Secure data transmission in power systems using blockchain technology

Anand Srivatsa[1], Ananthapadmanabha Thammaiah[2], Likith Kumar MV[3], Rajeshwari D[4], Suma AP[2]
[1]Department of Electronics and Communication Engineering, The National Institute of Engineering, Mysuru, India
[2]School of Engineering, University of Mysore, Mysuru, India
[3]Department of Electrical and Electronics Engineering, The National Institute of Engineering, Mysuru, India

Article Info

Article history:

Received May 18, 2024
Revised Aug 1, 2024
Accepted Aug 6, 2024

Keywords:

Blockchain
Consensus
Proof of stake
Proof of work
Secured data transmission

ABSTRACT

Recent advances in intelligent systems have significantly improved power management, load distribution, and resource management capabilities, far beyond past constraints. Despite these gains, the development of internet-connected technology has brought various vulnerabilities, leading to negative results. The integration of intelligent technology has unintentionally offered chances for hackers to enter networks and modify data sent to central systems for analysis. One of the most serious risks is the false data injection attack (FDIA), which may drastically impair analytical outcomes. Previous research has shown that standard approaches for recovering data affected by FDIA are unreliable and inefficient. This paper investigates the use of the proof of stake (PoS) consensus method in this framework improves data integrity and makes it easier to identify illegal changes. Participating nodes may reject or change block transactions, ensuring the ledger's correctness. Our results show that the PoS consensus method is exceptionally successful in creating and adding transactions to the blockchain. Furthermore, the PoS mechanism's simplicity in block formation enhances both time and energy efficiency, resulting in considerable benefits in operational performance.

Corresponding Author:

Anand Srivatsa
Department of Electronics and Communication Engineering, The National Institute of Engineering
Manandavadi Rd, Mysuru, 570008 Karnataka, India
Email: anand.srivatsa@nie.ac.in

1. INTRODUCTION

Data transmission plays a vital role in contemporary power systems, enabling the monitoring, maintenance, and optimization of grid performance. It involves the exchange of real-time information among various electrical devices and systems, facilitating the efficient operation and management of power networks [1]–[3]. The risks associated with cyber assaults on power systems and cloud environments include data breaches, service disruptions, and unauthorized access. Data breaches include the unlawful infiltration of cloud services to get access to sensitive data, which may lead to data theft, compromised confidentiality, and legal ramifications [4]–[6]. Communication networks are essential in this process, connecting power plants, substations, distribution systems, and control centers, allowing the transfer of critical data such as voltage levels, power flows, and system status across long distances throughout the entire power grid [7]. Power systems use many essential protocols and technologies to ensure efficient data transfer. Supervisory control and data acquisition (SCADA) systems, for instance, are pivotal for data collection and control within power networks. Intelligent electronic devices (IEDs) are positioned in subnode stations and other important areas to collect and transfer data to centralized control centers for the purpose of monitoring and analysis [8].

Additionally, various communication protocols, including distributed network protocol (DNP3), Modbus, IEC 61850, and Conitel, ensure reliable and secure data exchange among devices and systems [9].

However, despite the advantages of data transmission in power systems, security vulnerabilities pose significant challenges. Unauthorized interception of data during transmission, for example, can compromise the (CIA triad) integrity, confidentiality, and availability of power system data. Encryption and secure communication protocols are essential to mitigate the risk of data eavesdropping [10]. Moreover, hackers may attempt to tamper with data during transmission, leading to inaccurate measurements or control directives that could disrupt the electrical system or cause equipment failures. Techniques such as digital signatures can help ensure data integrity and prevent unauthorized data modifications [11]. To address these security concerns and enhance data integrity in power systems, blockchain technology emerged as a better solution.

Researchers have proposed innovative solutions addressing such security hurdles, including the use of blockchain technology and cybersecurity information exchange frameworks, increasing over security in cyber grid environment [12], [13]. Experimental results demonstrated the efficacy of the model in terms of security and performance, this has been emphasized by the authors in their paper, highlighting the importance of blockchain based solution in power systems [14]. Avoiding tampering of data because of maintaining the mainchain of the blockchain preserving the integrity [15].

Blockchain is a distributed ledger technology (DLT) that provides segregated tamper-proof recording, guaranteeing the permanence and safety of data recorded on the blockchain. By leveraging blockchain, power systems have the capability to provide a reliable and open platform for transmitting and storing data, enhancing data integrity and validation [16], [17]. However, the scalability of blockchain solutions remains a key challenge, particularly in handling the massive volumes of data generated by power grids [18]. Proof of stake (PoS) consensus mechanisms, which are less resource-intensive compared to proof of work (PoW) methods offer potential scalability improvements for blockchain-based solutions in power systems [19], [20].

The techniques such as hybrid approaches using machine learning clustering models such as k-means and support vector, upgraded convolutional neural networks, multiobjective optimization frameworks, and empirical mode decomposition [21]–[23]. These approaches leverage simulation-based case studies to demonstrate their effectiveness, highlighting their potential for real-world application. Even though other researchers have proposed certain solutions, our research aims to contribute to the field by proposing a secure mechanism for data transmission between nodes while maintaining message confidentiality and integrity [24].

In this paper, our research looked into both consensus of blockchain technology for a comparative study. Then we explored other ways to see if mitigation of false data injection (FDI) attack which other researchers have mentioned in their work. Then we looked into blockchain technology to find an optimal solution which takes care of the security triad (CIA). The salient contributions can be itemized as follows: i) The proposed work utilizes substation data for an observation between PoS and proof of word consensus of blockchain technology for secured data transmission; ii) It is demonstrated that PoS is a superior choice for adding a single block of transactions compared to proof of work, since it needs less computational resources. The PoS consensus removes the need for prefix-based hashing, in contrast to the PoW consensus mechanism; and iii) Using blockchain technology proposed in this work we can prevent false data injection attack (FDIA) due to the complexity of hashing algorithm.

2. ALGORITHM

Many existing methods for ensuring secure data transfer fail to adequately address all challenges, including issues like data manipulation during transmission and maintaining data integrity. The threat of FDI at both ends of transmission is particularly concerning, as it can lead to skewed predictions and inaccurate outcomes [25]. To address this challenge, our proposed solution introduces a consensus mechanism whereby multiple nodes participate in voting and stake their credibility in updating the blockchain with transactions. Through a PoS system, transactions with the highest stake are given priority for inclusion in the blockchain. Each node contributes gas to vote and finalize block inclusion, with the chain promptly updating and informing other nodes of any changes made.

This blockchain-based solution will be readily accessible to nodes utilizing SCADA for forecasting purposes, ensuring immediate access to purified data and subsequent stages in the process. PoS operates similarly to earning interest on deposited funds, rewarding participants based on the amount and duration of their holdings [26]. In this model, stakeholders receive interest akin to a bank's interest on deposited funds, incentivizing participation and ensuring network security. Notably, while the bitcoin network's energy consumption is significant, efforts to conserve resources, such as situating mining operations near hydroelectric facilities, are being pursued. However, concerns remain regarding security issues like the risk of selfish mining processes, necessitating ongoing exploration of blockchain consensus mechanisms [27]–[30]. The architecture used in our framework of work has been modified according to our power system setup. Figure 1 discusses the methodology adapted in the implementation of blockchain in a power node is discussed here. The power data generated at sub-stations such as Megalapura, Jyothinagara in the CESCOM sub section of Mysore power distribution system, is sent to process through to convert the power files to process through their regular channel.

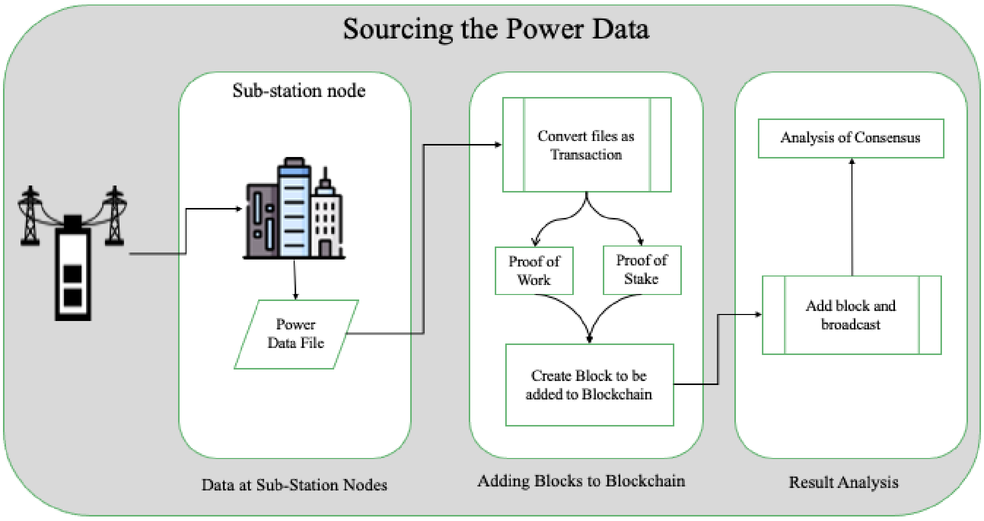


Figure 1. Creation of blocks using consensus

The sub-stations which act as nodes in the blockchain network infrastructure, the PoS as consensus is utilized to identify itself as part of the node participating to create a block in the blockchain. The identification and addition of block is based on the PoS algorithm. In the given methodology, the PoW consensus is done separately to have a final analysis, not done simultaneously. Algorithm 1 is used for PoS. In Figure 2, the proposed network architecture of blockchain in the premise of the sub-stations of the power grid is presented below are connected by p2p. The data generated at stations are validated and transactions are added as block to the existing blockchain.

The PoS technique may be expressed mathematically in the following manner: Every participant in the network has a certain quantity of bitcoin, referred to as their stake. Equation (1) represents the overall stake in the network, abbreviated as P, which includes the contributions of all users.

$$\sum_{j=1}^{m}[P] \quad (1)$$

A user is randomly chosen to verify the next block on the blockchain, depending on the amount they have at stake. The likelihood of being chosen is directly related to the quantity of cryptocurrency held. However, in the sub-station scenario, the higher stake is determined by the amount and timing of data generated and held as a stake. Therefore, a participant with the highest stake is sure to be picked, as described in (2).

$$Authenticate = Greatest(Variant(j)) \quad (2)$$

– In order to confirm the suggested block, the selected user transmits it to the network.
– Other network users evaluate the proposed block by assessing its compliance with blockchain requirements, such as the authenticity of the transactions and the sequencing of the blocks, as stated in (3).

$$Authenticate = AssociateUser(bc), \{where\ bc = blockchain\} \quad (3)$$

– Once the network gives its approval to the proposed block, it is appended to the blockchain. In return for their ongoing participation in the network, the selected user is granted a preset amount of bitcoin as a reward, as stated in (4).

$$AddABlockTo(bc) = (Accepted(Block))), \{where\ bc = blockchain\} \quad (4)$$

The aforementioned procedure is iterated for every new inclusion of a block on the blockchain, wherein users are chosen randomly according to their stake, DO Loop (for whole block). The PoS algorithm employs a stochastic selection procedure that relies on the quantity of bitcoin held as a stake to authenticate transactions and append newly created blocks to the blockchain in a safe and transparent manner. The algorithm is specifically developed to mitigate the substantial energy consumption and environmental repercussions linked to PoW, therefore establishing it as a more sustainable substitute for blockchain networks. The following Algorithm 1 allows for the testing of the approach on any file produced inside a subnode of the power system. The simulation was conducted utilizing the power data from the local power grid system.

Algorithm 1. Adding of block using proof of stake
```
Process(m,n) #(Initialize the system to test)
  o   Network allows all Participant Users to Join
  o   Check (Has New Block Added == True)
  o   Choose (Variant User’s Stake) Is Greater?
              Authenticate
                  Return (Authentication status)
  o   If(Authentication Status == Success)
              BlockAdd
  o   Else
              BlockReject
  o   CreateBlock = BlockNew,
Iterate through Each New Block
```

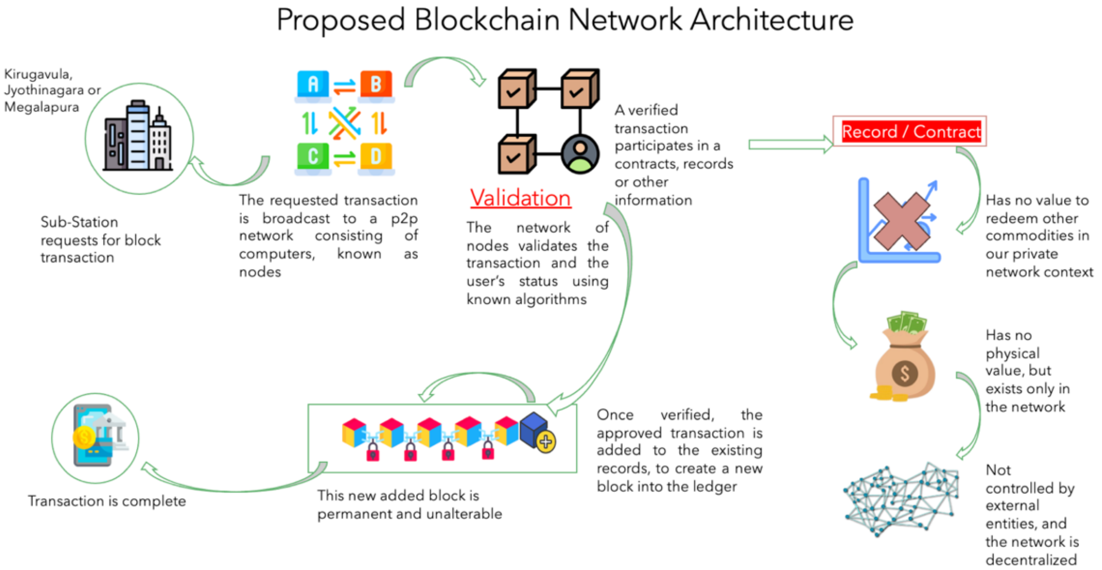


Figure 2. Proposed blockchain network architecture

3. METHOD

The dataset used in our experiment comprises power transmission data obtained from the power plants located in the Mysuru area. The dataset enables SCADA to examine and use these statistics for the purpose of predicting load forecasting of Mysuru station. The research work was based on the following:

The gathered data at known sub-station consists of time-series data. The device records current, voltage, active energy, power, reactive power sent to other stations, and data received from other substations in a phased manner. The collected values are of a continuous nature. Additionally, there are two additional sets of substation data that the corresponding nodes use to broadcast transactions as blocks, which are then appended to the blockchain. Since the produced values vary across each subnodes, the usual node data for raising its stake is not needed to add a new block. The data shown in Figure 3 of Kirugavula Substation only displays a limited number of data characteristics from the gathered dataset. Figure 4 depicts an additional substation, located in Megalapura, that has comparable characteristics and requires the transmission of data via a blockchain transaction.

The experiment was done in a controlled setting with three nodes. Every node has been designated as a substation and will generate the transaction for the block and contribute their stake in the network. Therefore, one of the nodes would have precedence depending on the number of stakes (here in our setting, data size, date and time created gets the stake) allocated for voting. Approval of a block's inclusion to the chain occurs upon verification of stake ownership. The third node in the environment is the Jyothinagara Substation as shown in Figure 5 of the Mysore District, Karnataka, India. The Jyothinagara Substation is the third node in the environment, as seen in Figure 5 of the Mysore District, located in Karnataka, India.

	.KIRUGAVALU_66			10		0 Stopped	
		KRGVL66HV1Y-B_PH VALUE	KRGVLSTNBATVOLTA VALUE	KRGVL66SFCACTIVE VALUE F1-SFC - DEVANOOR MYS	KRGVL66SFCREACT VALUE	KRGVL66SFCACTIVE VALUE	KRGVL66S VALUE
-	0:01:00	66.447	122.10944	1.9745	1.196	670353	700523
-	0:02:00	66.22	122.10944	1.9745	1.18	670403	700523
-	0:03:00	66.094	122.10944	1.9745	1.18	670436	700523
-	0:04:00	66.094	122.10944	1.9465	1.18	670470	700523
-	0:05:00	66.142	122.10944	1.9465	1.1685	670502	700523
-	0:06:00	66.022	122.10944	1.9465	1.1685	670534	700523
-	0:07:00	65.806	122.10944	1.9465	1.1685	670568	700523
-	0:08:00	65.394	122.10944	1.9465	1.111	670600	700523
-	0:09:00	65.394	122.10944	1.9465	1.111	670615	700523
-	0:10:00	65.275	122.10944	1.922	1.111	670647	700523
-	0:11:00	65.275	122.10944	1.922	1.1065	670696	700523
-	0:12:00	65.278	122.10944	1.9245	1.1065	670728	700523
-	0:13:00	65.278	122.10944	1.9245	1.1065	670761	700523

Figure 3. Sample data of subnode station Kirugavula

		.MEGALAPURA_66			10		0 Stopped	
			MGLPR66HV1Y-B_PH VALUE	MGLPRSTNBATVOLTA VALUE	MGLPR66SFCACTIVE VALUE F1-S F C	MGLPR66SFCREACT VALUE	MGLPR66SFCACTIVE VALUE	MGLPR66S VALUE
0:00	-	0:01:00	66.496	112.7189	6.173	2.611	1050470	1743610
0:01	-	0:02:00	65.964	112.7189	6.695	3.223	1050590	1743610
0:02	-	0:03:00	65.78	112.7189	6.207	2.968	1050700	1743610
0:03	-	0:04:00	65.78	112.7189	6.134	2.968	1050800	1743610
0:04	-	0:05:00	65.833	112.7189	6.134	2.968	1050900	1743610
0:05	-	0:06:00	65.752	112.7189	6.058	2.968	1051000	1743610
0:06	-	0:07:00	65.598	112.7189	5.892	2.845	1051100	1743610
0:07	-	0:08:00	65.3	112.7189	5.789	2.845	1051200	1743610
0:08	-	0:09:00	65.3	112.7189	5.725	2.777	1051300	1743610
0:09	-	0:10:00	65.244	112.7189	5.725	2.717	1051350	1743610
0:10	-	0:11:00	65.244	112.7189	5.643	2.682	1051490	1743610
0:11	-	0:12:00	65.244	112.7189	5.533	2.599	1051580	1743610
0:12	-	0:13:00	65.244	112.7189	5.597	2.714	1051670	1743610
0:13	-	0:14:00	65.244	112.7189	5.597	2.714	1051770	1743610
0:14	-	0:15:00	65.244	112.7189	5.597	2.714	1051860	1743610

Figure 4. Sample data of subnode station Megalapura

.JYOTHINAGARA_66				10		0
	Time	JTYNGR66HV1Y-B_PHVOLT VALUE	JTYNGRSTNBATVOLTAGE VALUE	JTYNGR66FTSACTIVEPOWER VALUE F1-FTS	JTYNGR66FTSREACTIVEPOWER VALUE	
3-Aug-16	0:00 - 0:01:00	67.114395	118.581497	0.000637		0
	0:01 - 0:02:00	67.046539	118.581497	0.000637		0
	0:02 - 0:03:00	67.046539	118.581497	0.000637		0
	0:03 - 0:04:00	67.002594	118.581497	0.000637		0
	0:04 - 0:05:00	67.002594	118.581497	0.000637		0
	0:05 - 0:06:00	66.921654	118.581497	0.000637		0
	0:06 - 0:07:00	66.859177	118.581497	0.000637		0
	0:07 - 0:08:00	66.75248	118.581497	0.000637		0
	0:08 - 0:09:00	66.75248	118.581497	0.000637		0
	0:09 - 0:10:00	66.668488	118.581497	0.000637		0
	0:10 - 0:11:00	66.668488	118.581497	0.002563		0
	0:11 - 0:12:00	66.703384	118.581497	0.002563		0
	0:12 - 0:13:00	66.703384	118.581497	0.002563		0
	0:13 - 0:14:00	66.703384	118.581497	0.002563		0
	0:14 - 0:15:00	66.703384	118.581497	0.002563		0
	0:15 - 0:16:00	66.703384	118.581497	0.002563		0
	0:16 - 0:17:00	66.703384	118.581497	0.002563		0

Figure 5. Jyothinagara substation sample data

3.1. Proof of work and execution of algorithms

Figure 6 shows the experiment which was conducted using the Flask framework which uses Python. The system was established using a Linux operating system, specifically utilizing Python version 3.8.10 and the Flask framework. The website utilizes a Python script to generate the first genesis nodes for three substations. Subsequently, every node that is involved in the process bets its priority by generating a random (variable) integer. Subsequently, the block transactions are appended as a cohesive unit to the chain. An observed trend is that none of the three nodes/substations simultaneously engage in the stake. However, if simultaneous execution of block creation, then the corresponding blocks are placed in a queue for future addition to the chain [31]–[33]. The blocks of the blockchain include distinct attributes that enable the identification of each block's association with a certain node and the date and time on which it was added to the chain, ensuring uniqueness.

This experiment using PoW is as shown in Figure 6, block chain creation, every time a new file is generated at the substation it creates the transactions and create a prefix-based hash and based on the blockchain creation rules checks for the previous hash value to authenticate and adds newly created block. This time taken is noted during the experiment for later graph analysis. The Block has the following properties as shown in Table 1.

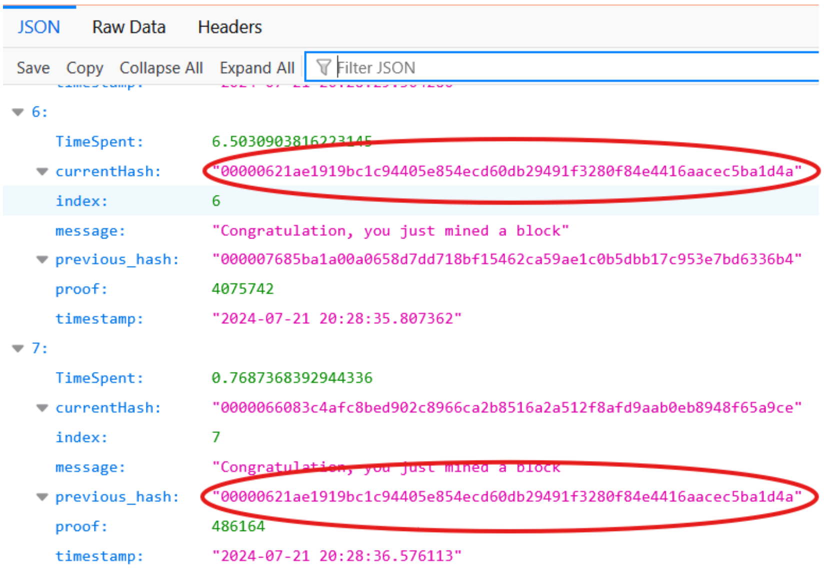


Figure 6. Block chain creation using proof of work

Table 1. File properties

Characteristics	Description
SN#	Block ID
NId#	This will aid in identifying the owner of the block and determining who has the authority to access and open it. It encompasses all the transactions held inside the block.
datetime#	Data and time creation of block
Prev_hash#	previous blocks hash value of previous block
Curr_hash#	Current block´s hash value of create block
Merkle#	Consolidated hash value of all the blocks added
Nonce#	Number used once to generate a prefix blockchain

3.2. Implementation of proof of stake

The PoS consensus used process flow is shown in Figure 7, initial power data created at the substation. The substation acts as a node to participate in the block creation to be added to the chain, so based on the priority and check on the time of creation of the file, participates in the getting a stake to vote and works with the other nodes/substations to be allowed to create the block and get the vote from other nodes so that it can participate and if it wins the stake creates the block and let other nodes know about the status of the blockchain. The other nodes also add the block to their blockchain. The time from notifying the nodes to updating the block to the blockchain has been noted for comparison purposes.

While the security of data transmission is anticipated to be maintained throughout the block building process in the blockchain, it is possible for the data received by other nodes to be compromised if the software executing on those nodes is targeted and modified via programming. To address this issue, it is necessary to verify the authenticity of the sent data packet by recognized nodes rather than by other entities inside the node. And further security measures involve using asymmetric key encryption to authenticate users by validating the data. To further alleviate this issue, one may include permission mechanisms that restrict the participation of certain nodes in block generation and block addition to the blockchain.

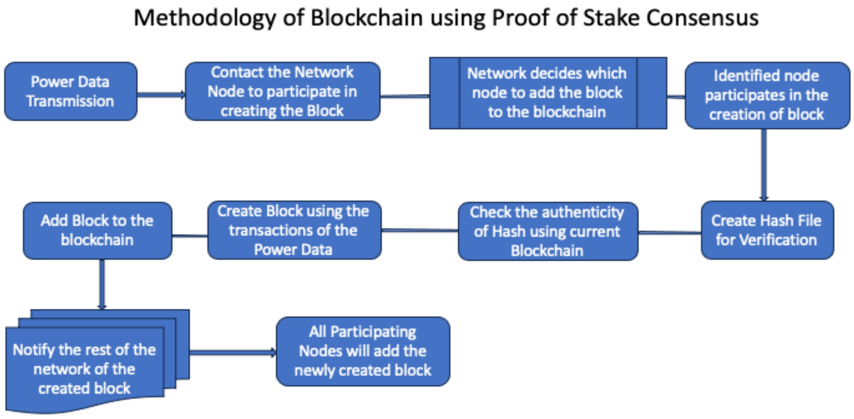


Figure 7. Methodology for PoS consensus

4. RESULTS AND DISCUSSION

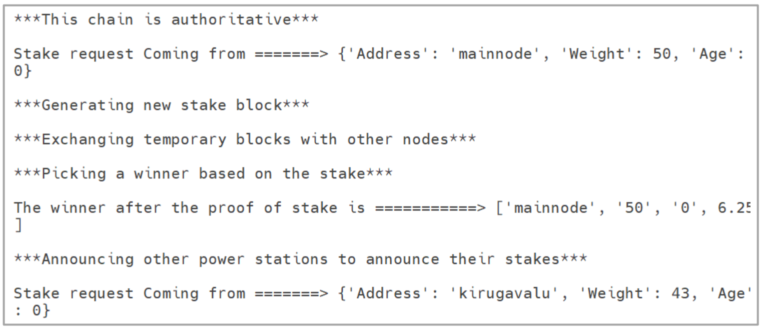
The consensus algorithms provided by different entities function in diverse scenarios and cater to the requirements of businesses. The consensuses were selected in our example to assess their behavior and feasibility in implementing them within an environment where power system status estimate data are monitored and sent to a centralized area (SCADA). These values are then processed to determine subsequent consequences based on business requirements. The two consensuses have been contrasted in Table 2, illustrating how transactions may be turned into blocks inside the blockchain. These blocks can either be kept centrally or by each participating node in a zonal node.

Table 2. Comparison of consensus

Consensus protocol	Pros	Cons
PoW	– Proven security: Its security model is well known, and many types of threats have not been able to break it. – Segregation: Anyone with the right tools can mine with PoW, the network can become less controlled. This is because it is hard for one group to take over. – Non-changeable: Changing a block requires a lot of computing power, therefore the blockchain history is unchangeable. – Simplicity: Miners solve cryptographic challenges to add blocks, and the longest chain is legitimate.	– Energy inefficient: PoW uses a huge amount of energy. – Central mining: Direct mining in ASICs, as well as the emergence of big mining pools, resulted in a concentration of power and resources, leading to centralization and the possibility of exposing the network to possible weaknesses. – High cost: Set up cost is high for mining. – Non-scalable: PoW networks often exhibit longer transaction processing times and poorer throughput.
PoS	– Energy efficient: PoS is far more energy-efficient than PoW since it requires less processing. Validators are chosen based on the willingness to "stake". – Scalable: PoS systems are more scalable than PoW systems because they process transactions quicker and can handle more transactions per second. – Low risk: PoS does not use ASICs unlike PoW, so centralized mining is less likely. Incentives to stake tokens create a more dispersed network. – Nodes can join: PoS makes the network more accessible by allowing more users to become validators without costly mining equipment.	– Priority based: Those who have reputed data and time and adapted early gets priority. – Security concerns: Not broken yet and mostly used in private networks. – Initial distribution: In a private network this is not a concern as to who have higher stakes or coins to start with.

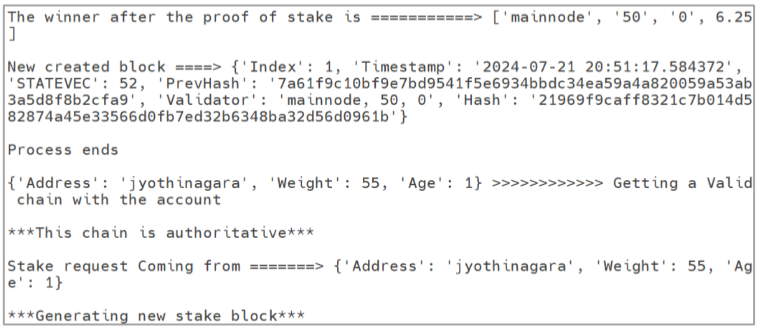
The findings indicate that the consensus mechanism based on proof of work relies only on computing power, whereas PoS waits for agreement to be reached based on the largest stake. Based on the prevailing agreement, proof of stake is a more favorable choice in the power system field, since each node is not needed to compete against one another; they simply need to have their block included. Each block transaction in the blockchain is significant for every node. The purpose of preparing the block's information is to ascertain the ownership of the block. The consensus algorithms suggested by various companies operate under distinct situations and function effectively according to the specific requirements of the company. In our case, the selection of the consensus was made to assess the behavior and feasibility of implementing these two consensus methods in an environment for further business outcomes. The consensus has shown the process of converting transactions into blocks on the blockchain. These blocks may either be kept centrally or by each participating node in a certain zone.

In power systems, one must have a sufficient stake or priority number to be eligible as a validator on a PoS blockchain and be allocated the duty of a block builder. Figures 8 and 9 depict the simulated result of running the program in the given context. In order to participate in PoW, miners are required to make substantial investments in processing gear and bear the burden of paying substantial energy expenditures to operate the computers that carry out the calculations. In our scenario of power station nodes, the security problem in a PoS system may not be applicable. A cluster of substations may function as a node, with one of them assuming the role of a leader node. The leader node is responsible for aggregating the data and participating in a vote/stake process to become a block maker in the blockchain. The integrity of this configuration may not be compromised by a 51% assault. Similarly, blockchain is updated after adding a new block after running PoS.



```
***This chain is authoritative***

Stake request Coming from =======> {'Address': 'mainnode', 'Weight': 50, 'Age':
0}

***Generating new stake block***

***Exchanging temporary blocks with other nodes***

***Picking a winner based on the stake***

The winner after the proof of stake is ===========> ['mainnode', '50', '0', 6.25
]

***Announcing other power stations to announce their stakes***

Stake request Coming from =======> {'Address': 'kirugavalu', 'Weight': 43, 'Age'
: 0}
```

Figure 8. PoS dataset as block for Kirugavula



```
The winner after the proof of stake is ===========> ['mainnode', '50', '0', 6.25
]

New created block ====> {'Index': 1, 'Timestamp': '2024-07-21 20:51:17.584372',
'STATEVEC': 52, 'PrevHash': '7a61f9c10bf9e7bd9541f5e6934bbdc34ea59a4a820059a53ab
3a5d8f8b2cfa9', 'Validator': 'mainnode, 50, 0', 'Hash': '21969f9caff8321c7b014d5
82874a45e33566d0fb7ed32b6348ba32d56d0961b'}

Process ends

{'Address': 'jyothinagara', 'Weight': 55, 'Age': 1} >>>>>>>>>>>> Getting a Valid
 chain with the account

***This chain is authoritative***

Stake request Coming from =======> {'Address': 'jyothinagara', 'Weight': 55, 'Ag
e': 1}

***Generating new stake block***
```

Figure 9. PoS dataset as block for Jyothinagara

The results of these two agreements demonstrate that the use of PoS enhanced the efficiency of generating transaction blocks for inclusion in the blockchain. Prefix was set to seven for PoW yielded a quantifiable outcome. For a low prefix, it was far lower, even on a local computer. One point put forward throughout our inquiry was that reducing the prefix would be acceptable. Our work showed that it would significantly reduce the time required for creating the blocks. However, in our environment or network, it is more advantageous to use a more advanced consensus process in which block creation is determined by the participation of certain nodes. This was achieved by using the PoS mechanism instead of PoW. Therefore, in a closed net of interconnected nodes, PoW may be acceptable. However, the results indicate that PoS is more effective and appropriate for environments where several sub-nodes are involved. The graph shown in Figure 10 illustrates the constant and efficient nature of block production in PoS, as indicated by the yellow line. Experimentation of varying prefixes from five to seven demonstrates that it may considerably decrease the time required for block generation. However, it remains lacking in energy efficiency. Based on the above timeline comparison between PoS vs PoW shows a 90% reduction in creation of blocks when PoS is used.

Recent years have seen a growing recognition of the necessity for strong and adaptable security measures in intricate systems like power grids. A range of security measures have been investigated and put into practice, each with distinct benefits and difficulties. The present study undertakes an evaluation of many mechanisms, with a specific emphasis on blockchain-based security, conventional encryption techniques such as advanced encryption standard (AES), Rivest-Shamir-Adleman (RSA), secure multiparty computation (SMPC), and homomorphic encryption. Blockchain technology has intriguing characteristics like decentralization, immutability, and transparency. Through the elimination of a single point of failure and the guarantee of immutability of recorded data, blockchain technology significantly improves security. Nevertheless, the use of this technology might result in delays as the network expands, and the capacity to handle higher transaction volumes becomes a consideration.

The efficiency and established trustworthiness of traditional encryption methods, such as AES and RSA, have led to their widespread use. However, they need careful key management, and the storing of keys in a centralized location provides a possible single point of failure. SMPC and homomorphic encryption provide sophisticated methods to ensure the strict secrecy and privacy of data. SMPC guarantees the preservation of computations and data privacy, but with the trade-off of higher computational complexity and protocol complexities. Homomorphic encryption enables data processing without the need for decryption, therefore preserving secrecy. However, it creates substantial overhead and presents practical difficulties. The security approaches, each with unique advantages and constraints, highlight the intricate nature of safeguarding extensive, decentralized systems such as electricity networks. Table 3 provides a concise overview of the advantages and disadvantages of different approaches.

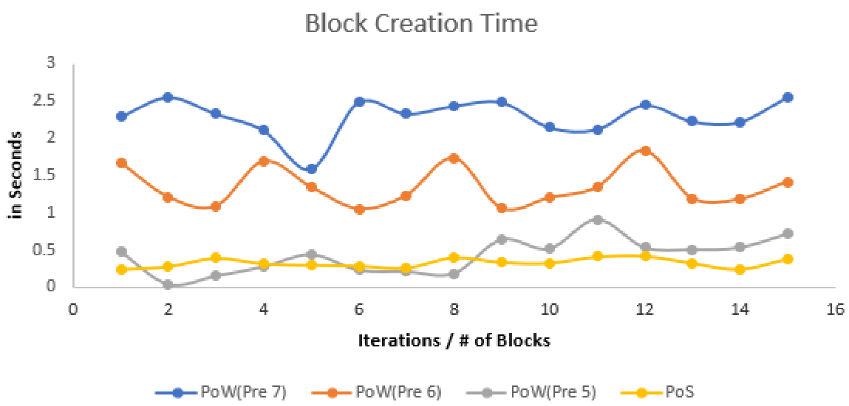


Figure 10. Block creation time chart

Table 3. Pros and cons of different security implementations

Security implementation	Pros	Cons
Blockchain based security	– Decentralization: Elimination of failure at single point. – Immutable: Cannot change once recorded – Transparency and traceability: Possible only if the transactions are public, but since this is a private network within the power system, traceability is achieved.	– Latency: as the chain increased or the number of transaction increases, this may lead to latency in creating and adding the block. – Scalability issues: May occur if the amount of transactions increases. And unknowingly if the adding of transactions are not controlled.
AES, RSA	– Efficiency–Fast, well known and proven algorithms. – Widely adopted in various applications.	– Key management: Encryption key needs high level secure management. – Failure: Centralized key storage can lead single point failure if compromised.
SMPC	Keeps the computation, encryption and data private and not exposed	Complexity of computation and has privileged protocols.
Homomorphic encryption	Can process data without decryption keeping the confidentiality	Had lots of overhead than traditional encryption. Implementation is challenging.

5. CONCLUSION

Through our study, we have uncovered several methods for transmitting data securely by employing blocks of transactions inside the framework of blockchain technology. The original experiment included transmitting power substation transactions from their origin location to a data collection station, which then sent the data to the central station for examination using SCADA technology. Our objective was to communicate data using different approaches without being vulnerable to FDIA, which includes the manipulation of data. The use of blockchain technology has significantly enhanced the preservation of data integrity.

We evaluated the feasibility of implementing two consensus procedures. One of them needs "proof of work," which entails a substantial amount of computational power and energy. However, we may still use this agreement, since it can be achieved in a confidential environment, unlike Bitcoin which operates in a public context. However, PoS is a superior choice for incorporating the known blocks that have been generated and included in the blockchain, since it offers proof of block addition by showcasing a greater stake. This has been shown by assigning a level of importance to the data from each station and using a sufficiently enough stake to evaluate and incorporate it into the blockchain as a block. One observation relating temporal complexity and security is that there is a tradeoff between the two. If we prioritize security, it will take a significant amount of time to implement checks and balances. On the other hand, if we want to add blocks to the chain quickly, security will be compromised.

Some of the future directions are, limitation of our study is the possibility of a false data injection attack occurring during the transmission of data to other nodes before it is converted into blocks. This means that the created data itself may be incorrect. Recreating inaccurate data that closely resembles the original data may be difficult, especially if it does not include numerical values. The prospects of this study include a thorough examination of the regeneration of fabricated data prior to its inclusion as a block. Smart contracts are susceptible to weaknesses, since they are deployed as distributed applications and may be targeted by programmable attacks. If high-speed data transmission is required, it may be necessary to develop a strategy to ensure scalability and speed. Should look into how nodes can be utilized to be more scalable in creating blocks without compromising on the outcome of purpose of keeping it secure and reliable.

REFERENCES

[1] M. E. El-Hawary, "The smart grid—state-of-the-art and future trends," *Electric Power Components and Systems*, vol. 42, no. 3–4, pp. 239–250, 2014.

[2] N. Kaur and S. Bhalla, "Combined energy harvesting and structural health monitoring potential of embedded piezo-concrete vibration sensors," *Journal of Energy Engineering*, vol. 141, no. 4, 2015.

[3] M. S. Mahmood and N. B. Al Dabag, "Blockchain technology and internet of things: review, challenge and security concern," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 1, pp. 718–735, 2023, doi: 10.11591/ijece.v13i1.pp718-735.

[4] P. Mell and T. Grance, "The NIST definition of cloud computing," *Communications of the ACM*, vol. 53, no. 6, pp. 50–56, 2010, doi: 10.1145/1721654.1721672.

[5] A. Parwekar and S. B. Navale, "Service level agreement (SLA) violation detection techniques in cloud computing," *International Journal of Computer Science and Information Technologies*, vol. 5, no. 3, pp. 2950–2954, 2014, doi: 10.1109/ICNWC57852.2023.10127520.

[6] Y. S. Abdulsalam and M. Hedabou, "Security and privacy in cloud computing: technical review," *Future Internet*, vol. 14, no. 1, 2022, doi: 10.3390/fi14010011.

[7] F. Aminifar, M. Abedini, T. Amraee, P. Jafarian, M. H. Samimi, and M. Shahidehpour, "A review of power system protection and asset management with machine learning techniques," *Energy Systems*, vol. 13, no. 4, pp. 855–892, 2022, doi: 10.1007/s12667-021-00448-6.

[8] F. W. Almuhammad and R. A. Jabr, "Data communication requirements for power system automation and protection," *IEEE Transactions on Power Delivery*, vol. 27, no. 3, pp. 1227–1235, 2012, doi: 10.1109/TPWRD.2012.2189750.

[9] H. Farhangi, "The path of the smart grid," *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18–28, 2010, doi: 10.1109/MPE.2009.934876.

[10] T. Docquier, Y. Q. Song, V. Chevrier, L. Pontnau, and A. Ahmed-Nacer, "Performance evaluation methodologies for smart grid substation communication networks: a survey," *Computer Communications*, vol. 198, pp. 228–246, 2023, doi: 10.1016/j.comcom.2022.11.005.

[11] R. S. Ghorbani and G. A. Ghassami, "Efficient communication protocols for wide-area monitoring and control systems," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 4, pp. 2170–2178, 2013, doi: 10.1109/TII.2013.2257016.

[12] L. Li *et al.*, "Cyber attack estimation and detection for cyber-physical power systems," *Applied Mathematics and Computation*, vol. 400, 2021, doi: 10.1016/j.amc.2021.126056.

[13] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, pp. 841–853, 2020, doi: 10.1016/j.future.2017.08.020.

[14] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3162–3173, 2019, doi: 10.1109/TSG.2018.2819663.

[15] L. Hirtan, P. Krawiec, C. Dobre, and J. M. Batalla, "Blockchain-based approach for e-health data access management with privacy protection," *IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD*, vol. 2019-September, 2019, doi: 10.1109/CAMAD.2019.8858469.

[16] N. N. Vo and S. K. Das, "A blockchain framework for secure data sharing and collaboration in power systems," *IEEE*

Transactions on Smart Grid, vol. 10, no. 4, pp. 4214–4225, 2019, doi: 10.1109/TSG.2018.2888274.
[17] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in *2017 IEEE International Conference on Web Services (ICWS)*, Jun. 2017, pp. 468–475, doi: 10.1109/ICWS.2017.54.
[18] I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev, and J. Mendling, "Blockchain technology in the energy sector: a systematic review of challenges and opportunities," *Renewable and Sustainable Energy Reviews*, vol. 100, pp. 143–174, 2020, doi: 10.1016/j.rser.2018.10.014.
[19] F. Saleh, "Blockchain without waste: proof-of-stake," *The Review of Financial Studies*, vol. 34, no. 3, pp. 1156–1190, Feb. 2021, doi: 10.1093/rfs/hhaa075.
[20] C. Pujari, B. Muniyal, and C. B. Chandrakala, "A decentralized consensus application using blockchain ecosystem," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 6, pp. 6399–6411, 2020, doi: 10.11591/IJECE.V10I6.PP6399-6411.
[21] "Cryptanalysis of the affine cipher," *Practical cryptography*, http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-affine-cipher/ (accessed Oct. 02, 2022).
[22] C. Cid, "Cryptanalysis of RSA: a survey," *SANS Institute*. 2003, Accessed: Oct. 04, 2022. [Online]. Available: https://www.sans.org/white-papers/1006.
[23] M. Holovský, "Unhyped comparison of blockchain platforms," *medium*, 2021. http://medium.com/p/679e122947c1 (accessed Oct. 02, 2022).
[24] Bitcoin, "Proof of stake instead of proof of work," *Bitcoin Forum*. 2011, https://bitcointalk.org/index.php?topic=27787.0. (accessed Oct. 16, 2022).
[25] N. Sahani, R. Zhu, J.-H. Cho, and C.-C. Liu, "Machine learning-based intrusion detection for smart grid computing: a survey," *ACM Transactions on Cyber-Physical Systems*, vol. 7, no. 2, pp. 1–31, Apr. 2023, doi: 10.1145/3578366.
[26] W. Zhao, S. Yang, X. Luo, and J. Zhou, "On PeerCoin proof of stake for blockchain consensus," in *2021 The 3rd International Conference on Blockchain Technology*, Mar. 2021, pp. 129–134, doi: 10.1145/3460537.3460547.
[27] Q. Wang, J. Huang, S. Wang, Y. Chen, P. Zhang, and L. He, "A comparative study of blockchain consensus algorithms," *Journal of Physics: Conference Series*, vol. 1437, no. 1, 2020, doi: 10.1088/1742-6596/1437/1/012007.
[28] N. Bui, A. P. Castellani, P. Casari, and M. Zorzi, "The internet of energy: a web-enabled smart grid system," *IEEE Network*, vol. 26, no. 4, pp. 39–45, 2012, doi: 10.1109/MNET.2012.6246751.
[29] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *Decentralized Business Review*, 2008.
[30] C. C. Sun, A. Hahn, and C. C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power and Energy Systems*, vol. 99, pp. 45–56, 2018, doi: 10.1016/j.ijepes.2017.12.020.
[31] R. Chen, X. Li, H. Zhong, and M. Fei, "A novel online detection method of data injection attack against dynamic state estimation in smart grid," *Neurocomputing*, vol. 344, pp. 73–81, 2019, doi: 10.1016/j.neucom.2018.09.094.
[32] D. Ding, Q. L. Han, Y. Xiang, X. Ge, and X. M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, 2018, doi: 10.1016/j.neucom.2017.10.009.
[33] M. Dehghani *et al.*, "Blockchain-based securing of data exchange in a power transmission system considering congestion management and social welfare," *Sustainability (Switzerland)*, vol. 13, no. 1, pp. 1–22, 2021, doi: 10.3390/su13010090.

BIOGRAPHIES OF AUTHORS

Anand Srivatsa received B.E degree in ECE from Vasavi College of Engineering (VCE), Hyderabad, did his M.S in software engineering from University of Houston, ClearLake, Texas. He has 19 years of industrial experience in software development and project manager. He is currently working as an associate professor in the Department of Electronics and Communication Engineering, The National Institute of Engineering, Mysuru. He can be reached at email: anand.srivatsa@nie.ac.in.

Ananthapadmanabha Thammaiah received BE degree in EEE from The National Institute of Engineering (NIE), Mysuru Karnataka affiliated to University of Mysore with 9th Rank in 1980. ME in power systems with 1st rank and gold medal and PhD with gold medal in power systems from University of Mysore, Mysuru in 1984 and 1997, respectively. He is currently Director of School of Engineering, University of Mysore. He has 250+ publications and guided 18 candidates for the doctoral degree. His research interests include soft computing application in power system engineering, reactive power compensation, renewable integration, and distributed generation. He can be reached at email: drapn2015@gmail.com. His profile can be found at https://www.researchgate.net/profile/Ananthapadmanabha-Thammiah.

Likith Kumar MV received BE degree in EEE from VTU, Belagavi, Karnataka in 2010. MTech in power systems and PhD in Faculty of Electrical Sciences from The National Institute of Engineering, Mysuru affiliated to VTU, Belagavi, Karnataka in 2016. He is currently working as associate professor in the Department of Electrical and Electronics Engineering, The National Institute of Engineering, Mysuru, India. His research interests include soft computing application in power system engineering, power quality, distributed generation, smart and microgrid. He can be reached at email: likith@nie.ac.in.

Rajeshwari D has awarded by B.E, MTech. and Ph.D. degree in computer science and engineering from Visvesvaraya Technological University Belagavi, India. Currently she is working as assistant professor, in the Department of Information Science and Engineering, The National Institute of Engineering (North Campus), Mysore. She has published 12 journal papers in peer reviewed journals, 5+ conference publications and book chapter. Her research interests include data mining, internet of things, block chain technology and data analytics. She has around 18+ years of teaching experience. She can be contacted at email: drrajeshwari@nie.ac.in.

Suma AP has completed her PhD in cyber security from VTU, her MTech in bio medical and instrumentation BE in electronics and communication engineering. She is working as assistant professor in Mysore University School of Engineering, University of Mysore, India. Her area of interests is in security, communication, bio medical and electronics. She can be contacted at email: sumapadmanabh@gmail.com.