International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-4, February 2019

A Rumor Algorithm Propagation Considering Block Omission in a Blockchain System

Arif Sari, Samson Oluwaseun Fadiya, Acheme Okolobia Odeh.

Abstract: ***In this article we experimented the rumor spreading algorithm of data propagation in a blockchain system with specific focus on the block omission rate. The algorithm introduced here was modeled and simulated by a new class of extended Petri nets called "Elementary nets". This type of nets is suitable for the representation of the functions of an information system. The descriptive and analytical power of the elementary net was employed in this article to model and perform simulation experiments to measure the omission rates of blocks propagated in the blockchain network using the rumor algorithm. The aim of the research is to model and simulate block data propagation in the blockchain system considering block omission. The modified rumor algorithm for the blockchain system was proposed in our Ph.D. thesis with the introduction of a switching module that regulate block dissemination in the model. The result of our research shows a steady decline in the block omission rates with increasing number of nodes. This is a very significant criteria in the implementation of a reliable and scalable block propagation scheme for the blockchain system.***

Keywords: Blockchain, Block propagation, Elementary nets, Petri nets, Rumor Algorithm.

I. INTRODUCTION.

The Blockchain system is gradually becoming a major area of interest for academic researchers. A blockchain is a continuously growing lager of value transactions managed by a peer-to-peer network implemented with the use of distributed consensus algorithm. The blockchain technology possess very interesting characteristics such as persistency, auditability, decentralization, and anonymity. These characteristics could remarkably enhance the effectiveness and cost of business processes. Blockchain has found application in various areas such as cloud computing, big data, digital economy, Internet-of-things, contract systems, security, etc. To improve the efficacy of blockchain, there is a need for non-functional innovations in blockchain-centric services computing. Communication can be a complex phenomenal to decipher in a distributed network such as the blockchain network. Communication in the blockchain network is a key element to the performance of the network. Nodes on the blockchain network communicate on a peer – to – peer bases [1]. This type of communication removes the need for a central coordinator, thereby solving the problem of "single point of failure" and other security and privacy related risks [6], [4].

Manuscript published on 28 February 2019.
***Correspondence Author(s)
Arif Sari, Department of Management Information Systems, Girne American University, Cyprus.
Samson Oluwaseun Fadiya, Department of Management Information Systems, Girne American University, Cyprus.
Acheme Okolobia Odeh, Department of Management Information Systems, Girne American University, Cyprus.

The management, analysis and performance of this network is an intricate part of the network that must be studied for a clear picture of how the blockchain network can be organized and deployed successfully on the internet [23], [7]. Scalability also becomes an immediate concern, if we consider how communication is organized in the current blockchain network.

The origin of blockchain dates back to 2008 when "Satoshi Nakamoto" first deployed the blockchain technology as a peer-to-peer electronic cash system [1]. The objective of their research was mainly to solve the "double spending" problem faced by the financial system. In the proposed system each node on the network works independently to ensure that they meet the network requirements. Nodes work all at the same time with little or no coordination. The nodes don't need to be identified since routing is not implemented in the block chain network [1]. Messages are delivered on the best effort basis and do not need to be routed to any specific node. Processing power is decentralized and determined by majority of honest nodes [1]. This perhaps makes a unique mode of a robust unstructured communication network.Transactions are distributed to all nodes for verification and validation. To maintain the privacy in the blockchain system, public keys are kept anonymous [8].

Previous studies have focused more on possible areas of the application of the blockchain technology [13], [12], [5]. We are making a quick diversification from this to consider the foundation of the operations of the technology itself. It is necessary to understand how communication in the network is organized and can be modified for future adoptions. Not so much has been done to clearly experiment on the possible communication paradigm suitable for the blockchain system. This has become necessary now that many organizationsare considering the adoption and utilization of this technology in various business processes. The major disadvantage is that the latency problem is yet to be completely addressed. Currently transactions on the blockchain network takes an interval of 10min to complete. This time need to be cut down as much as possible and the security of the system still maintained.

Nodes need to be organized in such a way that blocks are delivered to intending nodes and transactions can be verified quickly and without any security challenge. For this reason, faster communication algorithms need to be experimented and tested on already existing blockchain infrastructure. If this is not done, it will not be possible to achieve scalability in the blockchain system. A suitable, reliable and safe data propagation method is required for this to happen. A data dissemination scheme considering node failure was proposed by [2].

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

The result of their experiment was quite interesting showing that the validation time of blockchain transaction could be shortened if the resistance of node failure can be improved upon. In our proposed model, we take a different approach by proposing a novel data propagation algorithm – "the rumor spreading scheme considering block omission". In our proposed scheme, nodes that leave the network does not adversely affect the functioning of the network, unlike the model proposed by [2].Our model also shows that the rate of block omission in the network decreases with increasing number of nodes, making the network a very robust, scalable and dependable one.

Our proposed model is classified into two modules: "the switching module and node module". These modules are discussed in detail in the succeeding sections. In this article we described the rumor spreading model and performed simulation experiments to measure the rate of omission of blocks in the network. Our result showed that with our proposed data propagation scheme, blocks are delivered safely to intending nodes even as the network of nodes increases. The failure of any node during the process of block propagation does not adversely affect the overall delivery of blocks to nodes in this case.

The remaining part of this article is organized as follows. Section two focuses on related studies. Section three is dedicated to a description of the proposed rumor spreading algorithm. The extended Petri nets structure of the model is presented in section four. In section five we described the simulation procedure, results and analysis. In section six we present a conclusion to our study.

II. LITERATURE REVIEW

Many people have attributed the term "blockchain" to bitcoin or other cryptocurrency's alone. While other groups of people are not very comfortable with this classification. Bitcoin has gotten a wider acceptance in the global economy other than any other blockchain based application. Others see blockchain as a data structure. Not minding whose opinion is right, one thing is obvious, the terminology surrounding blockchain is still undergoing various reformation [11]. Hence, we see a rapid increase in the number of blockchain developments these days. The blockchain network is dominated by homogeneous nodes. An overview of the blockchain technology: Architecture, consensus, and future trends was conducted by [14]. They defined blockchain as an immutable ledger that permits transactions in a decentralized manner. They also pointed out that blockchain is still confronted with many unanswered challenges, such as security, and scalability. A blockchain imitate a "trusted" computing process through a distributed protocol, operated by nodes that are on the internet [22]. A blockchain as a decentralized technology that allows for the sharing of transactions across a huge network of untrusted nodes [16]. "Blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way" [17]. No node is responsible for coordination; therefore, each node stores a copy of all the information on the network, especially those needed to verify the validity of new transactions. Transaction data, basically referred to as block data are copied on every node. Each node requires computational, storage and network resources to function on the blockchain network [2].

Blockchain is uniquely positioned to support a huge number of transactions; mostly accruing simultaneously. Nodes are connected in a peer-to-peer fashion. Each node connects to one or more validator nodes to modify or know the status of blocks in the network. To interact with the network, nodes need to be synchronized with the updated copy of blockchain created or stored by validator nodes in the network. The consensus algorithm ensures that blocks that are added to the blockchain are authentic and verified by trustable nodes on the network. In the bitcoin proof of work, various miners contend for the right to add the next block in the blockchain, by competing to solve an extremely difficult puzzle. The first node or miner to arrive at the correct solution to the puzzle wins this privilege. The miner also receives some rewards in form of some bitcoin amount. The proof of stake also provides a consensus mechanism where by the node with the most likely hood to be picked to generate the next block is the node with a higher deposit of coins. Nodes that have higher stake or coins in the network are more likely to be selected to generate new blocks. Some other algorithms include: Proof of activity, proof of burn, proof of capacity, proof of elapsed time, and many others that are yet to be developed or being developed.

Even though a consensus algorithm is an intricate part of any successful blockchain, it is out of the scope of our current study. Consensus in the block chain becomes a concern when we focus on specific blockchain applications such as bitcoin. Nevertheless, the blockchain application domain is limitless, hence, we narrow the scope of our article to focus on the basic communication paradigm required for effective and efficient block data propagation; showing exactly how block data can be effectively distributed among geographically dispersed blockchain nodes. Once a node generates a block, that block still needs to be communicated to the entire network. Therefore, we are not concerned with validating the block data. Meaning, any validation protocol can be implemented to adopt our proposed data propagation scheme with necessary definitions and modifications to already existing protocols. For example, the flooding technique implemented in the bitcoin can be replaced with our rumor spreading scheme with possible modifications to the protocol to suit the requirements of a successful bitcoin application.

Previous studies addressing the communication protocols of the blockchain network was performed to "model the role of wireless connectivity in blockchain-powered IoT systems" [10]. The communication mechanism discussed in this article is a "Point – to - Point topology" followed by the IoT devices to communicate with the blockchain network made possible through a Proxy node. Although this study gives us a glimpse to how communication can be organized for a blockchain network, it was not able to explicitly illustrate or describe the exact nature of the blockchain communication paradigm for complex scenario other than the IoT devices.

An architectural modelling and simulation system was used to predict the latency of blockchain-based systems [18]. They observed that very little is known about predicting the behavior of the blockchain based systems.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

To tackle this issue, they showed that using the architectural performance modelling and simulation tools, the latency of blockchain based systems could be predicted. New blockchain specific issues were explored using established tools and techniques. Some of these issues include: "configuration of the number of confirmation blocks and inter-block times". Their report was based on a lab experiment of an incident management system that display the predictions of median response time of the system at an error rate of 10%. The “block withholding attack in a blockchain cloud considering distinct pool reward mechanism" was modelled by [21]. The rogue miner's disrupting capability was verified by simulations. Simulation models have also been performed to detect fraudulent activities in blockchain bitcoin protocol [20]. They simulated attacks in local area network to identify the various types of attack and the reasons for attacks. A new mechanism was proposed to check against attacks and recognize double spending transactions in the network. They also made some analysis which shows that their model was effective in cutting down the rate of double spending.

The effect of communication delay in the bitcoin network was studied by [19]. The Markov model was used to track the various states of the blockchain. The discrete-event simulation was used to study the behavior of the bitcoin miners that use the selfish-mine approach. The result of their model showed that both honest and dishonest miners were worse without the activities of dishonest miners. They also showed that it was possible to detect and stop block-hiding behavior of miners by observing the rate at which orphan blocks are produced. Another research focused on "the Transaction Graph for modeling Blockchain Semantics" [22]. Prior to this model, there was no formal model of blockchain based transaction semantics. To fill this gap in the literature, they proposed a model that can capture the semantics of transaction in the blockchain network using a directed acyclic graph. This model was specifically designed for Ethereum, Bitcoin and Hyperledger Fabric.

A reliable blockchain system requires that blocks are efficiently delivered to participating nodes through a well-organized communication algorithm. Existing blockchain algorithms for data propagation such as the flooding scheme implemented in the bitcoin blockchain system does not guarantee this. We are interested in ensuring that block data are successfully delivered to all participating nodes with minimal omission in the block delivery rate. The most recent and closest research to ours was done to propose a data propagation algorithm considering the failure of nodes [2]. Their scheme first sets a response benchmark to identify “failure nodes”, thereafter, they employed the “greedy idea” to constructs a communication tree (hierarchy) to begin the forwarding of block data by all nodes. They deployed a multi-link concurrent communication tree model that maximizes the propagating capacity of nodes on the blockchain network. These nodes are identified and assigned corresponding task as well as other nodes. Task are assigned based on the capacity of each node. Their results showed that validation time of blockchain transaction is shortened, improving the resistance to node failure. To avoid node failure during data transmission, the author implemented a connection-based transmission scheme which requires source nodes to receive confirmation message from other nodes before disseminating the block data.

Our new model implements a connection-less based transmission scheme based on the rumor spreading idea with the introduction of a switching module that regulates the block generation interval and does not require any confirmation message from participating nodes. In principle, time is saved by adopting this method and to avoid cases of nodes not transmitting received data, we implement a node threshold value which ensures that block data can go around the blockchain network irrespective of a failed node during transmission. Generally, the method discussed above could face scalability and performance issues as the network grows, especially in the IoT device domain. Our article aims to provide a data dissemination algorithm considering block omission. It has been shown that our model has high block delivery rate measured at various probabilities.

III. THE RUMOR SPREADING ALGORITHM

This is synonymous to the real-life scenario where a rumor is carried by the first person to someone. The rumor carriers (in this case the nodes) decide if to forward the rumor to other people and what direction they prefer to spread the rumor. Nodes on the blockchain network has the liberty to choose what node to forward data to. The nodes also decide if to forward a received data or not. The behavior of nodes on the blockchain system can led to loss or omission of block data. They may refrain from forwarding block data to other nodes or they may fail in the process of block propagation. Putting this in consideration we have proposed our experiment for various probabilities of refrain and loss for forwarding block data by nodes. As we stated previously, the current algorithm of block propagation in the PoW and PoS algorithms is the flooding mechanism, which can cause high latency and congestion in the network traffic.

The rumor spreading algorithm has been around for quite a long time. It is known for its robustness and simplicity in the organization of communication in distributed systems [9]. The major problem with the rumor spreading scheme is the repeated delivery of data to nodes that already have the copy of data. To solve this problem, we set all the nodes to immediately discard any data that it has previously received if same copy of data is delivered to it again. The major modification made in our proposed model is the introduction of a switching module responsible for the random selection of nodes to assign it as a block generator, the incrementation of block number and passing to selected nodes, the incremented number to begin block generation and its propagation. The following steps and assumptions were put in consideration in preparing our proposed model.

i. We assume that the blockchain network is made up of N nodes. Each of these nodes can be selected at random to become a block generator by the switching module.
ii. Newly generated blocks are immediately propagated in the entire network.
iii. There are chances that some nodes will not get a copy of the newly generated and propagated block.
iv. We do not assume any network structure such as tree, bus or ring topology.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

v. We did not consider the spatial distributions of nodes in our model. Nevertheless, the distance of nodes from one another can be 1, 2, …, h_{max}, hop, where $h_{max}$is the maximum distance that a new block can pass from the generating node.
vi. The nodes randomly select n<N different other nodes for different block propagation. Therefore, it is not necessary for each node to keep address information of other nodes that where previously contacted.
vii. Inter-node propagation time is assumed to be uniformly distributed with specified minimal and maximal values which are the same for each node.
viii. No centralized control is assumed in the blockchain system. In order to simplify our model, we assume that only one node can generate a block within any specified block dissemination interval. Hence, we included a generator of periodical Block Dissemination Interval in the model.
ix. At the inception of the interval, the generator randomly selects a node for new block generation and passes the incremented block number to the chosen node.
x. The most recent block number is kept in the memory of the interval generator.
xi. In our model we assume that the length of the interval is large enough for all the messages in the network to die out before the next interval begin. In this case the network becomes quiescent. This can be compared to the 10min time interval of the bitcoin blockchain.
xii. In order to cut down traffic we assume a connection-less inter-node communication powered by the UDP protocol, without the need for confirmation of delivery to nodes.
xiii. Since the maximal hop value (h_{max}) is restricted and inter-node communication is connection-less, some nodes in the system will not receive the blocks. This was a model parameter in our previous research.
xiv. All the nodes in the blockchain system are assumed to have the same functionality.
xv. Nodes have the choice to refrain from forwarding received blocks.
xvi. We set three refrain probabilities as a model parameter thus: PREF = 0.1, 0.2, and 0.3. This is illustrated in figure 1 where node six (6) refuses to forward the block data after receiving its first update from node three (3).

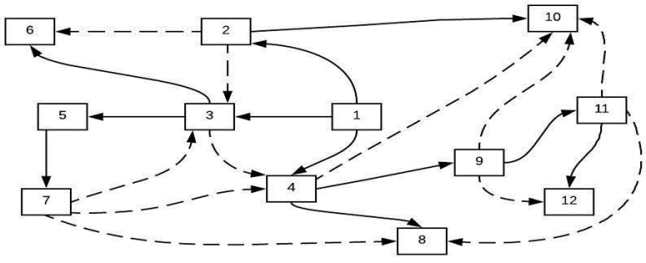

Figure 1. The proposed rumor spreading scheme:

Figure 1 is an illustration of a communication scenario in the network of 12 nodes with 3 contacts by each node (messages on dashed arcs are duplicates and are discarded)

Because of the time difference in block propagation, the same block can arrive at separate nodes at different times. We employed a loss probability as a model parameter to demonstrate the chances that messages can be lost during propagation. This probability is referred to as "Loss probability": PLOS = 0.05, 0.1, and 0.2. When a node receives first copy of a block, it tabulates the difference $t_r - t_s$ where t_s is the moment of time the block was generated, and t_r is the moment of receiving this copy by this node. The intervals of generation of new blocks are illustrated in figure 2.

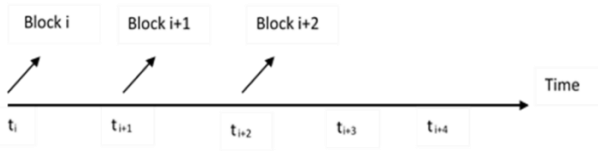

Figure 2. Interval of generation of new blocks.

In figure 2 above $t_{i+1} - t_i = t_{i+2} - t_{i+1} = \ldots = t_{i+4} - t_{i+3}$ are equal block generation intervals. When a new block is disseminated in the network of nodes, each participating node will posses a copy of the new block with number í and a copy of some previous block with number j. If í = j+1, then this node has a copy of the previous block and will immediately discard the incoming block. But if í > j+1, then the node is missing one or more previous blocks. When a block is propagated in the network it is possible that a node will receive several copies of similar block. The node only keeps the first copy of the received block, the second, third and fourth blocks having the same number as the first copy are immediately discarded as illustrated in the flowchart in figure 3. When a node receives a block, it randomly selects other nodes to forward the block to. This means that for two subsequent blocks, different sets of nodes can be contacted for forwarding the block. The number of nodes to contact is a variable parameter. We set the number to 3, 4, …, 5.

IV. STRUCTURE OF THE MODEL

A new class of extended Petri nets is used to model block propagation of the rumor spreading algorithm. This class of extended Petri nets were developed by[3].The principal component of this extended Petri net is called "Elementary nets." Elementary nets possess the following structural elements: - transitions, places and directed arcs. For each place in the elementary net, is associated an input or output places. An elementary net can be defined in by the expression below:

$$E(t) = \{C, P_1, P_2, r_1, r_2, d, ƒ\}, \qquad (4.1)$$

where C is "the condition that must be satisfied for the transition t to fire; The input and output places are represented by P_1 and P_2 with $P_1 \cap P_2 = \emptyset$ and $P_1 \cup P_2 \neq \emptyset$; r_1 and r_2 are input and output functions respectively; d is a delay function; ƒ is a data transformation function."By way of definition two main actions must be completed for a transition to fire in an extended Petri net scheme. The first action is that the firing condition "C" must be satisfied. Then the functions r_1 *and* r_2 must be evaluated. A comprehensive description and illustration of this class of Petri nets is given in the book of [3].

We have used this extended Petri nets to describe the structure of our proposed model and subsequent simulation of the model by the "WINSIM" simulation component of the scheme.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

In this model we selected 50 nodes for the design of the model. We structured the model into two functional modules as shown in figure 4. The switching module is represented by the upper section of figure 4. It is responsible for attaching the node module and linking them and to generatea periodic block dissemination interval. It is also the responsibility of this module to switch message among nodes.Nodes are selected at random based on a probability distribution by the switching module for block generation. The task of the node module is the generation of new blocks; storing new received blocks and deletion of duplicate blocks; Probabilistic handling of received block sand the forwarding of copies of received blocks. Each node from the node module directly attaches itself to the switching module as we see in figure 8.

Figure 3. F low chart of the node algorithm

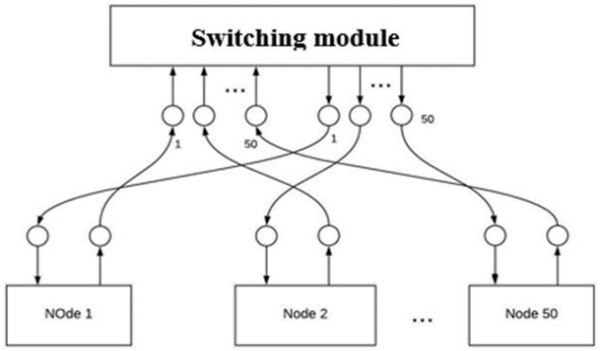

Figure 4. Structure of the model

Figures 5 and 6 shows a fragment of the extended Petri net representation of the node and switching module respectively. Without the switching module, each node on the network will require (N-1) connections with other nodes totaling N(N-1) connections. This requires huge network resources and will amount to massive network traffic as well. But with the introduction of the switching module each node can connect to it by only two connections. The switching module introduced here has no actual implementation in the real-world – it is only a virtual component of the proposed model. We did not attach time delays to the switching module but with the node module just for simplicity. To demonstrate the concept of the Petri net scheme, we show here a fragment of the node and switching module in figures 5 and 6 respectively. In the Extended Petri net scheme of figure 5**Error! Reference source not found.**, the transition Y1000 is responsible for collecting output messages from all nodes, while the transition X2000 of the elementary net shown in figure 6 passes the messages forwarded by each node to other nodes. The transitions Y1000 and X2000 represents the switching segment of the scheme.

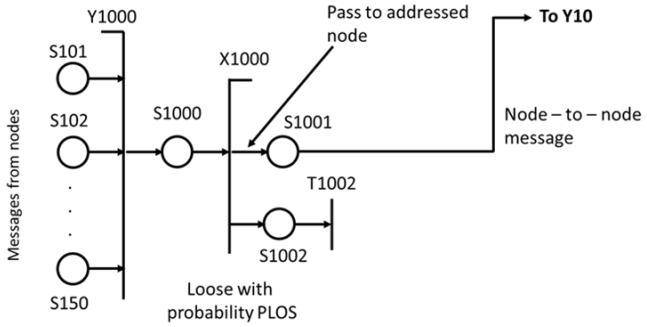

Figure 5. A Fragment of the Extended Petri net scheme of the node module

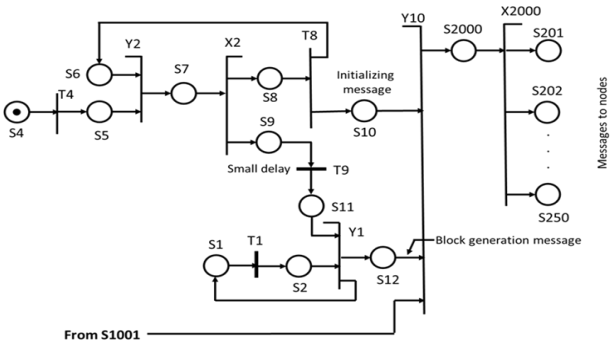

Figure 6. A Fragment of the Extended Petri net scheme of the switching module

V. SIMULATION PROCEDURE

Simulation experiments were performed on the proposed model to measure the omission rate of blocks for the rumor spreading algorithm. The omission rate of blocks is described by the expression below:

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

$$K = \frac{k}{M} \qquad 4.2$$

where $K = \sum_{i=1}^{N} K_i$ is the number of blocks which were missed by N nodes of the system, k_i is the number of missed blocks at node *i*, *i* = 1, 2, …, N, and *M* is the number of generated blocks. In the model, this metric was calculated with the use of the number of firings of the corresponding transitions. This metric was evaluated versus the number of contacted nodes.

In the simulation experiments, separate simulation runs were conducted for the number of contacted nodes represented in the model by NFWD with the values 3, 4, …, 7, and given values of loss probability (PLOS), refrain probability (PREF) and the maximum hop value (MHOP). Three values of MHOP were used: 4, 7 and 10; PREF = 0.1, 0.2, and 0.3; PLOS = 0.05, 0.1 and 0.2. The inter-node propagation time is assumed to be random in the range (t_{min}, t_{max}) without taking into account the spatial distribution of nodes in the network. The values "t_{min} and t_{max}" are model parameters. Thus, maximal duration of existence of a block in the system is hxt_{max}. If h=10, this will be 10xt_{max}. This value was used for the choice of block generation interval. Table 1 shows the complete list of simulation parameters used in the simulation procedure.

Table 1. Simulation parameters

Parameter	Values(s)
1. The number of nodes	50
2. PLOS value	0.05, 0.1, 0.2
3. PREF value	0.1, 0.2, 0.3
4. MHOP value	4, 7, 10
5. Number of generated blocks in each run	1000
6. Simulation time in each run, ms	3.0E+7
7. Number of contacted nodes	3, 4, …, 7
8. Starting time to collect statistics, ms	0

We performed a total of 135 simulation runs considering 5 NFWD, 3 values of PLOS and PREF and 3 MHOP values as shown in table 1. From which graphs were plotted to measure the omission rate of blocks. The results of the simulation runs are shown in tables 2, 3, 4, 5, 6, 7, 8, 9, and 10. Where the numbers 3,4,5,6, and 7 are the number of contacts as represented in the graphs in figures 7,8,9,10,11,12,13,14 and15. The table are in three sets showing results for Maximum hope values of 4, 7 and 10. Table 2, 3 and 4 shows a set of three result for MHOP value of 4, while table 5, 6, and 7 shows a set of three results for MHOP value of 7 and finally table 8, 9, and 10 shows a set of results for MHOP value of 10. From these values the graphs have been plotted to show the relationship between the omission rates of blocks and the number of contacts for the various values of refrain probability and loss probability.

Table 2. Simulation results for MHOP=4, and PREF = 0.1

PREF 0.1					
	3	4	5	6	7
PLOS 0.05	17.153	5.88	3.03	2.2	1.1
PLOS 0.1	19.99	7.66	2.85	1.52	1.14
PLOS 0.2	25.78	12.52	4.83	2.27	1.39

Table 3. Simulation results for MHOP=4, and PREF = 0.2

PREF 0.2					
	3	4	5	6	7
PLOS 0.05	21.59	9.04	3.51	1.77	1.23
PLOS 0.1	24.59	11.24	4.44	2.25	1.37
PLOS 0.2	30.07	16.37	7.81	3.56	1.84

Table 4. Simulation results for MHOP=4, and PREF = 0.3

PREF0.3					
	3	4	5	6	7
PLOS 0.05	26.06	13.16	5.64	2.85	1.63
PLOS 0.1	28.51	15.76	7.8	3.47	1.89
PLOS 0.2	33.36	21.6	11.57	5.88	3.76

Table 5. Simulation results for MHOP=7, and PREF = 0.1

PREF 0.1					
	3	4	5	6	7
PLOS 0.05	5.9	2.55	1.58	1.22	1.09
PLOS 0.1	7.4	3.95	1.73	1.27	1.13
PLOS 0.2	11.78	4.47	2.36	1.54	1.25

Table 6. Simulation results for MHOP=7, and PREF = 0.2

PREF 0.2					
	3	4	5	6	7
PLOS 0.05	9.1	3.79	2.07	1.39	1.18
PLOS 0.1	11.35	4.32	2.3	1.62	1.26
PLOS 0.2	16.63	6.91	3.65	2.08	1.49

Table 7. Simulation results for MHOP=7, and PREF = 0.3

PREF0.3					
	3	4	5	6	7
PLOS 0.05	13.22	5.63	3.04	1.82	1.39
PLOS 0.1	15.36	6.69	3.79	2.11	1.69
PLOS 0.2	20.97	10.47	5.47	2.87	1.97

Table 8. Simulation results for MHOP=10, and PREF = 0.1

PREF 0.1					
	3	4	5	6	7
PLOS 0.05	5.493	2.537	1.563	1.218	1.083
PLOS 0.1	6.47	3.011	1.74	1.29	1.13
PLOS 0.2	10.07	4.221	2.472	1.532	1.249

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table 9. Simulation results for MHOP=10, and PREF = 0.2

PREF 0.2					
	3	4	5	6	7
PLOS 0.05	8.185	3.702	2.162	1.402	1.173
PLOS 0.1	9.89	4.25	2.38	1.52	1.26
PLOS 0.2	14.649	6.31	3.248	2.018	1.493

Table 10. Simulation results for MHOP=10, and PREF=0.3

PREF0.3					
	3	4	5	6	7
PLOS 0.05	13.218	5.63	3.061	1.832	1.402
PLOS 0.1	15.354	6.695	3.785	2.104	1.684
PLOS 0.2	20.971	10.47	5.372	3.718	2.917

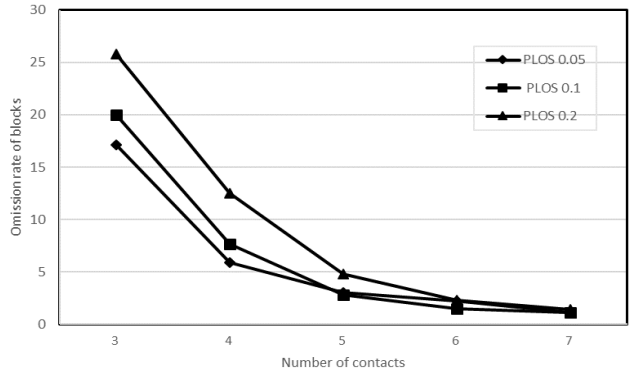

Figure 7. Omission rate of blocks vs the number of contacts, with MHOP = 4 and PREF = 0.1

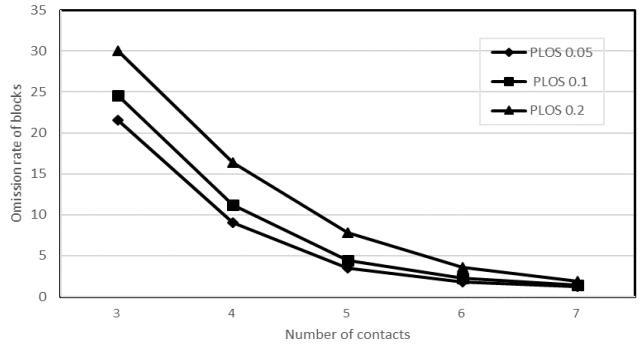

Figure 8. Omission rate of blocks vs the number of contacts, with MHOP = 4 and PREF = 0.2

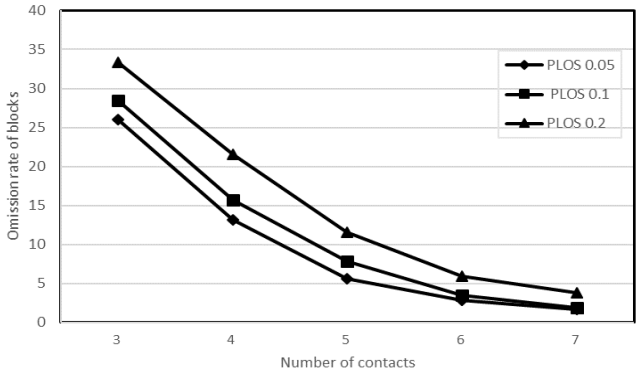

Figure 9. Omission rate of blocks vs the number of contacts, with MHOP = 4 and PREF = 0.3

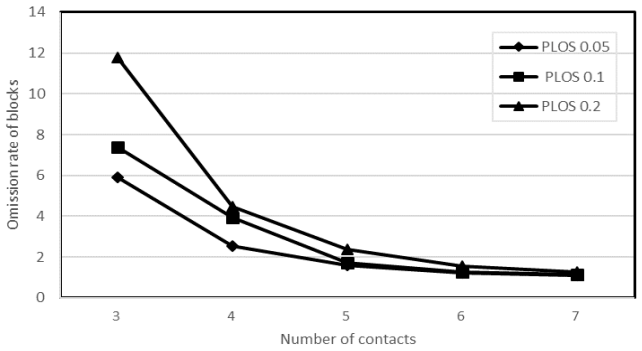

Figure 10. Omission rate of blocks vs the number of contacts, with MHOP = 7 and PREF = 0.1

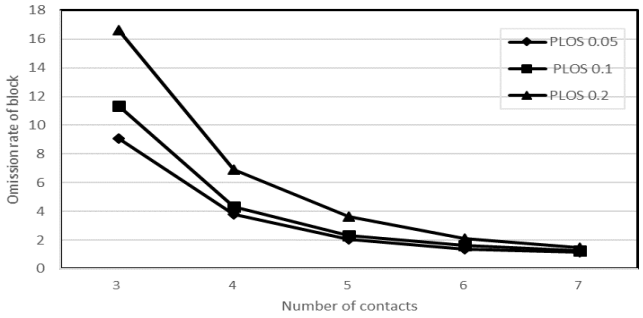

Figure 11. Omission rate of blocks vs the number of contacts, with MHOP = 7 and PREF = 0.2

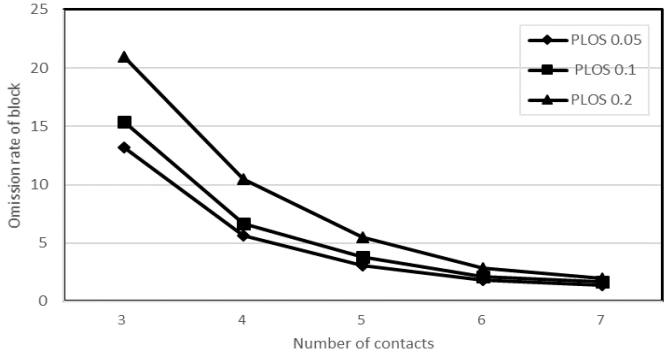

Figure 12. Omission rate of blocks vs the number of contacts, with MHOP = 7 and PREF = 0.3

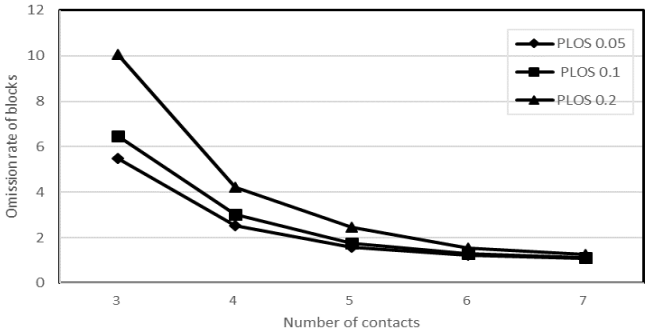

Figure 13. Omission rate of blocks vs the number of contacts, with MHOP = 10 and PREF = 0.1

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

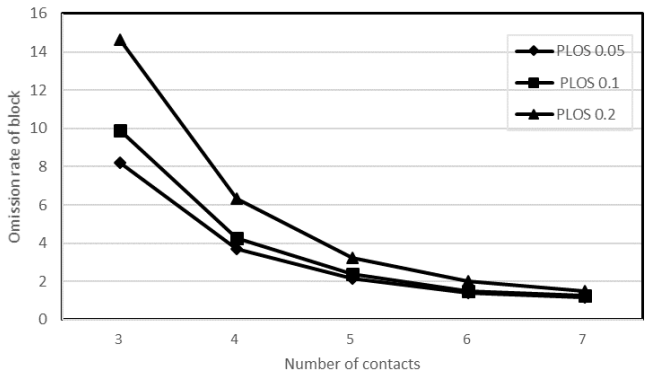

Figure 14. Omission rate of blocks vs the number of contacts, with MHOP = 10 and PREF = 0.2

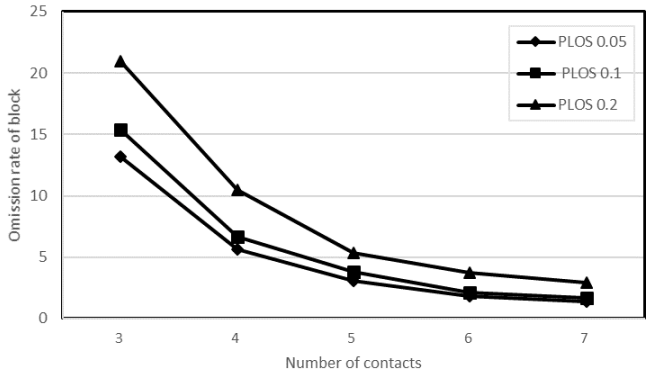

Figure 15. Omission rate of blocks vs the number of contacts, with MHOP = 10 and PREF = 0.3

Some interesting analysis of the various graphs plotted can be made thus: each probability of refraining, that is PREF of 0.1, 0.2, and 0.3, shows that the loss probability of 0.05 gives the highest omission rate while the loss probability of 0.2 produces the lowest omission rates. This behavior could be a useful factor in selecting the right parameters for the implementation of our proposed scheme. It was also observed that all the MHOP values of 4, 7 and 10 showed the same pattern of behavior. Further more, we observed that the value of block ommision increases with increasing refrain probability, with PREF of 0.1 giving the lowest value of block omission. This behavior is displayed by all the other MHOP values of 7 and 10 as well as we show in figures 10, 11, 12, 13, 14, and 15. Once again, these parameters are neccesary in making configuration and implementation decision for specific consensus algorithms when our proposed scheme is to be deployed. The scheme can be easily implemented in various concensus algorithms such as the popular “Proof of Work” algorithm and “Proof of Stake” algorithm. The decreasing rate of block omission indicates that the rumor spreading scheme is highly efficient and a reliable algorithm for data coordination in the blockchain system if properly implemented.

IV. CONCLUSION

In this article we have modelled and simulated the rumor spreading algorithm considering block omission with the use of a new class of extended Petri nets. A modification of the rumor spreading algorithm to include a switiching module has shown a great improvement in data dessimination in the blockchain system. In our algorithm, nodes are selected at random by a random selection parameter. Selected nodes can generate new blocks and forward the blocks to other selected nodes which will in turn randomly select other nodes to forward the received blocks. The extended Petri nets scheme used in the modelling and simulation of block omission as a performance metrics has a strong analytical and descriptive ability as we see in the results presented in form of graphs in section five (5). The results of the experienment shown on the graphs for all the values of PLOS and PREF indicates a steady decline in the ommision rate of block with increasing number of contact nodes on the network. As we mentioned from the begining, block omission could be caused by nodes refusal to forward block data to subsequent nodes on the network. It could also be caused by the failure of nodes on the network. By modifing the rumor spreading algorithm to include a switching module, the rate of omission of blocks delivered to nodes is greatly reduced. As we notice from all the graphs presented in this article, the more nodes we have on the network, the less the ommision rate. The reason for the improvement in block omision is the flexibility and simplicity of our scheme. Node selection is highly simplified and there are no complications in forwarding received data. Nodes are not under any obligation to forward received data or retransmit lost data. They are not also required to comfirm the delivery of blocks to selected nodes. Our scheme has greatly simplified the process of block propagation in the block chain system.

A further real life implementation of this scheme and comparison with other experimented schemes will be the focus of future research in this area.

REFERENCES

1. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
2. Li, J. (2018). Data Transmission Scheme Considering Node Failure for Blockchain. Wireless Personal Communications, 1-16.
3. Kostin, A., & Ilushechkina, L. (2010). Modeling and Simulation of Distributed Systems:(With CD-ROM). World Scientific Publishing Company.
4. Bahri, L., Carminati, B., & Ferrari, E. (2018). Decentralized privacy preserving services for online social networks. Online Social Networks and Media, 6, 18-25.
5. Biswas, K., & Muthukkumarasamy, V. (2016, December). Securing smart cities using blockchain technology. In High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016 IEEE 18th International Conference on (pp. 1392-1393). IEEE.
6. Qin, B., Huang, J., Wang, Q., Luo, X., Liang, B., & Shi, W. (2017). Cecoin: A decentralized PKI mitigating MitM attacks. Future Generation Computer Systems.
7. Sagirlar, G., Carminati, B., Ferrari, E., Sheehan, J. D., & Ragnoli, E. (2018). Hybrid-IoT: Hybrid Blockchain Architecture for Internet of Things-PoW Sub-blockchains. arXiv preprint arXiv:1804.03903.
8. Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2018). A survey on privacy protection in blockchain system. Journal of Network and Computer Applications.
9. Karp, R., Schindelhauer, C., Shenker, S., & Vocking, B. (2000). Randomized rumor spreading. In Foundations of Computer Science, 2000. Proceedings. 41st Annual Symposium on (pp. 565-574). IEEE.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

10. Danzi, P., Kalør, A. E., Stefanović, Č., & Popovski, P. (2017). Analysis of the Communication Traffic for Blockchain Synchronization of IoT Devices. arXiv preprint arXiv:1711.00540.
11. Mattila, J. (2016). The blockchain phenomenon.):'Book The Blockchain Phenomenon'(Berkeley Roundtable of the International Economy, 2016, edn.).
12. Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Security and Privacy (SP), 2016 IEEE Symposium on (pp. 839-858). IEEE.
13. Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In Security and Privacy Workshops (SPW), 2015 IEEE (pp. 180-184). IEEE.
14. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In Big Data (BigData Congress), 2017 IEEE International Congress on (pp. 557-564). IEEE.
15. Cachin, C. (2016, July). Architecture of the Hyperledger blockchain fabric. In Workshop on Distributed Cryptocurrencies and Consensus Ledgers.
16. Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., ... & Rimba, P. (2017, April). A taxonomy of blockchain-based systems for architecture design. In Software Architecture (ICSA), 2017 IEEE International Conference on (pp. 243-252). IEEE.
17. Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. Harvard Business Review, 95(1), 118-127.
18. Yasaweerasinghelage, R., Staples, M., & Weber, I. (2017, April). Predicting latency of blockchain-based systems using architectural modelling and simulation. In Software Architecture (ICSA), 2017 IEEE International Conference on (pp. 253-256). IEEE.
19. Göbel, J., Keeler, H. P., Krzesinski, A. E., & Taylor, P. G. (2016). Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. Performance Evaluation, 104, 23-41.
20. Lee, V., & Wei, H. (2016, June). Exploratory simulation models for fraudulent detection in Bitcoin system. In Industrial Electronics and Applications (ICIEA), 2016 IEEE 11th Conference on (pp. 1972-1977). IEEE.
21. Tosh, D. K., Shetty, S., Liang, X., Kamhoua, C. A., Kwiat, K. A., & Njilla, L. (2017, May). Security implications of blockchain cloud with analysis of block withholding attack. In Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (pp. 458-467). IEEE Press.
22. Cachin, C., De Caro, A., Moreno-Sanchez, P., Tackmann, B., & Vukolic, M. (2017). The Transaction Graph for Modeling Blockchain Semantics. Cryptology ePrint Archive, Report 2017/1070.
23. Xiong, Z., Zhang, Y., Niyato, D., Wang, P., & Han, Z. (2017). When mobile blockchain meets edge computing: challenges and applications. arXiv preprint arXiv:1711.05938.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)