International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 10, No.1 (Jan-2021)

http://dx.doi.org/10.12785/ijcds/100103

Evaluating Quality-of-Service in Blockchains Using Modelling and Simulation Tools

Auqib Hamid Lone[1] and Roohie Naaz[2]

[1]Dept. of CSE NIT Srinagar J&K, India
[2]Professor and Head Dept. of CSE NIT Srinagar J&K, India

Received 14 Feb. 2020, Revised 22 May 2020, Accepted 31 May 2020, Published 1 Jan 2021

Abstract: A Blockchain is a distributed, decentralized and ordered list of special data structures called as blocks, where each block is connected to its previous block by a special pointer called as hash pointer, resulting in an append only system which only grows in size with time. In designing and implementing Blockchain driven systems many decisions about configuration parameters need to be made in advance. However investigation and experimentation on real systems is not feasible. Blockchain simulators help in deciding about best configuration parameters for design and development of Blockchain based solutions before actually building the real solution. Quality of service is an important aspect in any distributed system, so is the case with Blockchain driven systems. Security, Auditability, Transparency, and Tamper resistance are key features of Blockchain. In this paper we collected and defined Quality of Service metrics for Blockchains that drive their key characteristics. We also review and evaluate BlockSim and VIBES as Blockchain simulators to study the effect of Blockchain configuration parameters on Blockchain Quality of Service metrics.

Keywords: Quality of Service, Ethereum, Bitcoin, Consensus, Blockchain

1. INTRODUCTION

A Blockchain is a distributed, decentralized and ordered list of special data structures called as blocks, where each block is connected to its previous block by a special pointer called as hash pointer, resulting in an append only system which only grows in size with time.

In essence Blockchain technology is amalgamation of various technology layers like Peer-to-Peer network, Cryptography, Consensus and Game theory. Blockchain technology's first practical and successful application is Bitcoin cryptocurrency [1]. The motivating force behind the interest in Blockchain research are its key characteristics that provide security, anonymity and integrity without relying on trusted third party organizations. Initially Blockchain usage was restricted to cryptocurrencies only, since the advent of Ethereum: A next generation smart contract and decentralized application platform [2], applications beyond cryptocurrencies are being developed and explored. Smart contract [3] is actually a piece of computer code stored and executed on the Blockchain network. Smart contract defines the conditions and rules on which all parties using contract agrees and actions described in the contract can be executed only if the required conditions are met and rules are followed. As the smart contract is stored on every computer in the network, they all must execute it and get to the same result. The decentralized ledger functionality coupled with security provided by Asymmetric cryptography (Elliptic curve cryptography [4]) and distributed consensus algorithms (Proof of Work in case of Bitcoin and Ethereum [5]) of Blockchain, makes it a very attractive technology to solve the current financial as well as non-financial problems.

Design and development of Blockchain driven systems require proactive decisions about certain configuration parameters, since investigating and experimenting on real infrastructure is not feasible because of cost overhead. Simulators help in modelling and simulation of Blockchains thus help in deciding about best configuration parameters for design and development of Blockchain based solutions before actually building the real solution. Simulators also provide platform for testing new ideas with different scope and sizes of Blockchain and also helps in measurement of various parameters that drive the Blockchain Quality of Service (B-QoS) metrics [6]. Rest of the paper is organized as follows: Section 2 presents Blockchain Quality of Service metrics, Section 3 provides brief description of BlockSim and VIBES, Section 4 presents experimentation and analysis on

E-mail: ahl@nitsri.net, naaz310@nitsri.net

Bitcoin and Ethereum simulations, finally Section 5 concludes the paper.

2. QUALITY OF SERVICE IN BLOCKCHAIN DRIVEN SYSTEMS

QoS is an important aspect in any distributed system and mainly deals with the management of system and network resources to provide performance guarantees. However guaranteeing QoS in Blockchain driven systems is more challenging because Blockchain itself is an amalgamation of different technological layers like Peer-to-Peer Network, Consensus, Cryptography and Game Theory. Each technological layer has a role in driving the B-QoS. In this section we collect and define various parameters that drive QoS metrics in Blockchains. Below are some of the important parameters that help in evaluating the efficiency of Blockchain based systems.

- **ATS (Average Transaction Size):** The average transaction size in Bytes. Larger ATS means block can accommodate less number of transactions as block can't exceed block size limit defined in the Blockchain protocol itself. In case of Ethereum ATS is actually ATC (Average Transaction Cost) in terms of gas (cost of computational task on Ethereum Virtual Machine) as Ethereum block size is limited by block gas limit and determines how many transactions can fit in a block.
- **ABS (Average Block Size):** The average block size in MB. It depends on size and number of transactions selected by a validator/miner for a block which is to be mined. In case of Ethereum ABS is actually ABC (Average Block Cost) as Ethereum has block gas constraint rather than block size.
- **BTP (Block Time Period):** The average time taken by miners/validators to generate a valid block and to commit it to main chain. BTP is extremely important parameter, as it has role in determining the scalability and security of Blockchain systems. Shorter BTP results in more blocks being generated by miners/validators over a time period *t* thus more chances of forks and hence vulnerable to attacks. Larger BTP results in smaller number of blocks being generated by miners/validators over a time period *t* thus severely affects throughput of the system as less number of transactions get processed over a time period *t*.
- **TBM_t (Total Blocks Mined)**: The number of blocks that have been mined over a specific time period *t*. The value of this parameter is directly controlled by BTP. The smaller BTP the larger value of TBM and vice versa.
- **TPB (Transactions per Block):** transaction selection strategy employed by validators/miners for selecting transaction from MemPool and the block limit in terms of size in case of Bitcoin and gas in case of Ethereum. Transaction selection strategy employed by validators/miners for maximizing transaction fee collection is best represented by well-known unbounded 0/1 knapsack problem. Where goal is to :

$$maximize \quad \sum_{txn_i \in MemPool} TxnFee(txn_i) \qquad (1)$$

For Bitcoin

$$subject\ to \quad \sum_{txn_i \in MemPool} Size(txn_i) \leq Block\ Size\ limit$$

For Ethereum

$$subject\ to \quad \sum_{txn_i \in MemPool} gas(txn_i) \leq Block\ Gas\ limit$$

$$i = 1,\ldots,n$$

Where *txn* represent items to fit in the knapsack, transaction size (in case of Bitcoin) and consumed gas (in case of Ethereum) represent weight of items. Optimal solution to equation (1) is a set of transactions that will result in maximum transaction fee collection for miners/validators.

- **TPS (Transactions per Second):** In Blockchain terminology this is also called throughput and is defined as the number of transactions that are successfully executed and recorded in Blockchain over a time period of one second.

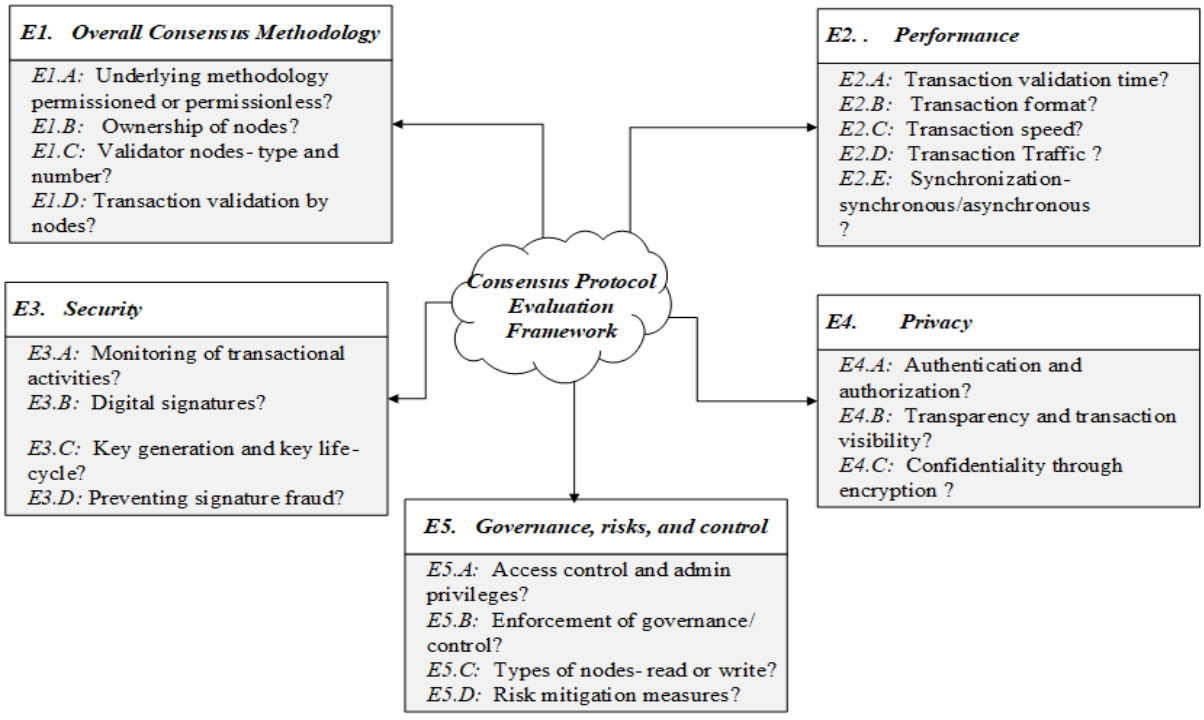

Figure. 1. Basic Consensus Evaluation Framework

- **MpS (Mempool Size):** The aggregate number of transactions waiting to be mined and get locked in Blockchain. New unconfirmed transactions are broadcasted on peer to peer network are collected by the validators/miners in Mempool for mining new blocks.
- **CPC (Consensus Protocol Characteristics):** Key characteristics of consensus mechanism used by Blockchains. Consensus protocols are heart and soul of Blockchains as they help in building trust among untrusted parties. Figure 1 presents key characteristics and what features to look for under each characteristic of consensus protocols. Seeking answers to questions in evaluation framework provides a broader measurement about B-QoS.
- **SW_t (System Workload):** Total number of transactions send over a time period *t*. This parameter is important as higher SW can hamper the scalability of the system in order to meet the system requirements.
- **TBS_t (Total Blockchain Size):** Total size of Blockchain at any given time period *t*. Blockchain size heavily depends on the workload of the system, which in turn depends on many different factors like block size limit (in case of Bitcoin) /block gas limit (in case of Ethereum) and block time period . Total size of the Blockchain TBS_t at time t can be approximated by the following equation:

$$TBS_t = S(TBM_t) \quad (2)$$

Where $S(TBM_t)$ represents total size of all blocks mined over a time period of t. Since size of each block comprises of its block header size and sum of sizes of all transactions inside a block. if $M_t(txn)$ is set of transactions included in the Blockchain at time *t*, H_s is the header size of the single block, then size of the Blockchain TBS_t at time *t* can be approximated by the following equation:

$$TBS_t = \frac{t}{T} * H_s + \sum_{\substack{txn_i \in M_t(txn) \\ i=1,..,n}} S(txn_i) \quad (3)$$

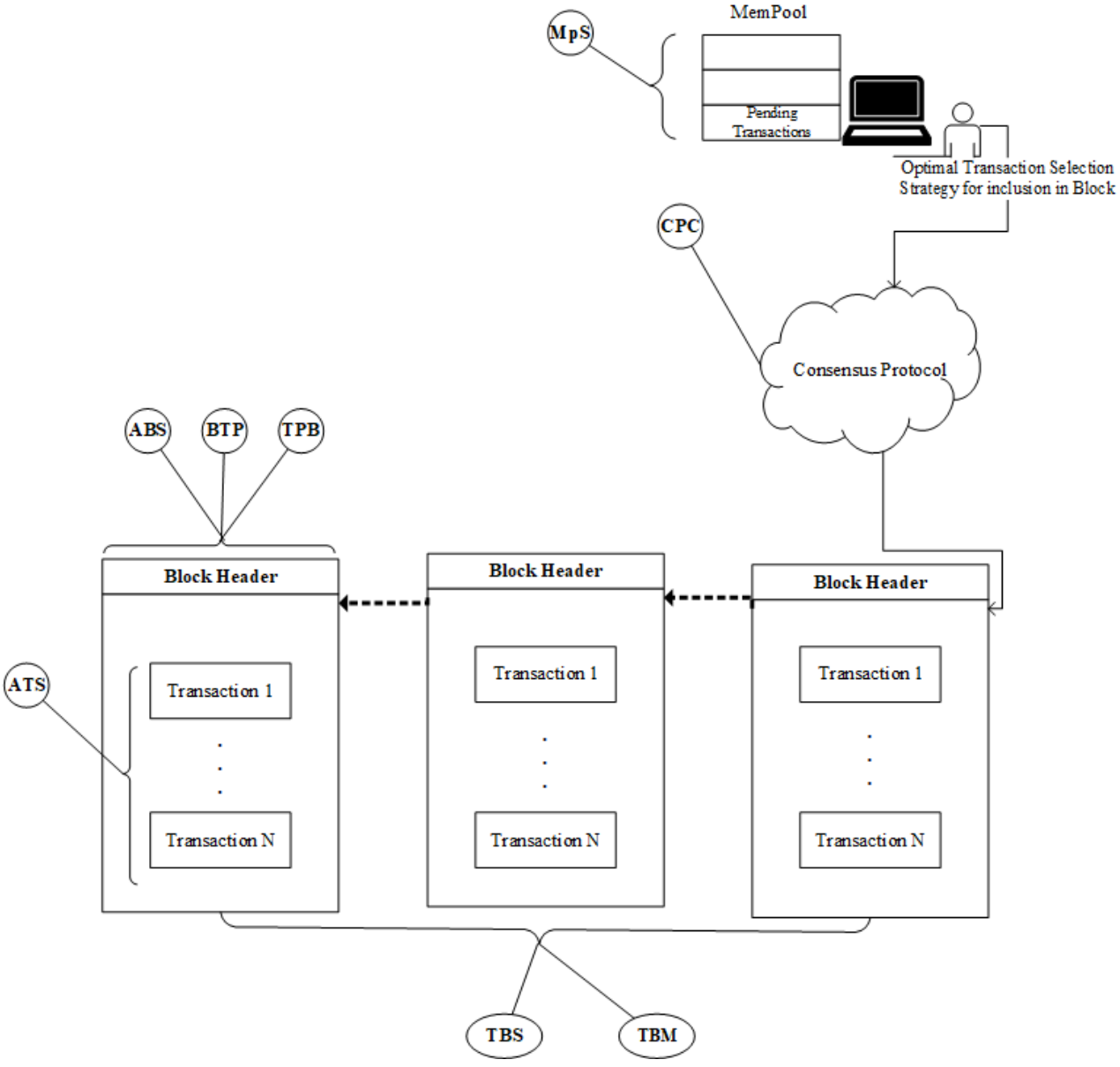

Figure 2. Parametric view of Blockchain at Miner/Validator for determining B-QoS

Where *S(txn)* is size of the transaction. Since block creation rate is constant, with new block being generated after every T units, thus equation (3) can be rewritten as:

$$TBS_t = TBM_t * H_s + \sum_{\substack{txn_i \in M_t(txn) \\ i=1,..,n}} S\,(txn_i) \quad (4)$$

Figure 2 represents the parametric view of Blockchain at validator/miner. Blockchain parameters that drive its QoS should be appropriately configured in order to achieve balanced mix of security and performance.

The factor $TBM_t * H_s$ is the total overhead due to block headers in the Blockchain at time *t*, thus equation (4) can be rewritten as:

$$TBS_t = H_o + \sum_{\substack{txn_i \in M_t(txn) \\ i=1,..,n}} S\,(txn_i) \quad (5)$$

Where H_o represents total overhead due to headers in the Blockchain at time *t*.

3. BLOCKSIM AND VIBES AS BLOCKCHAIN SIMULATORS

In this section we present brief overview of BlockSim and VIBES Blockchain simulators with focus on their strengths and limitations in terms of their capabilities for modelling and simulating both public and private Blockchains.

A. BlockSim: BlockSim [7] is discrete event dynamic system simulation framework for modelling and simulation of Blockchain protocols. It was developed mainly with a purpose to provide assistance in exploring design trade-offs in implementing and evaluating existing or new Blockchains. BlockSim also helps in exploring different configuration parameters and their effect on the behaviour of Blockchain systems. Currently, BlockSim supports only 2 models to simulate Bitcoin and Ethereum.

BlockSim Components: BlockSim comprises of six main components namely 1) Discrete Event Simulation Engine 2) Simulation World 3) Transaction and Node Factory 4) Programmatic Interface and simulation Example 5) Monitor and Reports and 6) Blockchain Modelling Framework.

1. Discrete Event Simulation Engine: BlockSim uses Python based Discrete Event Simulation Engine, called SimPy. SimPy simulates real world processes using Python based Generator functions for representing asynchronous systems. Generator functions allow processes to exit at some point in time and later re-enter and start from the point of last exit, thus allowing processes to alternate execution between each other. Discrete Event Simulation Engine provides the functionalities like scheduling, queuing and processing of events, communication among components, simulation clock management and controlling access to object resources by subjects.

2. Simulation World: This component is responsible for handling input configuration parameters necessary for the simulation. BlockSim uses 1) configuration file for configuring Blockchain model being simulated and node locations. 2) Delays file for configuring delays incurred due to transaction validation and block time period. 3) Latency file for configuring latency among nodes at different locations. 4) Throughput received and sent files for configuring sent and received throughput between nodes at different locations. Configuration files used by Simulation World component of BlockSim are measured with iPerf3 bandwidth measurement tool and modelled using Kolmogorov-Smirnov test to obtain best probability distribution for simulation purposes.

3. Transaction and Node Factory: This component is used to generate nodes and transactions for simulation. Transactions are created in batches and broadcasted by a random node from nodes list generated by nodes factory of BlockSim. Users can specify number and location of nodes.

4. Programmatic Interface: This component allows users to simulate different Blockchains. It is also responsible for triggering simulation.

5. Monitor and Reports: This component captures the metrics during simulation and writes that as a report file. Simulation report contains important results like number of transactions and blocks broadcasted by each node, propagation time for block and transaction etc.

6. Blockchain Modelling Framework: BlockSim provides ability to simulate any arbitrary Blockchain by considering layered architecture for simulation. Essentially BlockSim considers Node layer for specifying operations and roles for nodes when being part of peer-to-peer network, Consensus layer for specifying rules of the consensus protocol, Ledger layer for specifying data structure of the ledger, Transaction and block layer for specifying how information is represented and transmitted, Network layer for specifying how nodes communicate and behave on peer-to-peer to network and Cryptographic layer for defining what cryptographic primitives will be used.

BlockSim offers flexibility to users for modelling and simulating any variant of Blockchain with minimal hardware, however it depends on hard-coded configuration parameters that need to be measured with other tools. Furthermore transaction gas limit could be set to include gas cost for storage also in order to simulate the behaviour of smart contracts. Other possible improvement will be to implement actual account based Ethereum model within BlockSim to further improve simulation results.

B. VIBES: Visualizations of Interactive, Blockchain, Extended Simulations (VIBES) [8] is a blockchain simulator for large scale peer-to-peer networks. VIBES is configurable in nature thus allowing users to explore important characteristics and metrics of the Blockchain network essential for determining QoS. VIBES is fast blockchain simulator and offers large-scale simulations with thousands of nodes. VIBES was developed with an aim to provide scalable and fast simulation environment for Blockchain users to evaluate and identify bottlenecks, and improve applications of blockchains. VIBES achieves scalability and speed by utilizing the concept of fast forward computing and co-ordination between orchestrator and reducer components. VIBES allows users to play with input configuration parameters which include: latency, bandwidth, number of nodes, number of neighbors, block size, block confirmation time, transaction size, maximum block size, transaction propagation delay. The simulator outputs the following metrics: simulation duration, Blockchain length, average block time, total number of transactions processed, throughput (transactions per second), and probability of a successful attack. The output metrics provide Blockchain users enough information to make educated decisions. VIBES also provides simulation environment for performing double spend and flooding attacks on the Blockchain network. The strength of VIBES lies in its easy to use and configuration interface and fast and scalable simulation environment. However it is less flexible in providing support to simulate any arbitrary Blockchain type.

4. EXPERIMENTATION AND ANALYSIS

We performed modelling and simulation of Ethereum using BlockSim and Bitcoin using VIBES, as they provide flexibility in playing with configuration parameters of respective Blockchains. Furthermore VIBES also provide simulation environment for launching attack against Bitcoin network [9]. The goal of experiments is to simulate Bitcoin and Ethereum for studying their QoS metrics. All experiments were conducted on a PC with 2.70 GHz Intel Core i7 processor and 32GB RAM.

A. Simulation of Ethereum using BlockSim

We simulate Ethereum Blockchain using BlockSim mainly to study effect of various parameters (Block size, Gas limit) on block propagation time,
Blockchain size and length. BlockSim requires input configuration files to simulate and analyze behaviour of any Blockchain. Input configurations for modelling and simulating Ethereum Blockchain is listed in Table I. For ease and simplicity we have taken same input parameters as used by developers of BlockSim about node locations (Latency and Throughput). In order to understand simulations better we considered two nodes only one miner and other non-miner. We set transaction gas limit to 21,000 during all execution runs, but varied block gas limit from 2.1 million to 8.4 million. We also set simulation time equal to 1 minute, which results in generation of 3 blocks. Simulation results are presented in Table II. Simulation results depict that increasing workload has lesser impact on block propagation time. We also observed that encryption has substantial impact on block propagation time.

TABLE I. INPUT CONFIGURATION FOR BLOCKSIM

Input Configuration	Distribution	Location	Scale
Block Validation Delay	Log-Normal	0.229 s	0.002 s
Transaction Validation Delay	Log-Normal	0.004 s	0.00005 s
Block Period	Normal	15.79 s	3.00 s

TABLE II. SIMULATIONS RESULTS IN BLOCKSIM

Transaction Gas Limit	Block Gas Limit	Transactions Per Block	Block Size	Average Block Propagation Time
21000	2100000	100	20.045 KB	1012.499968 ms
	4200000	200	40.045 KB	1020.200014 ms
	6300000	300	60.045 KB	1024.899721 ms
	8400000	400	80.045 KB	1035.799742 ms

B. Simulation of Bitcoin using VIBES

We simulate Bitcoin Blockchain using VIBES mainly to study effect of various parameters on block propagation time, Blockchain size and length. We also studied effect of attacker's hash rate on successfully launching double spend attack against the Bitcoin network. Input configurations for simulating double spend attack against Bitcoin is depicted in Table III and results are reported in Table IV.

TABLE III. INPUT CONFIGURATION FOR VIBES

No. of Nodes	No. of Neighbors	Block Period	Transaction Size	Latency	Transaction Propagation Delay	Block Size Limit	Network Bandwidth
20	4	600 s	1000 Bytes	900 ms	150 ms	50000 Bytes	1 MBps

From Figure 3 it is evident that with attacker gaining more hash power probability of attack being successful increases rapidly. Once hash power crosses 50% probability of attack being successful becomes 100% thus proving the fact that 51% network hash power can break the whole purpose of Bitcoin functionality. But achieving such hash power is not practically possible unless miners unite, furthermore Bitcoin is designed in such a way, that it is beneficial for miners to support network rather going against it.

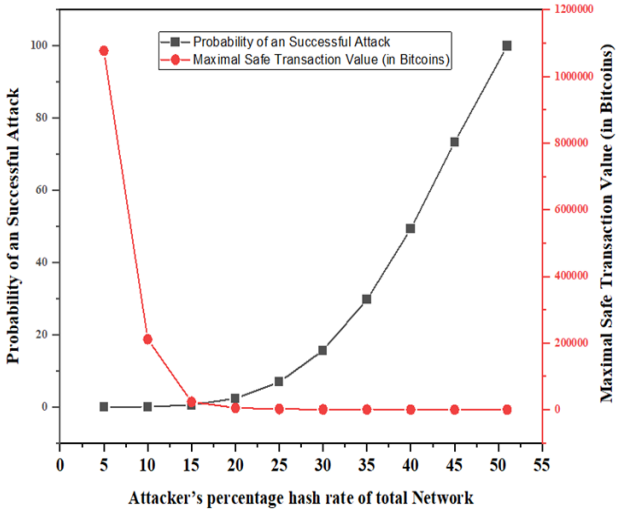

Figure 3. Attack simulation summary based on attacker's hash power

Also, with rise of attacker's hash power, maximum value of transaction (in Bitcoins) that can be securely performed on Bitcoin network decreases sharply and reaches to 0 once attacker gains more than 50% of total hash power of the network.

TABLE IV. ATTACK SUMMARY

Simulation Attack Summary	Attacker's percentage hash rate of total Network									
	5%	10%	15%	20%	25%	30%	35%	40%	45%	51%
Simulation Duration (in Seconds)	10	10	10	11	15	11	16	13	16	13
Average Block time (in Seconds)	601	783	849	847	551	1089	476	931	593	558
Blockchain Length (in Blocks)	33	27	25	25	38	19	34	22	33	36
Attack Duration (in Blocks)	50	50	50	50	50	50	50	50	50	50
Probability of an Successful Attack	0.001	0.059	0.521	2.331	6.866	15.645	29.737	49.3	73.375	100
Maximal Safe Transaction Value (in Bitcoins)	1077328	211233	23398	5237	1695	637	295	128	45	0
Minimum Wasted Blocks due to Attack (in Blocks)	2	1	2	4	7	13	9	15	16	6

5. CONCLUSION

In this paper we presented and defined various Blockchain configuration parameters that drive Blockchain Quality of Service. We presented problem of optimal transaction selection strategy from Mempool for maximizing transaction rewards for both Bitcoin and Ethereum validators/miners. We also provide basic framework setup for evaluating consensus protocol characteristics. For modelling and simulating Bitcoin we used VIBES and for Ethereum we used BlockSim. While simulating Ethereum using BlockSim we observed block

size has less impact on Block propagation time compared to encryption. In simulating Bitcoin using VIBES we observed growth in attackers hash power results in higher probability of success in launching double-spending attack in Bitcoin network. While evaluating BlockSim and VIBES we observed that they require to be more flexible in mimicking exact behavior of Blockchains for providing better evaluation.

REFERENCES

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

[2] V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform, 2013," URL {http://ethereum. org/ethereum. html}, 2017.

[3] N. Szabo, "The idea of smart contracts," Nick Szabo's Papers and Concise Tutorials, vol. 6, 1997.

[4] H. Mayer, "Ecdsa security in bitcoin and ethereum: a research survey," CoinFaabrik, June, vol. 28, p. 126, 2016.

[5] A. Gervais, G. O. Karame, K. Wust, V. Glykantzis, H. Ritzdorf," and S. Capkun, "On the security and performance of proof of work blockchains," in Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. ACM, 2016, pp. 3–16.

[6] B. Wang, S. Chen, L. Yao, B. Liu, X. Xu, and L. Zhu, "A simulation approach for studying behavior and quality of blockchain networks," in International Conference on Blockchain. Springer, 2018, pp. 18–31.

[7] C. Faria and M. Correia, "Blocksim: Blockchain simulator," in 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019, pp. 439–446.

[8] L. Stoykov, K. Zhang, and H.-A. Jacobsen, "Vibes: fast blockchain simulations for large-scale peer-to-peer networks," in Proceedings of the 18th ACM/IFIP/USENIX Middleware Conference: Posters and Demos. ACM, 2017, pp. 19–20.

[9] F. Schussler, P. Nasirifard, and H.-A. Jacobsen, "Attack and vulnerability simulation framework for bitcoin-like blockchain technologies," in Proceedings of the 19th International Middleware Conference (Posters), 2018, pp. 5–6.

Auqib Hamid Lone I did my Bachelors in Information Technology and Engineering with distinction, post my B. Tech my interest and passion towards information security took me into masters and I completed M. Tech in Information Security & Cyber Forensics from Jamia Hamdard University, New Delhi with first rank. Currently I am Research Scholar at NIT Srinagar J&K. My areas of interest are Blockchain, Cryptography, Network Security, Web Application Security and Digital Forensics

Roohie Naaz Mir is a Professor & HoD in the Department of Computer Science & Engineering at NIT Srinagar, INDIA. She received B.E. (Hons) in Electrical Engineering from University of Kashmir (India) in 1985, M.E. in Computer Science & Engineering from IISc Bangalore (India) in 1990 and Ph.D from University of Kashmir, (India) in 2005. She is a Fellow of IEI and IETE India, senior member of IEEE and a member of IACSIT and IAENG. She is the author of many scientific publications in international journals and conferences. Her current research interests include reconfigurable computing and architecture, mobile and pervasive computing, security and routing in wireless adhoc and sensor networks