MODELING OF BLOCKCHAIN BASED SYSTEMS USING QUEUING THEORY SIMULATION

RAHEEL AHMED MEMON[1,2], JIANPING LI[1], JUNAID AHMED[2], ASIF KHAN[1], M. IRSHAD NAZIR[2], M. ISMAIL MANGRIO[2]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology, China
[2]Sukkur IBA University, Sindh, Pakistan
E-MAIL: raheelmemon@iba-suk.edu.pk, jpli2222@uestc.ac.cn

Abstract:

Blockchain is the one of leading technology of this time; it has started to revolutionize several fields like, finance, business, industry, smart home, healthcare, social networks, Internet and the Internet of Things. It has many benefits like, decentralized network, robustness, availability, stability, anonymity, auditability and accountability. The applications of Blockchain are emerging, and it is found that most of the work is focused on its engineering implementation. While the theoretical part is very less considered and explored. In this paper we implemented the simulation of mining process in Blockchain based systems using queuing theory. We took the parameters of one of the mature Cryptocurrency, Bitcoin's real data and simulated using *M/M/n/L* queuing system in JSIM*graph*. We have achieved realistic results; and expect that it will open up new research direction in theoretical research of Blockchain based systems.

Keywords:

Blockchain simulation; Queuing theory for blockchain; Blockchain using jsimgraph; Bitcoin queuing simulation

1. Introduction

Cryptocurrency is emerging as a diverse community with the market capital of billions of US Dollars as of November 2018[1]. The first introduced digital currency Bitcoin has historical and most valuable coin of the time. This paradigm shift of digital currency is unstoppable[2]. Today's most mature digital currency is Bitcoin; maybe tomorrow we have different type of currency, but it is fact that digital currency has started to revolutionize the financial transactions in decentralized manner without any third party involvement.

Blockchain, which is underlying technology of Bitcoin, maintains a distributed ledger across the Peers of Peer-to-Peer (P2P) network as a database of blocks. Each block has a cryptographic signature or Hash as a reference point. A block in Blockchain has reference to its previous block, and all blocks create a chain by referencing to their prior block up to the genesis block (first block), which has no previous block reference[3]. Once the block is added to Blockchain, any change in block is impossible, because the cryptographic hash would alter and it will disturb the entire chain [4]. In the Bitcoin's Blockchain network, there are three types of nodes: (1) Wallet Nodes, which are available as a client to send or receive transactions (2) Mining Nodes, nodes with Mining power to performs the computational work for finding the correct hash of new block (3) Hybrid Nodes, nodes that work as both; client and mining nodes.

Finding the hash of any new block is not easy task, the mining nodes usually perform this task in groups also known as Mining Pools, a block can be mined by more than one mining pools but the mining pool who finds the correct hash first, will receive a remuneration as a reward of the good work. This reward is halved every 210,000 blocks mined (or after 4 years) [5]. In start the reward was 50 Bitcoins (BTC), there have been two halving of reward until now: first $50/2 = 25 \text{ BTC}$ in 2012, and second $25/2 = 12.5 \text{ BTC}$ in 2016 and the third will be in 2020 [6]. The miners get paid extra for the operations performed by them because it is the most challenging task, and by solving the challenging puzzle, miners are contributing to secure the Blockchain network by powerful computers.

Currently Blockchain is the one of the most popular subject discussed in research community[7–11]. The Blockchain has impact on not only finance but also greatly shifting the operations takes place in: business, industry, transportation, health care, smart homes, Internet of Things etc [12–16]. As Don Tapscott, The CEO of Tapscott Group, which is the world's leading authorities on the impact of technology on business and society said that: "*What if there was not just an internet of information but an internet of value? Assets can be transferred for the first time peer-to-peer without an intermediary. This is 'Blockchain'. It represents the fourth industrial age and will change the*

978-1-7281-1536-8/18/$31.00 ©2018 IEEE

nature of corporations"[17]; Thus the Blockchain has the real influence over technology, thus the potential of Blockchain for further applications continues to grow.

However, it is essential to know the assessment methods of Blockchain, working on the theory part of Blockchain, to observe its behaviors will enable the community to reveal the most influential parameters of the system. Currently, there is very less work (or no work) is done on the theory part of Blockchain, like; its optimization, analysis, simulation of system, tuning the parameters, finding relationship in between the parameters is very necessary and will reveal most critical parts of Blockchain based systems.

In this paper we develop the queuing theory simulation of mining operation, which is the most costly, time-consuming and essential part of Blockchain. Such simulation of Blockchain is necessary in performance analysis and optimization of Blockchain technology before adoption. We simulate the mining operation using single *M/M/n/L* queue in Java Modeling Tool JSIM*graph* [18], and obtained the results of Utilization of mining nodes, system performance and number of transactions included per block.

The rest of the paper is arranged as: Section II presents the background on working of Blockchain technologies, Section III is about the simulation setup and parameters used for Blockchain, Section IV presents the results before concluding in Section V.

2. Background

The Bitcoin maintains a publically distributed ledger of transaction blocks known as Blockchain, where each node has its own copy of the ledger and the network is widely distributed in decentralized manner[3]. Fig.1 shows the example of Blockchain P2P network where the gray nodes are the Wallet Nodes, and White Nodes are the Mining Nodes. We categorized this on functionality basis here, because the hybrid node, which is third type of node, as discussed in section I, is also performing any of these two functionalities at a given time.

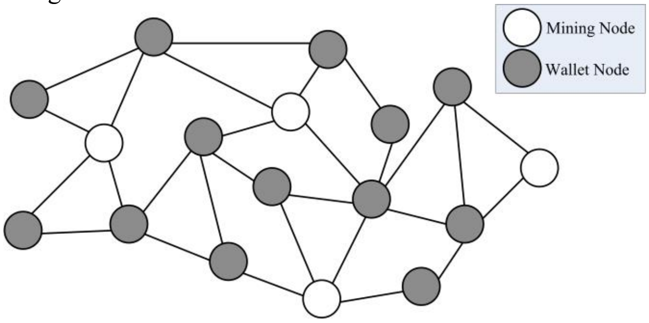

Fig.1 Blockchain Network of Bitcoin

The transactions in Bitcoin are trusted and verifiable by all the nodes of network and a fearless deal can take place even between unknown parties[19]. Blockchain is a list type dataset of data blocks in a distributed order where no one holds the command to alter because of inherited encryption attached with every block. It is almost impossible to break the chain of blocks or to modify any content due to its robust design except the clock which is needed for time stamping [20].

In Bitcoin, person A wants to send a fraction of BTC to person B. Person A initiates the transaction, and person B received BTCs transferred by person A, but it remains unconfirmed transaction until it is verified against double spending and other evil activities. The transactions are grouped together and verified by the mining nodes as a block. Mined blocks are further confirmed by other nodes in network to reveal validity, this process is known as consensus; where all the nodes verify that the transaction is not fake. Once the consensus is obtained the person A's Transaction is confirmed. Theoretically this process should take 10 Minutes[3], but practically it takes hours to days because of large number of pending transactions already available in memory pool. Fig.2 shows the mining process flow inside a miner.

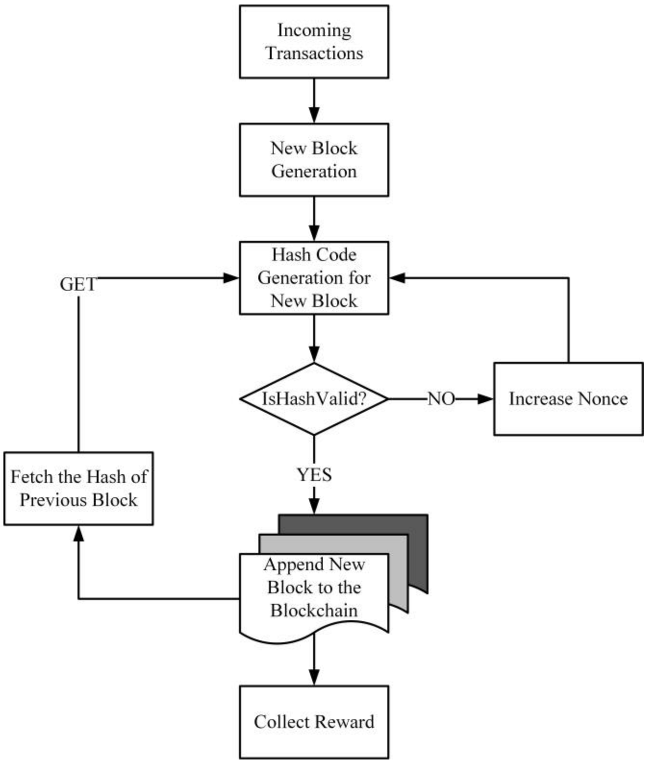
Incoming Transactions
New Block Generation
Hash Code Generation for New Block
GET
IsHashValid?
NO
Increase Nonce
YES
Fetch the Hash of Previous Block
Append New Block to the Blockchain
Collect Reward

Fig.2 Working of a Mining Node

i. Block Generation:

The miner(s) can choose the transactions and assemble them in a group as block at the specified interval of 10 minutes, it means in 24 hours there could be maximum number of 144 blocks[21]. The block is consists of five elements: Block Id, hash of current block, hash of previous block, timestamp and transactions detail such as: Sender Address, Receiver Address, and amount to Transfer[21].

ii. Mining Process:

Once the miner picks the transactions and assembles them into block the countdown timer starts. The miner has to perform three tasks, (a) Discovery of correct hash, (b) issues new BTCs in the economy (c) Consensus[3].

a) Discovery of correct Hash: Finding the hash is most significant part in the mining process in Bitcoin, the miner tries to iterate through the nonce to find a correct combination, which verifies the Target value[22]. The Generation of Hash is shown in equation 1:

$$Hash(String + Nonce) < Target \qquad (1)$$

Where, String representing the recent transaction, Target is the Target Value to found, Hash is the Bitcoin's hash function (SHA256), Nonce is a number, and symbol "+" represents concatenation operation. Once the correct nonce is found, the miners broadcast the new block and its nonce as his Proof-of-Work (PoW) to the network, and add it to the local Blockchain Ledger[22].

b) New Bitcoins in the Economy: In Bitcoin Blockchain there is a race in between the miners, the one who finds the correct target hash first add it to its local Blockchain and broadcast the nonce and new block to the network, will receive the reward and the *coinbase*. A *coinbase* is a fraction of BTC as a transaction fees which is deducted from the user account [23]. And reward is addition of new Bitcoins in the economy; as stated in section I, the reward is halved every 4 years or when 210,000 Blocks are mined. Currently reward for mining a Block is 12.5, and every day 144 blocks are mined, which means every day 1800 New BTC are released to the Bitcoin economy[24].

c) Consensus: The other nodes in network receive the block and its exact nonce to find the correct hash value. If hash is valid with its nonce, the consensus is achieved and transactions get stored as a block in their local Blockchain. But if it is invalid, the block is refused and discarded from all nodes[3].

3. Simulation Setup:

The simulation of Mining process in Bitcoin is done in JMT JSIM*graph*[18]. It is an open source toolkit developed in JAVA for performance evaluation and workload characterization of computer and communication systems based on queuing system[25]. For simplicity, we took the statistics from (www.blockchain.info) to simulate one-day transactions of real Bitcoin currency. Calculating the average number of transactions per block (Tx_B) can be obtained by:

$$Tx_B = \frac{Tx_{Day}}{144} \qquad (2)$$

Where TxDay is the number of transactions in a day and 144 is the number of blocks per day, which is standard. The size of a block is: And the Total Mining Power is:

$$M_{Total} = \sum_{nodes \in System} M(i) \qquad (3)$$

Where $M(i)$is the mining power of node i. And the Number of Transactions per second is:

$$Tx_{Sec} = B_{freq} \times Tx_B \qquad (4)$$

Where Bfreq is the number of blocks per minute.

The simulation of Blockchain is done in JSIMgraph as shown in Fig.3, where there is single queue and a number of miners, according to Kendall's notations it is *M/M/n/L* queuing model. The queue capacity is set as the Tx_B, queue policy is First Come First Serve (*FCFS*) and the drop rule is Block After Service (*BAS*), which means that only the transactions for the size transactions of a block Tx_B remains on the heap memory of the mining nodes, while the other transactions even if processed are resting in the Memory-Pool (Mempool).

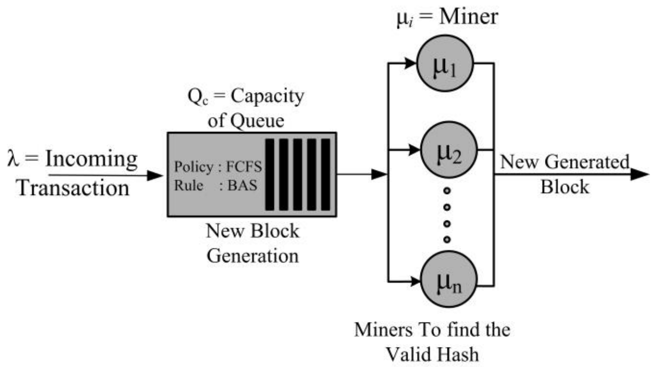

Fig.3 M/M/n/L Mining Queue in Bitcoin

The data for simulation was collected from the website (www.blockchain.info). On 17 November 2018, the numbers of transactions were 271,921 and the total hash rate was 47,956,936. Thus the calculated parameters for simulation are as given in table 1.

Table 1 Simulation Parameters

Parameter	*Value*
Transactions Arrival Rate	1900 (Poison Arrivals)
Mining Process (mean)	344 (λ=0.002994011976)
Queue Capacity (Q_c)	3000
Queue Policy	FCFS
Drop Rule	Block After Service (BAS)

Number of Miners	1000
Miner Strategy	Load Independent
Seeds	144

The total mining power is derived from the equation 3, and is further distributed into number of miners in the overall system. We assumed that there are 1000 miners, though in real, the number of miners is far more than that but we distributed mining power in 1000, thus it has no impact on the simulation results.

4. Results

The one-day traffic of Bitcoin in Blockchain network is measured through the simulation; the performance metrics are derived using queuing theory of M/M/n/L. Fig.4 shows the number of transactions in 144 blocks of a day. Where the minimum number of transactions in a block is 1640 and maximum is 2217.

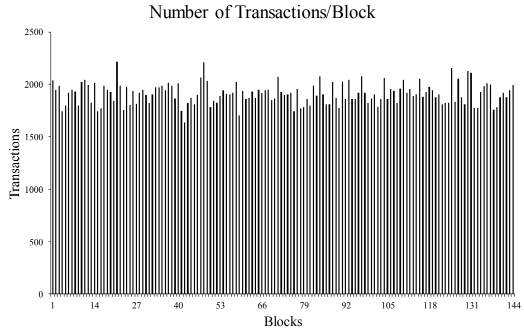

Fig.4 Number of Transactions per Block

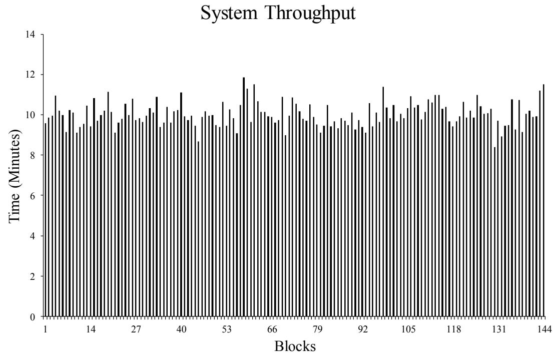

Fig.5 Block Generation and Mining Time of System

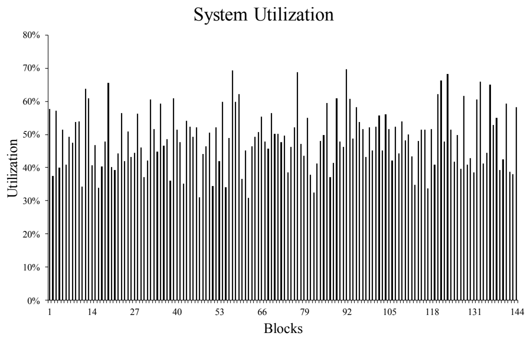

Fig.6 Utilization of Mining Resources by each Block

The generation of block is shown in Fig.5, where the minimum time spent by system to generate a block is 08 minutes and 40 seconds and maximum time taken for a block generation is 11 minutes and 51 seconds. The Utilization of available Mining power per block is shown in Fig.6, where the minimum utilization was 31% and maximum was 70%.

5. Conclusion

The simulation of any system is the key to correctly indicate the working behavior of a system. However, such type of work for Blockchain based systems very little or not available. In this paper we simulated the Blockchain mining process in Bitcoin digital currency to discover performance indices of one-day transactions in the system. We found that per block the number of transactions is in between 1640 to 2270. The mining time per block is in between 8 minutes and 40 seconds to 11 minutes and 51 Seconds. The utilization of mining power by each block is predicted in between 31 and 70%. The results achieved through simulation are realistic. Although, the presented model is simulating basic rules of Blockchain; but it will open up a new research direction of queuing theory for Blockchain based systems.

Acknowledgments

This paper was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province, and Chengdu Civil-military Integration Project Management Co., Ltd.

References

[1] “The most trusted source for data on the bitcoin blockchain.” [Online]. Available:

https://www.blockchain.com. [Accessed: 19-Nov-2018].

[2] A. Tapscott and D. Tapscott, “How Blockchain Is Changing Finance,” Harv. Bus. Rev., no. March, pp. 2–5, 2017.

[3] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Www.Bitcoin.Org, p. 9, 2008.

[4] R. MICHAEL J.W., C. ALAN, and R. B. JARED, “BLOCKCHAIN TECHNOLOGY AND REGULATORY INVESTIGATIONS,” 2018.

[5] M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan, “On the Instability of Bitcoin Without the Block Reward,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS’16, 2016, pp. 154–167.

[6] M. Belotti, S. Kirati, S. S.-I. RTSI, and U. 2018, “Bitcoin poolhopping detection,” www-phare.lip6.fr.

[7] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, vol. 4, no. , pp. 2292-2303, 2016.,” IEEE Access, vol. 4, pp. 2292–2303, 2016.

[8] M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” Futur. Gener. Comput. Syst., pp. 1–17, 2017.

[9] M. Singh and S. Kim, “Blockchain Based Intelligent Vehicle Data sharing Framework,” Jul. 2017.

[10] S. Underwood, “Blockchain beyond bitcoin,” Commun. ACM, vol. 59, no. 11, pp. 15–17, 2016.

[11] “Blockchain for the Internet of Things (White Paper) - RICHTOPIA.” [Online]. Available: https://richtopia.com/white-papers/blockchain-internet-things. [Accessed: 09-Mar-2018].

[12] A. Bahga and V. K. Madisetti, “Blockchain Platform for Industrial Internet of Things,” J. Softw. Eng. Appl., vol. 09, no. 10, pp. 533–546, 2016.

[13] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, “When Mobile Blockchain Meets Edge Computing,” 2017.

[14] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT security and privacy: The case study of a smart home,” 2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. (PerCom Work., pp. 618–623, 2017.

[15] R. Memon, J. Li, J. Ahmed, A. A. Memon, M. I. Nazeer, and M. Ismail, “TSAN: Backbone network architecture for smart grid of P.R China,” Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 1, 2018.

[16] L. Sun, Y. Li, and R. A. Memon, “An open IoT framework based on microservices architecture,” China Commun., vol. 14, no. 2, pp. 154–162, 2017.

[17] D. Tapscott, “Blockchain Revolution the Internet of Value,” Insight Invest., 2018.

[18] M. Bertoli, G. Casale, and G. Serazzi, “JMT Performance Engineering Tools for System Modeling,” ACM SIGMETRICS Perform. Eval. Rev., vol. 36, no. 4, p. 6, 2009.

[19] N. Kshetri, “Blockchain’s roles in strengthening cybersecurity and protecting privacy,” Telecomm. Policy, vol. 41, no. 10, pp. 1027–1038, 2017.

[20] N. Kshetri, “Can Blockchain Strengthen the Internet of Things?,” IT Prof., vol. 19, no. 4, pp. 68–72, 2017.

[21] P. Franco, Understanding Bitcoin: Cryptography, Engineering and Economics. 2015.

[22] D. Malone and K. J. O’Dwyer, “Bitcoin Mining and its Energy Footprint,” in 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communities Technologies (ISSC 2014/CIICT 2014), 2014, pp. 280–285.

[23] M. Möser, R. Böhme, and D. Breuker, “An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem.”

[24] M. Jabłczyńska, K. Kosc, P. Ryś, and R. Ślepaczuk, “Why you should not invest in mining endeavour? The efficiency of BTC mining under current market conditions,” 2018.

[25] S. El Kafhali and K. Salah, “Performance analysis of multi-core VMs hosting cloud SaaS applications,” Comput. Stand. Interfaces, vol. 55, pp. 1339–1351, 2018.