Proceedings of 12th IOE Graduate Conference
Peer Reviewed
ISSN: 2350-8914 (Online), 2350-8906 (Print)
Year: 2022 Month: October Volume: 12

Small World Network for Simulation of Blockchain Networks

Prabin Kayastha [a], Basanta Joshi [b]

[a, b] *Department of Electronics and Computer Engineering, Pulchowk Campus, IOE, Tribhuvan University, Nepal*
[a] 076mscsk007.prabin@pcampus.edu.np, [b] basanta@ioe.edu.np

Abstract

To understand the behavior of a blockchain system whether during the design or in the analysis, different simulators are used by enthusiasts and researchers to mimic the characteristics of the real blockchain technology in the Blockchain Under Test(BUT). Many blockchain simulation frameworks have been proposed and are being used for these use cases. However, most of the existing simulation frameworks seem to be focused only on certain layers of the blockchain system, usually in the consensus layer of the system. Almost all simulation systems seem to have overlooked the topology of the participating nodes on the overall behavior of the system as they use some deterministic functions to characterize the network behavior assuming that the topology is always holistic. This results in the wrong input parameters being fed to the subsequent building blocks in the simulation framework and thus yielding sub-par overall results. Recent studies suggest that the nodes of the blockchain system demonstrate certain small-world properties instead of being holistically linked. Small-World Networks show distinctive characteristics of having small average path lengths and high clustering coefficients. These characteristics help the information to be propagated within a fewer number of hops across the network.

This paper presents a state-of-the-art approach to effectively formulate the node topology design in a blockchain simulation system using Small World Networks approximation. This design yields a more realistic simulation of the network nodes and the upstream layers of BUT simulation. Simulations for various blockchains such as Bitcoin and Ethereum can be done with this simulator for various configurations.

Keywords

Blockchain, Simulation, Small-World Networks, Topology

1. Introduction

Growing applications of blockchain to fulfill the need for the distributed and transparent immutable ledger for storing the transactions and information within them by establishing trust within non-trusting entities has opened up a wide area for research and development within the blockchain industry. The complexity of mining valid blocks whilst maintaining trust by reaching global consensus and luring the miners to be part of the system for a long time has been some of the fundamental bottlenecks for the development and analysis of blockchain technologies.

One way to overcome such obstacles is by the means of simulation where the test environment is created to mimic the behavior of the real system using some mathematical formulation of underlying layers of the system. This architectural design and its driving parameters and configurations play a crucial role in the depiction of the real system using simulation.

Any blockchain systems can fundamentally be divided into 3 layers :

1. Network Layer
2. Consensus Layer
3. Incentive Layer

1.1 Layers of Blockchain System

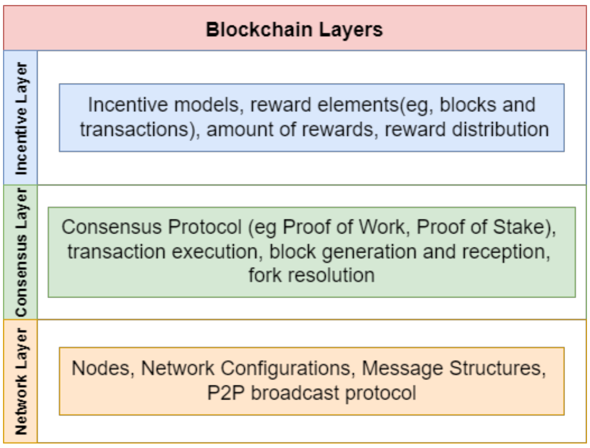

Figure 1: Layers of a Blockchain system

Network Layer This layer holds the network of participating nodes and is responsible for the mechanisms and protocols they use to communicate with each other. This layer plays a vital role in the information propagation and messages between the nodes.

Consensus Layer This layer implements the mechanism for the blockchain system to handle the events of block creation and propagation and for nodes to reach a global consensus to include the mined blocks into the ledger. This layer also holds the transaction pool from which the blocks are mined. In the case of forks, the consensus layer has to resolve them and maintain consistency in a fair manner.

Incentive Layer The Incentive layer is responsible for compensating the miners for contributing to the system. The miners need to be incentivized for contributing to the ledger by successfully mining the blocks and Ommer blocks in the case of the Ethereum ledger and also for block verification. This motivates the participants to be engaged in the mining process as they get financially compensated in terms of crypto-currency.

1.2 Topology of Blockchain Nodes

The topology of blockchain nodes refers to the interconnectivity of nodes. The nodes of the network greatly influence the propagation characteristics of the information between them. Based on whether the blockchain is permission-ed or permissionless, the nodes participating node has to be authorized by the system or can join the network as per their will. The network may consist of hundreds or thousands of nodes that act as full-time participants. If there are links between all the nodes then they form a clique, or else they can be represented as a semi-connected graph. Based on their interconnectivity and availability of nodes, the time taken for information to be broadcasted vary. The higher the number of hops required, the larger the overall propagation delay.

1.3 Mining Difficulty of a Blockchain System

Given a case when SHA-256 algorithm is used for encryption and validation of a block there are $16^{64} \approx 10^{77}$ possible hexadecimal combinations. If the puzzle is to find a nonce that results 18 leading zeros then $16^{64-18} \approx 2 * 10^{55}$ possible valid digest exists that satisfies the Proof of Work (PoW) i.e. the ratio of valid hash being $2 * 10^{-22}$.

Since nonce is an 32- bit integer, the probability that $2^{32} \approx 4 * 10^{9}$ possible integers that may result in the valid digest is given by $2*10^{-22}*4*10^{9} \approx 8*10^{-13} = 10^{-12}$ which shows a very low probability. This gives an idea of difficulty to mine a valid block.

Mathematically, the mining difficulty is given by :

$$MiningDifficulty = \frac{CurrentTarget}{MaxTarget} \tag{1}$$

This mining difficulty is revisited every 2016 blocks as a rule of thumb by considering the total mining power involved and the pending transactions in the Transaction Pool to keep updating the ledger by keeping the miners engaged.

1.4 Simulation as an Alternative

Since the mining difficulty of blockchain systems makes it computationally difficult to implement for the development and research purpose, Simulation can be a viable approach to setup BUT and perform analytical tasks on the behavior of the system. The use of simulation helps us test the design and analyze the concept without allocation of the real system by isolating the BUT from the live system. This even help us analyze the what-if questions and find impact of change in system characteristics in the overall behaviour of the system.

Limitation of Blockchain Simulators Blockchain Simulators, despite implementing mathematical modeling of the underlying layers of a BUT, often tend to focus primarily on certain layers over the other blocks of the system. These systems usually make assumptions and formulate some approximation to mathematically model the system. This yields in sub-par results in the behaviour and outcome of the simulation. During simulation, if the architectural design and key parameters and configurations in of each layer of BUT are not considered appropriately, gives the output far from the reality.

2. Literature Review

In Blockchain world, success of Bitcoin [1] was followed by other crypto-currencies such as Ethereum [2], Dogecoin [3], Tendermint [4], Hyperledger Fabric [5] and other industry applications as mentioned in [6] that can be permissioned or permissionless. All of these leverage blockchain technologies to offer some added values to their end users and vary on the basis of their underlying layers and protocols.

The increasing variants of blockchain applications have inspired the development of simulation frameworks for blockchain for development and analysis. [7, 8, 9, 10] have proposed some simulation frameworks for the various blockchain systems. They can simulate various blockchain technologies and provide plug-and-play features for different algorithms and area of focus as far as their respective use cases are concerned. The retrospective on these existing frameworks and simulators are done extensively by [11] and provides the insights as shown in figure 2.

Framework Name	Public Blockchain	Private Blockchain	Benchmarking	Simulator	Metrics	Blockchain	GUI
BlockBench	☒	✓	✓	☒	Throughput Latency Scalability Fault Tolerence	Ethereum, Parity, Hyperledger Fabric	☒
HyperLedger Caliper	☒	✓	☒	✓	Transaction Success Rate Transaction and Read Latency Transaction and Read Throughput Resource Consumption	Hyperledger Besu, Hyperledger Fabric, Ethereum, FISCO BCOS Networks	✓
BCTMark	☒	✓	☒	✓	CPU Consumption Energy Footprint	Ethereum Clique, Ethash, Hyperledger Fabric	☒
DIABLO	☒	✓	✓	✓	Throughput Latency	Go Ethereum, Open Ethereum, CollaChain, Quorum (IBFT, RAFT), Hyperledger Fabric	☒
Distributed Ledger Performance Scan (DLPS)	☒	✓	✓	☒	Throughput Latency	Ethereum, Ethereum Parity, Hyperledger Fabric, Indy, Quorum, Sawtooth	☒

Figure 2: Performance Evaluation of various blockchain simulators

Figure 2 shows the various aspects of the existing blockchain simulators and their use cases. This also highlights the areas and metrics that they can be used for. But the one area that they overlook is the design of the network layer. Simulators such as Blocksim [10] approximate the network propagation delays using normal distribution and other simulators use similar approximations for network level simulation.

A theoretical network model for Bitcoin nodes was given by Shahsavari, Zhang, et.al [12] as unstructured Peer-to-Peer model using a random graph and studied the block propagation analysis. Similarly, Wang, Zhao et.al. [13] presented that Ethereum P2P node topology has certain properties of a Small-World networks and the degree of connectivity of Ethereum nodes tails the power law distribution that represents a scale-free network.

These later analyses provide a better approximation to the nodal topology based on the network of real miners in contrast to assuming block propagation as an exponential function or normal distribution as done by the existing state-of-the-art simulators.

Watts and Strogatz [14] detail the small world graphs with behaviors of small characteristic path lengths and high clustering coefficient. Their mathematical model was later simplified by Song and Wang [15] where the probability of two nodes being connected is a function of the distance between the nodes in the cluster.

These new research on the topographic patterns of real nodes and simplified mathematical models can be leveraged to overcome the limitations of existing state-of-the-art blockchain simulators.

3. Methodologies

Figure 3 gives the proposed architectural design of the simulator framework. The Simulation module drives the underlying blockchain layers using parameters of configuration Module to mimic the characteristics of the real world into the BUT.

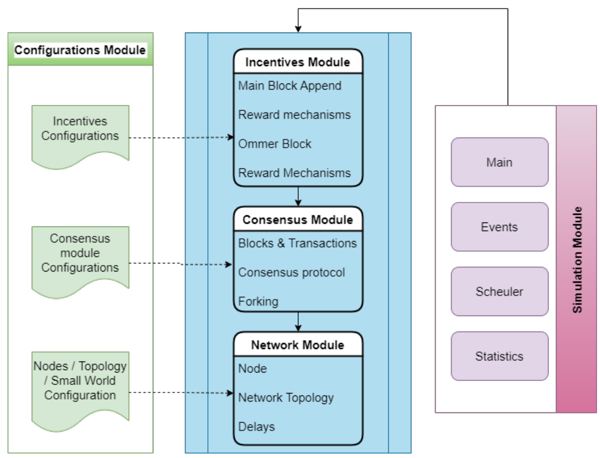

Figure 3: Proposed Simulator workflow

The following figure 4 shows the proposed methodology on how the node topology is generated based on the real network's behavior.

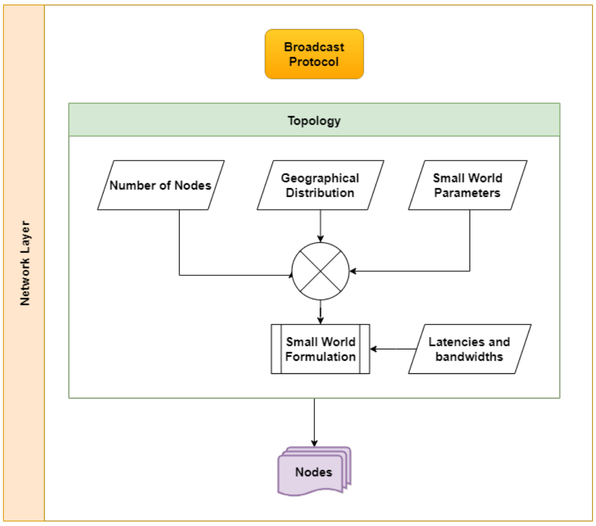

Figure 4: Proposed method for generation of Nodes

Here, the geographically distributed nodes are generated with small world formulation as suggested by [14, 15], and then their latencies are assigned as per their regional distribution. The topology can be changed by controlling their corresponding parameters.

The probability of an edge between two nodes, i and j, being reconfigured is given by [15] mathematically as:

$$p_{ij} \approx p(d_{ij}) = \beta * p_0 + (1+\beta) * \Theta(p_0 - d_{ij}) \quad (2)$$

The following parameters have the standard value when referring to the official sites such as blockchain.com and etherscan.io as shown in table 1:

Table 1: Standard Parameters Values configured for the Simulator

Configuration Name	Value for Bitcoin	Value for Ethereum
β_{size}	1 MB	1MB
β_{reward}	12.5 BTC	2
$\beta_{interval}$	600s	12.42S
β_{delay}	0.24S	6S
Γ_n	10	20
Γ_{delay}	5.1	3
Γ_{fee}	0.000062	$UsedGas * GasPrice$
Γ_{size}	0.000546 MB	0.000546 MB
Gas Limit	N/A	8000000

Table 2: Parameters considered for the Simulator

Entities	Configuration Name	Description
Blocks	β_{size}	Block Size (in Megabytes)
Blocks	β_{reward}	Reward for generating the block
Blocks	$\beta_{interval}$	Mean time (in seconds) to single generate block
Blocks	β_{delay}	Propagation Delay (in Seconds) of blocks through the nodes
Transactions	Γ_n	Rate of transaction generated
Transactions	Γ_{delay}	Propagation Delay (in Seconds) of transactions through the nodes
Transactions	Γ_{fee}	Fees charged for each transaction
Transactions	Γ_{size}	Transaction Size (in Megabytes)
Transactions	$\Gamma_{technique}$	Full Technique, Light Technique
Transactions	hasTransaction	Flag to turn transaction ON/OFF
Nodes	N_n	Number of Nodes in the Network
Simulation	Sim_{time}	Simulation Duration
Simulation	$Exec_{num}$	Number of execution of Simulations
Topology	Region Name	Names of the nodal geographical location
Topology	Region Distribution	fraction of nodal distribution by the region
Bandwidth	Latencies	Latency matrix between the regions
Bandwidth	Download Bandwidths	Average Download bandwidths of each region
Bandwidth	Upload Bandwidths	Average Upload bandwidths of each region
Small World Simulation	beta	Probability of reconnecting the nodes for small world n/w formulation
Small World Simulation	average degree	Average degree of the network

Table 2 enlists all the configurable parameters for the simulation along with their significance.

3.1 Simulator Evaluation

The evaluation of the simulator shall be based on its viability for analysis of existing blockchain technologies such as Bitcoin and Ethereum. The effects of various parameters such as simulation run time, number of miners, block delay, and propagation delay shall be compared with the throughput, % contribution of miners within main blocks, stale rate, and ommer rate. Additional validation is done to verify that the block count is proportional to the hash power of each miner. Throughput can be measured in terms of the number of transactions included in the ledger per second. The Stale rate is the rate at which the validated blocks get rejected by the consensus protocol with respect to the total mined blocks. Ommer rate for Ethereum is the rate at which the stale block is referenced to the main ledger.

4. Results and Discussion

Each simulation was done at least 10 times and averaged so as to remove the effects of the outliers.

4.1 Total Blocks vs Main Blocks vs Stale Blocks

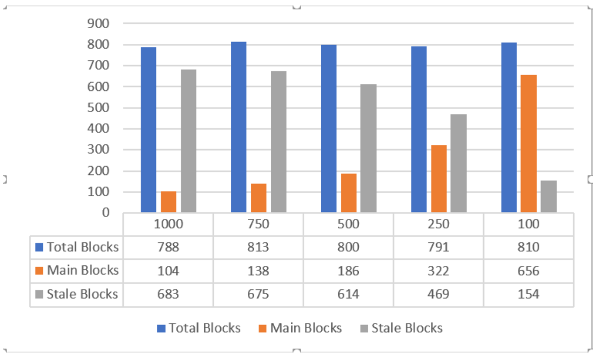

Figure 5: Different block counts for different network sizes

In Figure 5, the number of main blocks decreases and the number of stale blocks increases as the node size is increased. This is because as the node size increases, it takes longer time to reach the global consensus as a large number of blocks need to be validated and propagated across the network.

4.2 Transaction Rate and Throughput

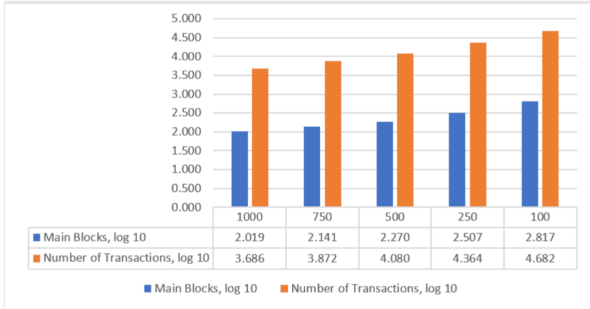

Figure 6: Transaction counts for various networks

The Transaction Rate is the number of transactions that resides in the global ledger. The simulation results for this validation are in Figure 6. The trend suggests that as the number of nodes is increases the number of transaction that gets incorporated into the blockchain system gets decreased as the number of blocks in the system is decreased,

4.3 Ommer Blocks for Ethereum Networks

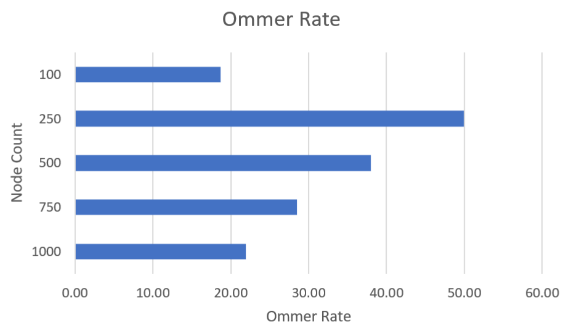

Figure 7: Ommer Rate for different network sizes

The above Figure 7 helps us understand the trend of Ommer Rate within an Ethereum network. The given trend is due to the fact as more nodes generate more candidate blocks for the global blockchain ledger, the Consensus Algorithm has to verify for each candidate blocks for the validity to get appended to global chain. This will be more time-consuming as more nodes are to get verified and there are chances of removing the whole fork if there is another valid block that had to be appended to the blockchain.

While this takes place, the ommer blocks are appended to Ethereum blocks providing only certain incentives lesser than those for the valid main block to the Ommer miners.

4.4 Hash power vs Mined Blocks

The following trend is seen when count of the mined block is tallied against the hash power of miners.

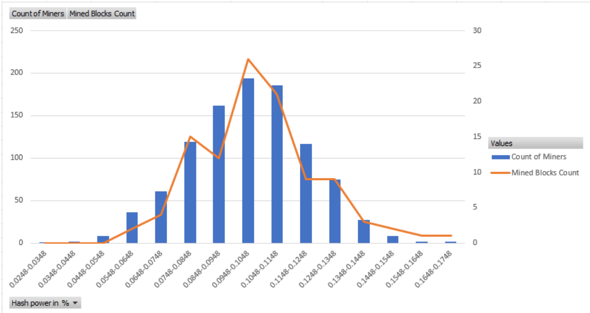

Figure 8: Hash powers vs Mined blocks count

From the trend analysis, we may conclude that the number of mined blocks is proportional to the hash power of the nodes as well as the count of the nodes. In the PoW consensus, the chance of a candidate block that is likely to get appended to the system is given by the probabilistic characteristic of the mining difficulty. The real life system depicts that the miners are distributed with the normal distribution in terms of the hash power i.e. higher number of miners with average hash power. This extends that the total contribution by the miners with average hash power is relatively higher than that of the ones with the hash power at the extremes.

5. Conclusion

Thus, implementation of the Small World properties to design the node topology resulted outcomes as expected. Simulator for blockchain was designed, which can simulate the Bitcoin and Ethereum under various configurations. Its outcomes were mesaured in terms of Transaction rate i.e. throughput, main block rate, stale rate and ommer rates, in case of Ethereum as well. The contributions of miners in the blockchain ledger was verified as being proportional to the hash power of the miners.

6. Future Works

While this work provides fair results for the simulation, the implementation can be extended so as to incorporate other blockchain technologies. Various other Consensus algorithms can be added to try and test other hybrids of the system. Mathematical models of the message passing algorithms can be included for analysis of the bandwidth consumption.

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Cryptography Mailing list at https://metzdowd.com*, 03 2009.

[2] Daniel Davis Wood. Ethereum: A secure decentralised generalised transaction ledger. 2014.

[3] Usman W. Chohan. A history of dogecoin. *Innovation Finance & Accounting eJournal*, 2021.

[4] Jae Kwon. Tendermint : Consensus without mining. 2014.

[5] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolić, Sharon Weed Cocco, and Jason Yellick. Hyperledger fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference*, EuroSys '18, New York, NY, USA, 2018. Association for Computing Machinery.

[6] Amy Nordrum. Wall street occupies the blockchain - financial firms plan to move trillions in assets to blockchains in 2018. *IEEE Spectrum*, 54:40–45, 10 2017.

[7] Arthur Gervais, Ghassan Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. On the security and performance of proof of work blockchains. In *Proceedings of the 23nd ACM SIGSAC Conference on Computer and Communication Security (CCS)*. ACM, 2016.

[8] Ari Keränen, Jörg Ott, and Teemu Kärkkäinen. The one simulator for dtn protocol evaluation. page 55, 01 2009.

[9] Atul Singh, Tathagata Das, Petros Maniatis, Peter Druschel, and Timothy Roscoe. Bft protocols under fire. pages 189–204, 01 2008.

[10] Maher Alharby and Aad van Moorsel. Blocksim: A simulation framework for blockchain systems. *ACM SIGMETRICS Performance Evaluation Review*, 46:135–138, 01 2019.

[11] Marios Touloupou, Marinos Themistocleous, Elias Iosif, and Klitos Christodoulou. A systematic literature review toward a blockchain benchmarking framework. *IEEE Access*, 10:1–1, 01 2022.

[12] Yahya Shahsavari, Kaiwen Zhang, and Chamseddine Talhi. A theoretical model for block propagation analysis in bitcoin network. *IEEE Transactions on Engineering Management*, PP:1–18, 04 2020.

[13] Taotao Wang, Chonghe Zhao, Qing Yang, Shengli Zhang, and Soung Chang Liew. Ethna: Analyzing the underlying peer-to-peer network of ethereum blockchain. *IEEE Transactions on Network Science and Engineering*, PP:1–1, 05 2021.

[14] Duncan Watts and Steven Strogatz. *Collective dynamics of 'small-world' networks*. 12 2011.

[15] H. Song and Xiao-Jing Wang. Simple, distance-dependent formulation of the watts-strogatz model for directed and undirected small-world networks. *Physical Review E*, 90, 08 2014.