International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

An Effective Randomization Framework to POW Consensus Algorithm of Blockchain (RPoW)

Sumathy Kingslin, Rafath Zahra

Abstract: ***Blockchain technology has become a buzzword due to its intuitive applications and its decentralized network architecture. Blockchain is a decentralized system that uses peer -to - peer networking and appropriate consensus algorithm for secure and reliable transactions and records them all in an immutable ledger as chain of blocks. The world got introduced to the blockchain technology, when Satoshi Nakamoto released Bitcoin in 2009[2]. Though this technology is famous for being the backbone of cryptocurrencies, it has got into various industry domains and many applications have been developed using blockchain [11]. The consensus algorithm used in Blockchain architecture influences how agreement is made to add a new block among all the nodes in the network. PoW (Proof of work) is the consensus algorithm applied in the Bitcoin network architecture and many other blockchain applications. PoW requires each node to solve a cryptographic puzzle with adjusted difficulty, to get the privilege to add a new block to the current chain. The first node that solves the puzzle will have this privilege and some reward. Proof-of-Work (PoW) uses extensive amounts of electric power and steep computing hardware as an effect of their consensus procedure [1]. This proposed work presents an effective randomization framework that reduces the execution time required to calculate the hash value. The number of instruction-set required to compute the PoW consensus is also reduced. This approach helps in maintaining a fair decentralized network to construct blockchain applications.***

Keywords—Blockchain, Decentralized, PoW, RPoW, Time, Instruction Set, Consensus, Hashing, Randomization.

I. INTRODUCTION

In recent globalized business environment, online transactions are the convenient and commonly used method for payments and any data exchange. The transactions in a traditional banking system and any online method of payment involves a central authority. All the transactions were only possible with the help of a middle-man who is in charge for supervising the transactions in a safe manner. This middle-man is a trusted intermediary and is responsible for any malfunction or fraud in the transactions. The data exchange happens through this intermediary.

Revised Manuscript Received on October 30, 2019.

* Correspondence Author

Dr. (Mrs.) Sumathy Kingslin, [1]Associate Professor, Department of Computer Science,Quaid-e-Millath Government College for Women(A), Chennai-600 002, TamilNadu, India

Mrs. Rafath Zahra, [2]M. Phil Scholar, Department of Computer Science, Quaid-e-Millath Government College for Women(A), Chennai-600 002, TamilNadu, India

This is known as Centralized network for information sharing or transactions. Fig1. represents the modes connected in Central network architecture. In the centralized system an intermediary gets the central influence and freedom of decision making to approve any transaction. The intermediary has the privilege to use the entire data whenever required [16]. All the guidelines and procedure for communication and transactions are decided by this intermediary. This intermediary has to be trustworthy for safe data exchange. If the servers of this middle-man malfunctions the entire network will get effected. Blockchain is a decentralized network that overcomes the issues observed in a centralized network system [12]. This network system doesn't provide easy access of data hence providing a secure data interchange architecture [3]. As in Centralized network, the rules are not decided by any intermediary, every node of the network is predetermined of rules. Consensus of every node in the blockchain is mandatory for any kind of exchange in the network. Blockchain uses peer -to - peer networking for information sharing [6]. Fig2. shows the nodes interconnected in peer -to – peer networking. It offers a different way of secure transaction by believing that the nodes involved in a network do not trust each other for any transaction. All the nodes are required to have their own copes of the updated ledger to eliminate the need of the central authority. Since it is a decentralized network, the architecture is not dependent of a central server [13]. Even if one node malfunctions the network remains stable with the help of the data available with the other nodes.

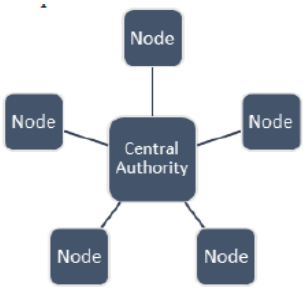

Fig1. Central Networking

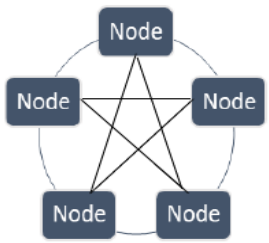

Fig2. Peer–to–Peer Networking

In the Blockchain architecture, the nodes come to consensus to authorize a transaction by following a set of procedures. All the nodes use one consensus algorithm. The main purpose is the undisputed agreement among the nodes, even if some nodes are untrustworthy. Miners are nodes of a blockchain network that devote a lot of resources to calculate difficult computation and validate transactions. As a recompense miner gets some reward based on the blockchain application. Proof of Work (PoW) is the consensus algorithm used in Bitcoin systems.

Wherein each node uses cryptographic computations to calculate the hash value of the block that includes transaction details. When a node calculates the hash value of a set of transactions, it is spread to all other nodes involved in the network. The other nodes evaluate the rightness of that hash value. A block with new hash is created and is appended to the chain of blocks. A lot of time and resources are consumed in the process of hash calculation [14]. This work provides a framework of using Randomization along with PoW Consensus algorithm to overcome the issues related with the traditional Proof of Work algorithm.

The paper structure is arranged in a way to provide clear description of blockchain architecture, the working of Proof of Work consensus mechanism, its flaws and the mechanism of the proposed algorithm and how it overcomes the issues of PoW. Section I included the introduction with an overview of the blockchain technology. Section II sketches the working of Blockchain. Section III contains mechanism of PoW Consensus Algorithm followed by Section IV that describes the proposed methodology, Section V includes the results and Section VI gives the conclusion.

II. WORKING OF BLOCKCHAIN

The creation of blocks in blockchain vary depending on the type of application being built based on blockchain such as sharing food resources among organizations or cryptocurrency transaction. Fig. 3[7] illustrates the working of blockchain.

A record is maintained of all the transactions. Any node can start a transaction in the distributed network. Digital Signatures are used to offer genuineness of the transactions.

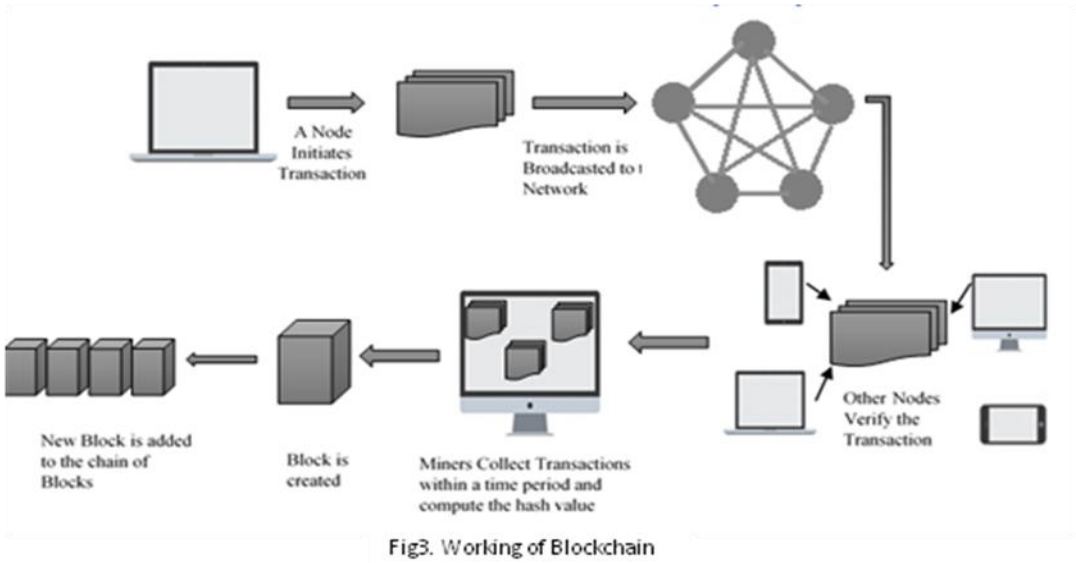

Fig3. Working of Blockchain

A verification process used by the system includes digital signature of the sender and the message and its combined and encrypted. The decryption process requires the public key of the sender. Blockchain also includes unique Transaction ID along with signatures for better security [7]. The nodes of the network are updated with the latest verified transaction and nodes replace their copies of the ledger with the updated copy. Blockchain uses the core idea of all the nodes trusting the ledger that has more amount of work put into. Blockchain uses Consensus algorithm for all the nodes to agree on one mechanism to authorize transactions and add blocks to the chain of blocks. With the help of this organized protocol of creating blocks, this structure permits any node to be a block maker also known as miners. Miners collect few transactions that are aired in a block and do the computations to find the hash value of the block begin with the specified number of zeros. Once they calculate the hash, they show their version of block in the network. The other nodes of the system do not trust the block instantly, the nodes delay for the longest chain and change their ledger copy of blockchain with the newly verified blocks. Miners are rewarded for the successful computation of hash and creation of blocks [8].

III. PROOF OF WORK (POW) CONSENSUS ALGORITHM

Blockchain maintains an architecture that is secure for every member of the network can share. The architecture does not require any central authority. The database of the network is distributed across the network and is updated with rising list of records. This distributed ledger is fault tolerant and cannot be tampered easily. The mostly used consensus algorithm in most of the blockchain applications is Proof of Work Consensus [4].

The new set of transactions are broadcasted in network for validation. The nodes of the network compute cryptographic puzzle to validate the transactions. Once the desired hash value is calculated the block containing the transaction details are added to the chain of blocks. This procedure of calculating hash value is known as proof of work [9]. High computation speed is required for complex calculation of hash value, specialized hardware is used for such high-speed computation and lot of energy is consumed during this process [5]. Most of the energy is consumed in computing SHA256 algorithm. In this distributed network, computation happens concurrently and there are chances of more than one node calculating the hash at the same time. The completed nodes broadcast their version of updated blocks to the network. A temporary fork occurs in the blockchain, few nodes append blocks to one branch, while other nodes append blocks to other branch. To overcome this issue and to maintain same ledger across the network, the architecture ensures that the branch with the longest branch gets appended in the network and others will be rejected [10]. Fig4. gives a clear understanding of working of the existing PoW Consensus algorithm.

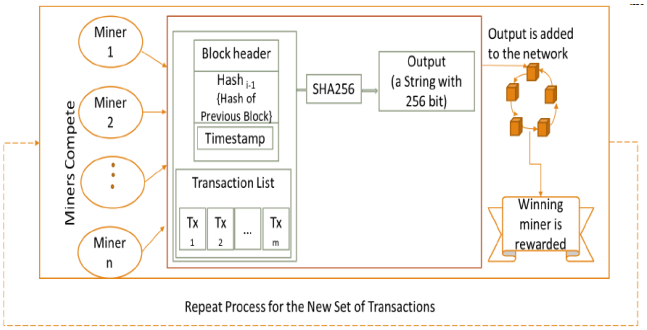

Fig.4 PoW Methodology

IV. RANDOMIZED PROOF OF WORK(RPoW)

In the existing PoW consensus algorithm, the competition between miners to calculate the hash value of transactions require more time and electricity. It involves the execution of the SHA256 cryptographic hash function to calculate the hash value for the given set of transactions. Each miner has to execute the SHA256 hash function which is very complex to solve. This results in the same instructions being executed repeatedly consuming more resources [15]. The Proposed algorithm is termed as Randomized Proof of Work Consensus as the time and resources consumed in computing the hash by every miner is reduced by eliminating the competing protocol. A randomization protocol is included in which one particular miner is selected by the network to compute the hash value instead of all the miners computing the same hash calculation wasting time and resources.

To select one miner from the set of miners of the network, a randomization algorithm is run before the process of hash calculation using SHA256 algorithm. The miners are assigned MinerIds and the MinerIds are taken as input for the algorithm. To eliminate the repetitive MinerId as output for new set of transactions, current time is set as Seed Value and a randomization function is run to retrieve a Working MinerId. Only the selected Working Miner is used to execute the Proof of Work algorithm. Fig5. depicts the process of RPoW algorithm. The working Miner calculates the $Hash_i$ of the block together with the new set of transactions. The calculation of hash requires the timestamp of the transactions and the set of transaction details and $Hash_{i-1}$ (the hash number of the previous block) to maintain the continuance of the chain of blocks. This protocol promises to save the time required by all the miners to calculate the hash value by eliminating the need of competing. Only the working miner executes the SHA256 algorithm. The calculated hash is announced to the network and the working miner is incentivized. The process of randomized selection is repeated for the new set of transactions.

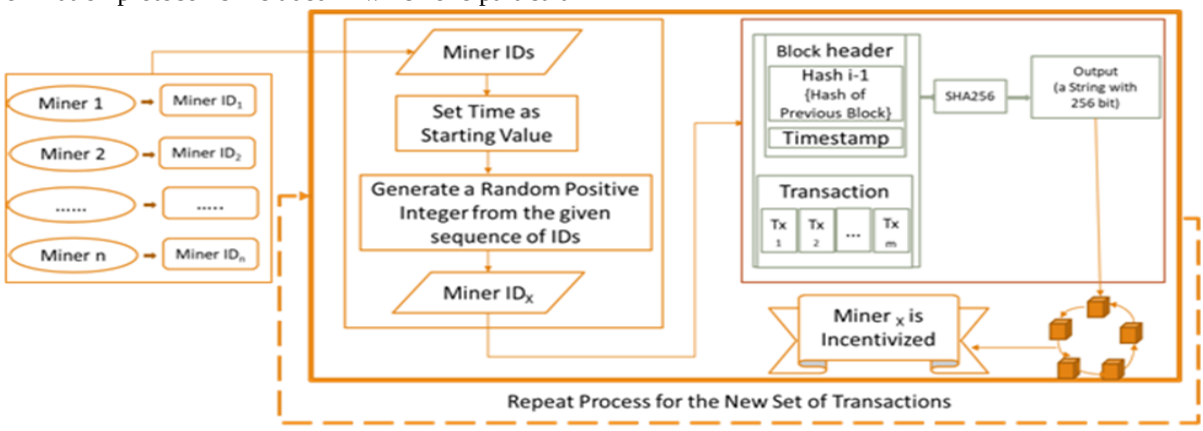

Fig.5. RPoW

Algorithm 1: RANDOMIZED PROOF OF WORK (RPoW)

Input: Miner ID, Current time(t_c), $Hash_{i-1}$, Transaction Info, Working Miner ID

Output: Hash value of the new set of transactions ($Hash_i$)

1: Assign MinerIDs for n number of Miners in the network.
2: Initiate randomization for selecting Working $MinerID_x$
  2.1: Input MinerIDs, id_1.....id_n
  2.2: Set current time, t_c as Seed for Rnd function
  2.3: $WorkingMinerID_x$? Rnd fn (t_c, id_1.....id_n)
3: Initiate Proof of Work (PoW) algorithm
  3.1: $Hash_{i-1}$? Hash value of previous transactions
  3.2: m? number of transactions in a given time
  3.2: transinfo ? [(SenderAC, RecieverAC, Amt)$_1$ ... (SenderAC, RecieverAC, Amt)$_m$]
  3.3: $Hash_i$? SHA256($Hash_{i-1}$, t_c, transinfo)
  3.4: Append $Hash_i$ to chain of blocks
  3.5: Incentivize $WorkingMinerID_x$
4: Go to Step2 for next new set of transactions

V. RESULT

The methodology used in PoW consensus involves (n) number of miners to compete with each other for the calculation of Hash value for the new set of transactions. It requires (n) number of miners compute the hash calculation i.e. (n) number of times, which causes repetition of same hash calculation. This repetition causes consumption of more time and resources. PoW algorithm consumes more time for the extra computation which results in more energy consumption affecting the environment.

In the proposed RPoW consensus, the repetition of hash calculation is eliminated by selecting a WorkingMiner through the process of randomization. The calculation of hash value is executed only once by WorkingMiner instead of executing (n) number of times. The results of this work prove that, using RPoW algorithm for Blockchain applications can save time and resources having a better impact on the environment.

The found result is useful for any type of blockchain application. The RPoW can be used to construct blockchain application with any type of transactions such as Supply chain management, Data sharing and so on. Fig6. shows the comparison of the calculated time value of the existing PoW methodology and the proposed RPoW.

Fig6. Time Comparison of PoW and RPoW

The hash value was calculated and compared with both algorithms with varied difficulty level and varied number of miners in the network. Fig 6. represents calculation with 4 miners and difficulty level from 1 to 5. The chart clearly explains that with all the difficulty levels, the proposed RPoW consumes less time to execute the hash calculation.

The analysis of instruction-set in the PoW algorithm shows that the competition among the miners in the methodology causes repetition of instruction-set consuming more resources. The proposed RPoW methodology adds the instruction-set required to select the WorkingMiner and eliminates the need for repeating the instruction-set to calculate hash value (n) number of times. This results in use of comparatively lesser number of instruction-set than PoW. Fig7. shows the comparison of instructions used in both the algorithms. The number of Instructions required to calculate the hash value is represented by I, the instructions of the main program are represented by (m), (s) represent code set of SHA256 algorithm and (n) represent the number of miners. The instructions required in PoW was calculated as

$$I= m+(s)*n$$

The calculation of instructions required in RPoW is

$$I= m+(r)*n+s$$

The number of instructions in RPoW algorithm include the instructions required to select the working miner and is represented by (r).

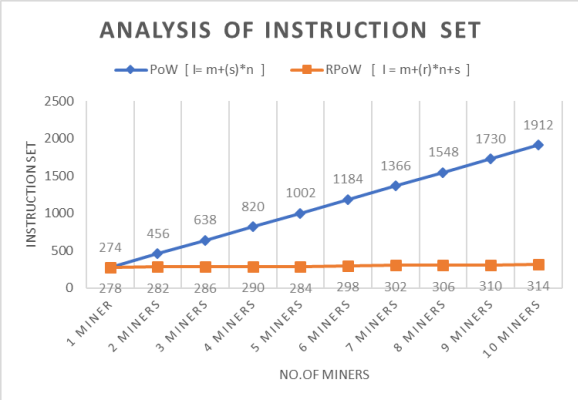

Fig.7 Analysis of Instruction Required

The number of instructions required to execute the hash calculation is also minimized. In PoW protocol as many numbers of miners are involved in the network, that many numbers of time the hash calculations instructions are executed. Whereas in RPoW the hash calculation is executed only once by the working miner.

VI. CONCLUSION

Applications built on blockchain, are used in various fields, and has proven its effectiveness through its promising secure features. But the protocol used by Blockchain has the flaw of more energy consumption due to the time required in complex calculations involved, and also consumes more resources when the PoW consensus algorithm is used, which involves competition between miners and repeats execution of same set of instruction. This proposed work proves that the time consumed in PoW consensus protocol can be saved by using the randomization framework. The analysis of Instructions set used to compute the hash value in RPoW is also comparatively less than PoW consensus protocol. It can be expected that preserving time and instruction sets also impact on preserving power consumption and also avoids wastage of various resources required to calculate the hash value by every miner involved in the network. The proposed framework of Randomized Proof of Work is designed in a manner that it can be applicable in any proof based blockchain application. The input values that go in the SHA256 algorithm will vary depending on the transactions involved in the blockchain application. The proposed methodology can be used in fields such as supply chain management, sharing of medical records, cryptocurrencies, data exchange or in any other peer – to – peer network structure.

REFERENCES

1. Michael Nofer, Peter Gomber, Olive Hinz, Dirk Schiereck (2017, March). *"Blockchain"*. Springer. Bus Inf Syst Eng 59(3):183–187
2. S. Nakamoto. "Bitcoin: A Peer-To-Peer Electronic Cash System". 2008.
3. Christopher Natoli, Vincent Gramoli, "*The Blockchain Anomaly*", (2016) IEEE 15th International Symposium on Network Computing and Applications.
4. L.M. Bach, B. Mihalijevic, M. Zagar, (2018, May) "*Comparative Analysis of Blockchain Consensus Algorithm*". MIPRO, Opatija Croatia.
5. Congcong Ye, Guoqiang Li, Hongming cai, Yonggen Gu, Akira Fukuda, (2018) "*Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting*". 5th International Conference on Dependable Systems and Their Applications (DSA)
6. Dr. Arati Baliga, (2017 April). *Understanding Blockchain Consensus Models*. Persistent
7. Sumathy Kingslin, Rafath Zahra, "*Compendious Summary of Blockchain*", International Journal of Computer Sciences and Engineering, Vol.07, Issue.05, pp.161-166, 2019
8. Deepak K. Tosh, Sachin Shetty, Xueping Liang, Charles Kamhoua, Laurent Njilla. "Consensus Protocols for Blockchain-based Data Provenance: Challenges and Opportunities*"*
9. Giang-Truong Nguyen, Kyungbaek Kim. (2018, February). *"A Survey About Consensus Algorithm Used in Blockchain*". Journal of Information Processing System, Vol.14, No.1, pp.101~128
10. Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wang Xiangwe*, Chen Qijun, (2017 October), "A Review on Consensus Algorithm of Blockchain". *IEEE International Conference on Systems, Man, and Cybernetics (SMC).*

11. Nitesh Singh, Jay Bothra, Sandeep Kothale. (2018, December). "*Blockchain Based Data Sharing Framework*". International Research Journal of Engineering and Technology (IRJET) Volume: 05 Issue: 12
12. Liang Wang, Wenyuan Liu, Xuewei Han. "*Blockchain-Based Government Information Resource Sharing*". IEEE 23rd International Conference on Parallel and Distributed Systems.
13. Shlok Gilda, Maanav Mehrotra. (2018 January). "Blockchain for Student Data Privacy and Consent". *International Conference on Computer Communication and Informatics*
14. Johanna Ullrich, Nicholas Stifter, Aljosha Judmayer, Adrian Dabrowski, Edgar Weippll, "Proof-of-Blackouts? How Proof-of-Work Cryptocurrencies Could Affect Power Grids".
15. Arthur Gervais, Ghassan O. Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, Srdjan Cˇ apkun, "*On the Security and Performance of Proof of Work Blockchains*"
16. Akanksha Kaushik, Archana Choudhary, ChinmayEktare, Deepti Thomas, Syed Akram, "*Blockchain Literature Survey*", 2017 2nd IEEE International Conference on Recent Trends in Electronics Information & Communication Technology (RTEICT), May 19-20, 2017

AUTHORS PROFILE

Dr. Sumathy Kingslin, PhD, is an Associate Professor in the Department of Computer Science, Quaid E Millath Government College, Chennai. She has a teaching experience of 25 years and is into the field of research since 2013. She has published a number of journals and has a good citation score. She has also presented her research ideas in many conferences and few of her work were recognized as best paper. She has conducted research projects approved by UGC. She is Board of Studies member in many different colleges and Universities in Chennai. Her research interests includes Information Security, Communication and Networking. She is currently working on Steganography and Cryptography.

Mrs. Rafath Zahra, received her Bachelor of Computer Science and the Master of Computer Application from University of Madras. She is currently with P.G and Research Department of Computer Science, Quaid-E-Millath Government College for Women as a M.Phil. candidate. Her research interest includes Security in Computing and Blockchain Technology. She has undergone courses for profound learning of Blockchain technology and has published a paper on the working and applications of Blockchain in International Journal of Computer Sciences and Engineering.