even after varying the number of transactions associated with each transaction fee. Let us have a look at what percentage of transactions actually have higher transaction fee in real time environments.

5.1.3 Analysis of Transactions and Transaction Fee

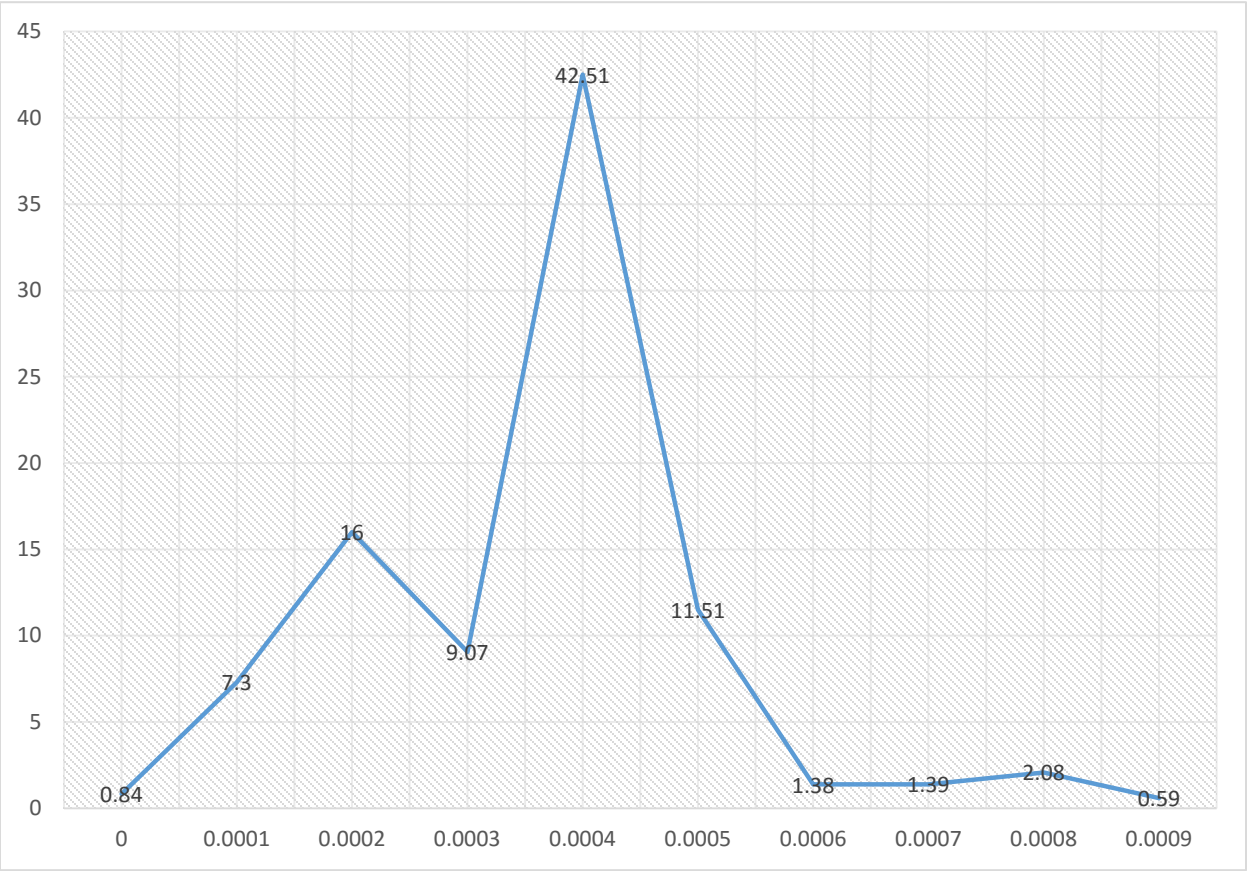

Figure 10: Percentage of transactions in the network per transaction fee

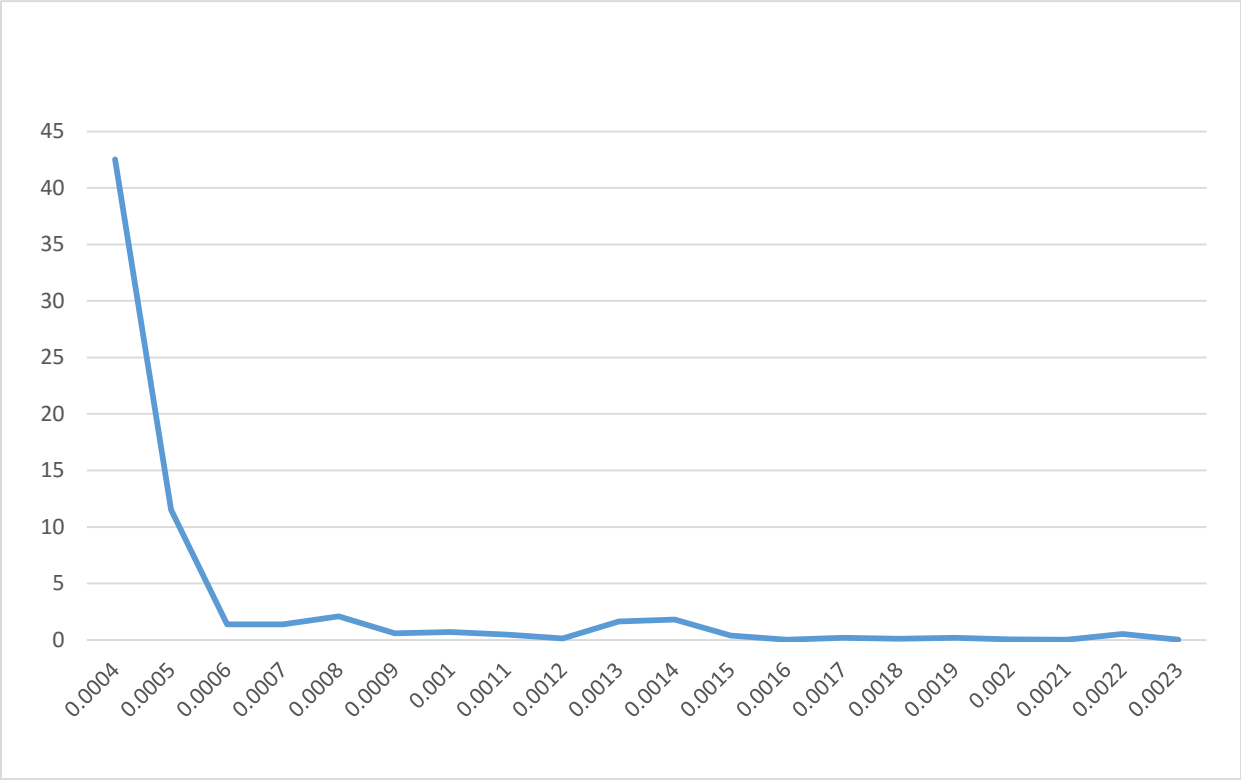

Figure 11: Percentage of transactions vs Increasing amount of Transaction Fee

Key Observations and Facts

- Note, 0.001 BTC corresponds to an average of 1.06 USD
- From the trend as observed from the graphs from the data gathered on the specific date, there were around 7.3 percent transactions with transaction fee 0.0001BTC, 42.51 percent of transactions with transaction fee 0.0004 BTC and an alarmingly low 0.59 percent of transaction with transaction fee 0.0009 BTC.
- So, even though transaction with higher transaction fee have faster chance of confirmation, real data trends indicate a very small percentage of transactions in the system with high transaction fees.
- This might have little or no effect in improving the overall scalability as its effect on network delay, latency and throughput might be negligible.

CHAPTER 6

BLOCKCHAIN SIMULATION

6.1 Model of the Blockchain Simulator

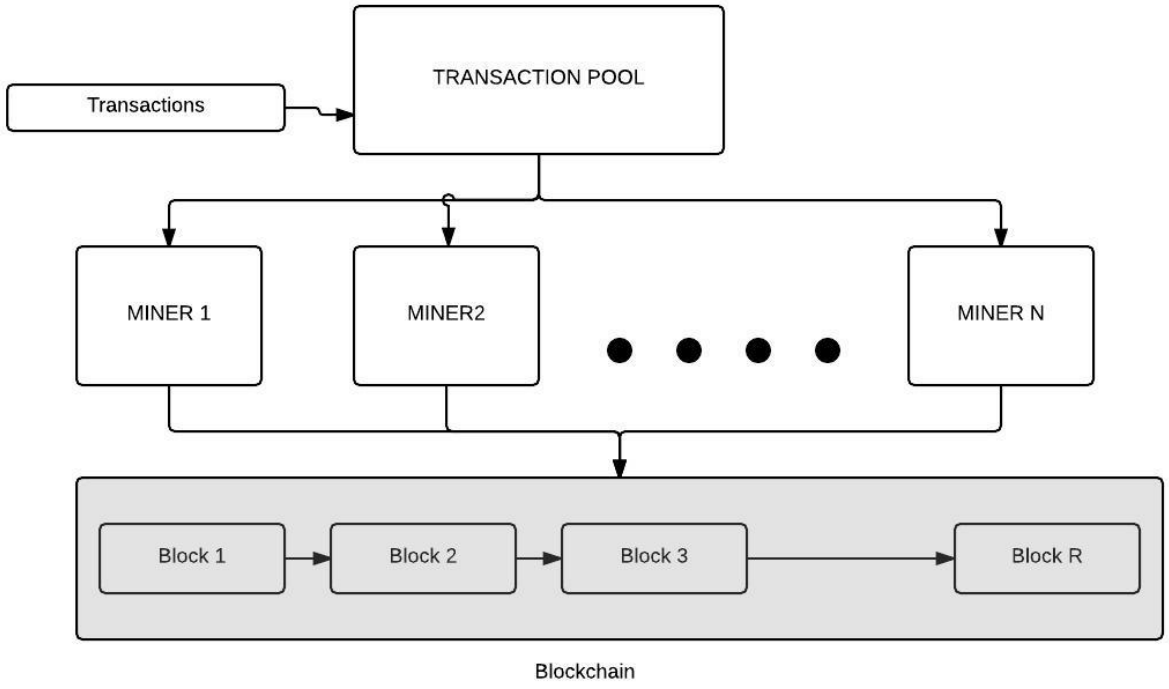

Figure 12: Model of the Blockchain Simulator

a) Transaction Pool - It is the pool containing all transactions. All incoming transactions are fed into the transaction pool and all outgoing transactions are taken from the transaction pool. In an ideal bitcoin system, the transaction pool is flooded with transactions after a specific period of time.

b) Transactions- A data structure that creates a message. This message initiates a transfer between two parties in the bitcoin system. This transfer is usually of an amount signifying the number of bitcoins [27][34][37][46]

c) **Miners-** Miners are responsible for including transactions in blocks and subsequent mining of blocks into the blockchain, the universal distributed ledger. The miners participate to solve a complex problem. The winner is awarded the block reward after successful addition of the block to the blockchain [45][49].

d) **Blocks-** A data structure that assembles transactions . It can be seen as a container of transactions.

e) **Blockchain-** It is an arrangement of blocks in a chronological order. Successful mining of blocks leads to its addition in the block chain. It represents a huge database that contains the record of transactions ever made in the bitcoin history.

6.2 UML Class Diagram for the Blockchain Simulator System

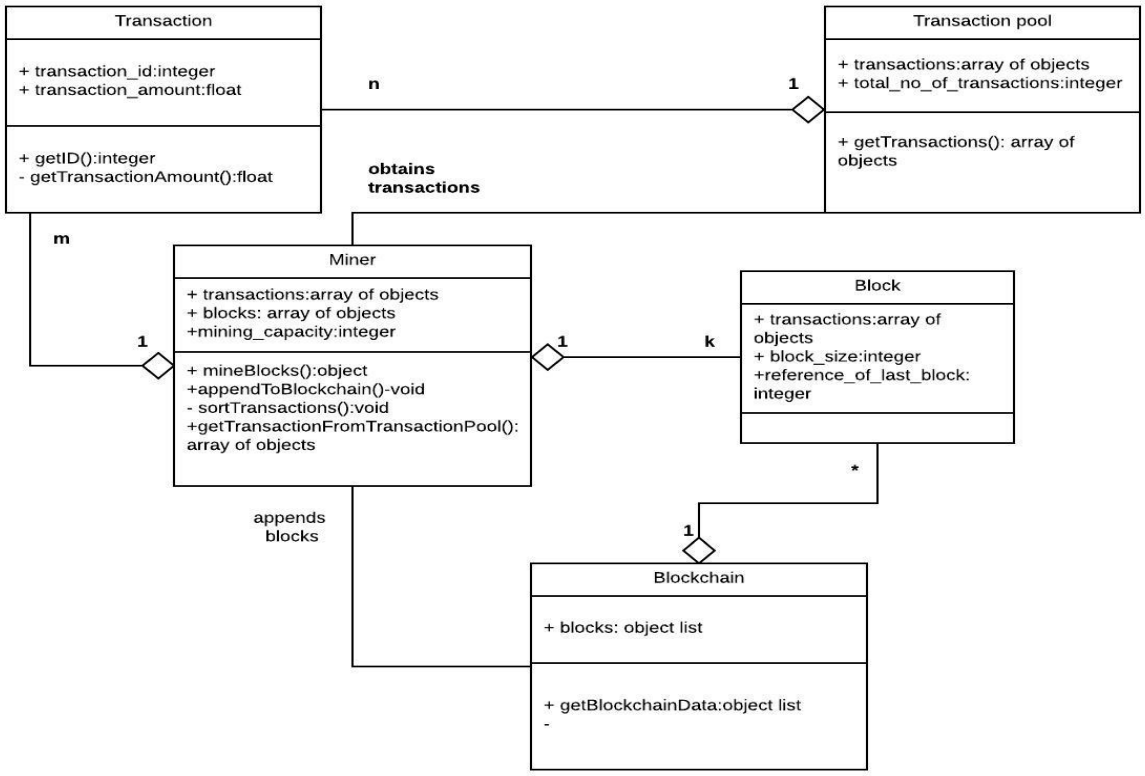

Figure 13: UML Class Diagram of the Blockchain Simulator System

6.3 Working of the Blockchain Simulator

To explain in detail what the Blockchain simulator does and how it re-enacts the blockchain system, we would go step by step in understanding the Blockchain in an ideal working system. When a transaction is made in an ideal Blockchain system, such as blockchain based Bitcoin protocol, the following happens:

6.3.1 A look into the Bitcoin Ecosystem: User Perspective

a) Alice wants to send money to Bob, say 0.004 BTC.

b) Alice has 0.004BTC in her wallet.

c) Alice and Bob are both registered users of the Bitcoin network.

d) Alice initiates transaction of amount 0.004 BTC to Bob

e) Alice's transaction is confirmed after a period of time.

f) Bob receives 0.004BTC in his wallet

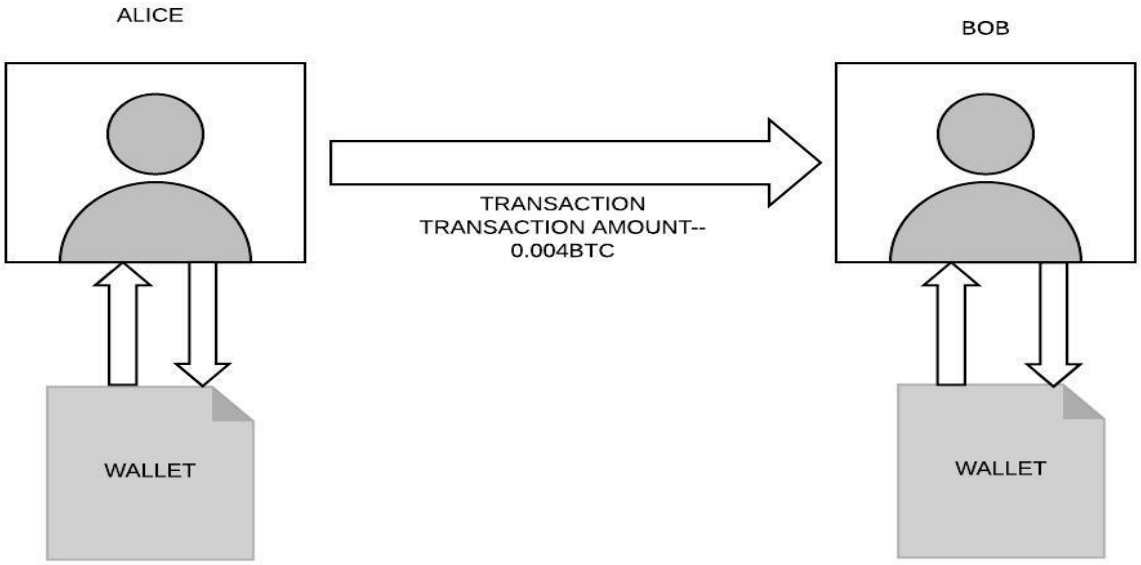

Figure 14: Illustration of the transaction between Alice and Bob

6.3.2 A look into the Bitcoin Ecosystem: System Perspective

a) Transactions like those of Alice are added into the transaction pool containing all transactions.

b) The transaction pool broadcasts these transactions.

c) Miners get a partial view of the transaction pool.

d) Miner will pick up the transactions he wants from the partial view of the transaction pool.

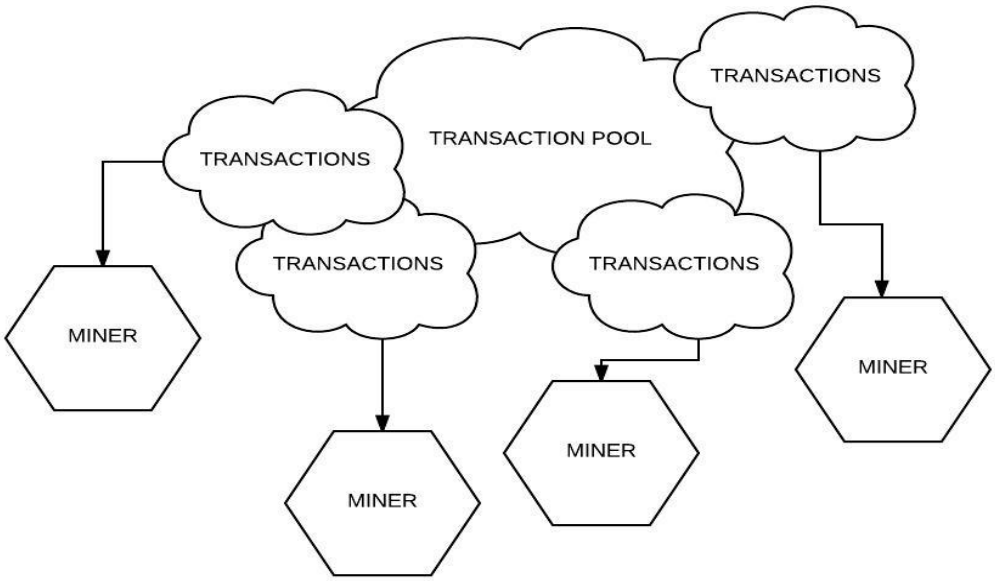

Figure 15: Illustration of Partial View of the Transaction Pool For Miners

e) This decision is based primarily on the transaction fee associated with the transactions.

f) The goal of the miner is to add the transactions into the global ledger.

g) Transaction fee is one of the biggest incentive for the miner to mine blocks.

h) Miners start hashing transactions pair-wise.

i) Ultimately, a single hash or digest value is obtained.

j) The single hash value is the encoding of all the transactions the miner wants in his block.

k) This hash is aggregated with the digest or the hash of the previous block that was incorporated in the blockchain.

l) In order to add this block in the block chain, the mining node will perform proof of work.

m) The proof of work entails solving a complex mathematical problem to append block at the end of chain.

n) The challenge numbers and the proof numbers are then hashed together to generate a large prefix of zeroes.

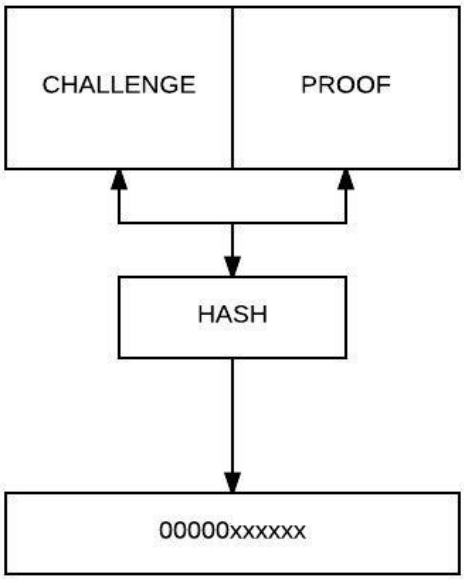

Figure 16: Illustration of the generation of Prefix

o) The difficulty associated with the proof numbers lies in the quantity of the prefix zeroes.

p) The average time taken to do this entire process in a traditional Bitcoin system is 10 minutes.

q) Lot of mining nodes are working on this proof at the same time.

r) Concurrent race to solve the problem and incentive of the transaction fee forms the basis of the blockchain network.

s) Once a mining node is able to generate a valid proof, its block is added to the blockchain.

t) This result is then broadcast over the entire peer to peer network to all the nodes which are a part of the current bitcoin system.

u) Once this has been achieved, the mining nodes start building on this new proof that is built on all the previous transactions and new challenge.

v) New proof refers to the updated blockchain of transactions.

w) The mining node that was able to solve the complex problem is awarded the block reward.

x) All the miners can take the first item in the block called the coinbase generation, the first transaction and assign a fee to themselves.

y) The successful mining node gets to collect the reward of all the transactions in his appended block.

6.3.3 Simulator Functions

a**) getID()-** This function is called to retrieve the transaction id associated with a particular transaction

b) **getTransactionAmount()**- This function returns the transaction fee associated with a transaction.

c) **getTransactions()-** This function is used to retrieve all the transactions in a transaction pool.

d) **mineBlocks()-** This function creates blocks by putting transactions into a block of pre-defined size.

e) **appendToBlockchain()-** This function appends block to the distributed ledger.

f) **sortTransactions()-** Function sorts transactions on the basis of transaction fee.

g**) getTransactionsFromTransactionPool()-** The miner calls this function to obtain transactions from his partial view of the transaction pool.

h) **getBlockchainData()-** This is an inbuilt function of the blockchain class and it is used to retrieve block data of each block that has been added to the blockchain.

6.3.4 Specifications

This code has been written in Java ECLIPSE Luna Edition. Operating System is Windows 7.

6.3.5 Functions Performed By the System

The Blockchain simulator enacts the Bitcoin system from the system view point.

a) Transactions are added into the system.

b) The transactions are stored in the transaction pool

c) Partial View of the transaction pool is generated for the miners.

d) Miners pool in transactions from the transaction pool on the basis of the transaction fee.

e) Miners add transactions to the block.

f) Miners add block to blockchain.

g) Transaction fee and id are generated by the system.

h) The system generates block generation time, mining time.

i) Block size is fixed at 100 transactions.

CHAPTER 7

SCALABILITY ANALYSIS THROUGH SIMULATION

7.1 Analysis of Transactions and Confirmation times

The following graph has been plotted for transactions within the range 0-60000. The confirmation time measured is in seconds. We see a gradual increase in the confirmation times with increase in the number of transactions. These values have been gathered from the Simulator for analysis.

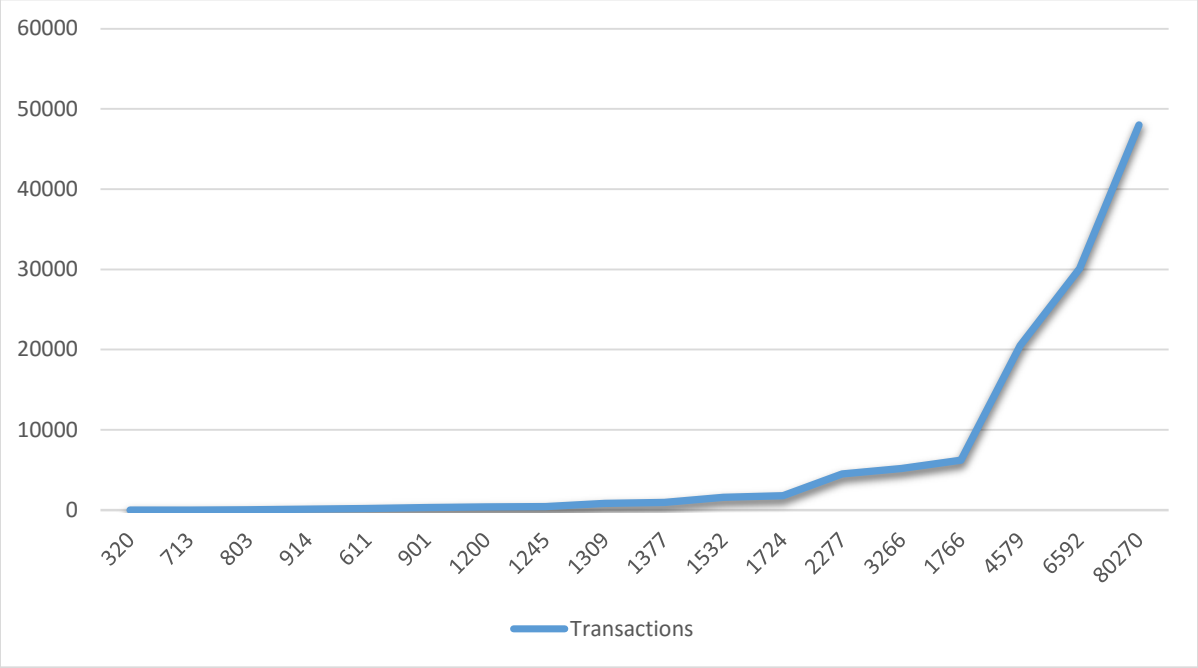

Figure 17: Graph representing Transactions (y- axis) with their Confirmation Times

In order for a more comprehensive understanding of the relationship between transactions and confirmation times, let us have a look at the confirmation time trend for a number of transactions. The data below has been gathered by fixing the transactions to a certain value and gathering their confirmation times .

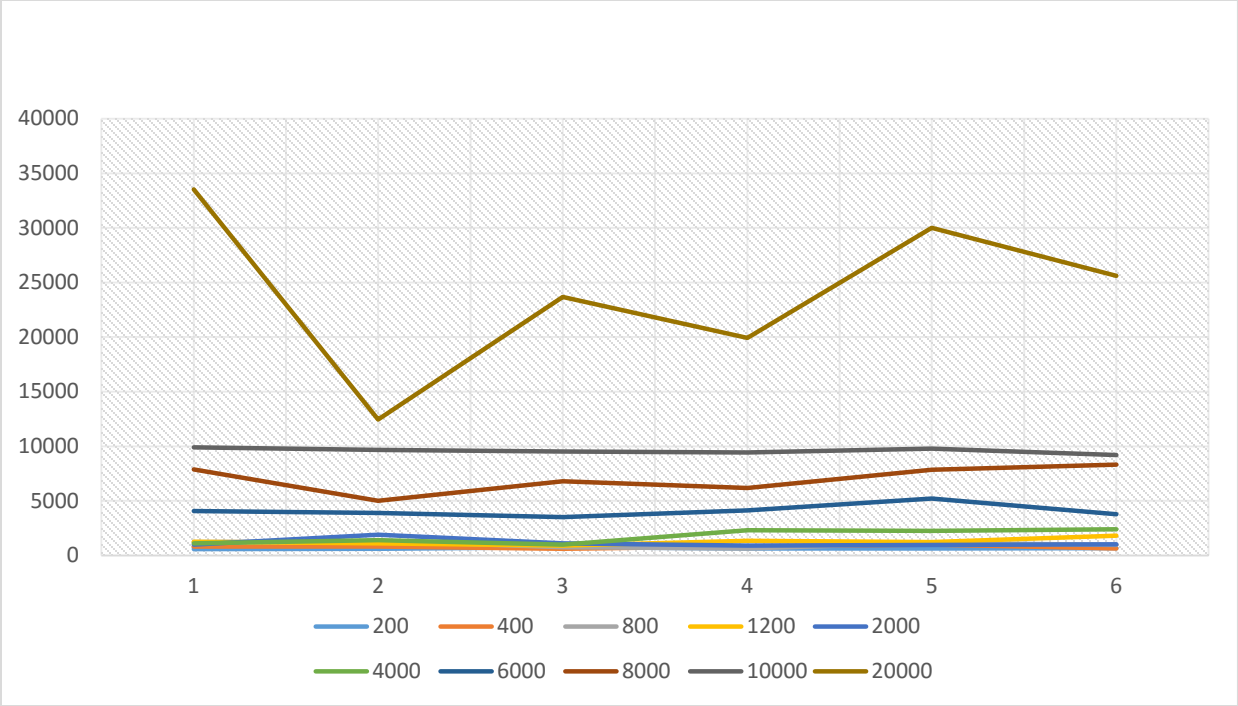

Figure 18: Graph representing Confirmation Times per Transactions

The above graph represents a series of 10 transactions over the values 200, 400, 800, 1200, 2000, 4000, 6000, 8000, 10000 and 20000. Data of confirmation time in seconds have been recorded accordingly.

Observation points:

- As evident from the graph, there is a steep increase in confirmation times for transactions over 5000.
- This is only natural, as increase in the number of transactions increases the system overhead for mining more transactions into blocks.
- Increase in the number of transactions increases the throughput of the system at the cost of increasing network latency.

Let us now examine, the relevance of the simulator data with real time data.

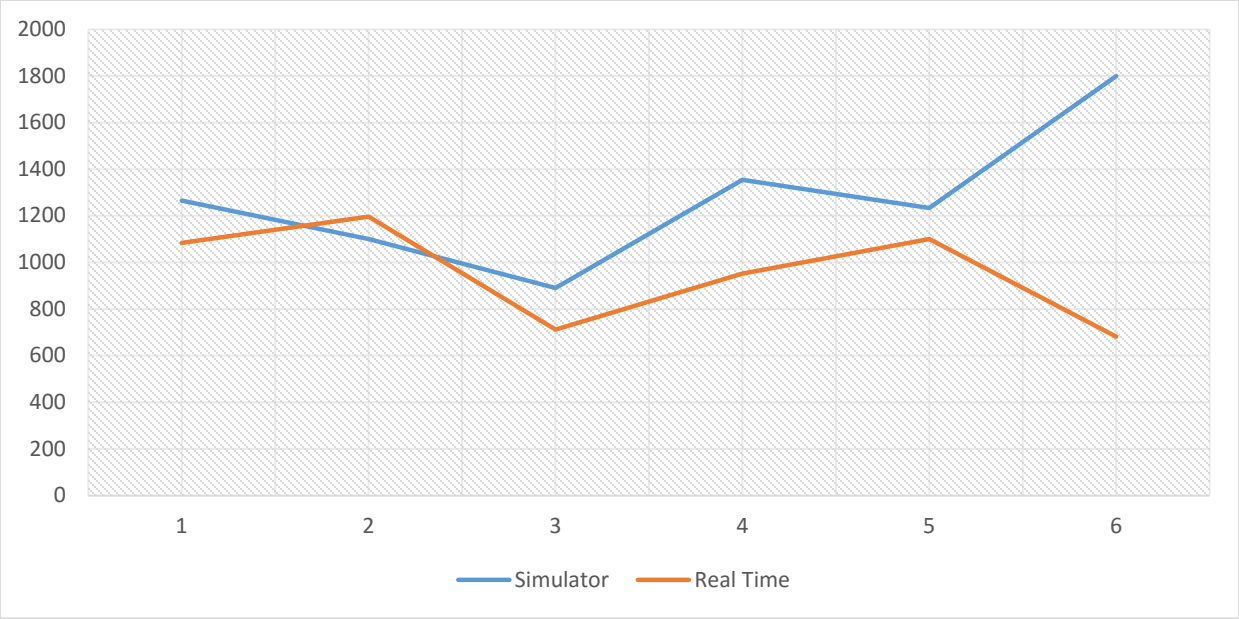

Figure 19: Graph representing Simulator and Real Time Confirmation Time for 1200 transactions

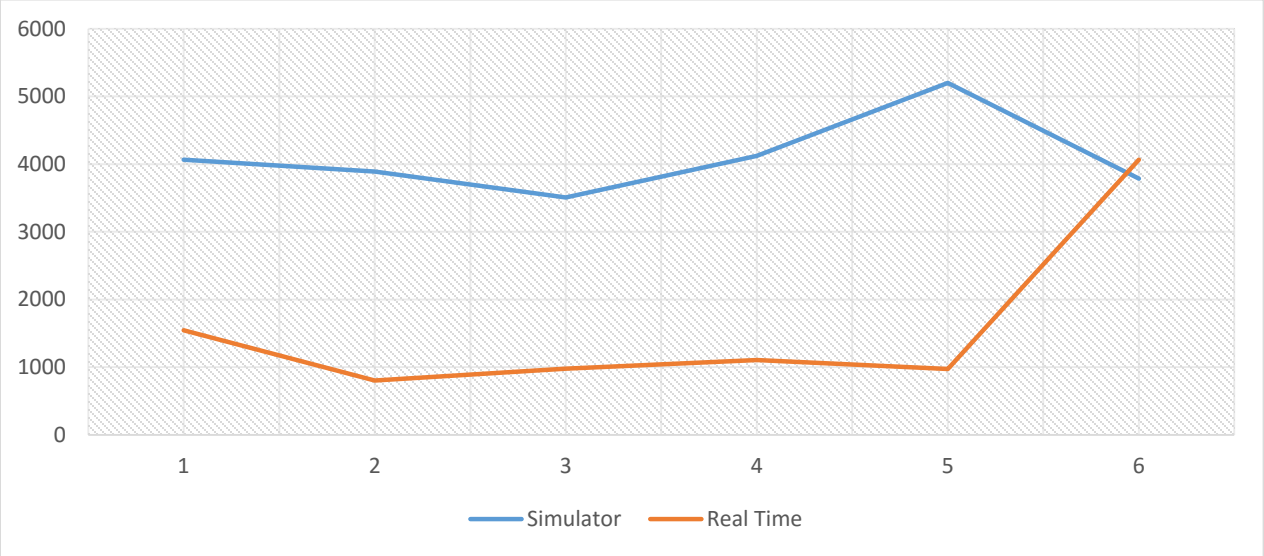

Figure 20: Graph representing Simulator and Real Time Confirmation Time for 6000 transactions

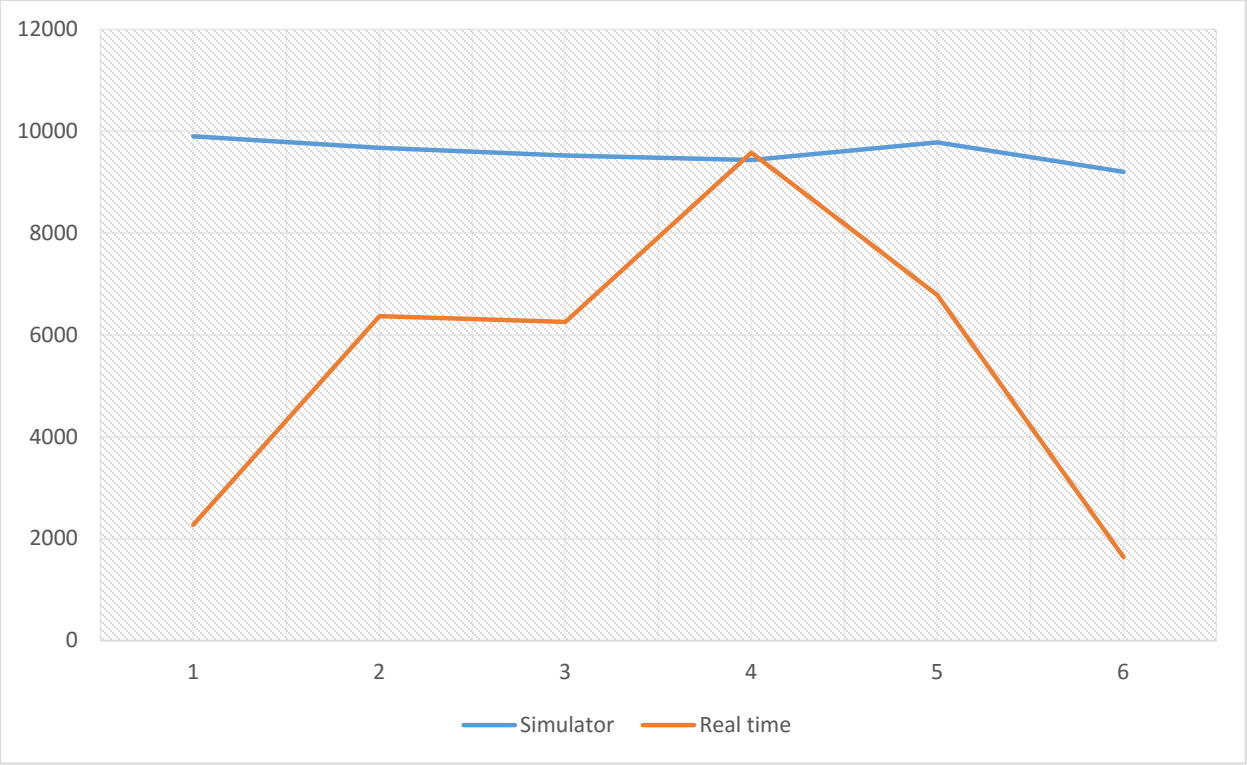

Figure 21: Graph representing Simulator and Real Time Confirmation Time for 12000 transactions

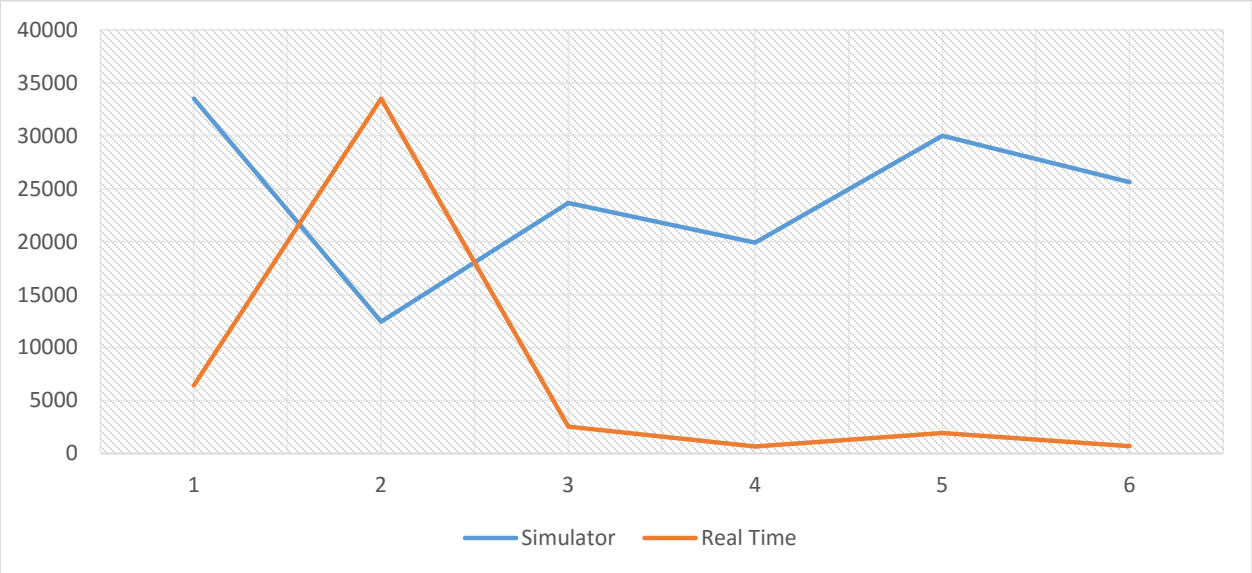

Figure 22: Graph representing Simulator and Real Time Confirmation Time for 20000 transactions

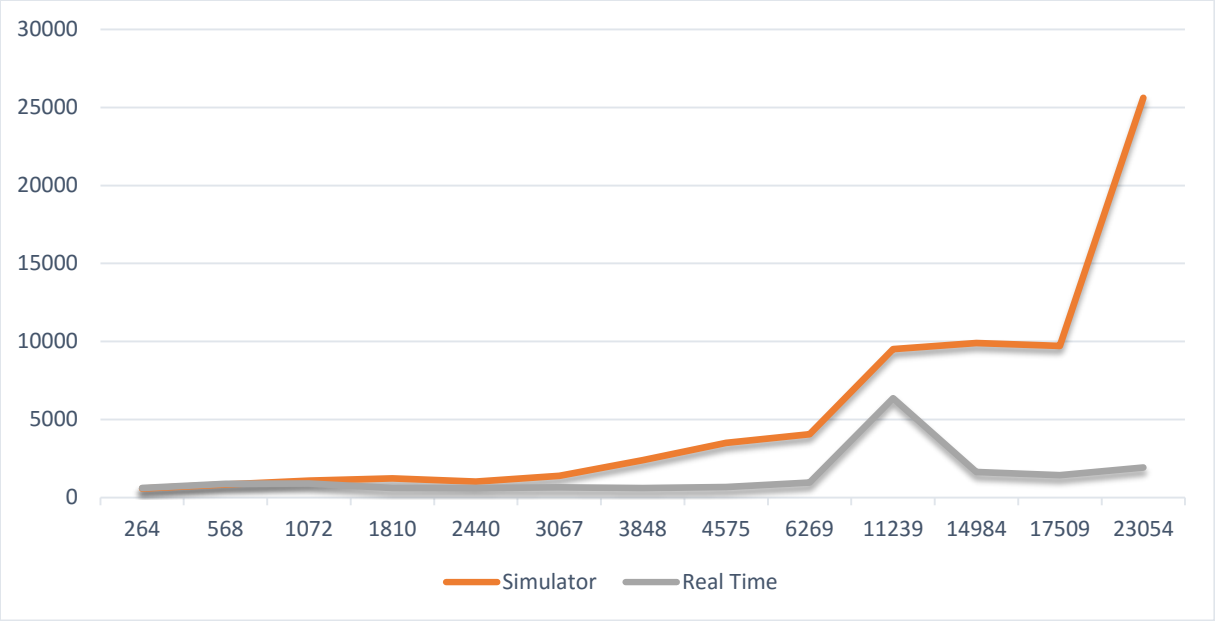

Figure 23: Graph representing Confirmation Time Trend for Simulator and Real time Environments

Key Observations:

- As is apparent from Fig 5.8, 5.9,5.10, 5.11 and 5.12, the confirmation times for real time environments is lower than that generated by the simulator. This is only natural, as computers with high power and mining capability are used to mine transactions in real environments.
- We also observe from Fig 5.12, that the trend of confirmation time obtained for varying transactions is similar in the simulator and real time environments ie, a general increase in confirmation times with respect to the increase in the number of transactions and steep increase after transaction threshold of 5000.

7.2 Analysis of Transaction Fee and Confirmation times

The chart below has been obtained after analysis of transaction fee in the range 0.0004 BTC to 0.04 BTC. The confirmation time for each have been recorded in seconds for analysis. Though we see uneven peaks in the chart for transactions in the range 0.001 to 0.002, the trend fairly remains uniform. It has been discussed in detail in the section below.

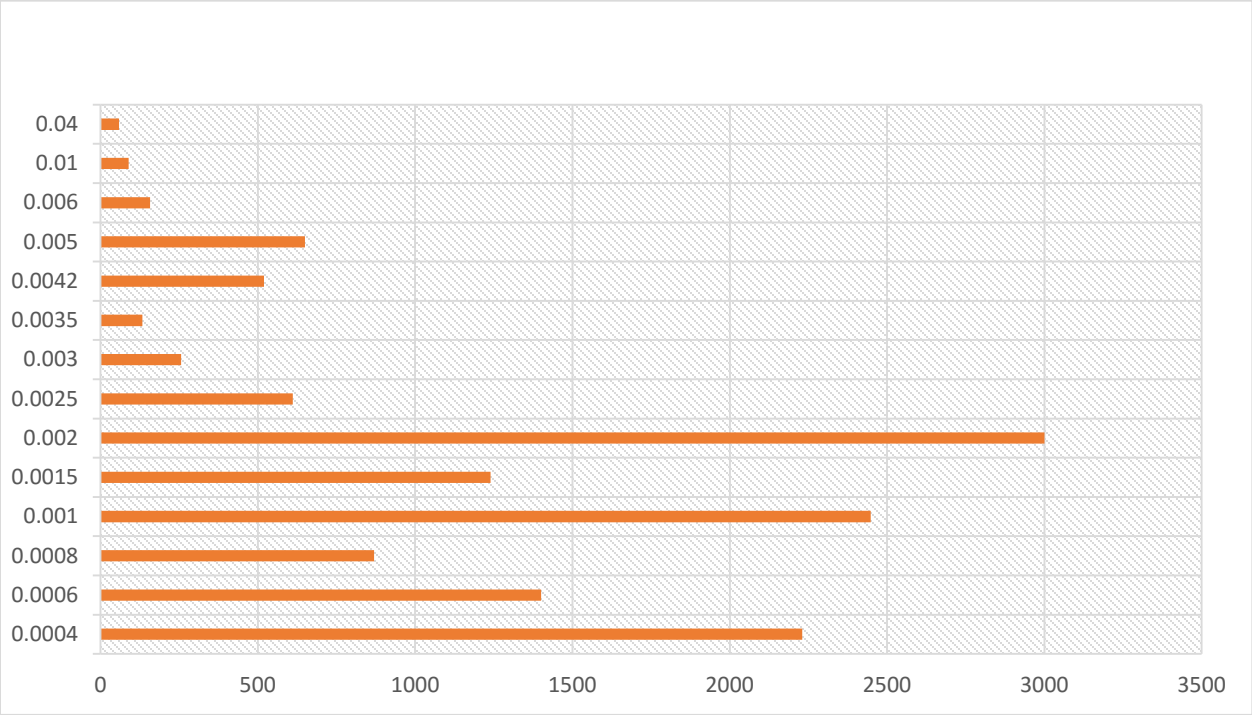

Figure 24: Chart representing confirmation Times with increase in Transaction Fee

For better understanding of the impact of transaction fee on confirmation times, let us have a look at confirmation times for specific value of transaction fee.

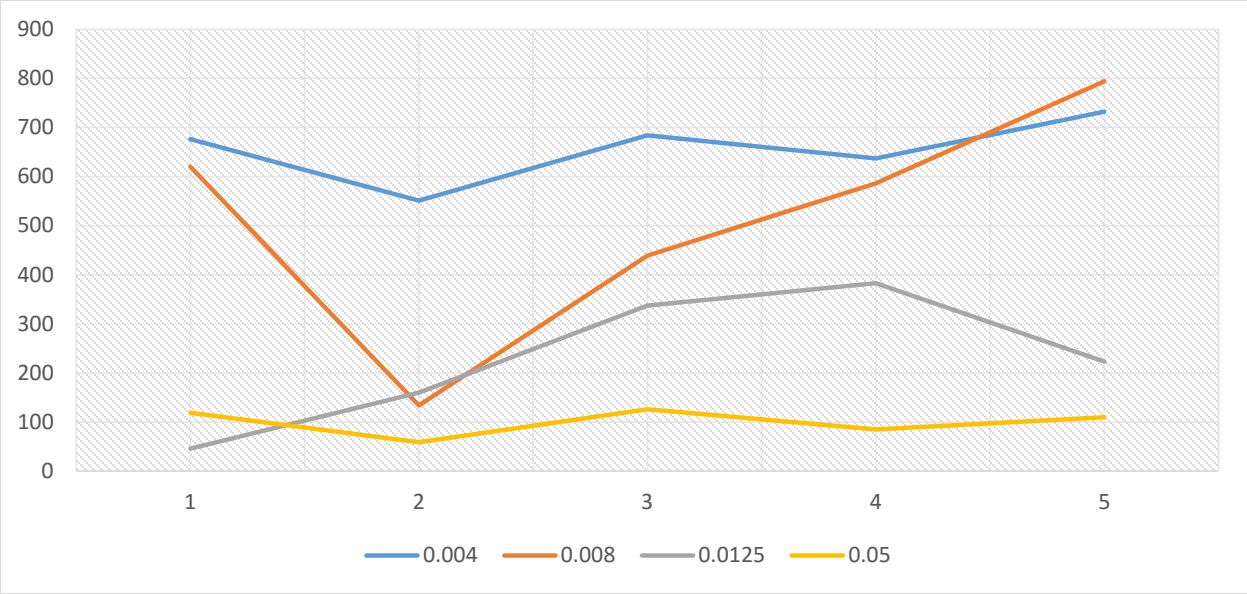

Figure 25: Confirmation time in Seconds per Transaction Fee

The graph above has been plotted with respect to confirmation fee of 0.004, 0.008, 0.0125, 0.05 Bit coin Units. The confirmation time for each has been recorded in seconds for analysis.

Key Observations

- We notice from Fig 5.13, 5.14 a sharp decline in Confirmation Time with increase in the Transaction Fee. So in general, transaction confirmation time decreases with increase in transaction fee.
- We also see un-uniform distribution for some transaction fee such as 0.002, 0.005, 0.0015, that is the confirmation time for them is higher than their previous counterparts. This can help us in understanding that some transactions even though with higher transaction fee might suffer due to its not being included in the block. This condition might occur due to several reasons, one of the primary reason for this to occur is the increase in transaction overhead due to increase in the number of transactions with same transaction fee, in such a case, a transaction is most likely to suffer leading to increased network latency and delay.

Let us now examine the simulator data with respect to data in real time environments.

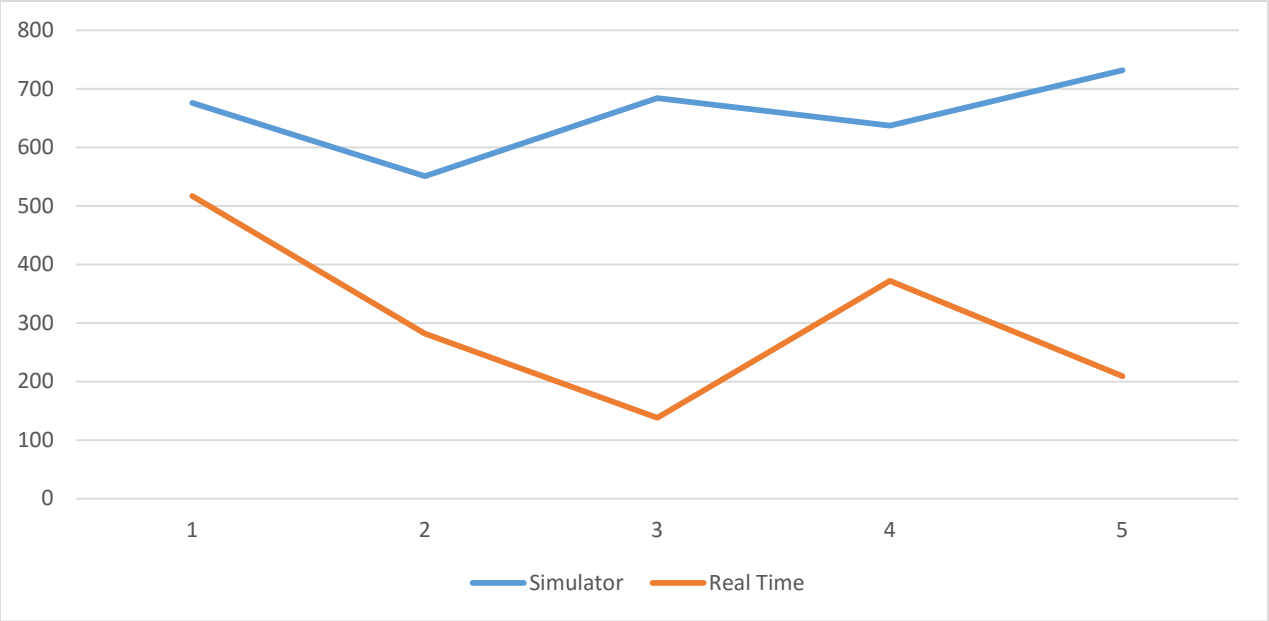

Figure 26: Graph depicting trend in Confirmation Time for Simulator and Real Time Environments for 0.004BTC

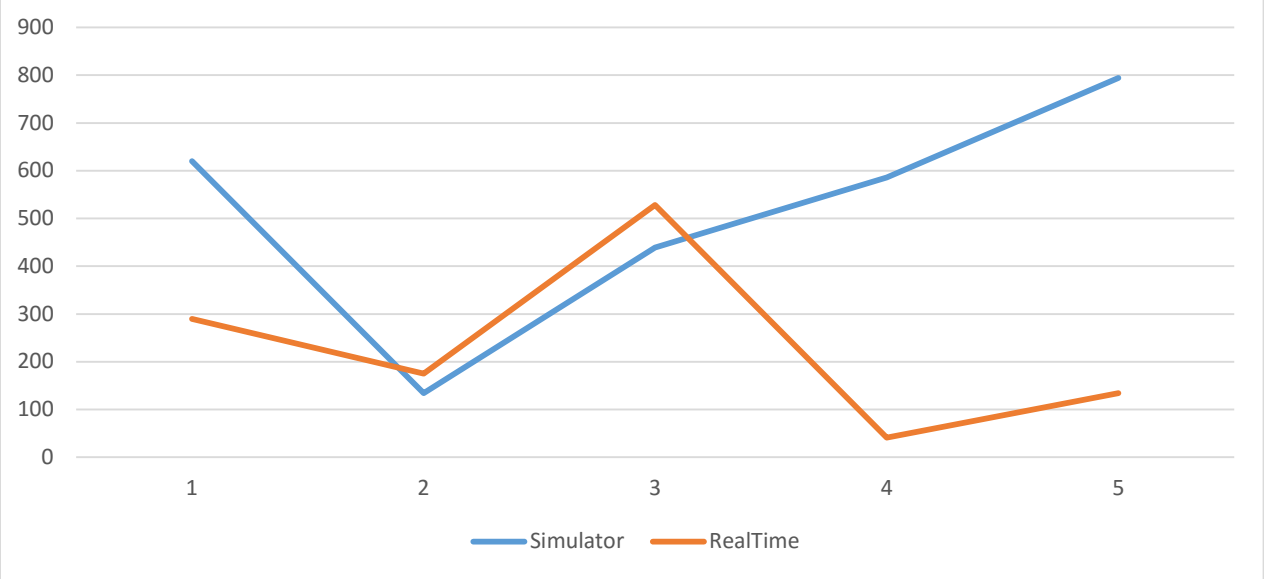

Figure 27: Graph depicting trend in Confirmation Time for Simulator and Real Time Environments for 0.008BTC

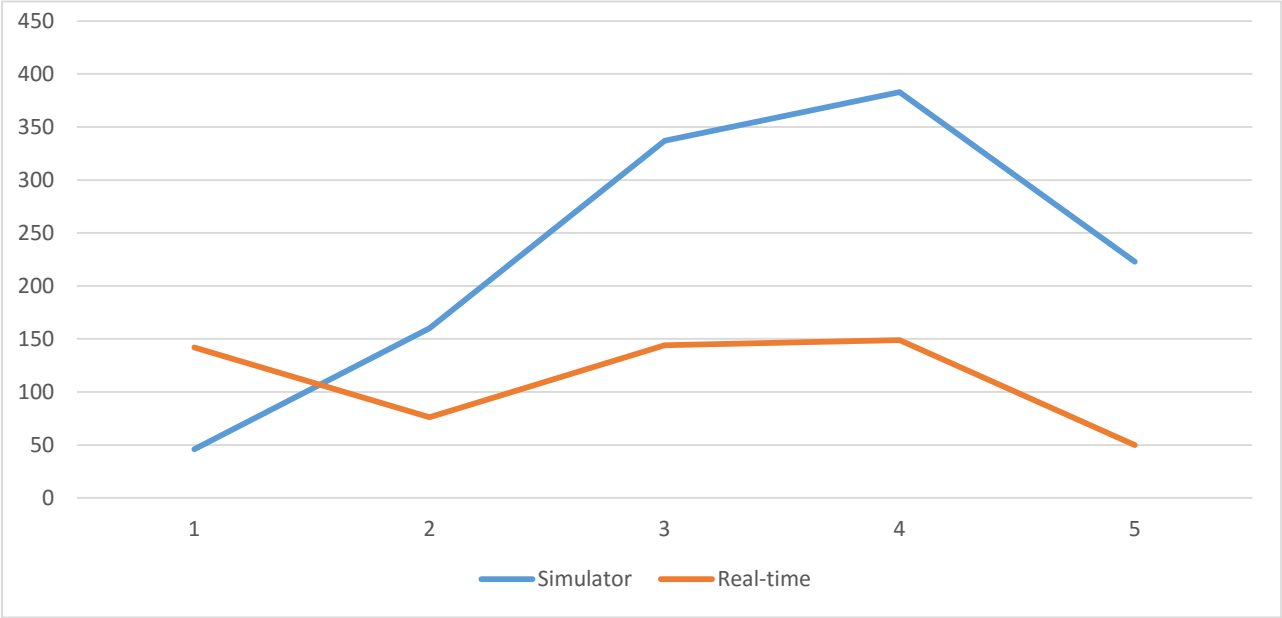

Figure 28: Graph depicting trend in Confirmation Time for Simulator and Real Time Environments for 0.0125BTC

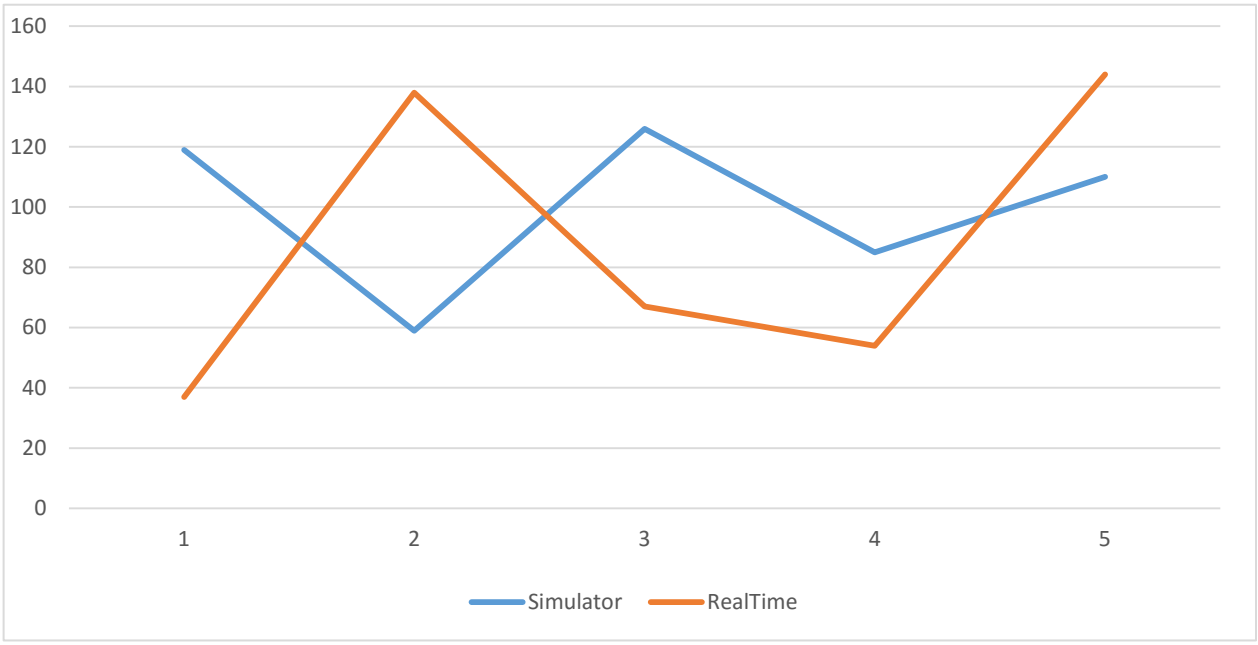

Figure 29: Graph depicting trend in Confirmation Time for Simulator and Real Time Environments for 0.05BTC

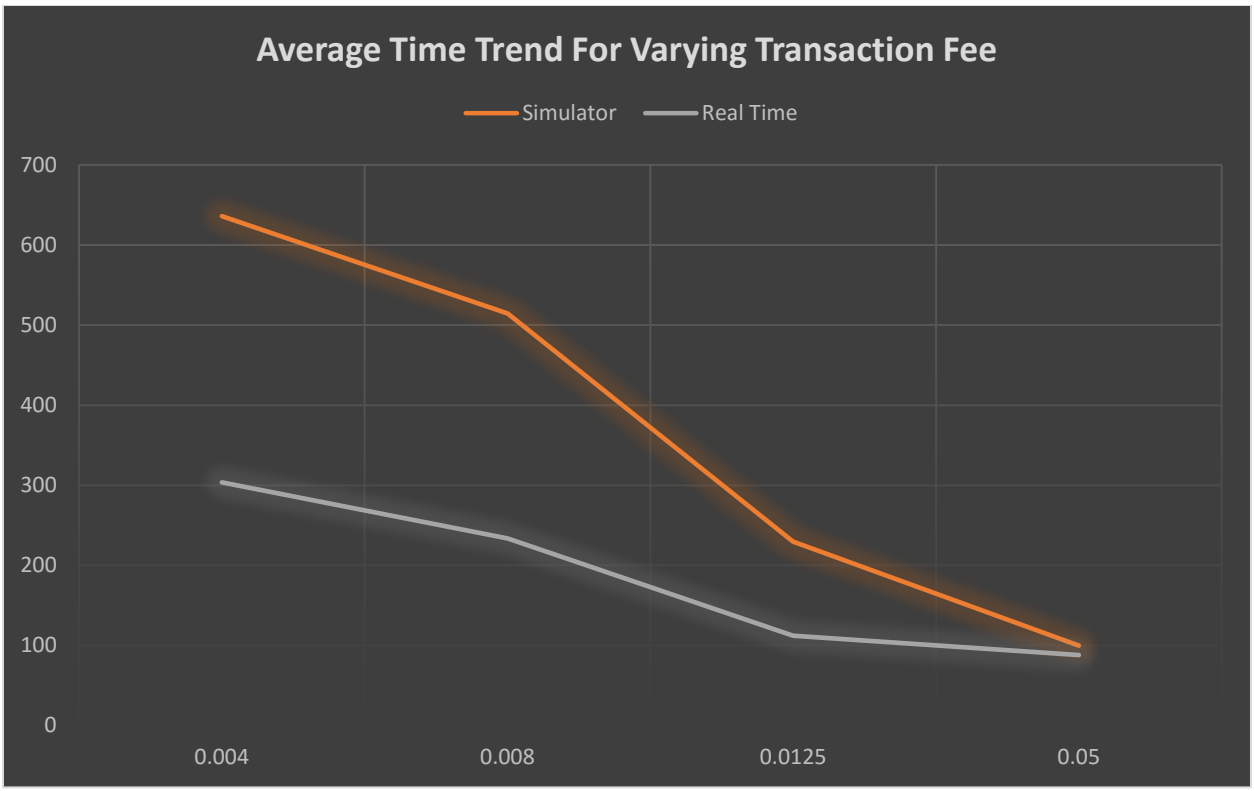

Figure 30: Average Confirmation Time for Increasing amount of Transaction fee

The above graph has been generated by averaging the confirmation time generated for 0.004, 0.008,.0.0125 and 0.05 BTC.

Key Observations

- From Fig 5.16, 5.17,5.18,5.19 and 5.20, we observe that confirmation time is less for that generated in real time environments to that generated by the simulator. This is obvious from the reasons discussed earlier.
- The average confirmation time trend as depicted in Fig 5.20, is gradually decreasing with increase in the transaction fee.

7.3 Analysis of scalability parameters

7.3.1 Latency- Latency in the blockchain network is defined as any sort of delay that is caused due to the propagation of the blocks in the network. The time taken for confirmation of a transaction has direct impact over the network latency. Faster confirmation times for transactions would mean lower latencies and faster network propagation. We observed from the analysis of the simulator and comparison to real time data that, to have lower network latency the following can be done, the open challenges to the ways prescribed have also been elucidated below:

- Increasing the transaction fee for transactions would increase the probability of a faster confirmation time for that transaction, will increase its chances of being included in the block and would ensure lower latency in some respects.
- Increasing the transaction load on the system would mean higher latencies. As we increase the number of transactions in the system, we would expect the block size to grow. In order to propagate heavier blocks, more bandwidth of the network would be consumed, more power would be used and would also lead to congestion in the network thereby increasing latency.

7.3.2 Throughput- Throughput of the blockchain system is defined in terms of the number of transactions confirmed per second. Most of the modern payment processing systems like Visa has an average throughput of 2000 transactions per second. Bitcoin based blockchain systems have an average throughput of processing only 7 transactions per second. Clearly, to bridge this gap with that of a modern payment processor, the scalability needs to be considerably improved by a large margin. A few observations from the analysis has been elucidated below:

- Increased block size to incorporate larger amount of transactions will effectively increase the transaction load in the system as well as will increase the throughput. In the current Bitcoin system, the block size is fixed at a cap of 1 MB. If we really want an increase in the efficiency, this seems like a reasonable claim.

- Increasing the block size for achieving higher throughputs come at the cost of compromising blockchain security and compromising decentralization.
- Increasing the transaction load on the system, higher block size would also necessitate hard forking.

7.3.3 Transaction Fee and its Effect on Scalability- One of the biggest problems with Blockchains that affect scalability are transaction delays. These transaction delays are caused by an accumulation of several factors, in which transaction fee pays a very major role. The fact that any user is able to add a certain transaction amount to a transaction which might push the transaction to the top of the queue leads to some transactions with low transaction fee starving. It might mean two things:

- First, that the transactions with higher transaction fee gets confirmed faster. This happens as obvious from the stated reasons when the transaction is pushed at the top of the queue due to its priority of having a higher transaction fee associated with it. This is especially profitable for the miners. This leads to transactions with lower transaction fees suffering heavily.
- Second scenario is when some transaction suffer regardless of having a substantial transaction fee associated with them. This happens when the transaction amount is substantial but there is a pool of transactions with the same amount or higher in the queue. So say in a pool of n transactions where all the n transactions have the same transaction fee associated with them, a transaction might starve and might take forever to be confirmed.

7.3.4 Block size- As stated earlier, the Bitcoin block size is currently fixed at a cap of 1 MB. On an average a block can hold around 1000-2000 transactions. Lowering or increasing the block size would have seminal impact on scalability metrics as explored below:

- Increasing the block size would lead to an increase in the capacity of blockchain. The potential of bitcoin based blockchain protocols subsequently increases with higher capacity for data and more security.

- Increase in the transaction load along with the block size increase, as obvious, would mean the ability of processing huge amount of transactions, hence higher throughput and more efficiency.
- Increasing the block size for more capacity and more transactions would lower security, and will shift the stance to a centralized body having more control

7.3.5 Number of miners in the system- More mining power in the blockchain system would help to relay the power consumption and the task of mining blocks evenly across the network. This would mean lower latencies and convergence. It would also mean faster confirmation times and higher throughput.

CHAPTER 8

FUTURE WORK AND CONCLUSION

8.1 Conclusion

The modern era solely relies on the services provided by a centralized authority such as a bank. This is so, as the bank is viewed as an entity of trust. The blockchain protocol is decentralized and slowly establishing its trust in the market. The pseudo anonymous and decentralized nature of blockchain makes it a coveted technology and enthusiasts are delving into it for full fledged exploitation of its potential not only as a digital currency but for other applications and services that can be built atop this [23][26][55]. The global pool of networkers, such as miners who make use of their resources, computation power to ensure security of the blockchain system [46][47]. As a part of the public domain, and lack of central authority ensures that no third party has any form of interference with the transaction. Also, this means, that no extra charges need to be paid for a third party initiating these services. This is the main cause and the reason for block chains potential in the future and for its popularity currently. The scalability metrics of blockchains which prevents its usage to match up to those of that of modern payment processors is still a cause of concern. However, a balance or a compromise according to the application service can be made in order to exploit blockchain in specific circumstances[53][54]. For example, if an investor is more interested in sending huge amounts of data and can allow some degree of compromised security and centralization, a blockchain based protocol can be designed accordingly, also, if the necessities are different such as increased security, the modern blockchain protocol can be used to relay perfectly. I

8.2 Future Work

The Blockchain being difficult to scale , puts forward a questionable environment for users and businesses to explore its potential as a full-fledged consumer technology. The way of viewing blockchain solely as the backbone of digital currencies need to be changed. Blockchains potential to carry huge amount of data and security can form the basis of other applications and services. Exploration into multichains, the potential to move all kind of currencies in one distributed ledger, paving way for a technology that takes into

consideration both security and legislation. Old ways of currency transactions are dying, hence, blockchains and its potential in digital currency, smart contracts, payment processors is huge. Also, with the increase in popularity of blockchains the number of users in the blockchain system is growing. Buying goods, micro transactions is just the beginning of this era in blockchain technology. Integrating mining in mobile phones, enhanced security for wallet handling, and building other applications and services over the blockchain protocol, trading with no boundaries is not an idea anymore, it is a reality.

BIBLIOGRAPHY

[1] Florian Tschorsch, Björn Scheuermann, *Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies*, IEEE Communication Surveys & Tutorials, Vol. 18, NO. 3, 2016.

[2] Yonatan Sompolinsky, Aviv Zohar, *Accelerating Bitcoin's Transaction Processing Fast Money Grows on Trees, Not Chains*, International Association for Cryptologic Research, 2013.

[3] Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, and Robbert van Renesse, *Bitcoin-NG: A Scalable Blockchain Protocol*, USENIX The Advanced Computing Systems Association, 2016.

[4] Rhett Creighton, *Domus Tower Blockchain*, Domus Tower Inc. (DRAFT), 2016

[5] Bellare, M., and Rogaway, P., *Random oracles are practical: A paradigm for designing efficient protocols*.,In Proceedings of the 1st ACM conference on Computer and communications security,1993

[6] Bitcoin community, Bitcoin source, *https://github.com/bitcoin/bitcoin*, Mar. 2015.

[7] Bitcoin community, Protocol rules, *https://en.bitcoin.it/wiki/Protocol_rules*, Sep. 2013.

[8] Bitcoin community, Protocol specification, *https://en.bitcoin.it/wiki/Protocolspecification*, Sep. 2013.

[9] BlockTrail,BlockTrail API, *https://www.blocktrail.com/api/docs#api_data*, Sep. 2015.

[10] Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., and Felten, E. W. ,*Research perspectives on Bitcoin and second-generation cryptocurrencies*, In Symposium on Security and Privacy,2015.

[11] Buterin, V. Slasher, *A punitive proof-of-stake algorithm*, January 2015.

[12]CNNMoney Staff. The Ashley Madison hack in 2 minutes., *http://money.cnn.com/ 2015/08/24/technology/ashley-madison-hack-in-2-minutes*, Sep. 2015.

[13] CoinDesk, Bitcoin venture capital, *http://www.coindesk.com/bitcoin-venture-capital/*, 2015.

[14] Colored Coins Project, Colored Coins. *http://coloredcoins.org/*, Sep. 2015.

[15] Corallo, M. High-speed Bitcoin relay network, *http://sourceforge.net/p/bitcoin/mailman /message/31604935/*, November 2013.

[16] Decker, C., and Wattenhofer R., *Information propagation in the Bitcoin network*.,IEEE P2P (Trento, Italy, 2013), 2013

[17] Decker, C., and Wattenhofer, R., *A fast and scalable payment network with Bitcoin Duplex Micropayment Channels. In Stabilization, Safety, and Security of Distributed Systems* ,17th International Symposium, SSS 2015, Edmonton, AB, Canada, August 18-21, 2015, Proceedings Springer, 2015

[18] Dwork, C., Lynch, N. A., and Stockmeyer L. J, *Consensus in the presence of partial synchrony*, ACM, 1988.

[19] Eyal, I., Birman, K., and van Renesse, R., *Cache serializability: Reducing inconsistency in edge transactions*,35th IEEE International Conference on Distributed Computing Systems, ICDCS, 2015

[20] Eyal, I., and Sirer, *Bitcoin is broken http://hackingdistributed.com/2013/11/04/bitcoin-is-broken/*, 2013.

[21] Eyal, I., and Sirer, *Majority is not enough: Bitcoin mining is vulnerable*, Financial Cryptography and Data Security (Barbados, 2014), 2014

[22] Garay, J. A., Kiayias, A., and Leonardos, N. *The Bitcoin backbone protocol: Analysis and applications. In Advances in Cryptology*, EUROCRYPT 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, So_a, Bulgaria, April 26-30, 2015, Proceedings, Part II , 2015

[23] Garcia-Molina, *Elections in a distributed computing system*, Computers, IEEE Transactionson, 1982

[24] Hearn M., and Spilman, *Rapidly-adjusted (micro) payments to a pre-determined party. https://en.bitcoin.it/wiki/Contract*, 2015.

[25] Heilman, E., Kendler, A., Zohar, A., and Goldberg, S. *Eclipse attacks on Bitcoin's peer to-peer network*, 2015

[26] Kosba, A., Miller, A., Shi, E., Wen, Z., and Papamanthou, C. Hawk, *The blockchain model of cryptography and privacy-preserving smart contracts*, Cryptology ePrint Archive, Report 2015/675, 2015.

[27] Kroll, J. A., Davey, I. C., and Felten, E. W, *The economics of Bitcoin mining or, Bitcoin in the presence of adversaries*, Workshop on the Economics of Information Security (2013).

[28] Lamport, L, *Using time instead of timeout for fault-tolerant distributed systems,*ACM Transactions on Programming Languages and Systems 6, 2 (Apr. 1984), 254{280.

[29] Le Lann, G. *Distributed systems-towards a formal approach*, IFIP Congress (1977), vol. 7, Toronto,2015

[30] Lewenberg, Y., Sompolinsky, Y., and Zohar, A., *Inclusive block chain protocols. In Financial Cryptography*,2015

[31] Litecoin Project,Litecoin, *open source P2P digital currency. https://litecoin.org*, 2014.

[32] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M and Savage, S. A *stful of bitcoins: characterizing payments among men with no names*. Proceedings of the 2013 Internet Measurement Conference, IMC 2013, Barcelona, Spain, October 2013

[33] Miller, A., and Jansen, R. Shadow, *Bitcoin: Scalable simulation via direct execution of multithreaded applications*,IACR Cryptology ePrint Archive, 2015.

[34] Miller, A., and Jr., L. J. J.,*Anonymous Byzantine consensus from moderately-hard puzzles: A model for Bitcoin. https://socrates1024.s3.amazonaws.com/consensus.pdf*, 2009.

[35] Miller, A., Litton, J., Pachulski, A., Gupta, N., Levin, D., Spring, N., and Bhattacharjee, *B. Preprint: Discovering Bitcoins public topology and influential nodes*, 2015.

[36] Moraru, I., Andersen, D. G., and Kaminsky, M. Egalitarian Paxos. ACM Symposium on Operating Systems Principles,2012.

[37] Nakamoto, S., *Bitcoin: A peer-to-peer electronic cash system*. http://www.bitcoin.org/bitcoin.pdf, 2008.

[38] Nayak, K., Kumar, S., Miller, A., and Shi, E. , *Stubborn mining: Generalizing selfish mining and combining with an eclipse attack*. IACR Cryptology ePrint Archive, 2015

[39] Pazmino, J. E., and da Silva Rodrigues, C. K., *Simply dividing a Bitcoin network node may reduce transaction verification time*, The SIJ Transactions on Computer Networks and Communication Engineering (CNCE) 2015

[40] Pease, M. C., Shostak, R. E., and Lamport, L., *Reaching agreement in the presence of faults*, 1980

[41] 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

[42] Poon, J., and Dryja, T., *The Bitcoin Lightning Network*, http://lightning.network/lightning-network.pdf, February 2015

[43] Sapirshtein, A., Sompolinsky, Y., and Zohar A., *Optimal selfish mining strategies in Bitcoin*, 2015

[44] Schneider, F. B., *Implementing fault-tolerant services using the state machine approach: A tutorial*. ACM Computing Surveys 22, 1990

[45] Sompolinsky, Y., and Zohar, A. Accelerating Bitcoin's transaction processing. fast money grows on trees, not chains. In Financial Cryptography, 2015

[46] Sompolinsky, Y., and Zohar, A., *Secure high-rate transaction processing in Bitcoin*, Financial Cryptography and Data Security - 19th International Conference, FC 2015, San Juan, Puerto Rico, 2015

[47] Stathakopoulou, C. ,*A faster Bitcoin network. Tech*, ETH, Zurich, January 2015. Semester Thesis, supervised by C. Decker and R. Wattenhofe, 2015.

[48] Swanson, E., *Bitcoin mining calculator*,http://www.alloscomp.com/bitcoin/calculator, 2013.

[49] The Ethereum community, *Ethereum white paper*, https://github.com/ethereum/wiki/wiki/White-Paper, July. 2015.

[50]Wikipedia. List of cryptocurrencies, https://en.wikipedia.org/wiki/List_of_cryptocurrencies, Oct. 2013.

[51] Ittay Eyal, *The Miner's Dilemma*, 2015 IEEE Symposium on Security and Privacy, 2015

[52] Marko Vukolic, *The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication*, IBM Research – Zurich, 2015

[53]Joseph Poon, Thaddeus Dryja, *The Bitcoin Lightning Network: Scalable Off - Chain Instant Payments* Guidance, 2016

[54] Yoad Lewenberg, Yonatan Sompolinsky, Aviv Zohar, *Inclusive Block Chain Protocols*, Financial Cryptography Conference, 2015

[55] www.blockhain.info/charts

[56] https://developers.coinbase.com/docs/wallet/coinbase-connect/two-factor-authentication

[57] www.blockchain.info/api

[58] Pedro Franco, *Understanding Bitcoin*, Wiley Finance Series, 2015

[59] https://en.bitcoin.it/

CURRICULUM VITAE

Graduate College

University of Nevada, Las Vegas

Sneha Goswami

Degrees:

Bachelor of Technology in Computer Science, 2014

St.Thomas' College of Engineering and Technology

Master of Science in Computer Science, 2016

University of Nevada, Las Vegas

Thesis Title: SCALABILITY ANALYSIS OF BLOCKCHAINS THROUGH BLOCKCHAIN SIMULATION

Thesis examination Committee:

Chair Person, Dr. Yoohwan Kim, Ph.D.

Committee Member, Dr. Ajoy K. Datta, Ph.D.

Committee Member, Dr. Ju-Yeon Jo, Ph.D.

Graduate College Representative, Dr. Venkatesan Muthukumar, Ph.D.