Rift: A High-Performance Consensus Algorithm for Consortium Blockchain

Fazeel Ahmed Khan, Adamu Abubakar, Marwan Mahmoud, Mahmoud Ahmad Al-Khasawneh, Ala Abdulsalam Alarood

Abstract— The emergence of Blockchain have revolutionize the decentralization in distributed architecture. The advances in the consensus mechanism techniques and the development of different variants of consensus algorithms gives a huge impact on its progress. These technologies allow to have a distributed peer-to-peer network in which each external entity can be able to interact with other entities without any trusted intermediary in a verifiable manner. The existing consensus algorithms are mostly concerned with public blockchain having focused on public ledgers in general. The consortium blockchain is least focused as compared with other variants of blockchain (public and private) showing the need to address this vacuum. In this paper, we proposed a consensus algorithm named Rift for consortium blockchain which works on the principle of trust mechanism for achieving consensus in a blockchain. The consensus is achieved by distributed nodes in a consortium blockchain which were controlled by consortium members to decentralize the arbitration by voting and trust metrics. In this paper, we elaborate the comprehensive idea of Rift and discuss the working model for this algorithm. We also perform simulation on the proposed algorithm and determine the performance variables to evaluate the effectiveness of Rift. The evaluated results show the improvement in the performance which is the objective requirement for the evaluation.

Keywords: Blockchain, Consensus Algorithm, Distributed Network, Peer to Peer Network.

1. INTRODUCTION

Blockchain is a decentralized architecture for software systems. Networks are classified into two major categories: Centralized and Decentralized networks. Centralized network requires a central authority for the flow of data among the nodes while in decentralized networks it is not required to have a central authority for the processing of any transaction inside the network as stated in Fig. 1. Blockchain comes in a decentralized classification of network. Similarly, it consists of Ledger Technology which is categorized into centralized and decentralized ledgers. Centralized Ledger requires to have a central administration for managing the flow of data transaction in the ledger while distributed ledgers are independent from these limited restrictions. [1] Blockchain Technology uses decentralized ledgers which are not controlled by any centralized authority as stated in Fig.2. It depends on comprehensive technologies comprised of the private key cryptography, peer-to-peer communication, distributed storage technology and protocols governing the incentivization process among the network nodes. [2] Apart from centralized system in which the control of database rests with the central authority, including the access, manage, amend and update of records. This centralization results in high dependency on a single authority for controlling the system. The distributed database introduced by blockchain technology has fundamentally changed the way of information processing. [3] With the blockchain, the information can be entered into record and a community of users can control the way the information will be update and amend. Every node in the blockchain have an equal status. The consensus among the nodes are achieved through rules and protocols based on majority agreement. The underlying architecture for blockchain system is different as it is design to focus more on decentralization of authority. This will ensure a secure way of data replication in the distributed storage. [4]

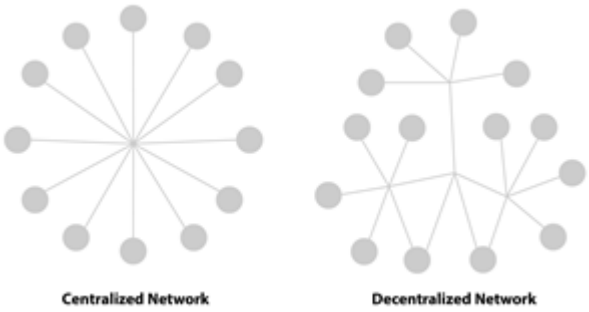

Fig. 1 Network Classification

It is first originated from Bitcoin [5] in the treatise "Bitcoin: A peer-to-peer electronic cash system" by Satoshi Nakamoto in 2008. Bitcoin is the first blockchain based application in the financial industry. The Bitcoin consensus is based on POW (Proof of Work) algorithm. It requires the use of computing power competition to achieve consensus among the blocks. Similar implementation is with Ethereum [6] which works on the POW mechanism but with the introduction of smart contracts protocol used to digitally verify the contracts without any third-party intervention. The emergence and introduction of Proof of Stake (POS) in PPCoin [7] using the concept of coin age. The age of a block multiplied by the time since its creation is considered to have a high chance of achieving a consensus among them. Bitshare [8] is also an example of Delegated Proof of Stake (DPOS)

Revised Version Manuscript Received on March 10, 2019.

Fazeel Ahmed Khan, Department of Computer Science, International Islamic University Malaysia

Adamu Abubakar, Department of Computer Science, International Islamic University Malaysia

Marwan Mahmoud, King Abdulaziz University, Jeddah, Saudi Arabia (e-mail: mahmoud@outlook.my)

Mahmoud Ahmad Al-Khasawneh, Faculty of Computer and Information Technology, Al-Madinah International University, Malaysia

Ala Abdulsalam Alarood, Faculty of Computing and Information Technology, University of Jeddah, Saudi Arabia

using the witness selection mechanism for each node. By having a witness, each node contains the most number of witnesses which increase the probability of high votes for any node for achieving a consensus.

In blockchain consensus, we need to solve two problems by considering performance variable with high priority. The Byzantine Generals Problem and Double Spending Problem [9] are the most common observed problems. The Byzantine Generals Problems occurred when the nodes are attacked by a malicious node exists inside the system which leads to tampering of content inside the nodes. The other nodes must maintain the communication among the network nodes to recognize the changes among them. Similarly, the Double Spending Problem means using multiple transactions to multiple destinations for the same process [10]. The blockchain technology solved this problem with the introduction of consensus among distributed nodes for verification of other nodes. The data transmission established in between the nodes is through the peer to peer networking topology.

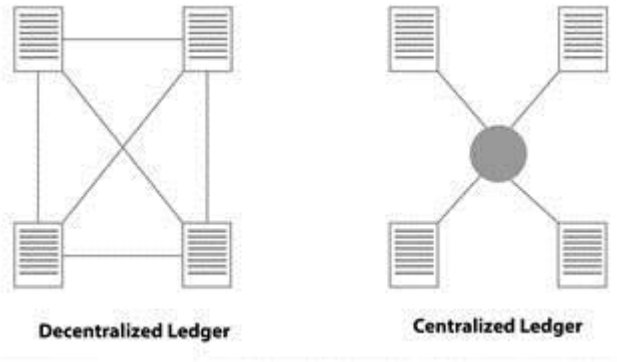

Fig. 2 Ledger Classification

Unfortunately, consensus mechanism designed for blockchain still undergo performance issues and security concerns during transaction process. It will also affect the consistency and reliability on the nodes communicating around the network. Our goal is to design a consensus algorithm which is based on Separation of Roles as the mechanism for achieving consensus. The central node of the blockchain will be the core node used for verification and production purposes for the blocks. The process is elaborate further on to the bottom level resulting in a decentralization through various roles. The impartiality is maintained through the team of elected representatives securing the rights for other members. The elected representatives will monitor the block production process thoroughly by monitoring the block producer's performance. The separation among each role will guarantees the fairness within blockchain. It supports expansion and growth of the blockchain with more focus into reducing the vulnerability related to security flaw arises in the development.

In this paper, we introduce the complete consensus process of Rift consensus-based algorithm. We introduce the concept of blockchain and discuss the technical feasibility and importance of consensus mechanism in blockchain in chapter I. We discuss on the existing approaches and proposed working solutions in resolving the consensus problem and identify the flaws arises in the blockchain in chapter II. We introduce the comprehensive analysis and system model of Rift consensus algorithm in chapter III. Similarly, we evaluate the performance analysis of Rift consensus algorithm and its shortcomings in chapter IV. Lastly, we summarize the paper in chapter V.

2. CONSENSUS ALGORITHM AND APPROACHES

2.1. Proof of Work (PoW)

The consensus algorithm has been a part of research for long period of time. The analysis of Proof of Work (POW) consensus shows that it requires a hashing power competition among the nodes in the blockchain to give responsibility rights and rewards to certain blocks. [11] The hashing power competition arises from the previous block information and it will use to solve the complex mathematical puzzle for the creation of new block. The winner will be the fastest block that has solved the mathematical puzzle in the blockchain. On the contrary, it will increase the dependency of the entire system on more hardware resources for mining the hashing power for achieving the special status which is one of the draw backs for this consensus. [12]

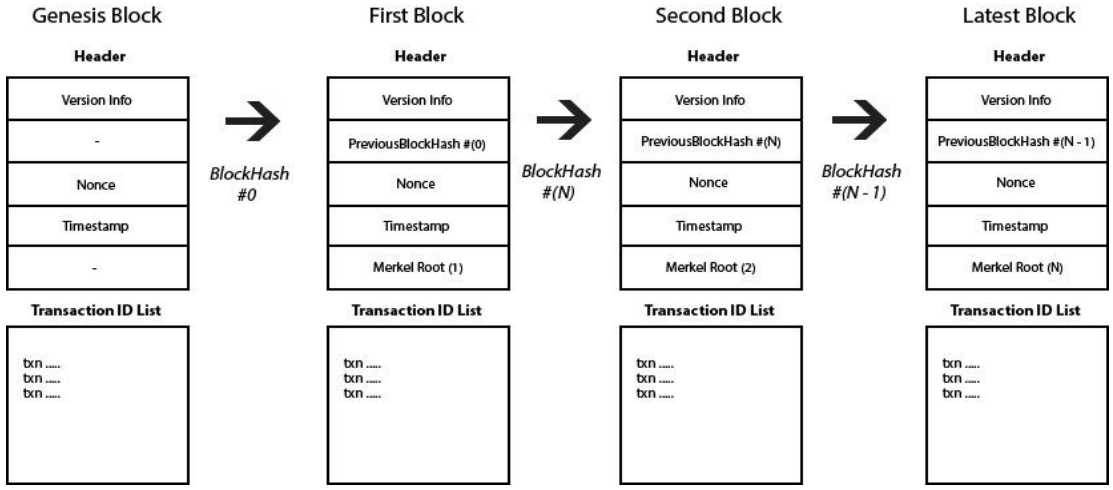

Fig 3. Block Diagram of Proof of Work Algorithm

2.2. Proof of Stake (PoS)

Similarly, the Proof of Stake (POS) consensus introduces the concept of age or timestamp in the blocks as a mechanism for achieving the responsibility rights and reward status. The term refers to "Coin Age" of the coin as the value and product of it by the time after the creation of it. [13] The probability to achieve the special status will be based on the longer time a block exists in the chain. It will give the holder of the block more rights and rewards. It motivates the block holder to increase the holding time which will improve the status of the block and it also helps to reduce the dependency on hardware resources in achieving the consensus in the system. [14]

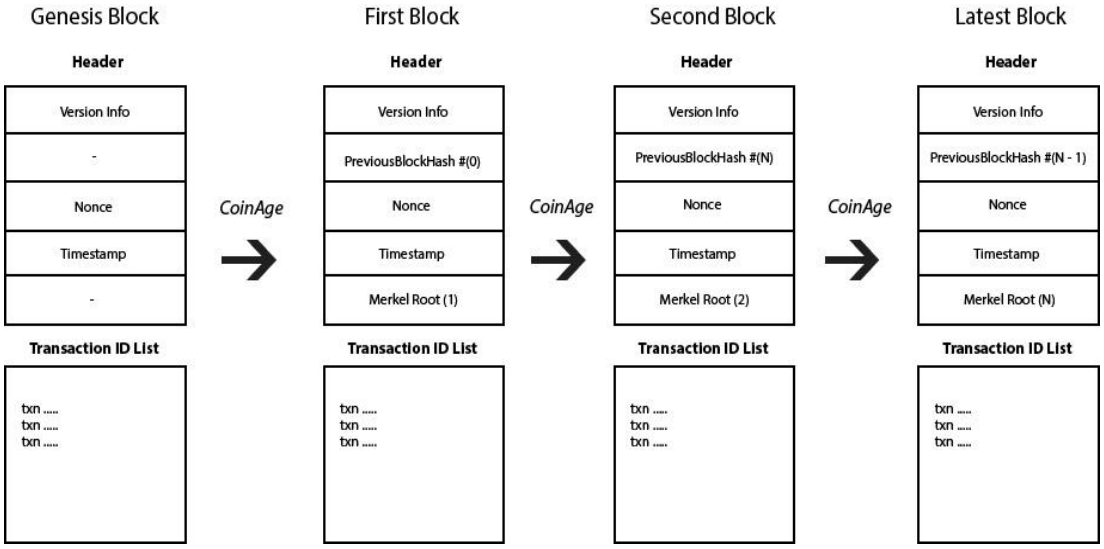

Fig. 4. Block Diagram of Proof of Stake Algorithm

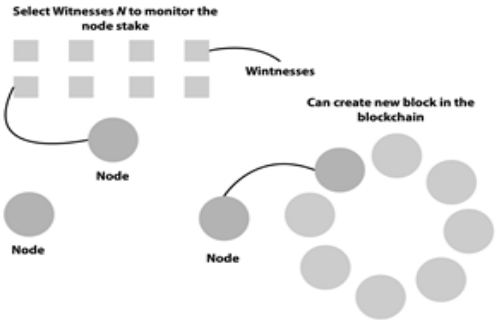

Fig 5. Delegated Proof of Stake

2.3. Delegated Proof of Stake (DPoS)

Furthermore, the Delegated Proof of Stake (DPOS) consensus introduces the concept of node approval voting for achieving consensus among the nodes. [15] It starts from N node that select any number of witnesses to generate blocks. Each node has allowed to give one vote per share on per witness. The top N witnesses that are selected on total approval such that at least 50% of nodes believed that there is sufficient decentralization in the system. [16] The successfully elected node have the right to create new blocks but in a specific period which was decided by the selecting node. If the elected responsible block failed to do so, then the responsibility will be shifted to other blocks and the starting node must nominate again new witness node to progress consensus in the system. Every node can nominate any node for witness. If in case a node has been previously elected, then the shuffle occurs to other nodes not previously been elected, then the shuffle occurs to other nodes not previously been elected and this process runs in a cycle. The DPOS based blockchain is more robust and efficient in performance than the POW and POS. [17]

3. RIFT CONSENSUS ALGORITHM

Organizations collaborate with other organizations to have a good nexus with each other. They share business data for wider business goals and prospects. Suppose that there is a peer to peer network among different organizations and several peers wants to connect with each other to have a collaboration among them for sharing data. There will be admin peers representing on behalf of their peer organization and managing the collaboration among them. The entire network uses distributed ledger technology for sharing the data among them. But no peer allowed other peers to have access to their system due to their own concerns. [18] To resolve this issue, every peer nominate a registrar and commissioner to register and elect a representative which have right to access to their system only. The process of nominating and electing the representatives will progress on real-time bases which means the representative for each peer will be introduced on any possible time of requirement. Based on this approach the elected representative will be observed by the electing authority for measuring the trustworthiness. The time frame for the observation phase will vary depending on the peers. After successfully passing through the observation stage the elected representative will become authorized to access the system all over the network.

Based on the given supposition which have proximity with the real live scenario in the organizations. We have proposed a consensus mechanism for multiple classifications of blockchain and distributed ledger technology. Rift is a trust-based voting consensus algorithm in which the

consensus is achieved by using a dual approach, voting in the first stage and measuring the trustworthiness of the elected node on the later stage. It is classified into various roles which provide benefits for separation of powers among every entity. Each entity is independent on its axis and it is linked with the other entities with limitations over their collaboration. Every process in the blockchain is independent without the interference from other processes for increasing efficiency in the consensus process.

3.1 Network Topology

Rift comprises of several actor for making the consensus process efficient. Every actor in the network will be terms as "Module" which has independent characteristic from the other modules. We propose the modules as follows: Registrar, Election Commissioner, Polling Chamber, Moderator and Block Producer. As shown in Fig. 7.

3.1.1 Registrar

Different organizations need an authority to register the candidate for entering the trust-based voting process by fulfilling the initial requirements of selection for the election. The registrar works as the initial actor in the process of voting by identifying the status and validity of the user applying to becoming the candidate for the polling process in the candidature.

a. The appointment of register is a consensus process among the organizations with mutual consent and agreement on the appointment and the limitation of power exercise by the registrar during election process (beyond the scope of this article).
b. The role of registrar is to perform all the preliminary checkups when an application has submitted to their module. The observation will be related to the current account status of the user, the duration of the account existed, the number of transactions performed by the user and the overall activities of the user with the account.

After fulfilling all the basic requirements and approval from the registrar, the candidate application will proceed to next module.

3.1.2 Election Commissioner

The major role of Commissioner in election is initially by verifying the candidate's ability with the compliance of the election policy proposed (beyond the scope of this article) as the data provide by the previous module.

a. The variables for measuring will based on the previous module's observation and the detailed procedure as proposed by the organizations after their consensus achieved on this matter.
b. The appointment of the commissioner is a consensus among the organization to avoid any biased decision making in the election process. This appointment will have based on collaboration agreement and consent by all the parties taking part in the consensus process.
c. The limitation of authority performed by the commissioner will solely depends on the mutual discretion of the organization decided during the appointment stages.

There will be an independent moderator monitoring the activities of election commissioner as part of fare election in ethical perspective from universal ethics.

3.1.3 Moderator

Moderator is an independent module function in the context of maintaining the integrity and fairness of the election process.

a. The moderator has right to access the relevant areas of concerns to measure the satisfaction level of performance done by the election commissioner and the data integrity passed by the registrar to the commissioner.
b. There will be certain metric on which the moderator will judge the integrity of the overall process before the polling proceeds.

The moderator will function the observation in dual stages of election. The initial will be in the election commissioner module and later will be in polling chamber module.

3.1.4 Block Producer (Candidate)

The block producer candidate are the official nominees taking part in polling process for achieving a consensus from the community of voters.

a. The user can only progress to block producer candidate by having an approval from the commissioner stating the criteria of officially granting the status of being a candidate for polling.
b. The block producer candidate has the right to be withdrawn from the election at any time without any further clarification needed for it.

3.1.5 Polling Chamber

The polling chamber perform the responsibility of conducting the election for block producer.

a. The block producer candidate can have the right to become the candidate in the polling chamber.
b. The polling chamber supervises all the votes casted by the voters and are responsible for announcing the results of the elections also.
c. The polling chamber will be in the observation from the independent moderators to avoid any inconsistencies over fairness in election process.

The result announced by the chamber will proceed to next module for further progression.

3.1.6 Probation

It is the stage of observation and testing the abilities of the winner while performing the dedicated roles for block production in the blockchain. The duration of this stage will be vary depending upon the requirement as set by polling chamber. This stage is the measuring phase of observing the trust level of the winners and their sincerity on block production with efficiency and within speculative time frame.

3.1.7 Block Producer

Block Producer perform the role of validating and creating of new blocks in the blockchain.

a. This status is the highest in the blockchain network due to its number of rights and authority as compared to others in the network.

b. They oversee producing blocks but the number of their presence in the system will be limited.

This limitation favor in the competition among them which results in more participation from the users and the growth in the maturity level of consensus in the blockchain.

3.1.8 User

They are ordinary user participating the blockchain. Their roles are beyond other roles which are depended highly of cryptographic mechanism to work.

a. They can enter and exit the system anytime without having an authorize permission from any module.
b. They can participate in the process of block validation. In simple, they can become the part of consensus process for block producer.
c. They can see the whole consensus process from any stage.

They have the right for message passing and communication over the network.1

3.2 Consensus Mechanism

The process starts from the common user in the system. Any user in the system have a right to become the block producer by submitting a request opened by the registrar at any time. The submitted application is authenticate by the registrar for fulfilling the eligibility criteria as stated in the eligibility policy. The registrar has the right to approved or not approved any application depending on the eligibility.

Let Suppose R is the Registrar, B is the candidate standing for block producer election, E is the eligibility criteria for nominating as a candidate, AY is for the approval of application and AN is for not approval of application and UA is for all the users in the system with active status for their presence. The system will perform the operation as shown in Fig. 8.

After approval from the registrar the application is transferred to election commissioner for verifying and judging the compliance with election policy. The election commissioner has the right to approve or not approve the application at the discretion of its own axis. The overall process of compliance will be monitored by an independent moderator for fare election process from all its dimensions.

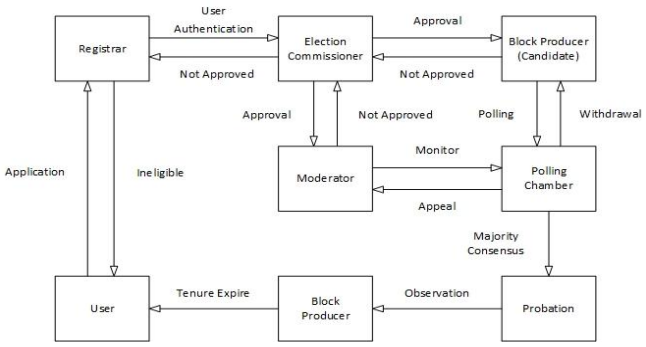

Fig 7. Nexus among different modules

Let Suppose, E is the election commissioner, P is the declared election policy, EPC are the election policies and compliances, SY is the satisfaction of compliance, SN is the non-satisfaction of compliance, PC is the polling chamber for election process and M is the moderator for observation of all the process as shown in Fig. 9 and Fig. 10.

The application proceeds further for entering into the polling for achieving consensus for block producer status. The block producer candidate has the right to take part in the election process after passing through the given processes. It will be done with polling chamber. Polling chamber manages and collect the votes and announce the result of the election.

Let Suppose, PC is the polling chamber, V are the votes for candidates participating in the elections and CA and CB are any candidate competing one another, W is the winner, R is the runner up candidate of the election and PB is to represent the probation module. The operation of the system works in the way as elaborated in Fig. 11.

The announcement of the result will grant the partial status of block producer to the winning candidate but with probation on the fulfillment of the criteria for achieving the trust from the polling chamber within speculative period of time. In case of failure from satisfying the polling chamber, the results will be the disqualification of candidate from the partial status of block produces as granted based on election results. The candidate can apply again for candidature with the process starts from the beginning.

Let Suppose, TL represents the trust level of the candidate, RY shows the satisfaction of candidate's performance, RN is non-satisfaction of candidate's performance and BP is to represent the status of block producer inside the system for the successful candidates. The system performed in way as defined in Fig. 12.

The successful completion from all the processes will give candidate a status of block producer which is the highest authority in blockchain for validation of new blocks. This status has a tenure cycle within which the producer can validate new blocks. After the expiration of this tenure the consensus process will start again from the beginning in the same way as did before. The priority for participating in the consensus will be given to the new candidates based on the eligibility criteria. The comprehensive consensus process of Rift algorithm is explained in Fig.13.

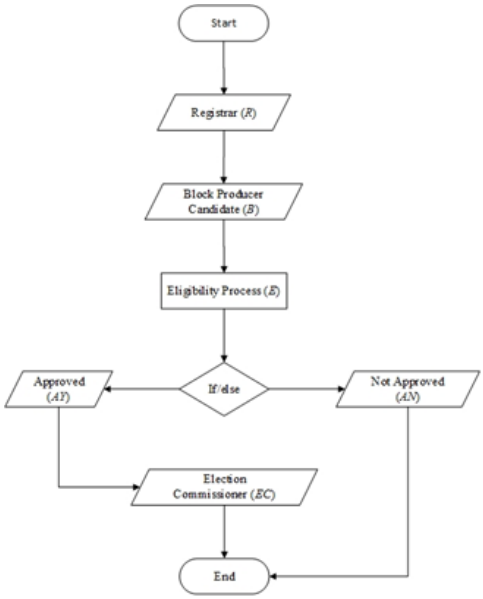

Fig 8. Flowchart for Registrar Module

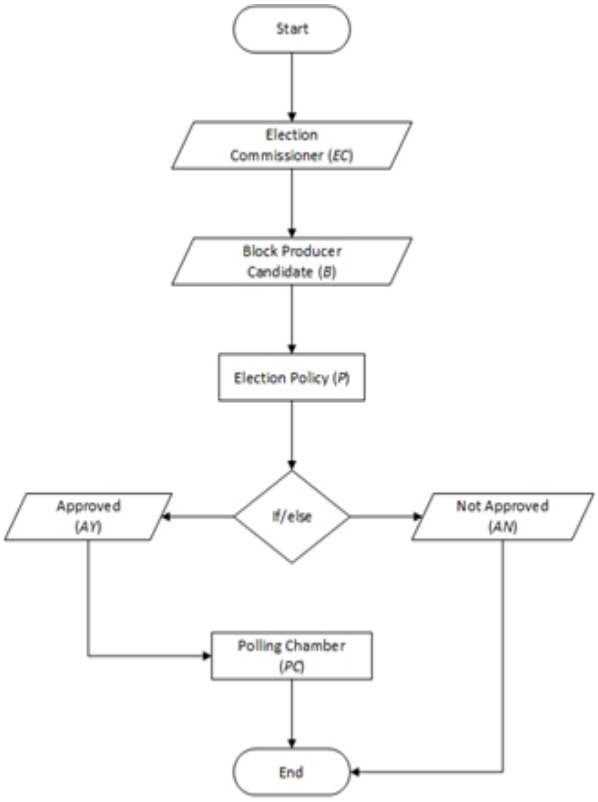

Fig 9. Flowchart for Election Commissioner Module

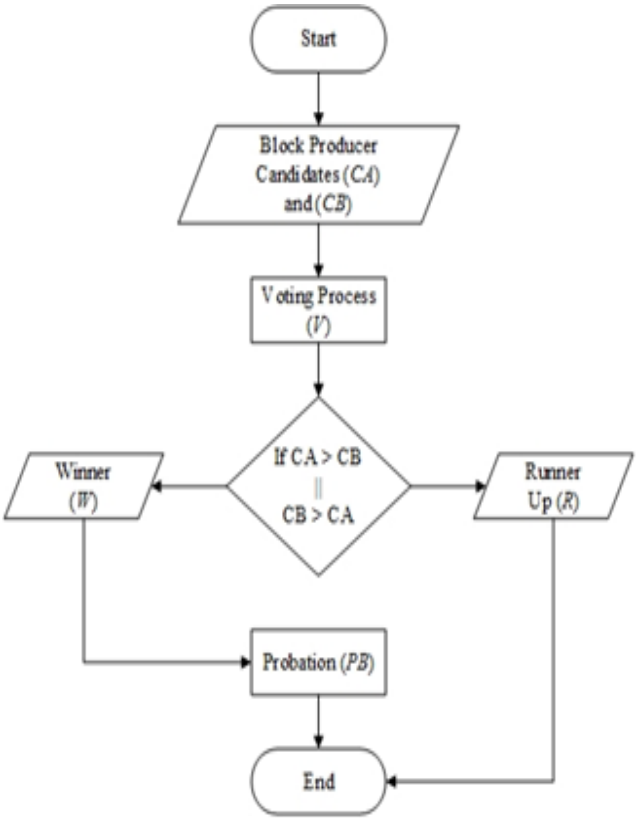

Fig 11. Flowchart for Polling Chamber Module

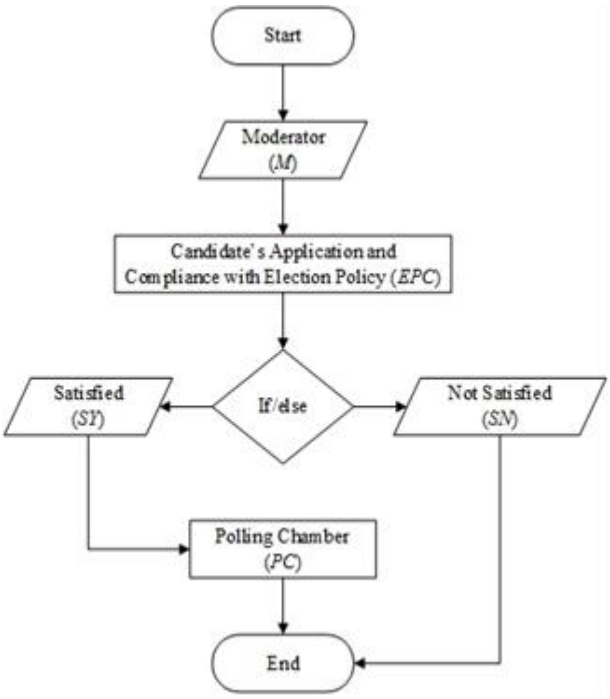

Fig 10. Flowchart for Moderator Module

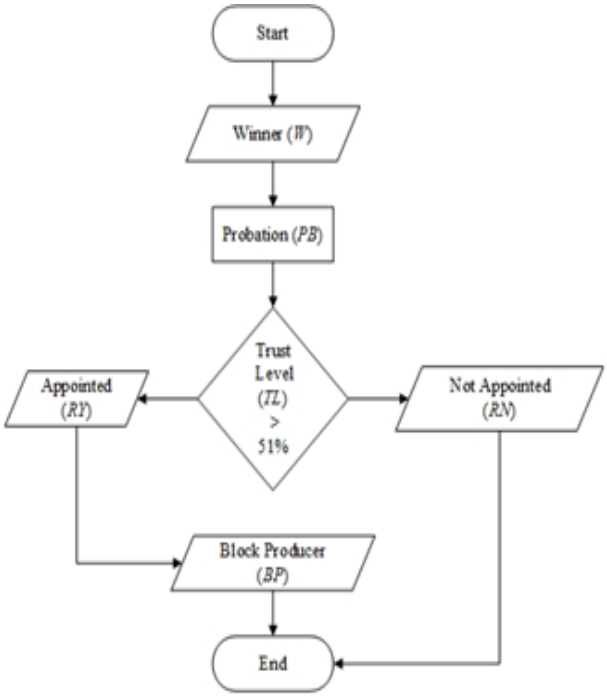

Fig 12. Flowchart for Probation Module

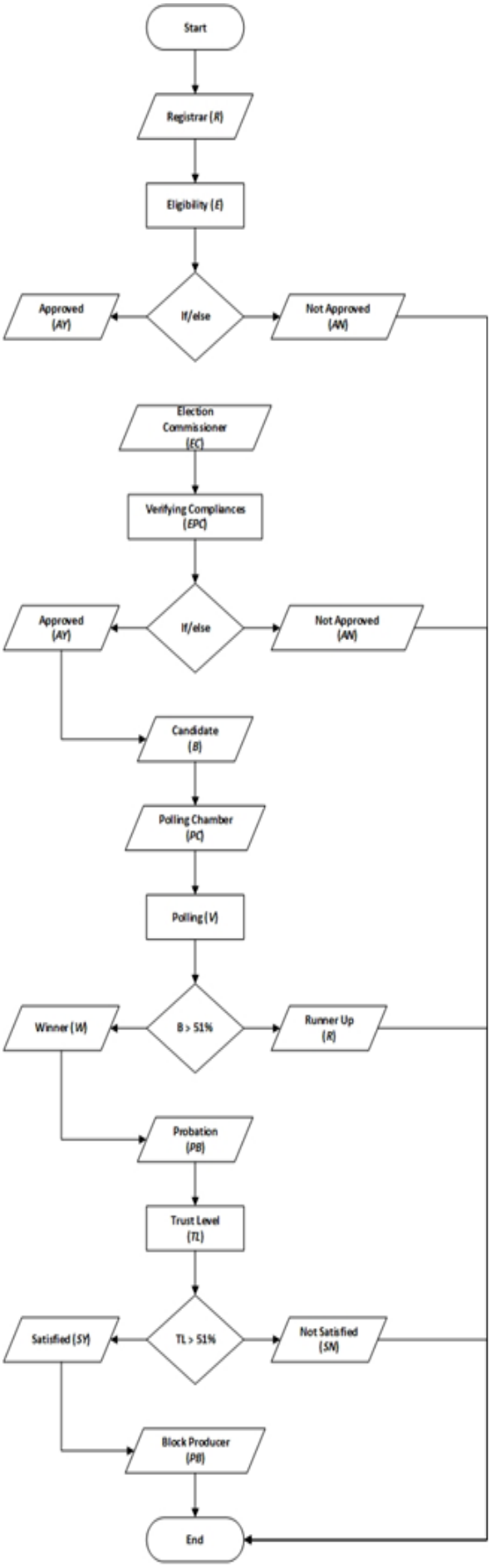

Fig 13. Flowchart for Overall Consensus Process

4. PERFORMANCE ANALYSIS

The consensus model proposed in this paper is based on trust metric with support from the voting mechanism. The importance of performance and efficiency is vital in achieving the consensus. Our proposed model can assure the high performance and efficiency of blockchain for a rapid data flow across the network. In this chapter, we will analyze the Rift algorithm from two major parameters, voting mechanism and trust mechanism. We will elaborate the key areas of the parameters and perform an in-depth analysis on the requirements and performance engineering of the Rift algorithm.

4.1 Performance

Lemma 4.1: A Block can be validated within seconds after achieving consensus.

Proof: Block producers make sure that the validation of blocks will be done on speculative time frame of 5 seconds per block when the consensus on any new block have been achieved. If the block producer fails to manage the efficiency in the block production, then the turn will be over on the responsible validator side and a new consensus will begin for getting a new block producer. The efficiency in the block validation is directly proportional with the time required by the block validator to validate any new block in the blockchain. Let suppose, E represent efficiency of the block validation and T is the time required for a validator for validation. Then,

$$E \propto T$$

If in case the efficiency of the block validation will decline due to time constraint factor, then the consequences of this will impact on the overall performance of the block validation process. In other case, we can say that the efficiency will become inversely proportional with the decline time required in block validation.

$$E \propto 1/2$$

Consider there are 100 new blocks need to be validated by the block produces. Each block requires average of 5 seconds to be validated and the total of 100 blocks required time will the product of average into total number of blocks. As the time limit is maintained during the block validation process, the efficiency of the blockchain will be consistent with performance as shown in Fig. 14. But if in case of non-maintainable condition occurred in the network then the efficiency will be affected with negative impacts on the overall process on block validation as shown in Fig. 15. Therefore, it is necessary for the block validator to be consistent with the time constraint as set by the consensus protocol for high performance orientation and effective implementation of block generation for the blockchain.

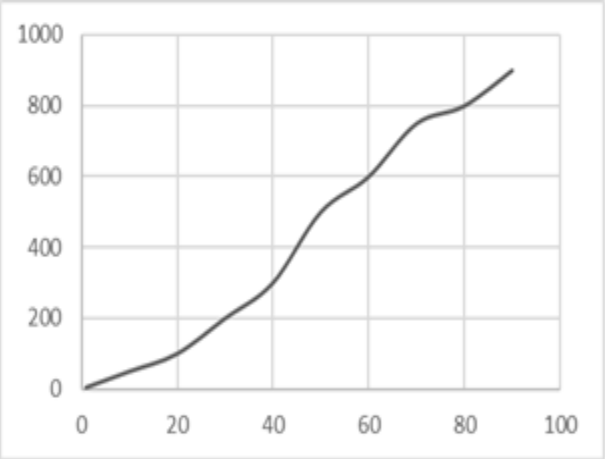

Fig. 14. Increase in Performance when block validation occurs within speculative time frame

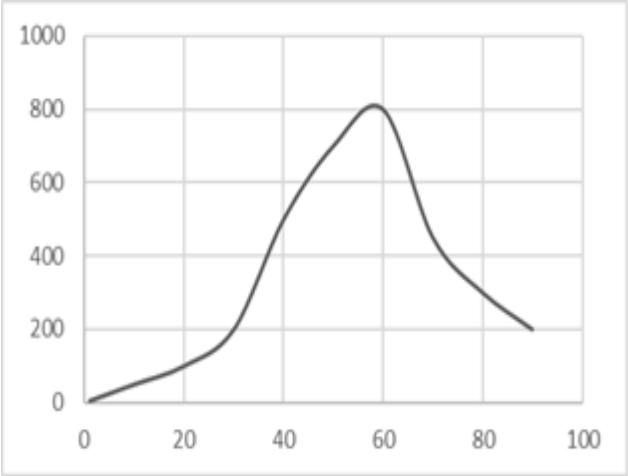

Fig. 15. Decrease in Performance when not maintaining the block validation within speculative time frame

4.2 Security

Lemma 4.2: The consensus process is secure from taking over by unwanted nodes and avoid tempering the consensus process by seizing from the majority nodes.

Proof: Considering the total number of positions for registrars and election commissioners, the blockchain will calculate the actual requirement of the needed positions. If the number of positions exceeds the current requirements, then the possibility of security risk arises in the blockchain. It is necessary to maintain the integrity of the calculation process by considering independent variables and implements access control inside this process. The access control can be implemented by authorization and authentication mechanism from computer security principles. Let suppose, the EC and RG are the total number of election commissioners and registrars required for the consensus process respectively. The RQ is the actual requirement needed for the blockchain to process the block validation process. The required number must have integrity constraint for securing the block validation process.

$$EC < RQ$$
$$RG < RQ$$

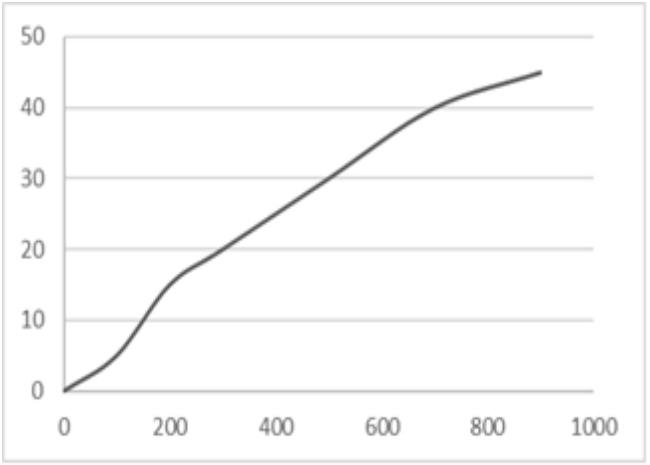

Fig. 16. Security profile when the number of positions required based on block requirement works accurately

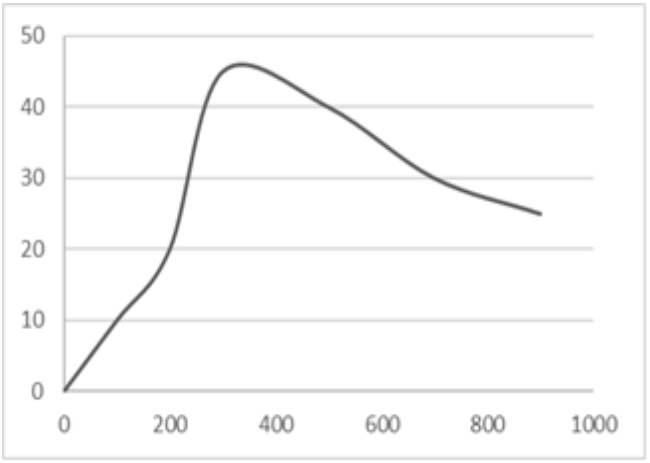

Fig. 17. Rise of vulnerability occurs due to lack of synchronization between the two stated variables

Consider that the need of actual number of blocks required is 1000 blocks and the positions required for per 100 block will be 5 position each. The security risk is the comparison between these two variables and the consistency among them respectively. The possible risk factor arises depend upon the required number of positions calculated by the system. The analysis between the stated variable are given in Fig. 16 and Fig. 17 respectively.

5. CONCLUSION

In this paper, we propose a new consensus algorithm Rift which can be used for multiple classifications of blockchain platform. Our mechanism is based on dual approach meaning thereby is that voting as the instrument for becoming an official candidate for block producer and trust as the sole metric for achieving the status of block producer. The voting mechanism supports the impartial process of consensus from any biasness while the trust guarantees the trustworthiness of an elected node for block validation process. Rift mechanism supports high performance and good efficiency in block validation process as well as provide robust safety from upcoming vulnerabilities from outside networks nodes.

`REFERENCES

1. D. Efanov and P. Roschin, "The All-Pervasiveness of the Blockchain Technology," Procedia Computer Science, vol. 123, pp. 116-121, (2018).
2. T. M. Fernandez-Carames and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things (IoT)," IEEE Access, (2018).
3. M. Isaja and J. K. Soldatos, "Distributed Ledger Architecture for Automation, Analytics and Simulation in Industrial Environments," IFAC PapersOnLine, Vols. 51-11, pp. 370-375, (2018).
4. K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for Internet of Things (IoT)," IEEE Access, (2016).
5. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," White Paper (2008). [Online]. Available: https://bitcoin.org/bitcoin.pdf.
6. C. Ethereum, "A Next Generation Smart Contract & Decentralized Application Platform," White Paper, [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper.
7. S. King and S. Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake," White Paper, (2012). [Online]. Available: https://peercoin.net/assets/paper/peercoin-paper.pdf.
8. F. Schuh and D. Larimer, "Bitshares 2.0: Financial Smart Contract Platform," [Online]. Available: https://bravenewcoin.com/assets/Whitepapers/bitshares-financial-platform.pdf.
9. L. Lamport, R. Shostak and M. Pease, "The Byzantine Generals Problem," ACM Transactions on Programming Languages and Systems, vol. 4/3, pp. 382-401, (1982).
10. X. Yu, M. T. Shiwen, Y. Li and R. D. Huijie, "Fair Deposits against Double-Spending for Bitcoin Transactions," IEEE Conference on Dependable and Secure Computing, (2017).
11. N. Houy, "The Bitcoin Mining Game," LEDGER, vol. 1, pp. 53-68, 2016.
12. A. Sward, I. Vecna and F. Stonedahl, "Data Insertion in Bitcoin's Blockchain," LEDGER, vol. 3, pp. 1-23, (2018).
13. M. Borge, E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly and B. Ford, "Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies," 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 23-26, (2017).
14. J. Kang, Z. Xiong, D. Niyato, P. Wang, D. Ye and D. I. Kim, "Incentivizing Consensus Propagation in Proof-of-Stake Based Consortium Blockchain Networks," IEEE Wireless Communications Letters, pp. 1-1, (2018).
15. B. Wang, J. Sun, Y. He, D. Pang and N. Lu, "Large-scale Election Based On Blockchain," Procedia Computer Science, vol. 129, pp. 234-237, (2018).
16. D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei and C. Qijun, "A Review on Consensus Algorithm of Blockchain," IEEE International Conference on Systems, Man, and Cybernetics (SMC), (2017).
17. Z. Chen and Y. Zhu, "Personal Archive Service System using Blockchain Technology: Case Study, Promising and Challenging," 2017 IEEE International Conference on AI & Mobile Services (AIMS), pp. 93-99, (2017).
18. H. Johng, D. Kim, T. Hill and L. Chung, "Using Blockchain to Enhance the Trustworthiness of Business Processes: A Goal-Oriented Approach," 2018 IEEE International Conference on Services Computing, pp. 249-252, (2018).