The efficient consensus algorithm for land record management system

A S Yadav¹, S Shikha², S Gupta³, D S Kushwaha⁴
Motilal Nehru Institute of Technology Allahabad

yadavamrendrasingh@gmail.com¹, swatishikha117@gmail.com²,
sulakshgupta988@gmail.com³, dsk@mnnit.ac.in⁴

Abstract: This research presents a scalable property/land registration framework. It is based on blockchain technology, where all registry offices come together on a single framework based on blockchain to improve the registration process. This paper mainly focuses on the problems in the land record and revenue sectors. In this paper, we explore the use of blockchain technology in current business scenarios. We discuss issues such as data security, privacy, and, more significantly, the absence of a shared forum amongst the involved organizations. This research proposes an efficient consensus mechanism to evaluate the performance of a blockchain-based implementation of a land revenue & recording automation system. The proposed Modified Round Robin Consensus Algorithm (MRRCA) reduced the 30% - 40% message overhead in committing a transaction to the network and thus adding the block to the blockchain.

Keywords: Blockchain, Peer-To-Peer Computing, InterPlanetary File System (IPFS), Property Transaction System, Consensus Mechanism.

1. Introduction

A blockchain is a chain of records that always grows. The primary element of blockchain is called a block. These blocks are linked to each other. Each block contains a cryptographic hash of the previous block's contents, transaction data, and a timestamp. The first block of blockchain has no parent. Since it is the first block, it is also called a genesis block [1]. In the blockchain, modification of the data is challenging. Blockchain is a distributed ledger that stores transactions between two or more parties securely and permanently. Blockchain is generally implemented by a peer-to-peer network in which every peer adheres to a protocol for communication between nodes and the validation of blocks. Once added, any block's information cannot be changed without modification of all subsequent blockchain blocks. This modification needs the permission of the majority of the network hence making the process very difficult. Although blockchain records are alterable, blockchain is considerably secure by design, and it has high fault tolerance.

So, through our paper, we have explored, and designed consensus algorithms in a Distributed Ledger Technology (DLT) based property registry transaction system. Analysis of their advantages and disadvantages is done in terms of performance. The concept of consensus is an essential topic in a distributed network. Consensus means a procedure to arrive at a common state in a decentralized or distributed network. The agreement is done to avoid incorrect results in the presence of faulty peers in
the network. Moreover, a distributed consensus mechanism should satisfy specific properties like validation, termination, integrity, and agreement. Since blockchain has a dynamically changing status, so it must have an efficient, fair, real-time, functional, and secure mechanism that ensures all the ongoing transactions are genuine. All participants on the network agree on the state of the ledger. Consensus mechanisms perform this important task. These consensus mechanisms are a set of rules or protocols that decides the contribution of various participants on the network.

The issue of land ownership is very serious in the majority of the states of India. The primary reason behind this is the unavailability of end-to-end effective land records management system. Many financial institutions depend upon the land ownership details for their proceedings, such as sanctioning of loans. Due to the insufficient data handling and the lack of communication across the departments, we find discrepancies, data being out of sync in land records. These inconsistencies are the primary cause of faulty ownership as one has to search several years of records to confirm the ownership claim. Thus, over the last three decades, various ideas have been implemented to solve the problem. Blockchain provides an excellent solution to these problems. The implementation of blockchain technology for the land registry system can address many issues due to its centralized nature. The resulting decentralization of control, along with the immutable record of the transfer of possession of the land, provides the opportunity to build collaborative, 'trustless systems.' This system is primarily intended to make registry store information related to a property transaction using blockchain. Using blockchain technology, storing the transaction in an everlasting distributed ledger, and overseeing the transactions more robustly and transparently is possible. Implementing blockchain can also reduce human errors and delays.

2. Related Work

The Proof-of-Work (PoW) consensus mechanism [2] is one of the most preferred consensus mechanisms in the Bitcoin blockchain. Peers accept the longest chain as the valid chain that depicts the system's historical transactions and increases its length. Although PoW is very successful, it also has some shortcomings. One of the significant drawbacks of PoW consensus is its low throughput, and it takes a long time to validate a transaction. Also, PoW is susceptible to a 51% power attack, which means that if the attacker's hash computing power exceeds 51%, he will take control and hamper the network. GHOST [3, 4] employs blocks on the sidechain to produce high transaction rates. Spectre [5] has shown improvement in performance by utilizing a Directed Acyclic Graph instead of using the traditional chain structure, enabling various miners to generate blocks concurrently. PoW based consensus has disadvantages like intensive power consumption, no external utility, and easy to lead to centralization, which created the need to develop a new consensus protocol by the name of Proof of Stake (PoS). Kiayias A et al [6], based on PoS consensus, randomly selects a subset of stakeholders as a contributor in an epoch. PoS based consensus trade-off efficiency with security.

Karan et al. [7] proposed that private or government financial institutions worldwide strive to shorten the payment, clearing, and settlement cycles of various transactions. Kumar et al. [8] proposed a block validation and consensus algorithm, which generates a new block randomly and adds it to the blockchain only if at least 51% of nodes in the blockchain network agree on it. Recently, the DLT-based e-stamp procurement system is suggested by Singh and Vardhan [9]. It is used to authenticate the stamp paper for real estate transactions. Another subscription system, proposed by Mallik and Kushwaha [10], is designed to inform the customer of content delivery facilities. Singh and Vardhan [11, 12] proposed a decentralized and secure peer-to-peer infrastructure to manage e-stamp and property registration systems with the support of IoT devices. Singh et al. [13] proposed a DLT based solution for the cheque settlement system for banking transactions and expanded the scope of the electronic cheque from local to global banking, and analyzes the weaknesses of e-cheque against double-spending and counterfeiting. Singh et al. [14] proposed distributed and decentralized blockchain-based architecture, which protects intrusive activities offset by the majority vote achieved in the consensus mechanism for each transaction and verification request. Chroma Way [15], in collaboration with the government of Andhra Pradesh, built a blockchain-based system for land
registration. The solution tends to eliminate fraud and errors and reduce land registration and ownership transfer's administrative workload. The solution improves processes associated with land registration and real estate transactions.

3. Proposed Work

In many cities around the world, the conventional method of storing land registries suffers from serious problems. Most people do not believe in the current traditional process. Even when they have legal documents for land deed, they are not entirely sure if they have all the land documents. People looking to buy that land go to great pains to ensure that they are legally buying and are not cheated in the deal. Most of these issues can be fixed by using blockchain. This article's main objective is to create a blockchain solution to fix problems associated with the traditional recording land registries method. Storing land registries in blockchain gives us many vital benefits: an immutable record of all the previous transactions, thus maintaining authenticity. This is because the records held in the blockchain cannot be changed once created. Thus no one can forge the documents, and also, the records are transparent so that anyone can verify these records. We use Distributed Ledger Technology to build our blockchain using a distributed consensus mechanism.

The blockchain system consists of peers which are connected by the peer to peer swarm network. All the peers in our blockchain network can access the blockchain using a hash of blocks. Each peer is connected to a land registry system. Each land registry system has its regional database. The regional database contains a list of land-id and their owners. Thus, whenever a transaction takes place, each peer has to validate that the seller owns the land or not. The government officials will entirely control the proposed land record management system. All the current government land records will then be stored in the new proposed blockchain system. We have developed the blockchain system using IPFS. The government can also configure mining policy and consensus mechanism according to their needs.

Here, the blockchain validates all the transactions by using a peer-to-peer network of computers. Blockchain is a data structure that creates and shares the distributed ledger of the transactions between networks of computers. All the users are allowed to make and verify the transactions immediately without concern of any central authority. This software's primary purpose is to demonstrate how blockchain can simplify land-ownership transactions in a real-world property registry transaction system. This software can be used only where each person has a unique identity. This Owner_ID acts as a primary key to uniquely identify each person along with the land they own. Every peer maintains its copy of the ledger. The ledger has two parts. The first part is called the word state, and the second part is blockchain. The following are the sequence of events for DLT based Property Registry Transaction System:

1. The client inputs the transaction details in the leader node.
2. The leader node creates a proposal for block and sends it to validator nodes. The block proposal contains transaction details.

3. The validator nodes send their response (i.e., vote whether the transaction stored in the block is valid or not) to the leader node. The node finds the node's validity by using its copy of the world state database to determine whether the seller owns the property or not. If the seller owns the property then only, he can sell the property.

4. The leader node, according to the consensus algorithm, decides whether the block is valid or not.

5. If the block is valid, then the block is added to the blockchain, and the client gets the message that the transaction was successful.

6. Otherwise, if the block is not valid, it will not be added to the blockchain, and the client gets the message that the transaction was invalid.

4. Consensus mechanism
   The consensus mechanism can reach a single data state based on an agreement between all the blockchain network systems. Many consensus algorithms have been proposed to achieve reliability in a network when there exists a threat of unreliable nodes in the system. PoW, PoS, Byzantine Fault Tolerance (BFT), Practical Byzantine Fault Tolerance (PBFT), and Delegated Proof of Stake (DPoS) are some examples of consensus algorithms. In the proposed consensus mechanism used before adding a new block in the blockchain, multicasting is done to reduce network load and enable a consensus on
a larger number of transactions in a short time period. The proposed consensus mechanism reduces the effort to add a new block and make it secure and synchronized.

4.1. Round robin consensus algorithm
Round Robin Consensus Algorithm is a standard consensus mechanism, and its modular flow chart is shown in figure 2 below. rr_allot_leader_node is responsible for selecting a leader node. In this module, a round-robin schedule among the nodes is used to find the leader node. This means that every node will assume a leader node role periodically for some fixed amount of time. put_block module is used to input the transaction that takes place between the buyer and seller. After completion of the transaction, its details are to be stored in a block. The leader node is responsible for creating a block proposal. This block proposal is sent to all the nodes in the blockchain network. The validate module is run in all peers and is used to vote whether the block should be added to the blockchain or not, i.e., these determine the validity of the block. The node's validity is found by using its copy of the world state database to determine whether the seller owns the property or not. If the seller owns the property then only, he can sell the property. These votes are later sent to the leader node as a block proposal response. The blockchain system's block is committed when the two-thirds majority of validators have verified and broadcasted acceptance for that block. Different modules for property registry transaction system using a round-robin consensus algorithm are:

4.1.1. rr_allot_leader_node module. This module creates a round-robin schedule among the nodes to find the leader node such that only the leader node is allowed to add a block to the ledger. Suppose there are three nodes in the blockchain system, the first node A will be the leader node for some fixed amount of time, then node B and after that node C and then again node A and so on. Only the leader node is allowed to add a block to the blockchain. It means that if any other node tries to add a block, then there will be an error, as shown in figure 3 below.

![Figure 2. Flow Chart of modules in round-robin consensus algorithm](image-url)
Algorithm 1. Allot leader node for the Round Robin Consensus algorithm

Input
n: number of nodes
ip[1]: ip address of nodes in the blockchain network

1: procedure RR_ALLOT_LEADER_NODE(n, ip[])
2: i ← 0
3: loop
4: leader_nodeip[i%n]
5: broadcast(leader_node)
6: i++
7: end loop
8: end procedure

4.1.2. put_block module. This module is used for adding a block to the ledger. First, it checks whether the node is a leader node and then only proceeds if it is a leader node. The value of the transaction is input by the user. Along with these input values, the hash of the previous block in the ledger, the system's timestamp, and transaction date are also added to the block. The block is added to the blockchain if 2/3rd of all validator nodes consent that the block is valid.

Algorithm 2. put_block for round-robin consensus

Input:
validator_consentus[]: list of consensus vote of various validators
leader_ip: ip address of leader node
transaction: values of transaction

1: procedure PUT_BLOCK(validator_consentus[], leader_ip, transaction)
2: if node_ip == leader_ip then
3: input(transaction)
4: block ← create block(transaction)
5: receive(validator_consentus)
6: if majority(validator_consentus) == true then
7: addBlockToBlockchain(block)
8: output("block successfully added")
9: else
10: output("block is not valid")
11:     end if
12:     else
13:         output("the current node cannot add block as it is not leader node")
14:     end if
15: end procedure

**Figure 4.** Flow chart of put block module

4.1.3. Validate module. This module is responsible for informing the leader node whether the block which the leader node wants to add is valid or not. The validity of the block is checked using a regional database. We check whether the seller owns that land through the regional database because if the seller does not own that land, then that transaction is invalid.

**Algorithm 3.** Validation of the block

**Input:**
- **block:** block for which validators are supposed to vote
- **db[]:** regional database of validator

```plaintext
1: procedure VALIDATE(block, db[])
2:     input(block)
3:     read(db)
4:     transaction ← block.transaction
5:     if transaction.land_id == db[seller_id].land_id then
6:         vote ← yes
7:         add_db(transaction.buyer, transaction.land)
8:         delete_db(transaction.seller, transaction.land)
9:     else
10:         vote ← no
```
11: end if
12: broadcast(vote)
13: end procedure

Figure 5. Flow chart of the validate module

4.1.4. View module. This module is used to view the last block added to the ledger. Through this module, we can verify whether the block was added or not.

Figure 6. Flow chart of view module

Algorithm 4. View the latest block added to the blockchain

Input:
hash: topmost block hash in the blockchain
1: procedure view(hash)
2: hash \leftarrow \text{get}\_\text{hash}()
3: block \leftarrow \text{get}\_\text{block}(hash)
4: output(block)
5: end procedure

4.2. Modified round robin consensus algorithm
In this research work, we propose a modified round-robin consensus algorithm that is an improved version of the round-robin consensus algorithm. The modular flow chart is shown in figure 7 below. The validate module will be run in all modules. \text{eff}\_\text{allot}\_\text{leader}\_\text{node} module runs in any one node of the blockchain network. This module is responsible for selecting the leader node. The transaction is
input through the make_block module. Any peer can run that module to input a transaction between buyer and seller. The leader node sends a block proposal for that particular transaction. This block proposal is sent to all the nodes in the blockchain network. The nodes now vote whether the block should be added to the blockchain or not, i.e., these determine the node's validity. The node finds the node's validity by using its copy of the world state database to determine whether the seller owns the property or not. If the seller owns the property then only, he can sell the property. These votes are then sent to the leader node as a block proposal response. The blockchain system's block is committed when the two-thirds majority of validators have verified and broadcasted the block's acceptance. We can verify the block we have added through the view module and view the block added from any peer.

Different modules for property registry transaction system using efficient consensus algorithm are:

4.2.1. **eff_allot_leader_node module.** The leader nodes are allotted in a round-robin way from only those nodes requested to add a new block. This means that first, the transaction values will be inputted by the user, then a request for adding that block will be created. Then suppose the request is made by node A two times and node B one time at any given instance of time, then first node A will be the leader then node B and then again node A, even though there are 3 nodes like node A, node B, and node C.

**Algorithm 5.** Allot leader node module for the modified Round Robin Consensus algorithm

| Input: |
|---|
| n: number of nodes |
| ip[]: ip address of nodes in the blockchain network |
| bl[]: list of nodes which have pending blocks to add to the blockchain |
| 1: procedure EFF_ALLOT_LEADER_NODE(n, ip[], bl[]) |
| 2: i ← 0 |
| 3: loop |
| 4: if bl[i%n] == 1 then |
5: leader_nodeip[i%n]
6: broadcast(leader_node)
7: end if
8: i ++
9: end loop
10: end procedure

Algorithm 6. Make a block module for the modified Round Robin Consensus algorithm

Input:
  transaction: values of a transaction between seller and buyer
1: procedure MAKE_BLOCK(transaction)
2: input(transaction)
3: block ←create_block(transaction)
4: broadcast(block,node_id)
5: end procedure
4.2.3. **add_block module.** This module is used for adding a block to the ledger. The transaction values and the hash of the previous block in the ledger, timestamp generated by the system, and transaction date are also added to the block. The block is added to the blockchain if 2/3rd of all validator nodes consent that the block is valid.

**Algorithm 7. Add block for the modified Round Robin Consensus algorithm**

| Input: |
|----------------------------------|
| `validator_consent[]`: list of consensus vote of various validators |
| `transaction`: values of transaction |

1: `procedure PUT_BLOCK(validator_consent[], transaction)`

2: `wait()`

3: `input(transaction)`

4: `block ← create_block(transaction)`

5: `receive(validator_consent)`

6: `if majority(validator_consent) == true then`

7: `addBlockToBlockchain(block)`

8: `output("block successfully added")`

9: `else`

10: `output("block is not valid")`

11: `end if`

12: `end procedure`

4.2.4. **Validate module.** This module will be responsible for telling the leader node whether the block which leader node wants to add is valid or not. The validity of the block is checked using a regional database. We check whether the seller owns that land through the regional database because if the seller does not own that land, then that transaction is invalid. This module is the same for both the round-robin consensus algorithm and the modified round-robin consensus algorithm. The algorithm and flowchart for the same can be found in the section of the round-robin consensus algorithm.

4.2.5. **View module.** This module is used to view the last block added to the ledger. Through this module, we can verify whether the block was added or not. This module is the same for both the round-robin consensus algorithm and the modified round-robin consensus algorithm. The algorithm and flowchart for the same can be found in the section of the round-robin consensus algorithm.
5. Result and Performance Analysis
We have successfully run our Property Registry Transaction System on multiple hosts. We have compared the round-robin consensus algorithm with our modified round-robin consensus algorithm. We have also analyzed the time taken for the transaction for both algorithms and the number of peers below.

Table 1. Time taken for the transaction for both algorithms along with the number of peers in the blockchain system

| S. No. | Number of Peers | Round robin consensus algorithm | Proposed consensus algorithm | Comparative difference |
|--------|----------------|-------------------------------|----------------------------|-----------------------|
| 1      | 5              | 2.46                          | 1.54                       | 0.92                  |
| 2      | 10             | 2.98                          | 1.98                       | 1.00                  |
| 3      | 15             | 4.62                          | 2.60                       | 2.02                  |
| 4      | 20             | 5.22                          | 3.05                       | 2.17                  |
| 5      | 25             | 7.92                          | 5.67                       | 2.25                  |
| 6      | 30             | 9.58                          | 7.12                       | 2.46                  |
| 7      | 35             | 13.18                         | 9.88                       | 3.33                  |
| 8      | 40             | 16.85                         | 12.58                      | 4.27                  |
| 9      | 45             | 22.60                         | 16.16                      | 6.44                  |
| 10     | 50             | 28.84                         | 20.92                      | 8.64                  |

The graph shown below illustrates the time taken for the transaction and the number of peers in the blockchain system. The round-robin algorithm, which is an existing algorithm, is shown with a blue line, and the modified round-robin algorithm, which is our proposed algorithm, is shown with a red line. The performance of the Modified Round-Robin Consensus Algorithm (MRRCA) is 30% - 40% better than the simple Round-Robin Consensus Algorithm (RRCA) for adding a single block to the blockchain.

Figure 10. Graph showing time taken for a transaction for both algorithms along with the number of peers in the blockchain system
6. Conclusion

This paper has compared two consensus algorithms on the property registration transaction system implemented using IPFS. In order to achieve this, we have implemented blockchain using IPFS on multiple hosts. We have used C as the underlying language for various modules of our research work. With the help of IPFS and its hashing techniques, we have developed a blockchain of immutable and tamper-proof transactions. After running the two consensus algorithms mentioned above, we conclude that the proposed Modified Round-Robin Consensus Algorithm (MRRCA) performs 30%-40% better than the simple Round-Robin Consensus Algorithm (RRCA) in committing a transaction to the network and thus adding the block to the blockchain.

References

[1] Nakamoto S 2009 Bitcoin: A peer-to-peer electronic cash system. Cryptography Mailing list at https://metzdowd.com 03
[2] Wright C Bitcoin: A peer-to-peer electronic cash system
[3] Sompolinsky Y, Lewenberg Y and Zohar 2015 A Inclusive block chain protocols 8975
[4] Yadav A S, Khushboo K, Singh V K, Kushwaha D S 2020 Increasing Efficiency of Sensor Nodes by Clustering in Section Based Hybrid Routing Protocol with Artificial Bee Colony. Procedia Computer Science 171 pp 887-896
[5] Sompolinsky Y, Lewenberg Y and Zohar A 2016 Spectre: A fast and scalable cryptocurrency protocol
[6] Kiayias A, Russell A, David B and Oliynyko R 2017 Ouroboros: A provably secure proof-of-stake blockchain protocol 357-388.
[7] Singh K, Singh N and Kushwaha D S 2018 An Interoperable and Secure E-Wallet Architecture based on Digital Ledger Technology using blockchain. International Conference on Computing, Power and Communication Technologies (GUCON) (978-1-5386-4491-1/18).
[8] Kumar A, Yadav A S and Kushwaha D S "VChain: Efficient Blockchain based Vehicular Communication Protocol", 978-1-7281-2791-0/20/ confluence2020-2020 IEEE
[9] Singh N and Vardhan M 2019 Digital ledger technology-based real estate transaction mechanism and its block size assessment International Journal of Blockchains and Cryptocurrencies 1 pp 67-84
[10] Mallick, Shrabani, and Kushwaha D S 2012 An Efficient Publish-subscribe Protocol for Collaborative Content Delivery-Ex-PUSH Int. Symp. on Cloud and Services Computing pp 152-156. IEEE 2012
[11] Singh N and Vardhan M 2019 Distributed ledger technology based property transaction system with support for iot devices International Journal of Cloud Applications and Computing (IJCAC) 9 2 pp 60-78
[12] Singh N and Vardhan M 2018 Blockchain Based E-Stamp Procurement System with Efficient Consensus Mechanism and Fast Parallel Search J. Mech. Contin. Math. Sci 13 4 pp 73-89.
[13] Singh N and Vardhan M 2019 Blockchain based e-Cheque Clearing Framework Scalable Computing: Practice and Experience 20, no. 3 (2019): 511-526
[14] Singh N and Vardhan M Computing Optimal Block Size for Blockchain based Applications with Contradictory Objectives Procedia Computer Science
[15] Schwartz D, Youngs N, Britto A, et al 2014 The ripple protocol consensus algorithm Ripple Labs Inc White Paper 5