Turkish Journal of Computer and Mathematics Education Vol.12 No. 11 (2021), 3705- 3714
Research Article

PPLFS: A High Performance Consensus Method for Improving Throughput and Scalability in Blockchain Network

[1]K. Lino Fathima Chinnarani, [2]M.P. Anuradha

[1]Assistant professor, Department of Computer Applications, Bishop Heber College, Affiliated to Bharathidasan University, Trichy, Tamilnadu
[2]Assistant professor, Department of Computer Science, Bishop Heber College, Affiliated to Bharathidasan University, Trichy, Tamilnadu

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract: Blockchain has decentralized and immutable data structures, similar to traditional transaction systems. In the proposed PPLFS (Parallel Proof of Luck and Fair Share Model) framework, a scheme is designed to allow more than one miner to use the block of transactions, eventually increasing the throughput in terms of transactions per second. In the meantime, more than one leader could increase the availability and avoid network roadblock. This work leverages fair share technique and parallel mining technique to transform the blockchain into a multi-users operating system and multiple leaders could be permissible to promote their computing resources. This also reduces the transaction confirmation time for the stakeholders.

Keywords: Block chain, Consensus, Proof of Luck, Parallel Mining, Fair share

Introduction

The Blockchain and Distributed Ledger Technologies (DLT) are gaining extensive attention from both the enterprise marketplaces and academia now-a-days [Xiaoying Zheng et al. 2019, Scaria Alex and DhiliphanRajkumar 2019]. A typical blockchain is a list of cryptographic records called blocks, where each block is developed using its predecessor's hash, a timestamp and the transaction data. Generally, miners validate new transactions and append them to the global ledger each time [Shafeeq Ahmad and Ajay Kumar Bharti 2019]. Miner spends a lot of time solving the problem to validate the transaction. Blockchain is data immutable, open and runs the ledger over a peer-to-peer (P2P) network that can handle transactions of multiple stakeholders without the intervention of a middleman in a verifiable and traceable way with the help of consensus algorithms. To achieve the above-mentioned goals, blockchain protocol needs to be empowered with tokenization, data security and privacy, decentralized data storage, smart contracts and permanent availability of data [Mansoor Ahmed and Kari Kostiainen 2019]. Asymmetric cryptography and distributed IT architecture is letting blockchain to produce a protected environment for ensuring trust and developing new ways of exchanging data, new kinds of transactions and new methods of contracts [Schuetz.S and Venkatesh 2019].

As Blockchain deals with large number of transactions, there is a strong trade of between the incoming unapproved transactions and the number of miners readily approving them and need more focus from researchers to enhance its scalability and transaction throughput [Monrat et al. 2019, Casino et al. 2018]. When using sequential transactional processing in Blockchain, the unapproved transactions pile up rapidly and affect the overall network performance. A single miner or leader blockchain deployments are no longer able to meet the transaction throughput requirements and demand parallel mining. Blockchain systems must overcome the high incoming transaction rate, occasionally increasing the reward for miners based on the volume will involve more miners, eventually increases the throughput. In parallel mining technique, [Matthias Fitzi etal. 2018, Rafael Pass and Elaine Shi 2017] the miner can rapidly reach the consensus, so that the transaction is readily validated as shown in Figure 1 and Figure 2.

Most of the blockchain systems are widespread for various commercial applications, which demand real time transaction throughput, and serve a large scale of individual users and need to fulfil all user requirements [T. Aste et al.2017, Sandeep Kumar et al.2019]. The field has broadened, several limitations and disadvantages of the original design are showing up, major of the concerned issues are the scalability of capacity and performance. Hence, the enhanced transaction throughput is an essential need. Limited research studies are exposed till date in this regard and the effort to improve the performance was infrequently ended in academic world.

This paper is structured as follows. Section II overview the various techniques, and the advantages and limitations of existing Blockchain network. Section III describes the proposed work model as well as mechanisms and also discusses the logic behind the proposed work. Section IV focus on the implementation and the performance metrics of PPLFS are discussed in Section V. Section VI concludes the paper and focus on future enhancement.

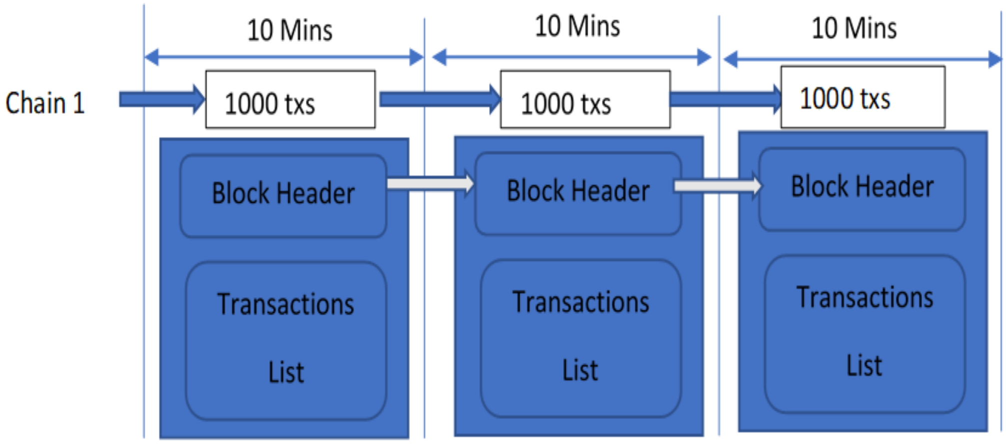

Figure 1: Traditional Block Transactions

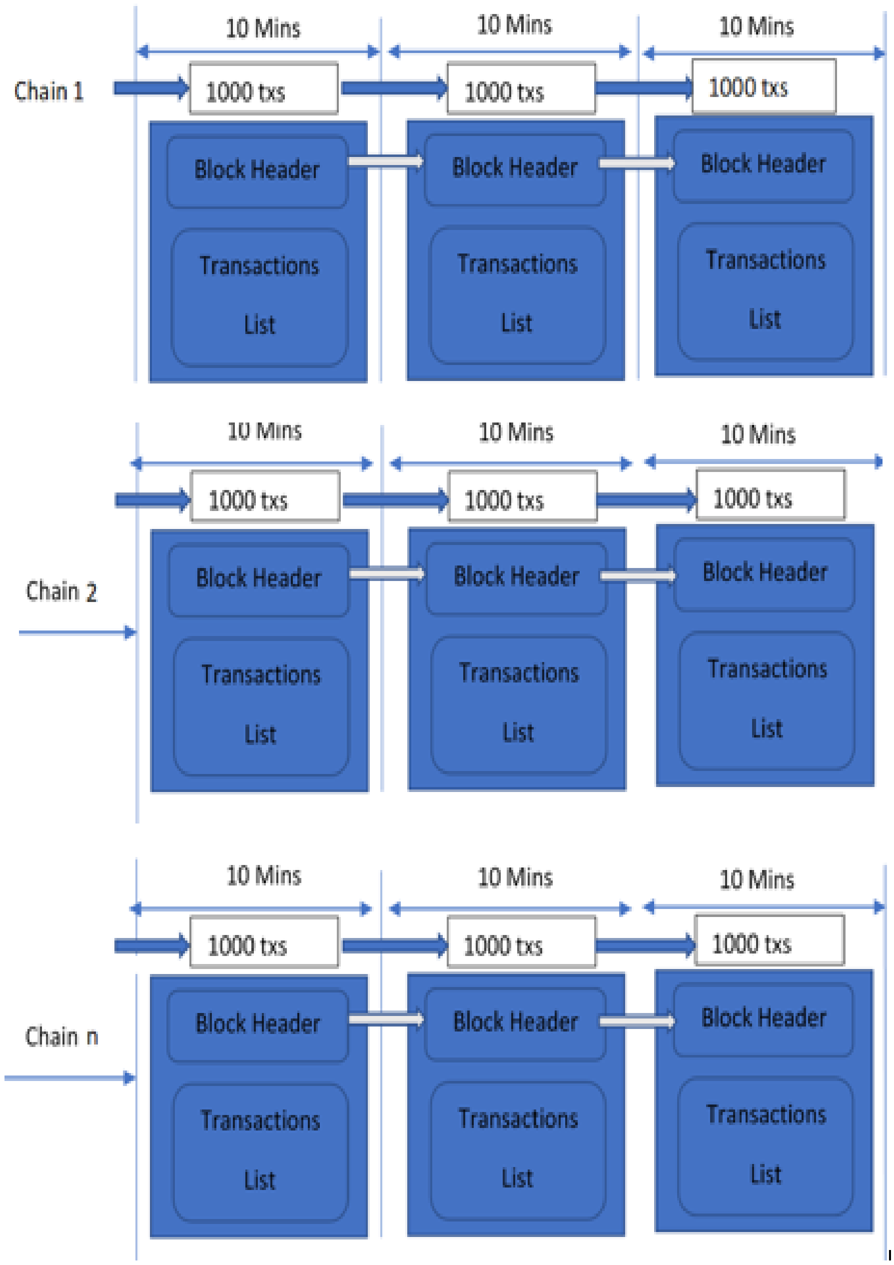

Figure 2: Parallel Block Chains

Literature Survey

Blockchain is the decentralised network and there is a need to indicate that all the transactions are valid. So, a well-designed consensus algorithm is needed to agree upon acceptance or rejection of a block to synchronize among the users [Hazari and Mahmoud 2019, Nakamoto, 2019]. The proof of work [Bashir, 2017] is applicable for the Bitcoin network. In this method to validate the block, heavy computations are performed to solve the puzzle and is done with the help of hash Function. Its advantage is highly secured and decentralised but to validate the blocks excess energy is needed. In Proof of Stake [Doc,2018] the miner is chosen via random selection combinations i.e., stake supply and his age etc., In the extended version of PoS, i.e., Leased Proof of Stake [Doc,2018] the node with good amount or some threshold cryptocurrency is eligible to add the block. Proof of Elapsed Time [Salimitari and Chatterjee 2018], popularized by Intel adopted a similar technique as PoW. As Multiple Miners are involved in validating the block, Miner is chosen in a shortest expected time by a trusted Execution Environment. In Proof of burn [Bitcoin-Wiki,2018], the motivation behind this work is not to waste excess energy to approve the block by the miner. Additionally, the Miner needs to spend some extra cryptocurrency to get more privileges on the network for mining. The Proof of Capacity (PoC) [Dziembowski et al. 2015] analyses the computation and storage capability before solving the puzzle. The hard drive with the fastest solution wins the block. In Proof of Importance (PoI) [NEM, 2018] the motivation is to incentivize the account holders to save coins rather than making the miner with high scores richer. In Proof of Activity (PoA) [Bentov et al. 2014], the author hybridised the PoW and PoS approach and proved it is highly secured against practical attacks.

Based on the research studies, the identified fact is that consensus mechanisms are protocols that make sure that the nodes processes transactions are synchronised with each other and approve on which transactions are valid and are further added to the blockchain. In the above survey, a variety of consensus mechanisms were implemented in order to reach the consensus of all the participants. The most important factors to be considered for designing a Consensus algorithm are: maximum throughput, cost per Confirmed Transaction, Bootstrap time, transaction validation, Bandwidth, Storage, Scalability of the peer network, Transaction finality and cost of participation. Based on the survey, two most recognized performance evaluation factors are scalability and throughput.

Scalability is continuously a major attention in blockchain executions and at a business point, to meet the business requirements it needs to be expanded. Transactions Per Second (TPS) value must be raised in order to attain the throughput and is considered as the number of transactions authenticated every second by a data framework. The greater the number of transactions every second, the more rapidly transactions will be accomplished, accepted and confirmed. Over the years it has witnessed blockchain technology growth in all fields. In such situations designing a consensus algorithm by considering scalability and throughput is a great challenge. In this work consensus algorithm is proposed to meet the challenges of scaling and the throughput of the blockchain system.

Proposed Work

Figure 3. shows the proposed PPLFS System Flow Model and a procedure is explained in procedure mining. The major objective of the proposed work is to address the problems in PoW i.e., wastage of excess energy because of performing computationally intensive tasks and this can increase the electricity utilization. To overcome this issue, the proposed parallel Proof of Luck and Fair share (PPLFS) mechanism is used. In this mechanism, the chance has been given to all the miners for handling the transactions. For this purpose, the following strategy is applied. The random number of length 64-bit is generated and simultaneously the miners generate the block hash value with combination of Previous block hash value, time stamp, private key and nonce value. This block hash value must be less than the 64-bit certain value and if the condition is satisfied, then the election process has been successfully completed.

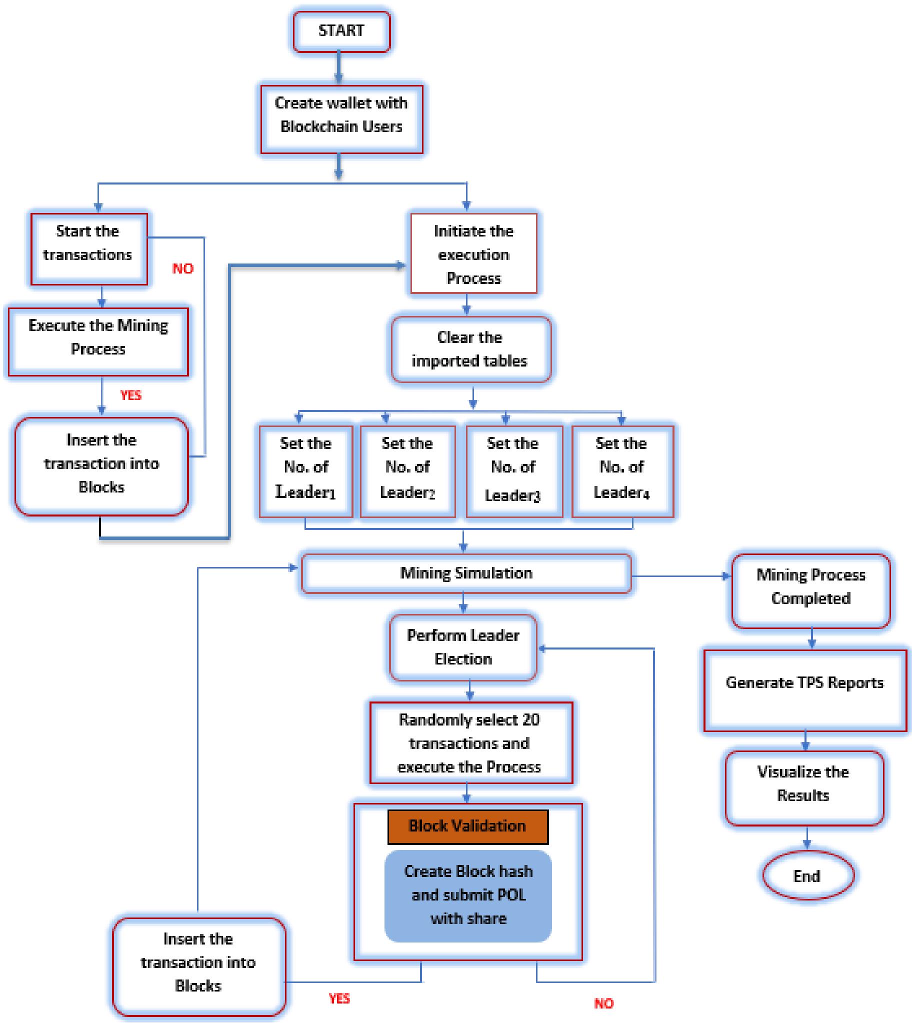

Figure3: PPFS System Flow Model

Parallel mining progresses the block chain from linear serialized dimension to parallel system. It comprises of dynamic data sharing, countless expansibility and long-chain interconnection. Significantly, this progress is well suited for parallel block chain system which is fully distributed, and has been legitimated. The parallel reliability among the chains must be attained. It ensures that individual chain runs simultaneously and creates an interrelated parallel blockchain system. Each blockchain system is comprised of 'X' nodes and each node contains the transaction statistics. In parallel mining there are 'Y' miners and are ready to solve the puzzle to place the transaction block into blockchain.

Pseudocode for Mining Simulation

Algorithm 1: Procedure mining(transactions)

Input: Existing-transactions-block
Output: Updated-transaction-block

```
    append (existingproc, subprocess("electleader"))
while size(result)<20:
    result=loadCommittedTxnFromDB ()
        cm=validate(result)
        tps=getCurrentTPS(result)
        Previous_tps=current_tps
if Previous_tps < Latest_tps
for txn in result
        append (txn, tps)
        time=time+1
 if   tps>500
        tpsf=0
        tps=time
        Previous_tps=current_tps
 if   time > pltcnt
 Calc_fair ()
      kill the processes
 if transactions<=4
      transactions=transactions+1
      sec=0
      roll_proc ()
      time=1
```

Now, the first step of Parallel Miner Selection is the Proof-of-Luck to elect the leader or miner in a specific round. Once the leader is chosen the miner task is to serialize of the block transactions. The role of miner is to solve a puzzle. In this work four miners are chosen at a regular interval time. Once the puzzle is solved the transaction are serialized and added to the current blockchain. The advantage of this proposed model is that as parallel miners are chosen the number of transactions blocks added to the blockchain is more i.e., there is an increase in the throughput thereby the performance of the system is improved.

In this arrangement, utmost all the individual miner has an equivalent chance to be a Leader. If a miner solves a task, then there is a chance to become a leader. Thus, a miner becomes a leader only by involving into the network. This makes the process become fair. Processing power gives more chance to be the Leader. If parallel mining technique is implemented, then the chance will be equal to all. Here the important note is that the Leaders who have more processing power can still compute more nonce than the rest of the others. Ultimately, if the block is not processed at the particular time interval, then they can complete their assigned range earlier than others and request for a new range to the leader.

Proof of Luck and Fair Share

In PoW algorithm, there are limitless challengers and only one individual of them can succeed. In the proposed parallel mining setting, the simple alteration of Proof of Work algorithm is termed as Proof of Luck. Here, few numbers of leaders make an effort to make a hash value which is generated by the composition of private key, time stamp and a previous block hash value and this value must be less than the certain value which is constantly generated. If a leader solves repeatedly for certain times and still cannot find out the result which is not less than the target, then he may get another chance. The outcome is that many blocks will be formed by different leaders for a one transaction.

Once the leader succeeds, they attach the transaction to the Blockchain data structure. Here, we are simulated by minimal number of leaders. Any one of the leaders can select from any unloaded transaction to added on into Blockchain structure and different orders are acceptable. For competence, Proof of Luck algorithm can be functioned into diverse leaders and to make sure those entire block transactions is attached into blockchain for at least once.

Verifying the accuracy of transactions can be divided into two steps.1. verification of all the block transactions history that connected to one user account 2. Iteration of the same process on all the user accounts. When the data history is relatively huge, it will be better to have the parallel verification on more than one node. In the proposed system, the data sharing can be occurred by diving the data by user. The proposed model requires the high TPS's need to be required for the production environment. Due to this requirement, the total size of data will be tremendously increased. Let us consider, there are 3000 TPS, about 30GB data will be produced each day.

Pseudocode for Proof of Luck

```
Algorithm 2: Procedure ProofofLuck(pk)
Input: Existing-transactions-block
Output: Updated-transaction-block
    nonce=0,threshold="00"+"fff... 62 times", longestHashChain=longest_chain("00...
    64 times")
        previous_hash=longestHashChain[-1]
      do
        blockhash=hexdigest(Hash256(Previous_hash,pk,currenttimestamp,nonce))
        nonce=nonce+1
      while block_hash < threshhold
          Insert the block_hash, previous_hash, nonce, pk, TimeStamp values into
          Leader Table
```

Pseudocode for Proof of Share

```
Algorithm 3: Procedure FairShareProcess(pk)
Input: Existing-transactions-block
Output: Updated-transaction-block
          threshold="00"+"fff... 62 times"
    for nonce from 1 to 100000000
        block_hash=hexdigest(Hash256(Previous_hash, pk, currenttimestamp,nonce))
    if block_hash < threshold and fair_stack < stack_campare_value
        insert the values hash, from_block, to_block, sender,receiver, nonce, data,
        transaction_id, timestamp into graph table
         fair_Stack=fair_Stack+1
         update the fair stack table with corresponding fair_Stack value
         append(processed_txids,existing_txid)
         break
         update leader and transactions finalised by leader
```

Implementation

Miners

In the proposed experimental set up, the blockchain miners are authorized with unique signing key, verification key and private key which has a 64-bit length.

Miners to Leader

In parallel mining if a Miners are chosen as leaders then the leaders service for a period of time. In this work the election timestamp is set for ten minutes and service period as one hour. During that time the leader constantly pays attention to the transaction request. When the new transaction arrives, the leader solves it and packs it into the transaction blockchain.

Accounts and Transactions

Based on the principle, an account generally initiates with zero balance. Account balance fluctuate because of transactions. Minimum two accounts are participated within a transaction i.e., Non transaction and Transaction Block. In Non transaction the block name is available but in transaction block the block consists of balance of two accounts i.e., senders and receiver account balance. Parallel mining will trigger the transactions processing speed by permitting more leaders to perform the mining task.

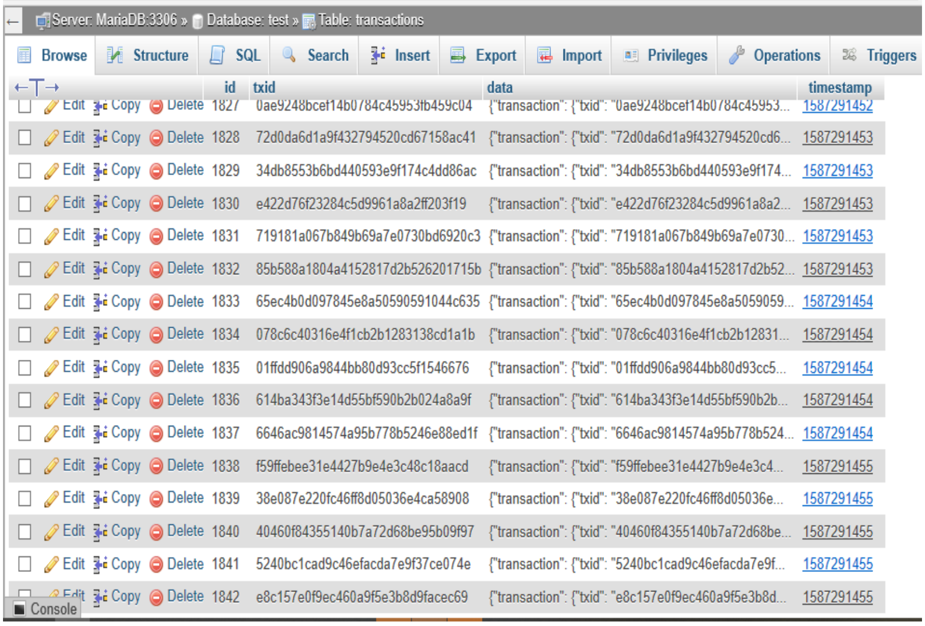

Figure 4: Validated transactions are stored in the Database

Results and Discussions

The implementation has been performed in a Windows 10 operating system with intel (R) Core (TM) i3-7020U CPU 2.30 GHz. The installed RAM is 4.00 GB and the system type is 64-bit Operating System, x64-based Processor. The proposed setting method has been developed using Python programming language. MySQL database was used to store fair stack, election, result and transaction tables. Block chain Transactions are injected into the MySQL databases table in a straight way as shown in Figure 4 and Figure 5 represents the step for validating the transactions.

To avoid variations, assume each miner will have common processing power with 10% of the available resource. To get the result the index, transaction hash value, timestamp value, nonce and previous hash value are reserved as inputs. In order to prove the performance upgrading in a proposed system, this experiment considered 4000 transactions were populating to be packed, then the performances were measured by the diverse numbers of leaders. Figure 6 & Figure 7 of the resultant graph.

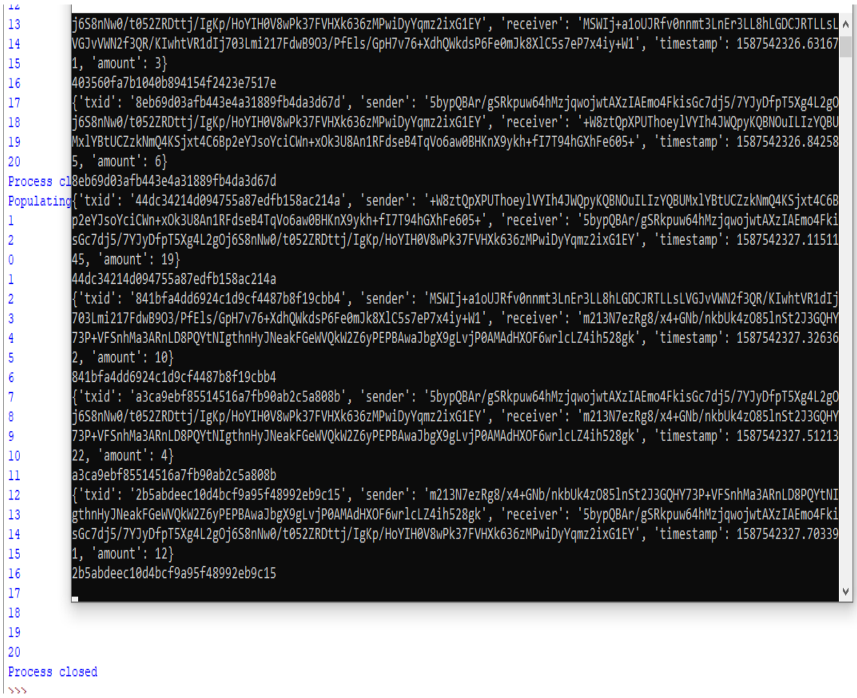

Figure 5: Transaction validation

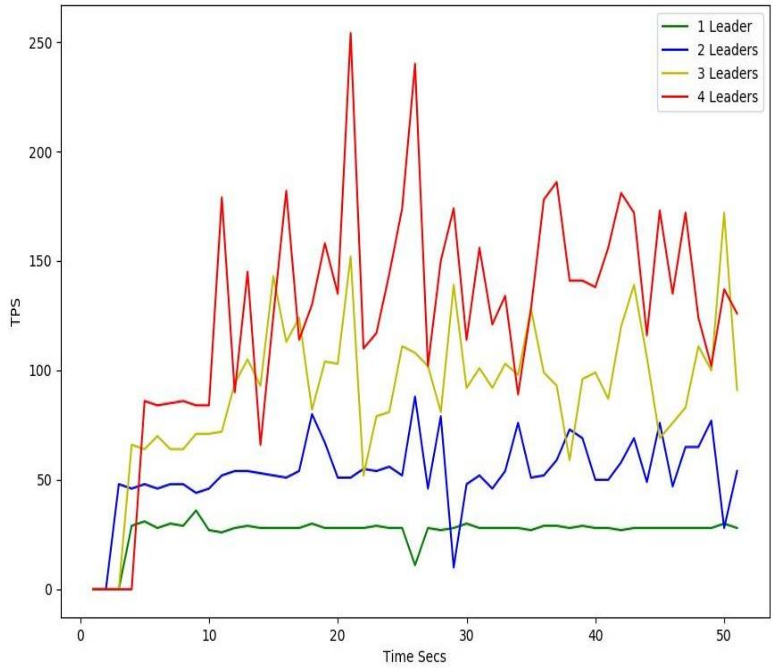

Figure 6: Graph plotted TPS against Time

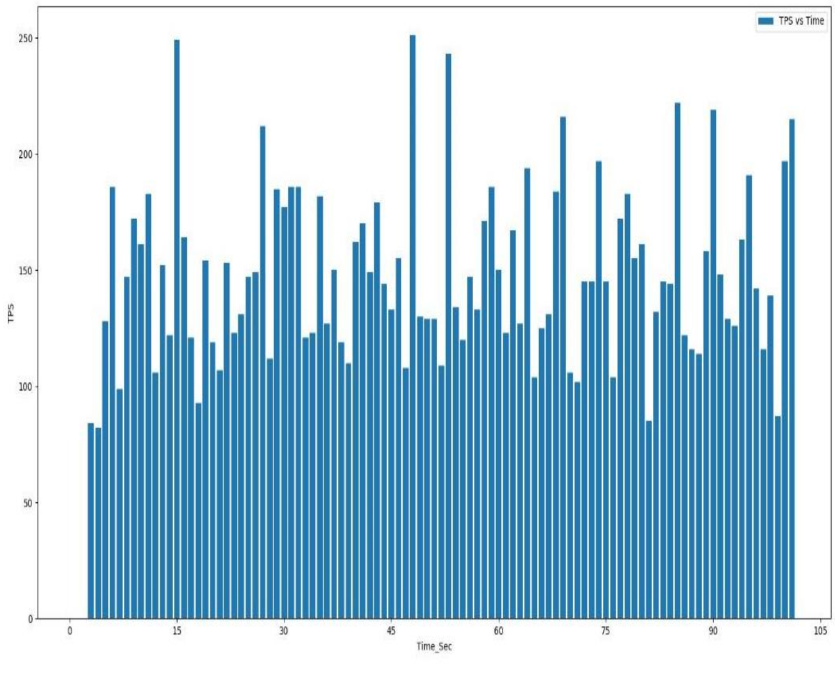

Figure 7: Graph plotted TPS against Time

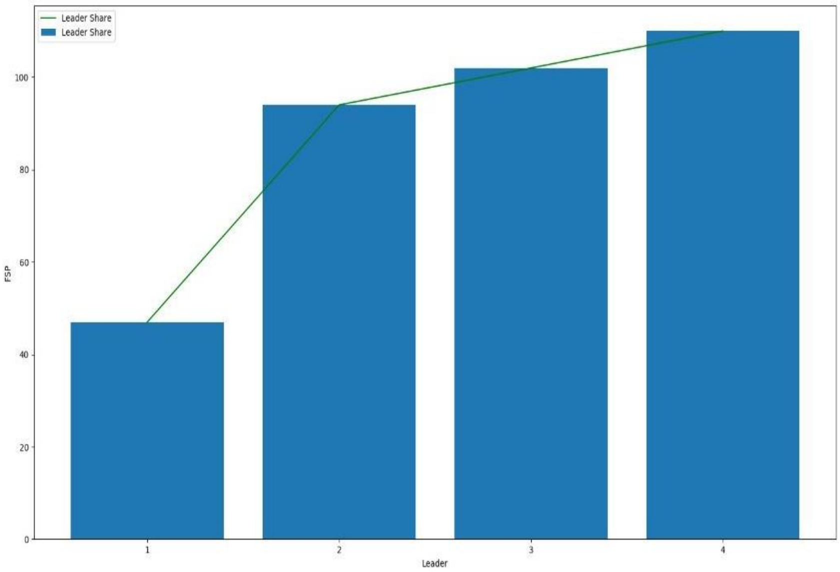

Figure 8: Parallel Mining Performance

The goal of PPLF model is for implementing parallel mining along with fair share technique to increase the throughput of the system. In parallel mining technique, the miner can more rapidly reach consensus so that the transaction will be confirmed more readily. This will be advantageous for the current user for blockchain transactions. Based on the evaluation test outcomes, when related to single mining, this method recorded four times better than the existing work which can be shown in the Figure 8 graph. All the miners shared the transactions equally by implementing Fair share technique. It's also detected that as the numbers of miners enlarged, the coincidental of all the nodes going offline would be close to zero.

Thus, this work significantly improves the shortcomings of existing work. ie., based on the intrinsic Proof-of-Luck features, more than one miner can be chosen, so that the power energy consumption issue has been avoided and predominantly the dominant lock to limit the blockchain performance has been overcomes. The maximum number of transactions has executed within the assigned period of time because more than one miner has validated the transactions. Interoperability and consensus between the miners have been easily reached. It improves the performance of overall architecture.

Conclusions

In this work, PPLFS model is proposed to meet the challenges of scaling and the throughput of the blockchain system. The proposed work separates the Leader election process and transaction serialization process. In place of electing a single miner, PPLFS proposed to elect four miners at one round thereby modifying the election process. This works provides insights into the effects of TPS on performance and scalability in blockchain networks. This work leverages fair share technique and parallel mining technique to transform the blockchain into a multi-users operating system and multiple leaders could be permissible to promote their computing resources. This also reduces the transaction confirmation time for the stakeholders.

Reference

1. [Xiaoying Zheng et al. 2019] Xiaoying Zheng., Yongxin Zhu., and Xueming Si.: A Survey on Challenges and Progresses in Blockchain Technologies: A Performance and Security Perspective, Appl. Sci. October 2019, 9, 4731.

2. [Scaria Alex and DhiliphanRajkumar 2019] Scaria Alex., T DhiliphanRajkumar.: BlockchainTechnology and Cryptocurrency, ISSN: 2277-3878, Volume-8 Issue-4S2, December 2019.

3. [Shafeeq Ahmad and Ajay Kumar Bharti 2019] Shafeeq Ahmad, Ajay Kumar Bharti.: Blockchain Scalability Enhancement using Parallel Miners Selection, ISSN: 2278-3075, Volume-8, Issue-12, Oct 2019.

4. [Mansoor Ahmed and Kari Kostiainen 2019] Mansoor Ahmed, Kari Kostiainen.: Don't Mine, Wait in Line: Fair and Efficient Blockchain Consensus with Robust Round Robin, arXiv:1804.07391v2 [cs.CR] 11 Jan 2019.

5. [Schuetz.S and Venkatesh 2019] Schuetz, S., & Venkatesh, V.: Blockchain, adoption, and financial inclusion in India: Research opportunities. International Journal of Information Management,2019.

6. [Monrat et al. 2019] Monrat, A. A., Schelen, O., & Andersson, K.: Survey of Blockchain from the Perspectives of Applications, Challenges and Opportunities. IEEE Access, 1–1,2019.

7. [Casino et al. 2018] Casino, F., Dasaklis, T. K., & Patsakis, C.: A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics and Informatics,2018.

8. [Matthias Fitzi etal. 2018]Matthias Fitzi, Peter Gazi, Aggelos Kiayias, and Alexander Russelly.: Parallel Chains: Improving Throughput and Latency of Blockchain Protocols via Parallel Composition, November 30, 2018.

9. [Rafael Pass and Elaine Shi 2017] Rafael Pass, Elaine Shi.: FruitChains: A Fair Blockchain, May 2017.

10. [T. Aste et al.2017] T. Aste, P. Tasca, and T. Di Matteo.: Blockchain technologies: The foreseeable impact on society and industry," Computer, vol. 50, no. 9, pp. 18–28, 2017.

11. [Sandeep Kumar et al. 2019] Sandeep Kumar, Abhay Kumar, Vanita Verma.: A Survey Paper on Blockchain Technology, Challenges and Opportunities, IJCTT Journal, Volume-67 Issue-4 2019.

12. [Nakamoto, 2019] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Manubot.2019.

13. [Hazari and Mahmoud 2019] Hazari, S. S., & Mahmoud.: A Parallel Proof of Work to Improve Transaction Speed and Scalability in Blockchain System, 2019 IEEE 9th Annual Computing and Communication Workshop and Conference, Q. H. 2019.

14. [Bashir, 2017] Bashir, I.: Mastering blockchain. Packt Publishing Ltd,2017.

15. [Doc,2018] Doc, W. (2018).: Leased Proof of Stake (LPoS), Retrieved from https://docs. wavesplatform.com/en/platform- features/leased- proof- of- stake- lpos.html,2018.

16. [Salimitari and Chatterjee 2018] Salimitari, M., & Chatterjee, M.: An Overview of Blockchain and Consensus Protocols for IoT Networks. arXiv: 1809.05613,2018.

17. [Bitcoin-Wiki,2018] "Proof of burn".
18. https://en.bitcoin.it/wiki/Proof_of_burn

19. [Dziembowski et al. 2015] Dziembowski, S., Faust, S., Kolmogorov, V., & Pietrzak, K.: Proofs of space. Paper presented at the Annual Cryptology Conference,2015.

20. [NEM, 2018] NEM, T.: Nem technical reference. URL https://nem.io/wpcontent/themes/ nem/files/NEM _ techRef.pdf,2018.

21. [Bentov et al. 2014] Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M.: Proof of activity: Extending Bitcoin's Proof of Work via Proof of Stake. IACR Cryptology ePrint Archive, 452 2014.