JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-9, Sept 2019 E-ISSN: 2347-2693

A Modified Consensus Algorithm with a Diminutive of Proof of Longevity - Augmenting the Effectuation of Blockchain

R. Thamarai Selvi[1], **Abigail Christina Fernandez**[2*]

[1]Department of Computer Applications, Bishop Heber College (Autonomous)
[2]Department of Computer Science, Bishop Heber College (Autonomous) Trichy, India

[*]*Corresponding Author: abszarun@gmail.com, Tel.: +91-9994369043*

DOI: https://doi.org/10.26438/ijcse/v7i9.6065 | Available online at: www.ijcseonline.org

Accepted: 13/Sept/2019, Published: 30/Sept/2019

Abstract— Blockchain, since its inception in 2009, has fuelled up innovation over a wide spectrum of applications that have beget from the technology and have harvested it manifolds in arenas such as smart contracts, digital currency, decentralised record keeping, securities in terms of crowdfunding and escrow. Bitcoin, the first brainchild of the Blockchain has been fine-tuned furthermore by the impending inflow of the many consensus algorithms that are being introduced by the many researchers, with the intent of making spectacular the impact of the technology, keeping in mind the network parameters, efficiency of the blockchain and optimization in the deployment of a decentralised application over the internet. This paper aims at introducing a novel qualitative framework of consensus algorithm called the Proof of Longevity (PoL), that would improvise the current blockchain in a way so as to rule out adversaries in terms of Node Identity management, computation energy and cost saving and strategize the double spending and selfish mining problems in the real world and to catalyse the blockchain network to its zenith.

Keywords— Blockchain, Bitcoin Mining, Consensus Algorithms, Smart Contracts, Distributed cryptocurrency

I. INTRODUCTION

Cryptocurrency have become the fast emerging need of the hour amongst investors looking to invest in a seamless decentralised organisation, as opposed to the usual centralised digital currencies and the regular banking systems. The inert reason behind this is the secure mechanisms deployed and the spruce transactions of funding done with no middle man to intermediate the show of financial operations. This being the current scenario of happenings in the field, it is of ardent interest to the many researchers and architects of the cryptocurrencies to rearticulate the potentiality of the cryptocurrencies that are in stake in the market Bitcoin, the very first of its kind, proposed by Satoshi Nakomoto in the year 2008 [1], has paved the way to an umpteen number of cryptocurrencies. But then the question arises to the point as to why the other coins/ cryptocurrencies emerge, what is the reason behind investors switching to other new cryptocurrencies. This rings a bell to the mind of any lay reader of cryptocurrency.

Bitcoin, the brainchild of blockchain, a distributed decentralised network of cryptocurrency and transactions ideally deals with the many participants who own blocks in the network and who do not necessarily have a trust amongst participating partners of other blocks, but still work together in unison with the intention of creating new blocks. The blocks inherently get added on due to the many monetary or notary transactions that keep happening in around the blockchain. The participants in the blockchain get to build blocks based on the bitcoin mining process that gets done every ten minutes. Satoshi proposed the first consensus to be the Proof of work(PoW) which underlays with the guessing of a nonce which is appended to the hashed contents of the block and the block verified and added to the blockchain. This detailed process happens in a limited time of ten minutes so as to maintain the replenishing fact of bitcoins mined from the start of its inception. This again involves miners or a pool of miners who try different computations and are at race at solving the puzzle in the specific time frame with the drive to win the reward of bitcoin mining. This mining process involves speed and accuracy in terms of an agreement called the consensus agreement and Bitcoin uses PoW as its consensus Algorithm.

Apparently many other consensus algorithms lined up after PoW to overcome the limitations of Bitcoin in terms of energy, power and cost and make the solving hassle of the puzzle to a slight minimal [3]. Enforcing and mitigating a consensus amongst the participants of any blockchain is the heart that keeps the cryptocurrencies tick on. So in order to achieve the most appropriate functionality of a blockchain many consensus algorithms have been proposed by the many researchers.

This paper gets to analyse the motive behind the need of consensus algorithm. It brings to light the niceties involved in the proposed Proof of Longevity(PoL) algorithm and the need for it to be overshadowed amongst the existing contenders of consensus algorithms.

This paper starts with a brief outlook at the current stature of Blockchain and the contribution of the many researchers in relation to the consensus algorithms, which is the catalyst behind the complete functionality of Blockchain. The paper then focusses on the empathy of the current consensus scenario and how this is backed by the epic ideology of the consensus elements. Finally, the proposed Proof of Longevity is elucidated in detail by a step by step process.

II. RELATED WORK

Blockchain has become the thirst area to many researchers who aim at fine tuning furthermore the key physiognomies of the Blockchain. Zibin Zheng et.al outline the key aspects of the Blockchain as decentralisation, persistency, anonymity, immutability, transparency, auditability, security and efficiency [10]. It is an affirmative fact that the Bitcoin Blockchain duo emerged in recent years with the promise to achieve a platform for the effectuation of a pseudonymous web- centric payment system that is cost effective, trustless transaction achieved through smart contracts [11]. To put it all in a nutshell the concept of Blockchain technology has been borrowed by many other trending technologies in the field of Information Technology due to its dynamic stature and functionality.

The mastermind behind the successful effectuation of the Blockchain is undoubtedly the consensus algorithm [6]. The vital verification process in a blockchain is to agree at a consensus on the content of the distributed ledger. The process underlying is decentralization and automation. That makes the consensus algorithm one of the most critical technologies in the blockchain. The blockchain consensus algorithm can be classified according to fault tolerance type and consistency degree.

The consensus algorithms are crucial for maintaining the integrity and security of a cryptocurrency network [4]. This opens tactic to distributing nodes reaching a consensus. Harmonizing the current blockchain state is essential for a digital economic system to function properly. The key aspiration of a consensus would be:

- Enforce propagation of information with a view to extend the blockchain to the longest point establishing a monotonic strategy amidst the nodes connected.
- All sub stages of the consensus should be incentive compatible and curb the unfaithful faults if any.
- The consensus protocol should proliferate decentralization and impartiality and discourage the adversaries of the cumulated computation power found in mining pools, but rather propagate healthy sharing and work together environment amidst miners with a shared open and unbiased minded notion.
- Proper balance between processing throughput and network scalability.

In order to simplify the description of the core mechanism of the consensus algorithm, the characteristics of the consensus algorithms are tabularised in Table 1 below.

Table 1. Different Characteristics of Consensus Algorithm

Consensus Algorithm Type	Characteristics
Proof-based	Proof is usually a race condition to complete a task that is hard to crack but verified at ease.
Voting Based	Miners who bagging more than half of the votes get the accounting rights.
Stochastic	A randomised methodology to Determine each round of accounting nodes.
Alliance	Representative nodes are elected established on a specific method, and acquire the accounting rights on a turn based by rotation or election.
Hybrid	A mixture of various consensus algorithms to choose accounting nodes.

Consensus – a consent in Accordance

A Consensus in general is achieved by the totalling of the hash values of all copies of the chain. This needs the people in the network to dedicate immense computing power to sustain the blockchain [5]. Here arises the question as to how do we reward people for contributing resources for upholding the network? This is where Satoshi, brought in the **Proof of work (PoW)** mechanism [2] which was the very first in the line of consensus algorithms. The problem here is that there are multiple miners trying to solve for the same block and so a lot of energy in terms of power, cost and computation are lost. To minimise this would be the key to idealising the consensus of any blockchain network. Many researchers have pulled in an array of consensus, each with a different way so as to curtail energy and optimise the blockchain credibility.

A series of consensus algorithms [9] that followed up after the PoW with the intent of attaining the cream features that make the Blockchain impeccable to its stature are tabularised below in Table 2.

Table 2. Different types of Consensus Algorithms

Consensus Algorithms	**Concept**
Proof of Work (PoW)	The first miner to crack the difficult puzzle bags rewards and gets to add the new block.
Proof of Stake (PoS)	The fraction of coin stake a miner holds decides the chance of the miner to add new block.
Proof of Activity	Mixture of PoW and PoS strategy, where PoW is used to create a new block and PoS to validates the transactions by group of nodes. Rewards are split into both winner and validators.
Proof of Burn	The miner who has spent(burnt) more coins from his wallet gets the new block added.
Proof of Capacity	The extent of the computation power and the storage space a miner owns decides his priority to participate in the mining of a new block.
Proof of Authority	Admin node decides the authority to accept or reject a transaction and this is the key to this consensus.
Proof of Elapsed Time	The Waiting time randomly distributed to miner approves the winning chance of a miner.
Delegated Byzantine Fault Tolerance	Selection of miner is based on a vote which should ideally reach a total of 66% of nodes participating in a consensus.
Proof of Importance	The importance score selects the Miner' to s get the chance to mine.

III. THE EPIC IDEOLOGY OF A CONSENSUS

A miner or a group of miners could indulge in validating a block depending on the number of coins they hold. This implies that the more number of Bitcoins a miner holds in stake- the more mining power he would possess. This was suggested with the intent to minimise the utilization of power and energy of miners. For theoretically, a miner with low percentage of blocks mines low percentage of blocks thereby saving energy. This unintentionally overcomes the 51% attack of a miner, for if a miner would own 51% stake of Blockchain, he would not indulge in malpractices that deter his holdings in the Blockchain as well.

In order to promote a seamless mining of a block and to minimise the cost incurred in the energy, power consumption required to mine a block and to reduce computational power, it is intended on deliberation a certain rules or constraints need to be checked or sufficed by the miners or a mining pool to participate in mining a block. This forms the very essence of Bitcoin mining as effectuation of this concept of consensus to a greater level could enhance the overall functionality of a block that is done every 10 minutes. In this paper it is aimed to further boost the existing consensus algorithms that have been proposed by many researchers. This is a Proof of Longevity(PoL).

Proof of Longevity - PoL

The crux of Proof of longevity is that a miner or a mining pool are allowed to mine a block or participate in validating a block, if and only if he has proof of a long tenure as a participant in the blockchain. But again the condition as to what if a new miner wants to enter into the mining field? Then in this case we propose that he could become a participant of a mining pool that already exists and participate therein and share rewards accordingly. This will allow the sharing of rewards amongst participants and distribution of energy usage amongst players in mining, thereby minimising huge cost at a particular node or miner. The proof of longevity can be clubbed alongside with any of the existing consensus algorithms to make it even more robust and efficient and to thereby mine bitcoins as per the scheduled number of coins of 2016 every fortnight.

The ultimate scope of this consensus is to efficiently enhance the functionality of the blockchain network and its area of utilisation in current times with a zealous pace of effectuation utilising the Proof of Longevity(PoL) proposed over here. The PoL aims at resourcefully curtailing the unnecessary economic cost in terms of energy, computational power and time. It inadvertently aims at restraining the limitations of the blockchain such as Selfish mining, 51% attacks and promote trust amongst participants thereby overcoming the incompatibility amongst miners.

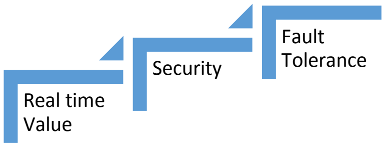

Figure 1. Key Elements of Consensus

This inadvertently promotes the attainment of the three key elements of a consensus as shown in the Figure 1 above.

Real Time Value of PoL

The ideology of using Proof of Longevity start by showing their longevity approval prior to the actual participation of the mining and the validation process that follows once the target is achieved. Proof of Work-based systems tend to generate more and more cryptocurrency as rewards for miners, the Proof-of-Longevity system usually uses transaction fees as a reward.

Users who want to participate in the mining process, are required to have a valid longevity trail that acts as a history of his participation in the blockchain network as their Longevity. The size of the Longevity determines the chances for a node to be selected as the next validator to mine the next block - the bigger the Longevity, the bigger the chances. When a node gets chosen to mine the next block, it will check if the transactions in the block are valid, signs the block and adds it to the blockchain. As a reward, the node receives the transaction fees that are associated with the transactions in the block. If a node wants to stop being a miner, its Longevity along with the earned rewards will be released after a certain period of time, giving the network time to verify that there are no fraudulent blocks added to the blockchain by the node.

Security of PoL

The Longevity works as a financial motivator for the miner node not to validate or create fraudulent transactions. If the network detects a fraudulent transaction, the miner node will lose a part of its Longevity and its right to participate as a miner in the future. So as long as the Longevity is higher the better the miner stands a chance to participate in the mining. In order to effectively control the network and approve fraudulent transactions, a node would have to own a majority Longevity in the network, also known as the 51% attack. Based on the value of a cryptocurrency, this would be unreasonable so as to gain control of the network thereby causing the need to acquire 51% of the circulating supply.

The main advantages of the Proof of Longevity algorithm are energy efficiency and security. This along with the randomization process also makes the network more decentralized, since mining pools are encouraged to be active and allow new comers of the chain to participate in the mining process and add up their longevity gradually, rather than being idle all the time. This in a way makes a huge impact on the energy and computational inputs of existing old miners, who could sit back and let the new comers rack their heads cracking the target value and give them a percentage of the rewards for mining rather than spending resources in the process. And since there is less of a need to release many new coins for a reward, this helps the price of a particular coin stay more stable.

Fault Tolerance of PoL

A surplus of algorithms and their variants are becoming eminent and trending utility to solve the problem of fault tolerance. The top notch to this would be a perfectly well organized agreement amongst the participating nodes of the blockchain before the actual happening scenario of block mining. So if this achieved to the fullest then there is no room for the prime attribute of disruption to a blockchain – the fault factor. This is also incorporated in the PoL proposition.

IV. PROOF OF LONGEVITY ALGORITHM

The Proof of Longevity(PoL) is a method of securing a cryptocurrency network through requesting users to show longevity credentials. This is something similar to a membership of their participation in the blockchain network by way of an enrolment date that could be probably maintained in the blockchain and which is verified each time a miner wishes to participate in the verification and validation of the block mined. This however could prove unfair to a new entrant miner. This is overcome by allowing the new comer to become a member of the existing mining pools, who could nominate or rather vote for these new comers to mine blocks on their behalf and thereby curb the unnecessary consumption of energy, monetary and computational resources and rewarding the new comer with a percentage of the mining reward. By this way, the new comer opens a membership in the blockchain and is not made disappointed due to his new entry, rather both the new comer and the mining pool benefit equally and the ultimatum on the PoL – energy conservation is preserved. The algorithm is given below.

Step 1: A new transaction is initiated by the miner

Step 2: All the other minors are intimated

Step 3: The miner enters his longevity code to participate

Step 4: Longevity code of the miner is verified by the blockchain network

Step 5: If the miner has a valid longevity code, the miner is allowed to participate in the guessing of the target value till it is cracked at.

Step 6: The miner participates in the mining

Step 7: The mined block is verified by the other miners

Step 8: The block is added to the chain

Step 9: Miner receives the mining reward

The following Figure 2. shows the step by step of a qualified miner with a legitimate longevity allowed to mine a block.

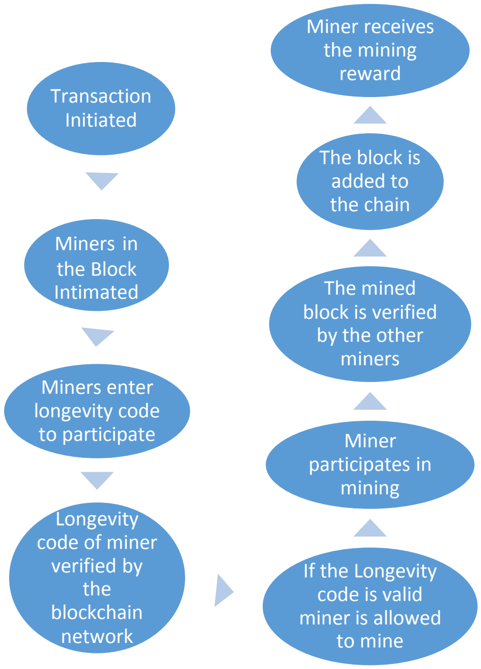
Transaction Initiated
Miners in the Block Intimated
Miners enter longevity code to participate
Longevity code of miner verified by the blockchain network
If the Longevity code is valid miner is allowed to mine
Miner participates in mining
The mined block is verified by the other miners
The block is added to the chain
Miner receives the mining reward

Figure 2. Flow of operations in Proof of Longevity.

In this algorithm, initially a new transaction is initiated by the miner which adds a new block needs to the blockchain. So, this transaction is being intimated to all the users and nodes of the blockchain. The Difficulty level is fixed in such a way that every block gets to be mined every 10 minutes. Then, the miner or the mining pool could enter their ID proof in the blockchain along with their Longevity code which is a distributed code that is known to all participants in the blockchain network. So, the Longevity code should match with the miner code to denote that the miner has a valid membership to participate in the validation and verification of the new block.

If the miner has a valid longevity code, the miner is allowed to participate in the guessing of the target value till it is cracked at. If the miner is a new entry, he will not have a credible membership period to mine blocks individually, rather, the new comer could become a member of the existing mining pools and render services in mining the block, and taking a percentage of the reward for the block mined.

In this way, energy, computation and cost is optimised, unlike earlier cases of PoW wherein all the miners were allowed to mine thereby incurring huge investment and expenditure to the part of the miners.

If the target hash value is guessed by some other miner, then the miners could indulge in the verification of the block mined and add the block to the existing blockchain. At the end of a transaction, a new block is added to the blockchain, the membership of a miner, who participated in the mining gets incremented. In this way, new comers of the mining pool, start earning their membership points appended, and could probably become individual miners once they have reached the qualifying criteria of the Blockchain Membership. The longevity variable of the miner is appended and relayed through the network.

V. CONCLUSION

This analysis focuses on the algorithmic steps taken by the PoL consensus algorithm, the scalability of the algorithm, the method the algorithm rewards validators for their time spent verifying block, and the security risks present within the algorithm. It's good to remember that the cryptocurrency industry is rapidly changing and evolving and there are also several other algorithms and methods being developed and experimented with.

The proposed PoL algorithm is being elucidated in a serial manner starting from the contextual clause behind the need of the algorithm under the existing conditions and is perpetuated towards the basic features of a consensus algorithm and how PoL aims at attaining those features. Node identity management, energy saving and tolerated power of adversary are the constraints aimed at being tackled by the PoL. The concept of centralisation becomes void gradually and there are seamless transactions over the web, curbing the double spending problem and tackling the selfish mining problem inadvertently. It is aspired to go into an in-depth implementation of the PoL and propose it on a larger scale to the many application areas of the blockchains brainchildren thereby propagating the intense potential of the blockchain.

REFERENCES

[1]. Abigail Christina Fernandez and Dr. R. Thamarai Selvi, "A Comprehensive Overview of the Constructive Minutiae of the Bitcoin - Blockchain", *IOSR Journal of Engineering* (IOSRJEN), vol. 09, no. 08, 2019, pp. 69-77

[2]. Andrychowicz, M., & Dziembowski, S. (2014). Distributed Cryptography Based on the Proofs of Work. *IACR Cryptology ePrint Archive*, *2014*, 796.

[3]. Bach, L. M., Mihaljevic, B., & Zagar, M. (2018, May). Comparative analysis of blockchain consensus algorithms. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1545-1550). IEEE.

[4]. Bentov, I., Gabizon, A., & Mizrahi, A. Cryptocurrencies without proof of work. In *International Conference on Financial Cryptography and Data Security*, 2016, February, pp. 142-157, Springer, Berlin, Heidelberg.

[5]. Daniel, F., & Guida, L. A service-oriented perspective on blockchain smart contracts. *IEEE Internet Computing*, 2019, *23*(1), pp. 46-53.

[6]. Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R. Bitcoin-ng: A scalable blockchain protocol. In *13th (USENIX) Symposium on*

Networked Systems Design and Implementation (NSDI), 2016, pp. 45-59.

[7]. Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S., On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, October pp. 3-16.

[8]. Schrijvers, O., Bonneau, J., Boneh, D, & Roughgarden, T, Incentive compatibility of bitcoin mining pool reward functions. In *International Conference on Financial Cryptography and Data Security*, 2016, February, pp. 477-498. Springer, Berlin, Heidelberg.

[9]. Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., ... & Kim, D. I.. A survey on consensus mechanisms and mining strategy management in blockchain networks. 2019,*IEEE Access*, *7*, 22328-22370.

[10]. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H., Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 2018, *14*(4), pp. 352-375.

[11]. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data (BigData Congress), 2017,* pp. 557-564.

[12]. Divyakant Meva, "Issues and Challenges with Blockchain: A Survey", in the International Journal of Computer Science and Engineering, 2018, Vol.-6, Issue-12, E-ISSN: 2347-2693.

Authors Profile

Dr. R. Thamarai Selvi pursued Master of Computer Science from Bishop Heber College, Bharathidasan University, Tamilnadu, India in the year 1992. She has finished her M.hil in Computer science followed by her Ph. D in 2018. She has also qualified in SET and NET in the year 2012. She is currently working as an Associate Professor and Head in the Department of Computer Applications, at Bishop Heber College, Tiruchirapalli. She holds professional membership of quite a few advisaries such as National Advisary Member of techresearchnet.com.She has published more than 15 research papers in reputed journals. Her main research work focuses on Data Mining, Information Retrieval, Big Data Analytics, Blockchain and Compiler Design. She has earned over 25 years of teaching experience.

*Mrs. Abigail Christina Fernandez p*ursued Masters in Computer Applications from Bharathidasan University in 2002 and Masters in Business Administration with specialisation in E- Business from Annamalai University in 2010 and M.Phil in Computer Science in 2019. She aspires to do her Ph. D. very soon . She has published a few papers in reputed Journals and a chapter in IGI- Global. Her area of interest include, Big Data Analytics, Cloud Computing , Blockchain, Machine Learning and Data Mining.She has around 6 years of experience as a System Analyst in the IT industry.She aspires to excel in the field of Analytics.