International Journal of Advanced Technology and Engineering Exploration, Vol 10(101)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2021.876426

Research Article

Blockchain-based voter registry management system

Swapna Donepudi[1, 2*] and K Thammi Reddy[3]
Research Scholar, Department of CSE, GITAM School of Technology, Visakhapatnam, Andhra Pradesh, India[1]
Assistant Professor, Department of CSE, PVP Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India[2]
Professor, Department of CSE, GITAM School of Technology, Visakhapatnam, Andhra Pradesh, India[3]

Received: 21-July-2022; Revised: 12-April-2023; Accepted: 14-April-2023

Abstract

In recent years, there has been a significant shift towards digitizing portals for user convenience and enhanced data security. Digitization of voter registration is required to manage vast data and protect sensitive information, and the current study focused on it to effectively address challenges such as duplicate entries, time delays, and mismatched voter information. Issues such as data ambiguity were sometimes encountered by the traditional voter registration method, making it difficult for users to trust the integrity of information. To address these challenges, the ecosystem was suggested to be decentralized using blockchain technology in the proposed design. All the essential elements of voter registration were considered, and the interplanetary file system (IPFS) was leveraged to seamlessly integrate multiple voter registration offices in the state or country. A consensus strategy was presented to enhance security while reducing communication costs for message exchange by 63%, and it required 53% less time than the proof of work (PoW) method, in which every node participated in the consensus. The proposed model for voter registration was more robust in exchanging messages confidentially, making it more viable in real-time scenarios. A more effective and secure approach to voter registration using blockchain technology was proposed in the study, which is able to address the current challenges in traditional voter registration methods.

Keywords

***Blockchain, Consensus, Credibility value, Voter registration*.**

1.Introduction

Voter registration is a crucial mechanism for electing leaders in most democratic countries. All people must undergo the voter registration process to participate in the election process. This procedure involves locating people entitled to cast ballots in elections and gathering their personal information into a list known as the registry of voters [1]. The right of a person to participate in any particular election to exercise their franchise is the first step toward credible and free elections in a democratic society. The right to vote is addressed through voter registration [2]. The essence of voter registration, according to [3], is to:

- Constrain access to voting
- Verify that only those allowed to vote in a specific jurisdiction may do so
- Verify that every voter casts only once
- The voter registration list may determine the best location for a polling site and how many voting stations and workers should be assigned to a specific polling location.

Technology advancement has significantly changed the government, industrial, administrative, and academic sectors. In the current era, the usage of technology is essential for the process of voter registration. India is the world's most democratic country. India has 1.3 billion people, accounting for 17.7% of the world's population. India is usually recognized as the world's second most populated country.

Based on the facts and data from the 2019 parliamentary elections, about 900 million of the world's 1.3 billion people are eligible to vote. Since the last election in 2014, 84 million new voters have been added to the voting rolls, but 300 million people are illiterate [4]. Thirty nine thousand people are

*Author for correspondence

identified as transgender. Voters are dispersed across the country, covering a distance of almost three thousand kilometers (from Jammu Kashmir to Kanya Kumari) [5].

The election commission at the state level governs the process of voter registration. The system of voter registration is standard throughout the country. It is inefficient since it is not integrated with other systems like the aadhaar card processing or birth certificate generation system.

In today's scenario, the election commission announces the voter registration dates. We can register as voters by submitting the necessary address and age-proof documents. However, the disadvantage here is redundancy check is not done. Because of this, a voter's name can be present in the list at two different places, resulting in a fraudulent voting mechanism. Numerous issues may arise due to the existing process of voter registration, like missing voter records, mismatched voter details, etc., The existing methods face several problems like misinformation, tracing out electoral registration offices, problems with acknowledgment, etc., shown in *Figure 1*[6]. Many of these issues can be solved with blockchain technology. Distributed ledger technology (DLT) based solutions provide an immutable history of transactional data, ensuring no one can question their legitimacy. Voter's information will be forever linked to the authenticated system, ensuring that their information is never manipulated or falsified. Any individual can check their records 24×7.

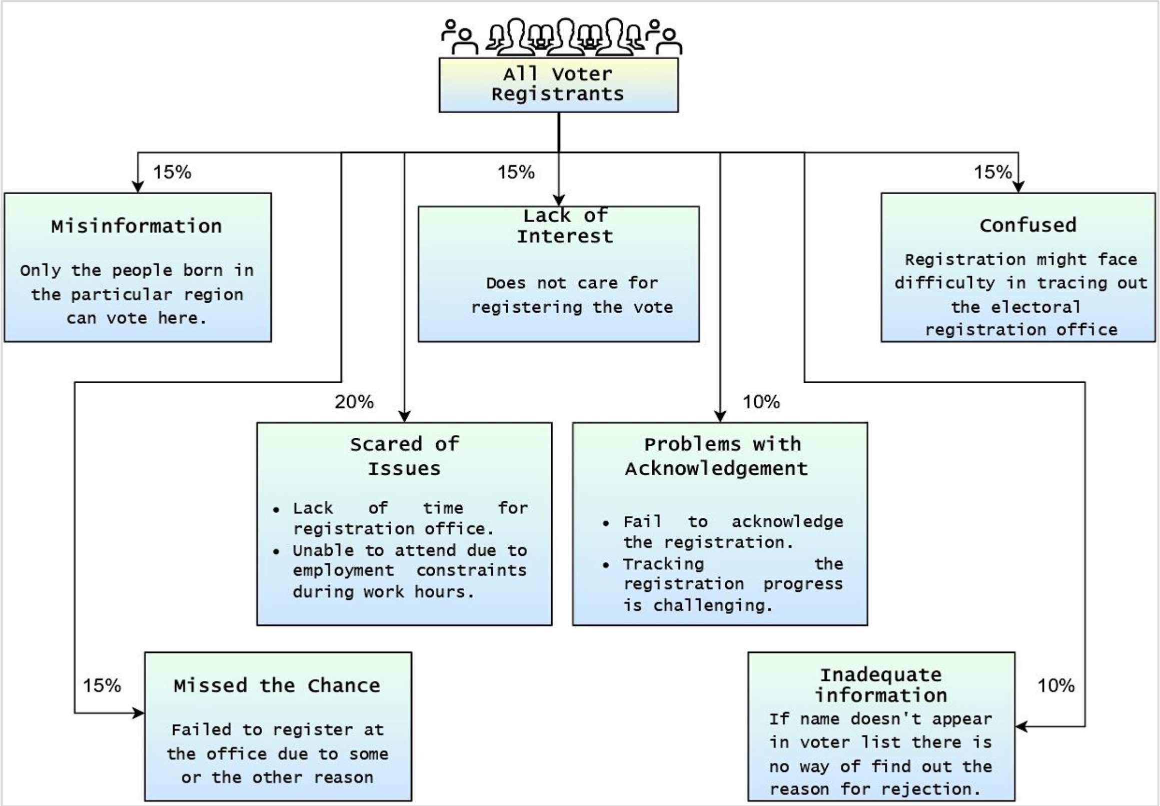

All Voter Registrants
15%
Misinformation
Only the people born in the particular region can vote here.
15%
Lack of Interest
Does not care for registering the vote
15%
Confused
Registration might face difficulty in tracing out the electoral registration office
20%
Scared of Issues
• Lack of time for registration office.
• Unable to attend due to employment constraints during work hours.
10%
Problems with Acknowledgement
• Fail to acknowledge the registration.
• Tracking the registration progress is challenging.
15%
Missed the Chance
Failed to register at the office due to some or the other reason
10%
Inadequate information
If name doesn't appear in voter list there is no way of find out the reason for rejection.

Figure 1 Problems with the existing system

Since Satoshi Nakamoto developed bitcoin in 2008, blockchain and DLT are often used interchangeably [6]. The blockchain and other distributed ledgers use blocks to disseminate records over a peer-to-peer network. Blocks record blockchain transactions. The blockchain's immutability comes from each block's cryptographically computed header, which commits to the previous block's header. To ensure the integrity of the blocks, active network participants must approve a transaction before it is committed to the ledger. Distributed ledger consensus protocols establish which database state is genuine and truthful. After consensus, the current transaction is appended to the block and connected to the blocks in the chain by a cryptographically hashed reference to the former block.

The recommended solution is a blockchain model for "voter registration" The research aims to provide a resolution allowing the voter details to be consolidated into a single system while maintaining their integrity. This article lays out a framework for voter registration that is decentralized, peer-to-peer, and secure. We used the inter planetary file system (IPFS) network to construct the blockchain-based system. Blockchain technology addresses all issues raised with the old voter registration framework. An access control system can be implemented by preventing unapproved users from manipulating the data.

One of the most significant issues in Indian cities is the steadily declining voter turnout. India is increasingly urbanizing. Every year, millions of diligent, educated young people relocate to cities. But just a tiny portion of this population casts ballots, which is a massive loss for the country. If intelligent and experienced individuals cast ballots, they would choose leaders pursuing progressive, development-focused policies. The primary factors leading to these issues are:

- Due to the long waiting time to have your name added to the voter list, an individual loses interest in registering.
- Only a 60percent of applicants have their names added to the voter registry. No justification for rejection is provided.
- When they relocate, their name is not added to the voter list at the new location, which causes fraudulent voting in their previous location on their name
- In the conventional approach, the security of voter details is given the least priority.
- The conventional approaches lack data standardization, resulting in data integration issues and information redundancy.

Several strategies have been implemented to modernize the voter registration system more effectively. On the other hand, the voter registration system's digitization adds duplication, parallelism, and accuracy features. These problems can be effectively addressed by using blockchain technology. Blockchain technology for voter registration can resolve numerous issues with the current centralized system. This article proposes a voter registration system based on blockchain technology.

As a reliable, secure, and transparent DLT, blockchain has significant potential to fix the previously discussed difficulties. As a result, it may be utilized to manage voter registration. This article proposes a system for a voter registry built on an architecture that uses blockchain and IPFS to provide a safe and scalable system. Voters can easily register their votes with this system. The most important contributions are outlined in the following way:

- The use of decentralized databases to reduce the risks associated with centralized storage and to assure the scalability of the system
- Proposed a scalable and unique framework for voter registration using blockchain technology and IPFS that is quick, secure, transparent, and tamperproof.
- An efficient credibility based consensus process is proposed, which is secure and scalable and reduces the number of message transfers for the consensus process.

This paper is structured as follows: Section 2 discusses relevant works that address technical gaps associated with state-of-the-art models. In Section 3, the methodology and internal workings of the proposed blockchain-based voter registration framework are briefly explained, along with how the framework enables complete control over all organizations participating in voter registration transactions under government supervision. Section 4 provides details on the validity and robustness of the proposed credibility-based consensus algorithm (CCA) based on experimental results. Section 5 outlines the model's performance, while Section 6 provides the conclusion statement and future research directions.

2.Related work

Blockchain technology emerged when Satoshi Nakamoto introduced bitcoin in 2008 [7]. Bitcoin was the first digital money to use a blockchain to overcome double spending. Barclays adopts blockchain technology first [8]. The first insurance blockchain application is InsurChain [9]. Starbase [10] used crypto-tokens to crowdfund from numerous sources. In their study [11], Guo and Lang explain how blockchain technology combines peer to peer (P2P) systems, distributed consensus algorithms, and encryption techniques. Cocco et al. [12] use the bitcoin system to discuss the sustainability and possibilities of blockchain as a financial technology. Niranjanamurthy et al. [13] used strength, weakness, opportunities, and threat matrix (SWOTM) to conduct a detailed analysis of blockchain technology, including its benefits and drawbacks. The researchers explored blockchain technologies and multiple kinds of blockchain, the development of blockchain due to technological convergence, blockchain functionalities, advantages, and problems.

A distributed database system, a blockchain, lies at the heart of bitcoin technology. Zhang et al. [14] explain blockchain structure, consensus, and future developments. Blockchain-based applications are rapidly gaining popularity in various industries, including banking, e-commerce management, and wireless sensor networks. Blockchain technology faces other obstacles, including scalability and privacy issues, which must be addressed. According to Tschorsch and Scheuermann [15], the mining inspection procedure might be carried out using a batch test or any other mechanism, making reaching a consensus easier. Otherwise, evil entities may abduct the consensus and bring the system down. Some researchers have proposed a ledger system that tracks digital data and could allow users to collateralize their assets. [16]. A variety of innovative technologies have incorporated blockchain technology. Singh et al. [17] developed an architecture built on blockchain technology to transfer wallet money within the bank. Singh et al. [18] presented an e-cheque idea based on the blockchain. To address concerns such as double-spending and counterfeiting, the writers used e-cheques. A DLT-based e-stamp purchasing approach proposed by Singh and Vardhan [19] addresses the validity of stamp paper in real estate deals. According to the authors [20], blockchain-based peer-to-peer infrastructure may be used to manage land registry systems.

With the blockchain's consensus mechanism, there is a significant likelihood of Byzantine failures. Consensus mechanisms address this. The proof of work (PoW) solves the Byzantine failure issue by perplexing the miners.51% of the miners must vote to add a new block to the blockchain. According to Nguyen and Kim [21], PoW is widely used to reach an agreement on the bitcoin blockchain network. They consider the longest chain the most accurate representation of system transactions. Despite its success as a proof-of-concept, it has significant downsides. The limited throughput of the proof-of-work consensus method is one of its major flaws.

Furthermore, PoW is vulnerable to a 51% attack, which implies that an attacker with far more than 51% hash processing power might take control of the network. However, with proof of stake [22], the miner may only mine the new block with the most significant stake, and the other miners must search for new blocks to receive. The authors of [23] presented a consensus technique for more secure and rapid access to exchanged record information and assessed the effectiveness of a blockchain-based deployment. Undoubtedly, blockchain technology is more secure and trustworthy than traditional systems, according to Li et al. [24]. Additionally, Singh and Vardhan [25] have suggested a blockchain model that safeguards invasive actions by permitting consensus.

Gupta et al. [26] have used a block-transfer approach to boost transaction rates. Instead of the traditional" chain" architecture, specter uses a directed acyclic graph (DAG), allowing more miners. Distributed Denial of Service (DDoS) assaults and stake grinding render the proof-of-work consensus vulnerable. It also demands establishing a new consensus method, proof of stake (PoS). Kiayias et al. [27] randomly picked a set of stakeholders as contributors during an epoch for a security-focused PoS Consensus Algorithm. Yadav et al. [28] proposed an efficient round-robin-based consensus approach for land registration administration systems.

Categorizing the consensus mechanisms employed in different blockchains based on their features and functions is possible. Participating nodes in the network are rewarded depending on the followed consensus procedure. PoW and PoS are two of the most used consensus mechanisms. Delegated proof of stake (DPoS) [29] helps to construct the original PoS consensus model more quickly. DPoS transactions are often significantly quicker to complete than those made using PoW's slowest method. In addition, DPoS suffers from several drawbacks, including a lack of decentralization and security issues. An elected delegate can vote in place of other users in DPoS. Therefore, the voter holds more power. An elected representative may be removed from office if they fail to perform or deceive the people they represent. It is up to those who elected them to decide the delegates' powers. A small number of people have access to the process of validation. Those responsible for verifying blockchains may abuse their authority since the system enables users to designate representatives.

Chen and Tso [30], in their study, have recommended a solution to the challenge of identity-based signatures by focusing on certificate-less signature security models. Kumari and Singh [31] highlight the need for fewer message exchanges to ensure an effective system. Mishra et al. [32, 33] provide examples that show how the trust value of nodes can be used to improve the efficiency of a distributed system. Using blockchain technology, Balasubramanian et al. [34] offered a method for securely storing data that would save money and time on verification processes and explain how blocks are checked to determine if they are legitimate or incorrect. The authors of the Kumari et al. [35] paper suggest a pooled trust-enhanced security approach for a distributed model that is both trustworthy and secure. Pippal et al. [36] explore how the trust value of any system can affect its integrity and the benefits that can be attained by lowering the total quantity of messages communicated inside any system. Boke et al. [37] provide further explanations of various gaps in security protocols and the vulnerabilities they provide. Nguyen et al. [38] have examined the security concerns surrounding blockchain technology to facilitate sharing of electronic health records via mobile cloud-based platforms.

Li et al. [39] suggested a scalable multilayer consensus technique based on practical byzantine fault tolerant (PBFT) that partitions nodes into several levels. Despite the significant reduction in communication complexity, the increased number of layers will still result in lengthier transaction confirmation rates. Xu et al. [40] article proposes a new consensus algorithm called score grouping-practical byzantine fault tolerant (SG-PBFT) for blockchain-based systems in the internet of vehicles (IoV) context. The authors introduce a new component called the trust management system (TMS), which manages the reputation of network nodes and ensures the integrity of transactions. Arun and Ravindran [41] proposed a technique that achieves scalability and high throughput while maintaining Byzantine fault tolerance, making it suitable for large-scale distributed systems; however, it is complex to implement and may require specialized hardware. Jiang et al. [42] proposed a new mechanism for achieving consensus within a consortium blockchain in a smart grid context. The mechanism likely utilizes a trust-based hierarchical approach to ensure the security and reliability of the blockchain, which could enhance the decision-making capabilities of a complex distributed system. Prabha and Chatterjee [43] Combining PoW and PoS mechanisms to achieve better security and scalability in blockchain healthcare networks is less secure than traditional PoW or PoS mechanisms and may require significant computational resources. Liu et al. [44] the proposed technique is efficient Byzantine fault tolerance while reducing computational and communication overhead. Haddaji et al. [45] the technique improved the reliability and robustness of federated learning by using a trust-based consensus algorithm; however, it requires additional communication overhead. Li et al. [46] technique reduced communication overhead and improved efficiency in multi-agent systems by using event-triggered communication.

This section provided an overview of blockchain technology, its services, and the consensus processes utilized in blockchain applications. Considering the findings of this research, it was abundantly evident that a peer-to-peer model that relies on blockchain technology was essential to achieve an efficient, tamperproof, fraud-free, and trustworthy system for a property transaction. Currently used methods of reaching consensus, such as PoW, required most of the time spent on handling authorization puzzles. If all the nodes in a blockchain-based application engaged in the consensus process, not only would a large amount of time be consumed, but the application's throughput would also be significantly diminished. Consequently, effective means for reaching consensus were required, and all miners had to evaluate consensus. Based on the observed gap, a framework was necessary to perform effective, quick, tamperproof, and reliable transactions. As they existed then, voter registration procedures were cumbersome, time-consuming, and inefficient. This article suggested a fast and effective consensus mechanism and a voter registry system based on blockchain that worked well with few messages.

3.Methods

The proposed voter registration framework is a blockchain-based application. *Figure 2* depicts the network architecture of the suggested framework for voter e-registration. The components of this framework are registration offices from various districts that have the validator installed on their computers to make up the network entities engaged in the proposed system. Together with all the validator nodes in other areas, it creates a single P2P network. Under blockchain specifications, the registration offices replicate their web servers. A cloud-based distributed server is connected to all these organizations. The underlying network is set up through registration offices to enforce this blockchain-based application. The electoral registry office (ERO) and booth level officers (BLO) are part of the validation process. Some professional miners with good infrastructure are also engaged. Every district in the network maintains its blockchain termed as B1, B2---Bn.

IPFS is used to build the suggested blockchain-based P2P framework. Ethereum, Coinbase, Hyperledger Fabric, and other frameworks are accessible to deploy blockchain applications. These sites have regulations about security and mining. IPFS allows developers to create their policies for mining and consensus procedures for blockchain applications. The IPFS platform includes many features, including content-addressable data sharing, a peer-to-peer network, and decentralization.

The electoral registration office confirms voter registration using multiple levels of verification. The validators store a complete blockchain replica connected through a peer-to-peer network in the proposed method. IPFS networks may connect intra-district or interdistrict validators in the framework. The IPFS network is a decentralized, Swarm-based peer-to-peer system, meaning that swarm nodes interact with all peers inside the same network rather than a centralized server.

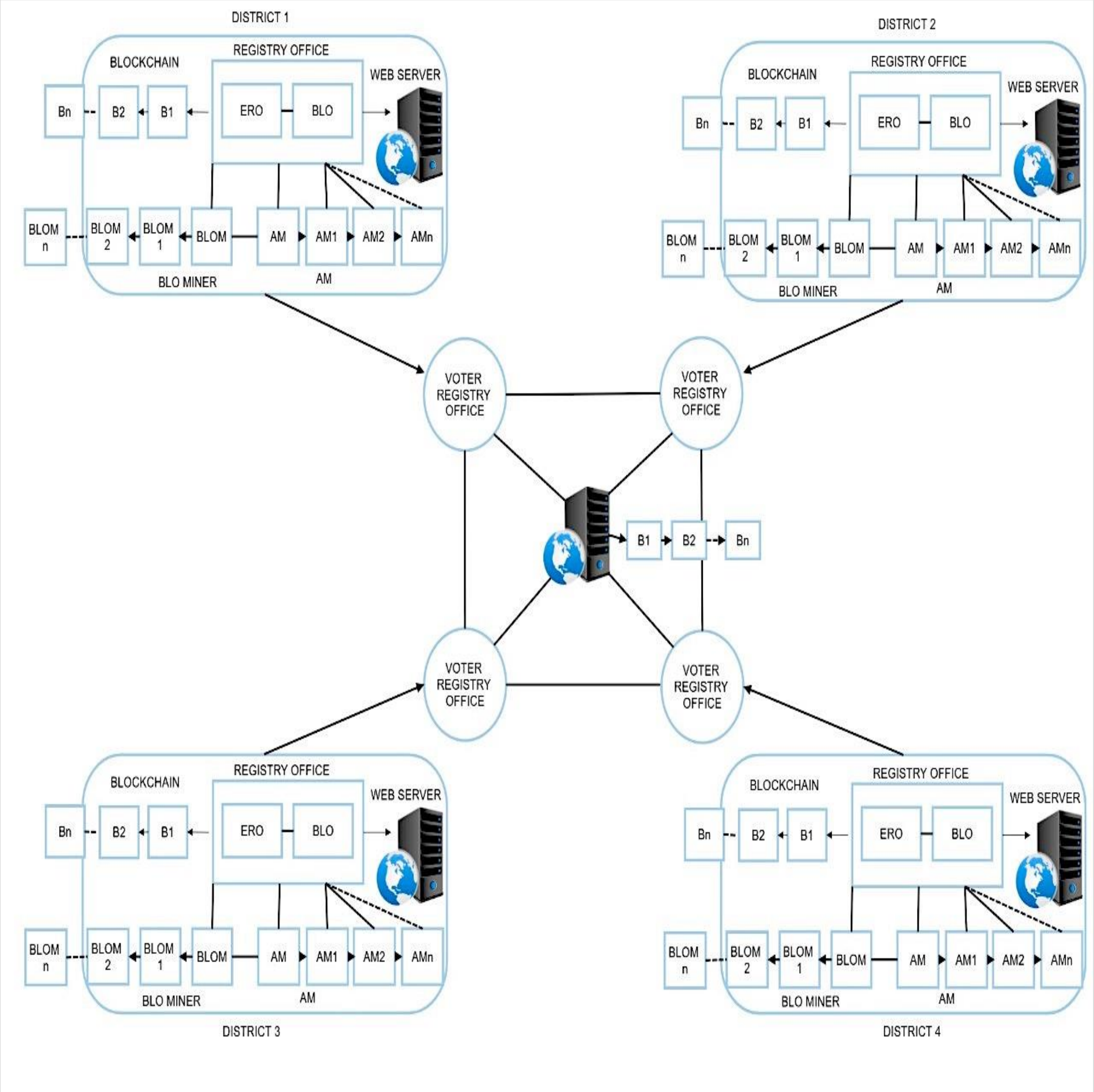


Figure 2 Proposed framework for voter registration

The ERO uses the BLO to authenticate voter registrations on many levels. All documents submitted, including identity and witness identification, are verified by the first BLO. After reviewing the paper, the BLO sends it to the Electoral registrar's office. After authenticating the provided documents, the registrar's office issues the voter identity card.

The region has several nodes and registered offices connected via a web server. The regional voter's data is kept on a web server connected to a specific location. Participants in the ERO include registry office miners. Both high credibility booth level office miners (HCBLOM)" and "low credibility booth level office miners (LCBLOM)" can be used to describe them. The authorized miners (AM) nodes carry out crucial tasks, including validating transactions and mining.AM are employees with extensive computational resources allowing registration offices to scale operations and do more.

The proposed framework completely controls all organizations participating in voter registration transactions under the supervision of the Government. The suggested P2P architecture is built around a network of voter registration offices and web servers. Each registry office has a web server, which also has a copy of the most recent blockchain on it. In the proposed system, each regional office is connected to the other through the P2P network and has a replica of the whole blockchain. People who wish to register their vote communicate via the "Voter Registration Framework" by submitting the necessary documents for voter registration. The miner constructs a block of transactions when the transaction pool has sufficient transactions. A principal miner (PM) sends a message to all nodes about the newly generated block. Finally, the block that has been verified is appended to the blockchain.

3.1Working of the proposed system

The flow of transactions of the proposed framework is shown in *Figure 3*. The voter registration process begins with the user submitting a transaction request. The ERO receives the voter registration request along with the digital signature. The ERO checks the digital signature and adds the request for registration to the transaction pool. In order to validate the transactions, a consensus mechanism is proposed. Validators are selected based on the proposed consensus algorithm. PM broadcasts the freshly created block to selected miners. Miners evaluated the block's transactions and generated a validity report based on its properties. Once the block is verified, the block is added to the blockchain.

3.2Creating a block for voter registration

When a person wishes to register as a voter, the necessary information must be submitted to the online portal. The information provided by the user must be saved as a transaction. *Figure 4* depicts the attributes that are kept in a block. Voter registration transaction comprises of name, father name, age, address, Aadhaar, pin code, and qualification.

3.3Proposed credibility-value-based method

Distributed systems are based on a consensus-based that yields a single value. To improve network performance, many dependable solutions are offered. Examples include PoW, PoS, DPoS, and other consensus methods. For introducing a block to the blockchain, an agreement must be reached. The CCA is an agreement technique suggested in this article that leverages multi-casting to reduce the load on the network and allow faster consensus over a considerable number of transactions.

The suggested consensus approach reduces the time and effort required to add and secure a new block. The transaction ledger is synchronized through the network only when the associated miners authorize the transactions, which is a necessary activity. If it is a legitimate transaction, it is recorded on the blockchain. The miners of the blockchain network oversee adding blocks to the blockchain. When a person requests a transaction to register them as a voter, they must provide information about their identity. Finally, PM generates a block and sends it to all nodes in the network. Validation is done by the PM nodes selected as AM.

The validator oversees reviewing transactions on the blockchain. Each AM confirms the transaction by looking for the PM's answer and sending it to its blockchain. Two categories of miners are engaged in the proposed voter registration system. AM are the first category that invests in advanced hardware and provides services to their forms. The second sort of miner is booth level office miners (BLOM), who are part of the office facilitating voter registration.

3.3.1Computing credibility value:

The proposed e-voter registration would employ two sorts of miners: 1) From the voter registration office and 2) From an AM. Voter registry office miners include HCBLOM and LCBLOM. Upon initially joining the IPFS network, miners are assigned a credibility value (CV) of 35. The CV table divides the BLOM into two categories: The two types of miners are HCBLOM and LCBLOM.

Calculating the CV is done at each node concurrently. The correctness of a newly produced block's verification response time determines the CV. The process for calculating CV is considered the initial CV to be 35, and the maximum value is assumed as 125.

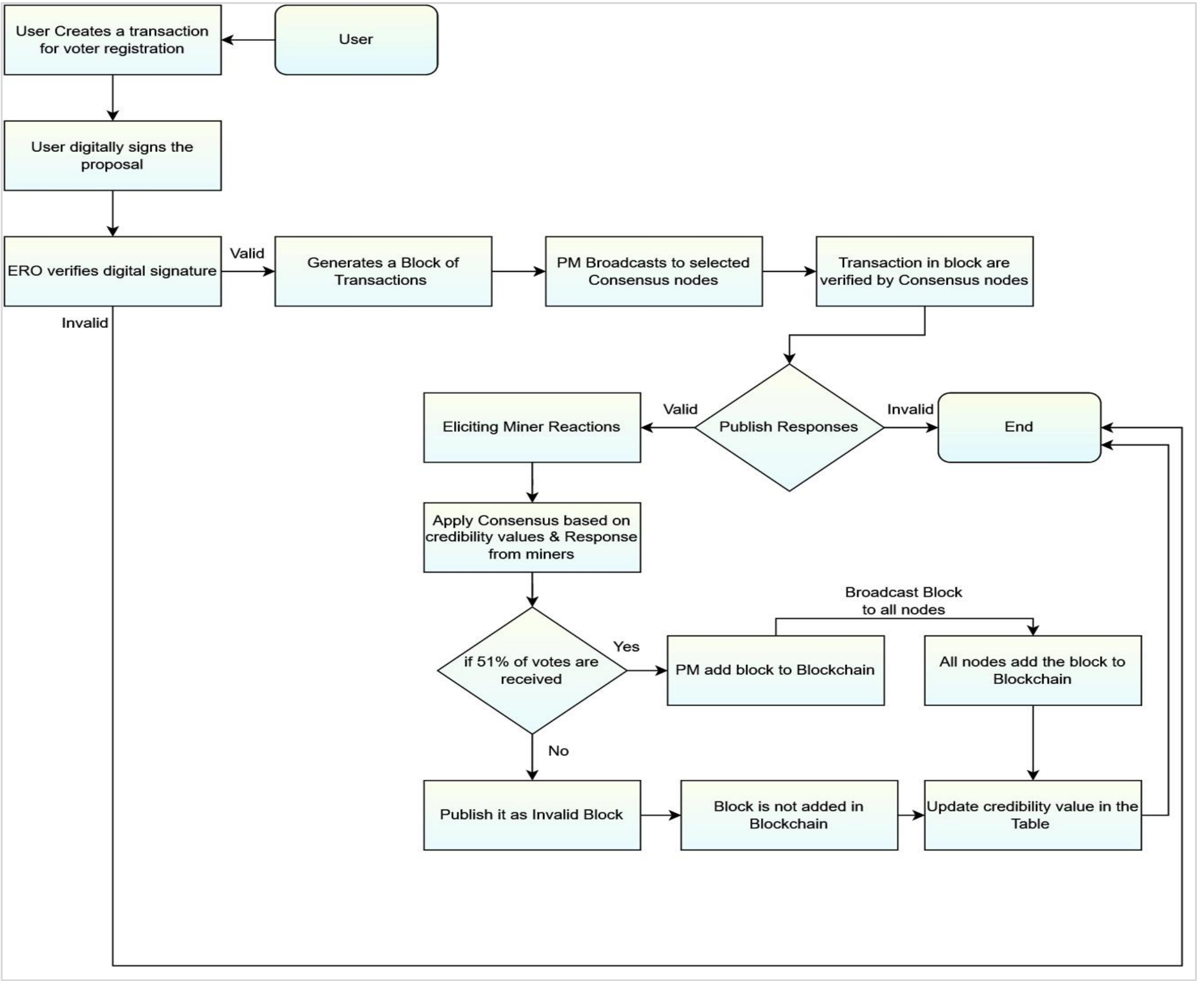

User Creates a transaction for voter registration
User
User digitally signs the proposal
ERO verifies digital signature
Valid
Invalid
Generates a Block of Transactions
PM Broadcasts to selected Consensus nodes
Transaction in block are verified by Consensus nodes
Publish Responses
Valid
Invalid
Eliciting Miner Reactions
End
Apply Consensus based on credibility values & Response from miners
if 51% of votes are received
Yes
No
PM add block to Blockchain
Broadcast Block to all nodes
All nodes add the block to Blockchain
Publish it as Invalid Block
Block is not added in Blockchain
Update credibility value in the Table

Figure 3 Workflow of the proposed voter registration System

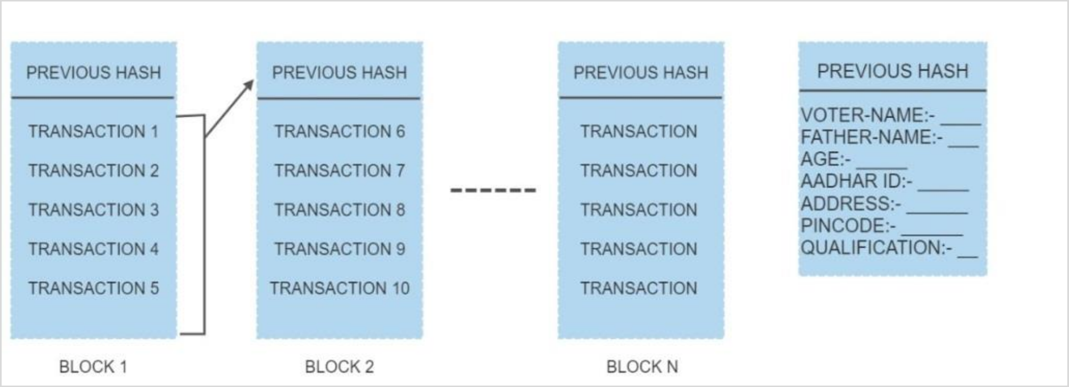


Figure 4 Block structure

Algorithm 1: CV Computation

```
procedure CV Computation( )
for each Miner do
        if (Miner is new) then
                Miner.CV=35
                if (Miner.response==final result) then
                        if Miner.CV<0 then
                                Miner.CV=0
                        else if Miner.CV>0 and Miner.CV<120 then
                                Miner.CV+=3
                        else if Miner.CV==125 then
                                Miner CV is unchanged
                        else
                                Miner.CV-=12

        if Miner.response time<30 then
                Miner.CV+=2
EndFor
EndProcedure
```

Miners and nodes whose CV is lower than 20 have a lower level of credibility. These miners would be unable to participate in the mining process and would be excluded. The table of CV is updated as shown in *Table 1*. The CV is increased or dropped depending on block verification and response time when a new block is created. After the votes from the PM, the final results are obtained. Every miner keeps a status table. Based on the CV, the table splits each node into HCBLOM, LCBLOM, and AM groups. Any random node can act as the miner at system startup, broadcasting the most recent block and its CV to all other nodes. An LCBLOM node gets transferred from the LCBLOM group to the HCBLOM group when its CV surpasses 20.

Table 1 Status of credibility value table

HCBLOM		LCBLOM		AM	
PEERID	**CV**	**PEERID**	**CV**	**PEERID**	**CV**
A	41	D	19	H	64
T	57	M	14	Z	76
S	67	F	15	L	84

3.3.2Selection of the PM:

To maintain blockchain integrity, mining the block must be synced. The principal election process is in charge of preserving blockchain by coordinating the mining technique. The miner's principal election process selects miners from a pool of many for each block's mining phase. The PM mines a new block, which is then given to the remaining miners for transaction confirmation. Only 50% of HCBLOM and 50% of AM nodes will choose the PM to participate in consensus. The term "validator nodes" refers to these nodes.

3.3.3Choosing a validator for a consensus:

Mining and adding a block to the blockchain need much processing power and time under the current consensus algorithm, PoW. We also suggested replacing the hash power method with a consensus CV-based agreement structure. Compared to the current proof-of-work method, the new algorithm is recommended to involve fewer message exchanges and adds blocks faster. Each node has a CV that is regularly updated. The peer's id and CV are displayed in the CV table. For the consensus process, the PM randomly chooses 50 percent HCBLOMs and 50 percent AMs. The nodes that have been picked are referred to as consensus miners (CM). After reaching the final consensus, the CV of the miners will be updated. The majority vote is used to decide the final consensus conclusion. If the block is verified, PM adds it to its existing blockchain. The PM also broadcasts the block hash to every node.

3.3.4Validating the voter registration:

This module will ensure that the transaction is valid across the network. The user registration data will be updated if the voter details are stored on the blockchain. However, having one's name enrolled as a voter on more than one Electoral roll is illegal.

- For the first time in their life," Person X" applies to the election commission to have their name entered into the electoral roll of their appropriate constituency (say" Constituency 1"), and they have their name entered into the electoral roll and an election photo identity card(EPIC) (say" EPIC 1").

- "Person X" moves from" constituency 1" to" constituency 2" and then applies to the commission for inclusion of their name in the electoral roll of" constituency 2." Still, this time with a request to delete their name from the electoral roll of" constituency 1,"-" Person X" has their name deleted from" Constituency 1" and included in" Constituency 2 (s).
- Now" Person X" has" EPIC 1" and" EPIC 2" and legally carries them.

To avoid this situation while registering, the voter enters his name, Aadhaar number, age proof, and address proof after submitting the data need to be validated. Assume no voter is registered with the Aadhaar card number specified in the transaction in this case. To verify the proposal of adding a new block, the principal node will submit a verifying proposal request towards the' validate' process. The validator node is responsible for checking the legitimacy of the transaction proposal request. If a validator receives a majority of votes equal to or more than 51%, it will respond to the principal node by appending a new block to the blockchain. If this does not occur, then the block will be discarded.

3.4Proposed credibility–based consensus algorithm

Under the current consensus process, mining and submitting a block in the blockchain require substantial time and computer resources. We implemented a CV-based consensus protocol for voter registration to solve this issue. The proposed algorithm is described below. CCA requires less message exchange and reduces the time spent appending a new block to the blockchain. Each node updates and maintains the CV table. The CV table stores the node id and its corresponding CV.

Algorithm 2: Credibility based Consensus Algorithm (CCA)

```
1: procedure Consensus ( )
2: SUM=0
3:  Block broadcasted by the PM to every node
4: if  it is the initial block then
5:       Every node participates in the consensus
6: else
7:       The PM randomly chooses 50 percent of HCBLOM and 50 percent of AM.
8: Endif
9: count= The number of miners chosen for Consensus as a whole
10: SUM =$\sum_{i=1}^{count} responsetime * credibilityvalue$
11: if SUM>0 and 50% of  the votes are in favor of adding a block then
12:     Add and disseminate the block to every node.
13: else
14:      Block won't be added
15: Endif
16: End procedure
```

The PM randomly selects 50% of CM and uses its peer id to send its votes to every node (principal, consensus, and remaining) in the system. Consequently, after obtaining the final consensus result, all nodes may adjust the CV in the table. The final decision relies on the proportion of votes. If the block is legitimate, the primary miner adds it to its current blockchain and broadcasts it to all nodes. As a result, additional nodes incorporate that block into their blockchain. The PM is responsible for selecting the miners who verify the freshly produced block depending on the CV. Each miner modifies the status matrix according to the CV.

4.Results and discussions

4.1Implementation

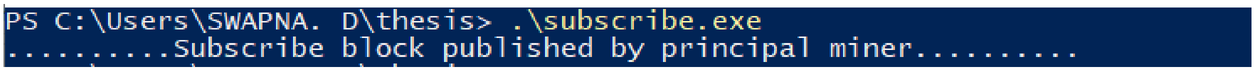
A scalable, unique voter registration framework and an efficient CV-based consensus technique have been implemented to deliver a rapid, safe, transparent, and tamperproof voter registration system. Our blockchain-based design uses IPFS as a distributed and P2P network to deploy our application. As a result, to facilitate speedy and transparent verification, all state voter registration offices that wish to adopt the proposed method must join the blockchain-based framework. Creating a blockchain network has been accomplished by utilizing IPFS on a Windows computer.

4.1.1Blockchain creation

- The block structure must be determined in advance to manually create a blockchain within IPFS.
- Enter "Genesis Block" in the preceding block, the initial block.
- The following commands must be executed to upload this block to IPFS: IPFS block put text filename.
- Following the effective execution of the command, the corresponding block hash value will be returned. Repeating the procedure described above is necessary to add blocks to the blockchain. The solitary change that needs to be made is to refer to the "hash value of the preceding block" rather than the "Genesis Block."

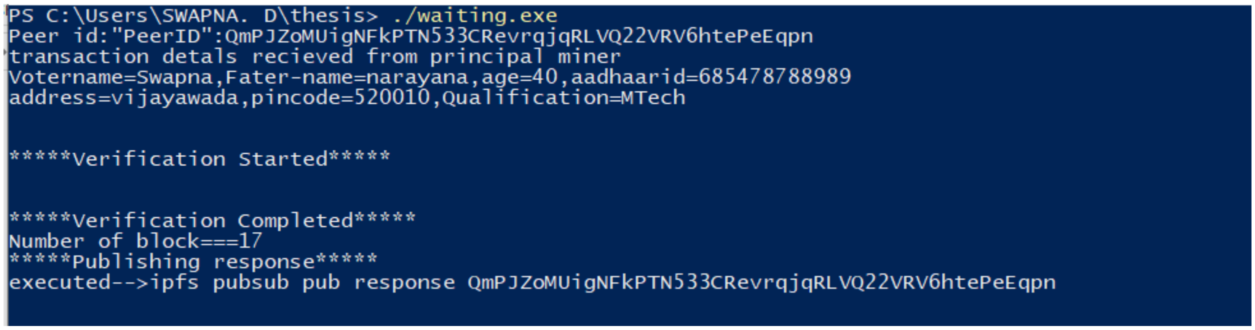
4.1.2Process of consensus

Figure 5 demonstrates that all other nodes, except the PM, subscribe to the block produced by the PM. The process that takes place at the consensus nodes is illustrated in *Figure 6*. Block information is delivered to the node and verified by searching for the corresponding blockchain. After that, a response copy is forwarded to the miner in charge. Additionally, it displays the total number of blocks a node had to go through to verify the transaction. The principal node, depicted in *Figure 7*, collects the responses, applies consensus, and publishes the results. In addition, it displays the CV before consensus was reached and the revised CV after miners reached a consensus.



```
PS C:\Users\SWAPNA. D\thesis> .\subscribe.exe
..........Subscribe block published by principal miner..........
```

Figure 5 Other nodes—PM publishes subscriber data

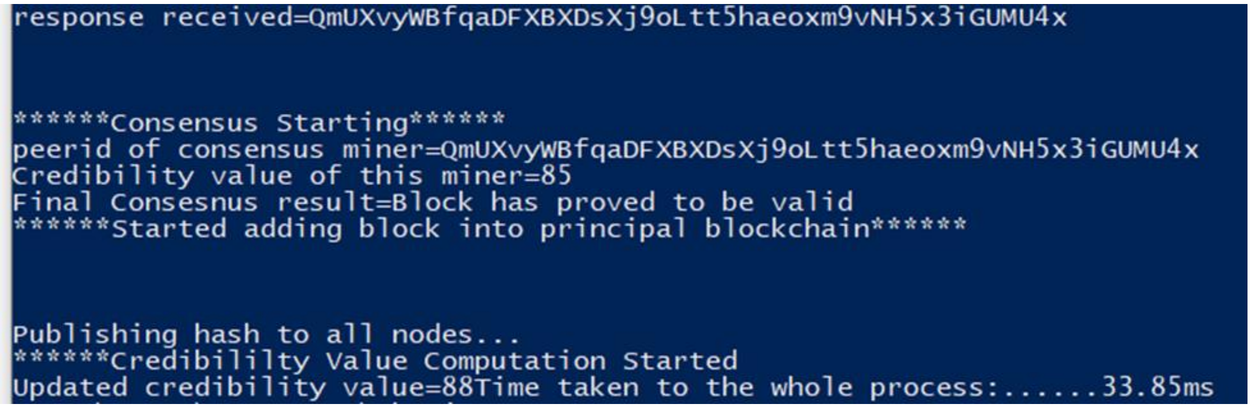


```
PS C:\Users\SWAPNA. D\thesis> ./waiting.exe
Peer id:"PeerID":QmPJZoMUigNFkPTN533CRevrqjqRLVQ22VRV6htePeEqpn
transaction detals recieved from principal miner
Votername=Swapna,Fater-name=narayana,age=40,aadhaarid=685478788989
address=vijayawada,pincode=520010,Qualification=MTech


*****Verification Started*****


*****Verification Completed*****
Number of block===17
*****Publishing response*****
executed-->ipfs pubsub pub response QmPJZoMUigNFkPTN533CRevrqjqRLVQ22VRV6htePeEqpn
```

Figure 6 Verification of the block is submitted by the PM to consensus nodes



```
response received=QmUXvyWBfqaDFXBXDsXj9oLtt5haeoxm9vNH5x3iGUMU4x



******Consensus Starting******
peerid of consensus miner=QmUXvyWBfqaDFXBXDsXj9oLtt5haeoxm9vNH5x3iGUMU4x
Credibility value of this miner=85
Final Consesnus result=Block has proved to be valid
******Started adding block into principal blockchain******



Publishing hash to all nodes...
******Credibililty Value Computation Started
Updated credibility value=88Time taken to the whole process:......33.85ms
```

Figure 7 Apply consensus at the principal node after getting a response from the chosen miners

4.2Performance comparison with existing methods

The suggested CCA's performance is evaluated to determine its accuracy and dependability. Based on the following metrics

1) The number of messages required to be exchanged.
2) Average block mining time
3) Time to finality
4) Transaction Latency
5) The time required for processing

Evaluation based on message exchanges: *Table 2* shows how many messages are needed to reach a consensus with the proposed CCA consensus approach. In the traditional PoW, All the 'N' miners take part in the consensus process and disseminate their results to "N-1" nodes." N(N-1)" messages are sent and received, causing network overhead. The suggested strategy selects fewer nodes based on credibility and involves them in consensus. Many simulations show how a growing number of miners affects consensus messages.

Let the HCBLOM, LCBLOM, and AM group miners be G1, G2, and G3. Let A1, A2, and A3 be the chosen nodes from G1, G2, and G3 for the consensus process.G1 is calculated as shown in Equation 1, and G3 is calculated as shown in Equation 2. The miners in group G2 are Nill since the proposed strategy excludes nodes having less CV from engaging in the consensus procedure. Consequently, the minimum number of messages must be exchanged using the proposed method, as in Equation 3.

$$G1 = (A1 \times 50)/100 \qquad (1)$$

$$G2 = (A3 \times 50)/100 \qquad (2)$$

$$\text{Number of Message Exchanges(NME)} = (\text{G1} + \text{G2} + \text{G3})(\text{N} - 1) \qquad (3)$$

Table 2 shows that the proposed method needs 63% less NME than the current PoW method

Table 2 Evaluation of the proposed CCA and PoW mechanism for message exchange

N	G1	A1	G2	A2	G3	A3	NME(POW)	NME(CCA)	Reduction (%)
100	50	25	25	0	25	12	9900	3663	63
200	100	50	20	0	80	40	39800	17910	55
300	136	68	65	0	99	49	89700	34983	61
400	140	70	75	0	85	42	159600	44688	72
500	245	122	125	0	130	32	249500	76486	69.3
600	285	142	156	0	159	79	359400	132379	63.1

Using *Figure 8*, we can see how the proposed method stacks up against PoW. The proposed model is evaluated across various nodes ranging from 100 to 600; the model has shown good performance with a 63% reduction in the number of messages being exchanged. The model has outperformed at the optimal number of nodes, i.e., at 400 nodes with almost 72% of reduction in message exchange, and the model has proven to be robust in dealing with larger size groups over the smaller size, as in the current model the participation of the node is dependent on CV, resulting in fewer number of nodes that involve in exchange of the data.

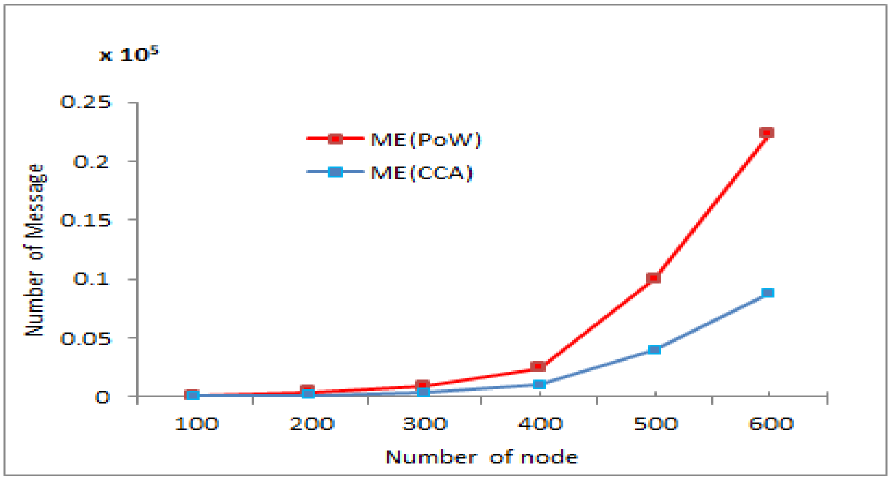


Figure 8 No of nodes vs. message exchange

Average Block Mining Time: The block mining time is interpreted as the amount of time required by the particular blockchain protocol to complete the processing of a transaction. The transactions on a blockchain can be completed at a faster rate when the block time is reduced. The average mining time the consensus algorithms take to mine a block is shown in *Figure 9*. The experimental results have proven that the PoW consumes exceptionally high mining time as all the nodes in the network are involved in consensus, followed by PoS and DPoS which consumes lesser mining times than the PoW as only a fewer number of nodes are involved in consensus. The proposed CCA algorithm consumes less mining time than all the state-of-the-art techniques considered in the current study. The CCA consumes less mining time with fewer miners who have better CVs, where the CV largely depends on the response time.

Time to finality (TTF): TTF is a metric that determines the time needed to ensure that the performed transaction in the block is irreversible. The mean time to finality is determined based on the mean time to mine the block identified by BM_t, the corresponding formula for TTF is shown in Equation (4).

$$TTF = B_C \times BM_t \quad (4)$$

In the above Equation, the variable B_c denotes the number of block confirmations. For better comprehensibility on TTF, an example with PoW with an average block mining time is 10 minutes, and the transactions cannot be reversed after adding six blocks. So, the TTF for PoW is 60 minutes.

Figure 10 shows that the proposed CCA approach has outperformed concerning the time to finality with a mean time of 2 minutes, which is minimal among the rest. It is desired that the value of TTF values must be minimal to the robust model.

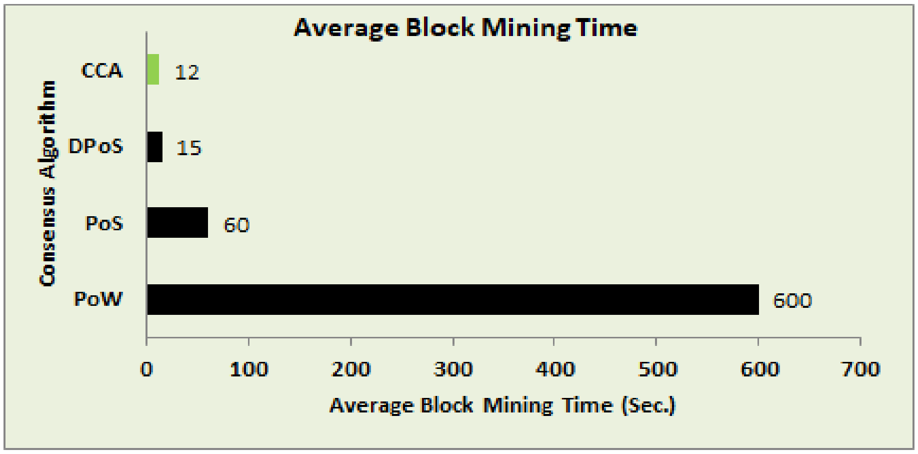


Figure 9 Average block mining time

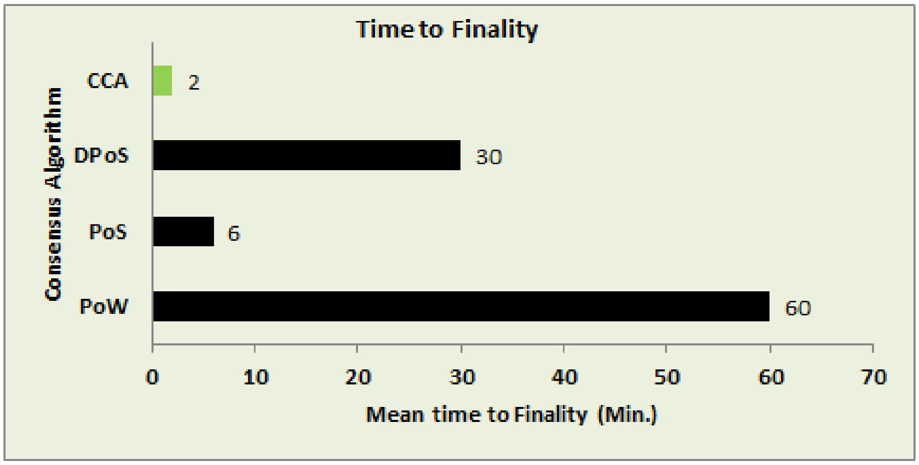


Figure 10 Mean time to finality

Transaction latency: transaction latency is the other pivotal metric used in assessing the blockchain-driven networks' performance, which approximates the delay associated with transaction execution. The latency is determined based on the time at which the transaction was added to a block identified by T_a and the time concerning to transaction transmitted to the network identified by T_n. The formula for transaction latency identified by $T_L$is shown in Equation 5.

$$T_L = T_a - T_n \qquad (5)$$

Figure 11 shows that PoW takes longer than all other algorithms. PoS take more time than DPoS but less time than PoW. In PoS, the request-response phase happens twice. CCA outperforms compared to the other consensus algorithms.

Comparison based on processing time: A graphical illustration of the node count, which ranges from 100 to 600, is shown in *Figure 12*. The proposed consensus algorithm, CCA, outperforms PoW, PoS, and DPoS in terms of performance. The outcome demonstrates that, compared to PoW, PoS, and DPoS techniques, the proposed approach—CCA—reduces execution time by 50.9%, 36.2%, and 32.3%, respectively. The proposed consensus algorithm, CCA, outperforms the current methodology..

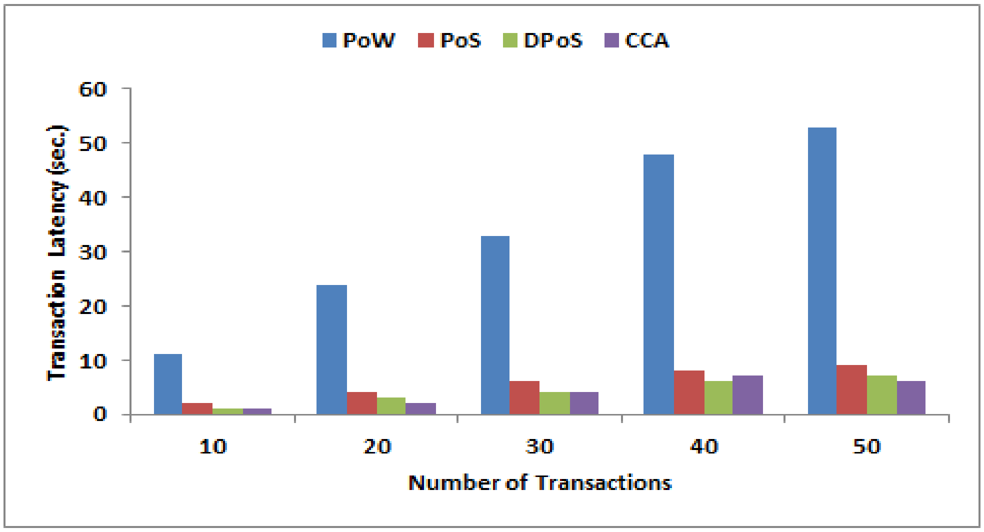


Figure 11 Transaction latency of consensus algorithms

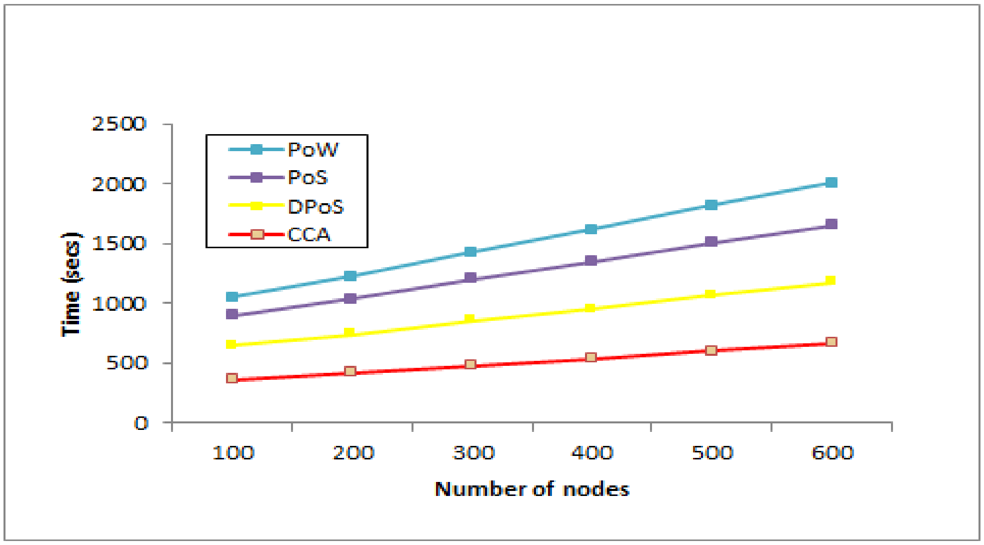


Figure 12 Processing time comparison

4.2.1Comparison with the load-based approach

In 2020, Singh [20] suggested a CPU load-based consensus technique for exchanging messages. This method places a greater emphasis on the use of the CPU. In addition, the approach that has been suggested, known as CCA, places a greater emphasis on the dependability and credibility component. Because the load-based technique keeps track of the load status table, the variation can be assessed in terms of the time it takes. It is time-consuming since it gets the miner's load status and updates it. The execution time is recorded as miners increase from 10 to 1000. *Figure 13* depicts the comparative evaluation of the proposed methods, CCA, and the CPU load-based approach. The number of nodes ranges from one hundred to one thousand. According to the findings, it can be inferred that the CCA speeds up the processing time.

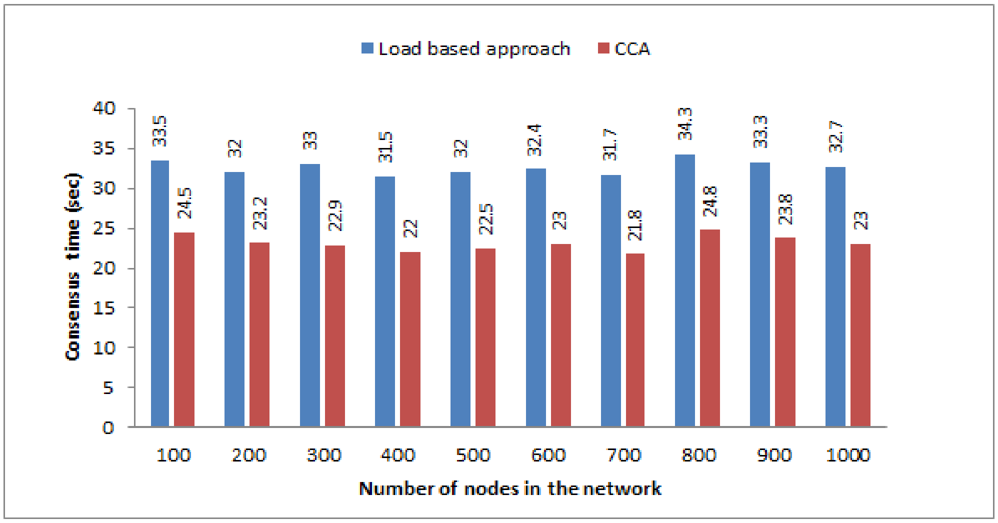


Figure 13 Performance analysis of load based approach and CCA

5.Discussions

Blockchain has transformed many industries recently, resulting in breakthroughs in banking, health, and other fields.

In this study, we aimed to demonstrate how to use blockchain for voter registration. To mine blockchain blocks, the credibility-based consensus algorithm is suggested. By utilizing DLT for voter registration, the need for intermediaries will be reduced, time and money will be saved, the process will be streamlined, and trust will be built between the various parties. Using blockchain to track voting rights results in yearly cost savings and provides a tamperproof ledger, among other advantages.

Transparency: Each register office maintains a complete blockchain of all transactions and keeps their history accessible from anywhere at any time.

Reliability: Any notable modification in records is only feasible if no consensus process exists, which is not the fact.

Cost-savings: Blockchain technology lowers costs. In contrast to the recommended strategy, where everything is digitalized, file holding and printing typically come at a high expense.

Shorter processing time: The suggested approach only needs 1-2 hours as opposed to the traditional process's 1–2 weeks.

The use of digital signatures provides greater security compared to manually filling out documents. The research problem of this article was addressed through the proposed mechanism in this study. Table 3 compares the suggested mechanism with PoS, PoW, and DPoS based on various characteristics.

Table 3 Performance comparison of PoW, PoS, DPoS, and CCA

Consensus Algorithm	PoW	PoS	DPoS	CPU load-based approach	Proposed Approach
Utilization of energy resources	High	High	Medium	Low	Low
Modern hardware	Needed	Not Needed	Not needed	Not needed	Not needed
Scalability	Low scalability	Less scalable	Not scalable	Scalable	Scalable
Security	It is feasible to launch an attack	Reduces the risk of threat	Reduces the risk of assault by 51%	Based on CPU load and	Based on CV.No security attack can

Consensus Algorithm	**PoW**	**PoS**	**DPoS**	**CPU load-based approach**	**Proposed Approach**
	with 51% of the hash power; however, this would be impractical in the actual world.			computational power	be done
The complexity of the system	High	Medium	Medium	Medium	O(1) less
Integrity	Multiblock verification	Multiblock verification	Multiblock verification	Hash-based addressing	Consensus-based

On average, around half of the network nodes participate in the proposed consensus method. The time needed by the proposed credibility-based consensus strategy is roughly 50.9% less than the current PoW, which makes the system efficient. The consensus is reached with 60% less communication overhead as fewer nodes participate. This framework made it easier for government to adopt a decentralized method for voter registrations.

The proposed model has been evaluated concerning various performance evaluation metrics concerning the NME, average block mining time, TTF, transactional latency, and processing time. The model has outperformed with a 72% reduction in the number of messages exchanged, considerably lower than the other techniques considered in the current study. Fewer messages being exchanged would result in optimal utilization of the network resources. The average block mining time is retained to be minimum by selectively choosing the miners based on the response time of the approaches. TTF is the other pivotal metric used in assessing the performance of the proposed approach in ensuring the irreversibility of the transactions; the CCA has taken a minimal amount of time, i.e., 2 minutes, to ensure the transaction is irreversible. Transactional latency and processing time are the metrics that determine the delay associated with the transaction and the processing time; the proposed CCA model has minimum transactional latency and processing time compared to other state-of-art models. A complete list of abbreviations is shown in *Appendix I.*

Our study has some limitations

- It is possible for some miners to reach the highest threshold CV, which is represented by the number CV = 120. In such a scenario, determining which miner or node is more trustworthy than others become challenging.
- Introducing people to blockchain-based technology can also be challenging.
- The storage and retrieval of data from the blockchain become challenging as the number of transactions increases. Therefore, it is necessary to develop efficient searching algorithms to enable swift and accurate retrieval of data.

6.Conclusion and future work

An application based on blockchain was proposed for managing voter registrations, addressing issues with the current voter registration system. A consensus mechanism was developed to minimize transmission overhead, resulting in a faster and more effective methodology than conventional methods like DPoS, PoW, and PoS. The proposed algorithm, CCA, reduced the overhead of exchanged messages by 63% and execution time by 53% compared to currently available algorithms. The credibility-based consensus method outperformed the currently available approaches, making the voter registration system based on blockchain technology highly scalable, safe against fraudulent practices, and suitable for real-world applications. Additionally, in future development, a side chain that stores all block data will be utilized to reduce blockchain overhead. The time required to access data in the side-chain will be measured and used to enhance the search performance of any registry record.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

Author's contribution statement

Swapna Donepudi: Conceptualization, investigation, writing –original draft, analysis and interpretation, and study. **K Thammi Reddy:** Editing, analysis and interpretation, study, and supervision.

References

[1] Igbani I, Jumase M. Manual for voter registration officials. 2006.

[2] Keyssar A. The right to vote: the contested history of democracy in the United States. Basic Books; 2009.

[3] Fischer E. A, colman KJ. Election getting better or worse. American University on the Centre for Democracy and Election Management. 2006.

[4] Kronstadt KA. India's 2019 national election and implications for US interests. Current Politics and Economics of South, Southeastern, and Central Asia. 2019; 28(4):481-502.

[5] Donepudi S, Reddy KT. Blockchain oriented hyperledger based performance driven framework for mass e-voting. Intelligent Decision Technologies. 2021; 15(4):579-89.

[6] https://www.slideshare.net/arishrajan/modernizing-our-voter-registration-system-to-awaken-indian-democracy. Accessed 20 December 2022.

[7] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. Decentralized Business Review. 2008:1-9.

[8] Kelly J. Barclays says conducts first blockchain-based trade-finance deal. Reuters Technology News. 2016.

[9] Alikhani A, Hamidi HR. Regulating smart contracts: an efficient integration approach. Intelligent Decision Technologies. 2021; 15(3):397-404.

[10] Srinivasu PN, Bhoi AK, Nayak SR, Bhutta MR, Woźniak M. Blockchain technology for secured healthcare data communication among the non-terminal nodes in IoT architecture in 5G network. Electronics. 2021; 10(12):1-26.

[11] Guo Y, Liang C. Blockchain application and outlook in the banking industry. Financial Innovation. 2016; 2:1-12.

[12] Cocco L, Pinna A, Marchesi M. Banking on blockchain: costs savings thanks to the blockchain technology. Future Internet. 2017; 9(3):1-20.

[13] Niranjanamurthy M, Nithya BN, Jagannatha SJ. Analysis of blockchain technology: pros, cons and SWOT. Cluster Computing. 2019; 22:14743-57.

[14] Zhang R, Xue R, Liu L. Security and privacy on blockchain. ACM Computing Surveys. 2019; 52(3):1-34.

[15] Tschorsch F, Scheuermann B. Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials. 2016; 18(3):2084-123.

[16] Garg K, Saraswat P, Bisht S, Aggarwal SK, Kothuri SK, Gupta S. A comparative analysis on e-voting system using blockchain. In 4th international conference on internet of things: smart innovation and usages 2019 (pp. 1-4). IEEE.

[17] Singh K, Singh N, Kushwaha DS. An interoperable and secure e-wallet architecture based on digital ledger technology using blockchain. In international conference on computing, power and communication technologies 2018 (pp. 165-9). IEEE.

[18] Singh N, Kumar T, Vardhan M. Blockchain-based e-cheque clearing framework with trust based consensus mechanism. Cluster Computing. 2021; 24:851-65.

[19] Singh N, Vardhan M. Blockchain based E-stamp procurement system with efficient consensus mechanism and fast parallel search. Journal of Mechanics of Continua and Mathematical Sciences. 2018; 13(4):73-89.

[20] Singh N, Vardhan M. Distributed ledger technology based property transaction system with support for IoT devices. International Journal of Cloud Applications and Computing. 2019; 9(2):60-78.

[21] Nguyen GT, Kim K. A survey about consensus algorithms used in blockchain. Journal of Information Processing Systems. 2018; 14(1):101-28.

[22] King S, Nadal S. Ppcoin: peer-to-peer crypto-currency with proof-of-stake. Self-Published Paper. 2012; 19(1):1-6.

[23] Swapna D, Praveen SP. An exploration of distributed access control mechanism using blockchain. In smart intelligent computing and applications: proceedings of the third international conference on smart computing and informatics, 2020 (pp. 13-20). Springer Singapore.

[24] Li D, Cai Z, Deng L, Yao X, Wang HH. Information security model of block chain based on intrusion sensing in the IoT environment. Cluster Computing. 2019; 22:451-68.

[25] Singh N, Vardhan M. Digital ledger technology-based real estate transaction mechanism and its block size assessment. International Journal of Blockchains and Cryptocurrencies. 2019; 1(1):67-84.

[26] Gupta S, Sinha S, Bhushan B. Emergence of blockchain technology: fundamentals, working and its various implementations. In proceedings of the international conference on innovative computing & communications 2020 (pp. 1-5).

[27] Kiayias A, Russell A, David B, Oliynykov R. Ouroboros: a provably secure proof-of-stake blockchain protocol. In 37th annual international cryptology conference, Santa Barbara, CA, USA, 2017 (pp. 357-88). Cham: Springer International Publishing.

[28] Yadav AS, Shikha S, Gupta S, Kushwaha DS. The efficient consensus algorithm for land record management system. In IOP conference series: materials science and engineering 2021 (pp. 1-13). IOP Publishing.

[29] Yang F, Zhou W, Wu Q, Long R, Xiong NN, Zhou M. Delegated proof of stake with downgrade: a secure and efficient blockchain consensus algorithm with downgrade mechanism. IEEE Access. 2019; 7:118541-55.

[30] Chen YC, Tso R. A survey on security of certificateless signature schemes. IETE Technical Review. 2016; 33(2):115-21.

[31] Kumari A, Singh KD. Kerberos style authentication and authorization through CTES model for distributed systems. In computer networks and intelligent computing: 5th international conference on information processing, Bangalore, India, 2011 (pp. 457-62). Springer Berlin Heidelberg.

[32] Mishra S, Kushwaha DS, Misra AK. Jingle-Mingle: a hybrid reliable load balancing approach for a trusted distributed environment. In fifth international joint

conference on INC, IMS and IDC 2009 (pp. 117-22). IEEE.

[33] Mishra S, Kushwaha DS, Misra AK. An optimized scheduling algorithm for migrated jobs in trusted distributed systems. In international conference on computer and communication technology 2010 (pp. 503-9). IEEE.

[34] Balasubramaniam A, Gul MJ, Menon VG, Paul A. Blockchain for intelligent transport system. IETE Technical Review. 2021; 38(4):438-49.

[35] Kumari A, Mishra S, Kushwaha DS. A new collaborative trust enhanced security model for distributed system. International Journal of Computer Applications. 2010; 1(26): 127-34.

[36] Pippal SK, Kumari A, Kushwaha DS. CTES based secure approach for authentication and authorization of resource and service in clouds. In 2nd international conference on computer and communication technology 2011 (pp. 444-9). IEEE.

[37] Boke AK, Nakhate S, Rajawat A. Efficient key generation techniques for securing IoT communication protocols. IETE Technical Review. 2021; 38(3):282-93.

[38] Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for secure EHRS sharing of mobile cloud based e-health systems. IEEE Access. 2019; 7:66792-806.

[39] Li W, Feng C, Zhang L, Xu H, Cao B, Imran MA. A scalable multi-layer PBFT consensus for blockchain. IEEE Transactions on Parallel and Distributed Systems. 2020; 32(5):1146-60.

[40] Xu G, Bai H, Xing J, Luo T, Xiong NN, Cheng X, et al. SG-PBFT: a secure and highly efficient distributed blockchain PBFT consensus algorithm for intelligent internet of vehicles. Journal of Parallel and Distributed Computing. 2022; 164:1-11.

[41] Arun B, Ravindran B. Scalable byzantine fault tolerance via partial decentralization. VLDB Endowment. 2022; 15(9):1739-52.

[42] Jiang X, Sun A, Sun Y, Luo H, Guizani M. A trust-based hierarchical consensus mechanism for consortium blockchain in smart grid. Tsinghua Science and Technology. 2022; 28(1):69-81.

[43] Prabha P, Chatterjee K. Design and implementation of hybrid consensus mechanism for IoT based healthcare system security. International Journal of Information Technology. 2022; 14(3):1381-96.

[44] Liu S, Gupta N, Vaidya NH. Approximate byzantine fault-tolerance in distributed optimization. In proceedings of the ACM symposium on principles of distributed computing 2021 (pp. 379-89).

[45] Haddaji A, Ayed S, Chaari L. Federated learning with blockchain approach for trust management in IoV. In advanced information networking and applications: proceedings of the 36th international conference on advanced information networking and applications 2022 (pp. 411-23). Cham: Springer International Publishing.

[46] Li Y, Wang X, Sun J, Wang G, Chen J. Data-driven consensus control of fully distributed event-triggered multi-agent systems. Science China Information Sciences. 2023; 66(5).

Swapna Donepudi earned her M.Tech in Computer Science & Engineering from JNTU Kakinada, and she is currently pursuing her Ph.D. at GITAM School of Technology in Visakhapatnam, Andhra Pradesh, India. She has published 12 papers in Scopus indexed journals and conferences.
Email: dswapna@pvpsiddhartha.ac.in

Dr. K Thammi Reddy is working as a Professor at GITAM School of Technology. He has more than 25 years of teaching experience. He has more than 30 publications in reputed journals and conferences. His research interests are Data Mining and Distributed Systems.
Email: thammireddy.vsp@gmail.com

Appendix I

S. No.	Abbreviation	Description
1	AM	Authorized Miners
2	BLO	Booth Level Officers
3	BLOM	Booth Level Office Miners
4	CCA	Credibility based Consensus Algorithm
5	CM	Consensus Miner
6	CV	Credibility Value
7	DAG	Directed Acyclic Graph
8	DDoS	Distributed Denial of Service
9	DLT	Distributed Ledger Technology
10	DPoS	Delegated Proof of Stake
11	EPIC	Election Photo Identity Card
12	ERO	Electoral Registry Office
13	HCBLOM	High Credibility Booth Level Office Miners
14	IoV	Internet of Vehicles
15	IPFS	Inter Planetary File System
16	LCBLOM	Low Credibility Booth Level Office Miners
17	NME	Number of Message Exchanges
18	PBFT	Practical Byzantine Fault Tolerant
19	P2P	Peer to Peer
20	PM	Principal Miner
21	PoS	Proof of Stake
22	PoW	Proof of Work
23	SG-PBFT	Score Grouping- Practical Byzantine Fault Tolerant
24	SWOTM	Strength, Weakness, Opportunities, Threat Matrix
25	TMS	Trust Management System
26	TTF	Time to Finality