Received: 21 December 2021 | Revised: 6 March 2022 | Accepted: 28 March 2022

DOI: 10.1002/ett.4525

RESEARCH ARTICLE

WILEY

A novel game theory based reliable proof-of-stake consensus mechanism for blockchain

Kirti Bala | Pankaj Deep Kaur

Department of Engineering and Technology, Guru Nanak Dev University, Jalandhar, India

Correspondence
Kirti Bala, Department of Engineering and Technology, Guru Nanak Dev University, RC, Jalandhar, India.
Email: kirti.may1893@gmail.com

Abstract

The prominent achievement of blockchain technology stimulates exceptional innovation. The major component of blockchain is the consensus mechanism. The standard consensus mechanisms specifically Proof-of-Work (PoW) rely on mining procedures and stake-based mechanisms such as Proof-of-Stake (PoS) rely on massive stake investment as the sole criteria for selection of leader nodes. However, PoW impose huge computational power requirements and latter may incorporate malicious nodes as leader nodes in anonymous blockchain. These issues might fuel the way for distrust among the participants in blockchain. Henceforth, a novel game theory based reliable PoS mechanism for blockchain has been proposed. Federated learning has been used to compute trust_score for each node. The nodes are trained on locally generated dataset. Further, a game theoretic approach has been proposed that uses a reward and punishment scheme to ensure threshold level of trust_score maintenance by each node. Finally, a crop insurance use case has been developed with the consensus mechanism and blockchain coded in python. The insurance claims are made to operate through smart contract based mobile app system to impart more authenticity. The system is tested and results show an intrusion accomplishment rate reduced by approximate 40% when compared to the standard PoS mechanism and by approximately 33% for algorand, 29% for ouroboros and 20% for tendermint. The mean absolute error also decreases by 30% within specific time. Furthermore, the proposed federated learning-based system is compared with basic neural network-based machine learning model and the results reveal that a significant reduction in average training time amounting to 8.35 second is achieved. Test accuracy has also been analyzed for various learning mechanisms.

KEYWORDS

blockchain, consensus mechanism, crop insurance, federated learning, game theory

1 | INTRODUCTION

Emerging technologies play a significant role in upgrading the traditional industries. The novel technologies pave the way for digital world to enter into multiple application areas. These emerging technologies can certainly aid to transform the existing processes for improvisation. Blockchain is one such technology with huge potential for application in wider domain.

Blockchain is characterized by features of distributed shared ledger and database with the inclusion of attributes like transparency, traceability, decentralization, and immutability.[1] The distributed ledger can only be altered by consensus mechanism mutually agreed upon by all participants.[2,3] Some major consensus mechanisms are PoW (Proof-of-Work), PoS (Proof-of-Stake), DPoS (delegated PoS), PBFT (practical byzantine fault tolerance). The blockchain finds its applications in diverse fields including finance and Internet of Things (IoT) owing to its prodigious features. With the inclusion of smart contracts, the application domain of blockchain is extended from cryptocurrency to nonfinancial applications.[4,5] The smart contracts state the terms of contract with self-executing line of code and are recorded over the distributed ledger.[6] Likewise, numerous use cases of blockchain technology in agriculture domain have been presented.[7] Evidently, the agriculture production systems have been benefited by the inclusion of technologies like IoT, machine learning and blockchain in several operations of agriculture like food supply chain management, smart irrigation practices, yield monitoring, forecasting and harvest prediction and so forth.[8,9]

Simultaneously, blockchain also finds remarkable applicability in financial sector as well. Crop insurance is one such crucial financial area which aids to support the agriculture finances but is not studied and researched. Thus, it is discussed in this research work. While, technology enthusiasts have endured to succor the farmers in optimizing the yield production for their income proliferation, weather-based disasters might be responsible for influencing the farmer's income. Thus, to uplift the farmers' financial status crop insurance is encouraged among them. Crop insurance enables the farmers to repay their loans and simultaneously bear the natural as well as man-made calamities.[10] The process of insurance includes multiple organizations and individuals. The insurer offers risk protection to the insured individual who is a policyholder. Likewise, Pradhan Mantri Fasal Bima Yojna is an insurance scheme presented with a purpose to provide financial aid to Indian farmers. It aims to provide the risk coverage and insurance coverage to the eligible farmers.[11]

The process of crop insurance needs to include more outstanding features like transparency, trackability and security to offer trust and reliability among the farmers. Evidently, blockchain technology finds its apposite role in the offering insurance services to users. Blockchain based insurance system offers more transparency, real time traceability into the insurance services.[12]

However, one major issue of concern with crop insurance is the intrinsic and extrinsic risks associated with the insurance sector and the need for extended security features in technology. The insurance providers collect and store huge volumes of personal data from users which is frequently transferred over the networks. The networks might be prone to perilous cyber-attacks. This makes it necessary to have an insurance system which comprises highly advanced security and privacy features for end users.[13]

The information stored in a blockchain governed by conventional consensus mechanisms might be prone to attacks and the personal identifiable information might be vulnerable to unethical access.[14] Thus, more enhanced consensus mechanism is required for blockchain.

1.1 | Analysis of mainstream consensus algorithms

The mainstream consensus algorithms offer various anticipated properties which are crucial for the efficient working of blockchain procedure. Various conventional consensus mechanisms are analyzed as shown in Table 1.

PoW is a splendorous algorithm for offering the decentralization and security in the blockchain. It prevents various glitches from entering the network like double spending.[15-17] But PoW is inefficacious in providing the efficient resource usage. Huge resource consumption at the end of miners is the concern that drive the way for another consensus mechanisms.

Thus, PoS is the breakthrough in this concern. The PoS protocol was developed with the objective of eliminating the need for high energy and computational powers requirements in PoW.[18] In PoS, nodes referred to as validators initially have to deposit a stake which is in point of fact a number of coins. Likewise, DPoS[19-21] was developed to offer higher energy efficiency. However, DPoS is still in its inception stage. Thus, this research work proposes to extend the functionality of PoS.

TABLE 1 Various standard consensus mechanisms

	PoW	PoS	DPoS
Type of blockchain	Permissionless	Permissionless/consortium	Permissioned
Decision making aspect	Mining involving huge computing capabilities	Net stake incurred	Witness nodes
Decentralized governance	Intense	Intense	Low
Energy Consumption	Very high	High	Low
Trust level	Low	Low	Moderate
Level of development	High	High	Low
Computing expenses	Very high	High	Moderate
Platforms	Bitcoin, ethereum	Polkadot, eosio, cardano	No known platforms

1.2 Motivation

Although the PoS holds huge capability to offer vast applicability, yet it has its own vulnerabilities which are as follows:

- Low-cost attacks: The PoS based blockchain networks are more susceptible to attacks by the imposter validator node with the coveted idea of grabbing rewards on top. It might cost insignificantly low to the malicious node or even zero cost by creating and managing fake stakes.[22] The attacker node can just fill the spurious data in the RAM or the disk of the victim node to breakdown the network to create fake stakes. The attacker node will be successful in depleting the resources of outstanding validator nodes, thereby eliminating the opportunities for any other node to win the rewards and populate the blockchain with erroneous blocks.
- Anonymity of validator nodes: Although, anonymity is the upshot of blockchain networks, yet it can prove to be ruinous in case of validator nodes for PoS consensus protocol. The parties involved in transaction might be reluctant to share the personal information to any third party. Anonymity of users' identity is the way out to alleviate the chances of users' personal information from being stolen by the trickery nodes present in the network. There may be the malicious nodes which may be at ease of losing few stakes in the possibility of earning greater profits.[23]
- Trust-less environment: The blockchain environment is characterized by skeptical situation where every node is distrustful of the other node. The PoS algorithm allows to choose the next block validator cogitating the stakes owned by the respected nodes which might call for malicious activities in the network by awe less validator nodes. Thus, it would be more preferred, if at the time of selecting the new block, the other validating nodes are aware the trustworthiness of the node originated the transaction. Every node should reflect its trust score to enable other validating nodes while voting for the new block. A trust evaluation model will help scale down the detrimental activities from mischievous nodes in a network[24] .

The PoS consensus mechanism with some alterations toward improving the security ought to be the most apt choice for the blockchain based system for insurance sector. Besides, the insurance system requires a completely digital system with enhanced security features as it is more prone to external attacks. Thus, the presented research work proposes a novel PoS consensus algorithm combined with the federated learning for trust management among validator nodes to be used in crop insurance system based on blockchain. The behavior of validator nodes is modeled using game theory to maintain threshold level performance which retains the overall performance of the system.

2 LITERATURE SURVEY

Blockchain has been successfully able to gather engrossment equally from industry as well as academia. It finds numerous applications varying from cryptocurrency, internet of things, financial services to providing a secure and traceable solution to public services.[25]

The robust features of distributed ledger make it a secure and credible system operating in the absence of any centralized authority.[26] The Figure 1 shows the basic architecture of blockchain with different nodes in network generating

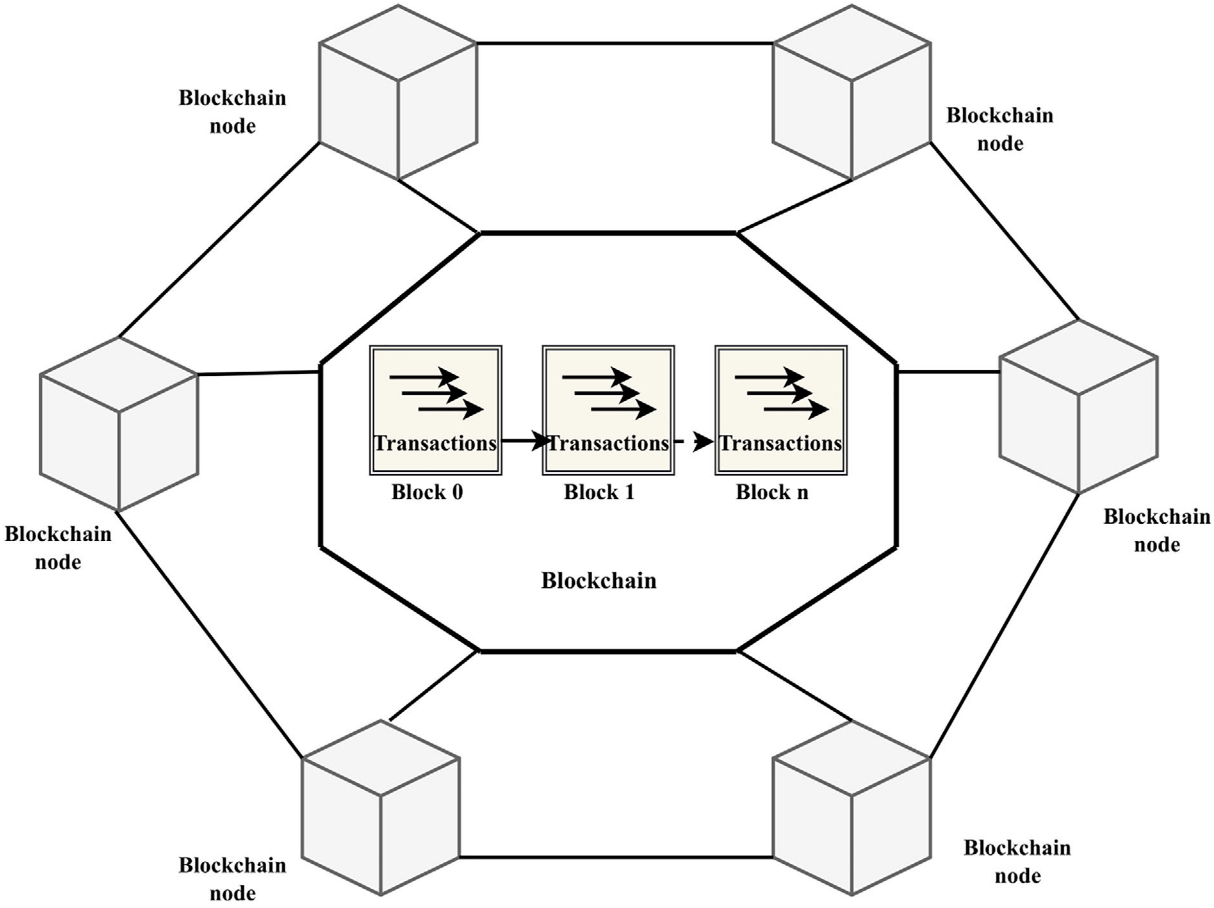


FIGURE 1 Basic architecture of blockchain

block consisting of transactions.[27] A block is added to the blockchain only after it is successfully verified by all participants under the requirements of consensus mechanism.[28] Consensus mechanism is one of the significant components of blockchain.

2.1 | Research trends in consensus mechanisms

The consensus algorithm is a mutual process which makes process of agreed decision making exist in decentralized network. Blockchain members use consensus mechanisms to verify the validity of transactions. The consensus algorithm is followed by every node in blockchain network to authenticate the data to be appended to blockchain.[29]

An exhaustive survey of major primitive consensus mechanisms and their related terminologies is presented in Reference 30. Conclusive analysis about the diverse consensus mechanisms is presented which reflect its significance for the future envisions in remarkable development in blockchain. The general consensus mechanisms such as PoW avoids the conflict among participating mining nodes through the computing capability priority order. Whereas the PoS consider the only the amount of stake in electing the node for block creation and validation.[31] Apart from the conventional consensus mechanisms some research works such as Reference 32 have shown interest to present reputation-based consensus mechanism for permissionless blockchain. Authors in Reference 33 have present a novel proof-of-activity consensus mechanism by integrating the conventional PoW and PoW consensus mechanism for refining certain parameters including cost but the inherent nature of PoW prevents it from energy efficiency improvement. Likewise, the proposed research work also presents a novel consensus mechanism but by extending the existing consensus mechanism that is, PoS.

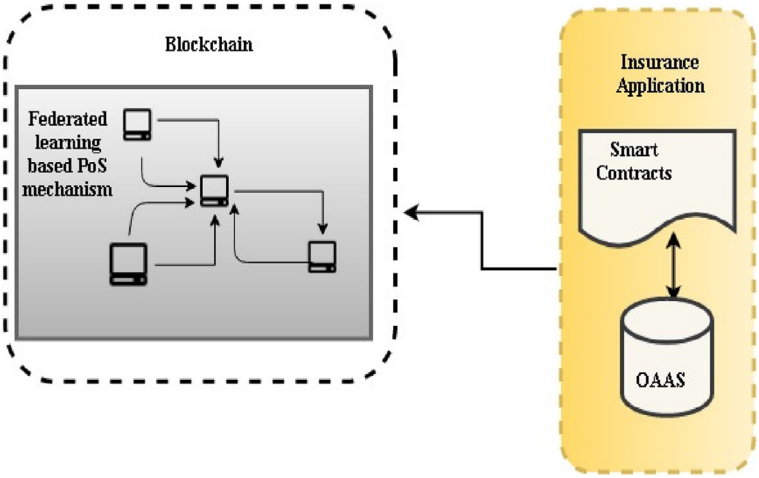


FIGURE 2 Conceptual overview of proposed system

The related work to present and augment PoS mechanism are discussed as it forms relevant part for the proposed consensus mechanism. Some researchers have been keen to explore the applications of PoS in diverse fields. In Reference 34, PoS public blockchain is used to evaluate the pricing scheme for the P2P energy trading market. Furthermore, PoS is expanded to handle IoT data streams in Reference 35. Authors in Reference 36 improves PoS consensus mechanism by considering security challenges but does not monitor the constant performance of the system nodes.

While some research works are focussed to enhance the PoS mechanism for removing some of its flaws. The authors in Reference 37 extends the standard PoS mechanism by integrating with identity for channelizing in trustless systems based on reputation. While Reference 38 presents an architecture for general staking based on novel data structure for multiple components of the system.

The proposed research work also proceeds with the basic objective of extending PoS mechanism for inclusion of trust-based factor for enhancing the security of the overall consensus mechanism. Figure 2 shows the conceptual overview of the proposed research work. The consensus mechanism can be improved with some machine learning mechanism. Thus, various learning paradigms have been studied in consequent sections.

2.2 | PoS based mechanisms

2.2.1 | Tendermint

The tendermint consensus protocol[39] uses BFT (byzantine fault tolerance) and PoS for block creation and confirmation. Similar to PoS, the validator nodes make deposit to get the voting rights. The final block proposing node is selected by voting and procedure including deterministic round robin voting in each communication round. The tendermint protocol is considered to be quit secure consensus but with the assumption of 2/3 participants of network being honest. The major applications of tendermint are the BigchainDB (https://www.bigchaindb.com)[40] and Ethermint[41] (https://ethermint.zone).

2.2.2 | Ouroboros

The ouroboros consensus[42] mechanism is a PoS based protocol. It selects a dynamic committee based on the net stake owned. The time is divided into epochs. The committee members in each epoch undergo the procedure for 3-phased coin tossing protocol and initiate the FTS (follow the Satoshi) algorithm which further helps in leader node selection. The FTS algorithm takes a string as input and provides a token index as the output. This token index address is chosen as the validator node for block selection.

2.2.3 | Algorand

The algorand consensus[43] also selects a dynamic committee based on net stake owned. It uses verifiable random function (VRF) as cryptographic sortition algorithm for leader node selection. The VRF takes private key of a node and a string as input to present a hash and a public verification proof as output. The hash is matched with the hash value range of each participating node. The matching node becomes the leader node. The hash value for each node is proportional to the stake amount owned. The VRF does not allow the leader node to be revealed before it submits the proof. The detailed comparison of these technologies with the proposed consensus is depicted in Table 2.

2.2.4 | Chains-of-activity

Chains-of-activity consensus protocol,[33] again uses FTS algorithm to choose the validation leader node. Here, the FTS algorithm uses different input. The chain is divided into equal parts of length l and the time into epochs. In each epoch, blocks of each part participate. The hash of each block in an epoch is combined to find the leader node for next epoch. The malicious behavior of the node is continuously supervised and in case found guilty, the deposit of that node will be confiscated.

2.3 | Different learning mechanisms

2.3.1 | Centralized machine learning classifier

Centralized machine learning requires a central server where the learning nodes are connected. The participating learning nodes, regularly upload their own local data to the centralized cloud server. The centralized server performs the complex computation and finally present the outcomes for test data making it computationally efficient for participant nodes. However, the data being used for learning purpose may be the personally identifiable data such as the health data records, location data, payment related details and many more. It could lead to data security issues like eavesdropping. Further, it may lead to other issues like the uploading of high range of data could lead to high communication overhead thereby leading to high latency in the network.[44]

2.3.2 | Distributed machine learning classifier

Distributed machine learning is designed to eliminate the need for moving the real time data to a central server. In distributed learning, the participant learning nodes train their models independently and send their model updates on central server at regular intervals. At central server, convergence testing is performed after certain decided rounds of communication for providing the average output for each node. It helps to train and test large scale dataset and provide a scalable solution for learning classification model.[45]

2.3.3 | Federated learning

The concern for enhancing the privacy and security of end user's personal data has led to the evolution of a novel learning mechanism which is termed as federated learning. The federated learning mechanism is based on a concerted deep learning framework which enables all the engaged devices to participate in training process while safekeeping their data on their local devices and regularly update the learning model by passing only the required meta data. Federated learning has been introduced by google in leu of preserving the security of user's data. The google authorities suggested that a global training model can be initiated on a central server which will be downloaded on individual devices. It will be trained iteratively using the local data of devices. The global model will be updated iteratively and consequently trained. The final model is again distributed to devices to get inference related results.[46]The difference between distributed learning and federated learning is that in federated learning training is initialized on local epochs.

TABLE 2 Comparison with other existing PoS consensus mechanism-based protocols

	Tendermint	Ouroboros	Algorand	Chains-of-activity	Proposed PoS
Consensus process	-Round-robin selection is used for leader selection -Blocks are confirmed by validators voting	-Committee leader -Leader selection by FTS algorithm and 3-phased coin tossing protocol	-Dynamic committee leader -Leader selection based on stake amount and VRF algorithm	-Leader selection is based on stake and previous block	-Leader selection is based on trust_score values calculated using federated learning.
Mining incentive mechanism	-Rewards distributed to validator nodes	-Rewards distributed to input endorsers and slot leaders	-Not defined	-Rewards are given to leader node	-Rewards are distributed to block adding validator leader nodes.
Decent behavior reward	-No	-No	-No	-No	-Yes, all nodes can earn rewards for decent behavior
Malicious behavior penalty	-Deposit is impounded in malicious behavior	-No penalty of incentives	-Not defined	-Leader node's deposit is impounded in malicious behavior	-Deposit confiscated for malicious behavior
Possible security challenges	-Dynamic stake distribution	-Certain security attacks like 51% attack	-Incentive capability is ignored	-Dynamic stake distribution	-Possible estimation of leader node information prior to selection
Network overhead	-High due to all -to-all communication	-High due to time divided into epochs	-Medium because of communication between relay nodes and participant nodes	-High due to communication between groups of blocks	-Low due to federated learning
Transaction originator	-Block creator	-Input endorser	-Block creator	-Block creator	-Leader node
Finality	-Absolute	-Probabilistic	-Probabilistic	-Probabilistic	-Absolute
Computing overhead	-Medium	-High	-High	-High	-Low

2.4 | Federated learning in blockchain

The security enhancement in standard consensus mechanisms is crucial to be used in financial sectors as the data security and privacy are quite imperative in financial applications. But data might be crucial for performing some data analysis and prediction. In the customary systems data collected at the edge nodes is transferred to the centralized server where the data is fed into the analysis algorithms and is shared by some team of data scientists. Federated learning enhances data security and privacy as it eliminates the need of uploading private data. Research communities have shown keen interests to study the exclusive characteristics and research potential of federated learning.[47,48]

Although the review study works[49,50] reveal the idea of convergence of blockchain with AI. Authors explore the possibility of using blockchain to do away the key challenges associated with AI. Similarly, Reference 51 have presented a peer-to-peer cryptocurrency, WekaCoin based on distributed learning consensus. The distributed learning consensus channelizes machine learning based system ranking. In the same lines researchers have tried to integrate the robust features of federated learning with blockchain. In Reference 52, authors had presented a blockchain integrated federated learning implementation for improving the collaboration among the mobile edge devices while reducing the communication overhead. This association between two technologies is used in numerous applications as discussed in Reference 53. The authors proposed a new design as FLchain. Various issues concerning the FLchain design are explored such as communication cost, decentralization, privacy protection, and resource allocation. The incessant research and development in federated learning is the major driving factor for adopting federated learning in integration with blockchain. Likewise, a blockchain based federated learning architecture is presented in Reference 54 which offers the opportunity to exchange as well as verify the local learning models.

2.5 | Game theory and blockchain

The presented research work also proposes to ensure the consistent performance through the mathematical model of game theory. Game theory is a mathematical concept that deals with the analysis of interaction among rational decision-making entities. The entities involved in decision making process acts as game players and tend to maximize their payoff also termed as utility, in view of the other players' strategies. Game theory is mathematical model to reach a consensus in case of conflict in decision making.[55,56] Game players choose the moves to reach decisive "win" and "loose" outcomes. Game theoretic model is grouped in two major categories: cooperative and noncooperative approaches. In cooperative games, the game players choose their strategies collectively after agreement among each other for the benefit of the system as a whole. It assumes that the game players adopt collective strategies as a group called as coalition and work cooperatively for decision making.[57] Whereas in noncooperative game theory, game players choose their strategies individually to maximize their own payoff. The players compete with each other being indifferent toward benefit or loss of others.[58]

The game theory was originally developed with the objective of assisting and analyzing the economic conduct of business firms, markets as well as individual consumers. In business economics,[59] game theory provides set of mathematical tools for predicting and analyzing the decisions of rivals for the firm managers. Also, it assists in strategic negotiation for the economic competition.[60]

In the recent years researchers have even tried to establish a gaining relation between the blockchain and the game theory. The main objective is to devise a blockchain network with the human behavior modeling for the greater benefit of the blockchain network. In the same context game theory has been used to enhance the security of the blockchain by preventing various security attacks such as selfish mining, majority attack.[61] The authors in Reference 62 have presented a novel system for secure information sharing leveraging the blockchain technology integrated with game theoretic approaches. Similarly, a game theoretic approach for calculating the reward in bitcoin mining is introduced in Reference 63 for encouraging the honest participation among blockchain nodes.

2.6 | Novel contribution to literature

Many research works that have been surveys the existing consensus mechanisms and some researchers have been keen to channelize the blockchain based solutions in specific applications. Although the credibility of the blockchain can be

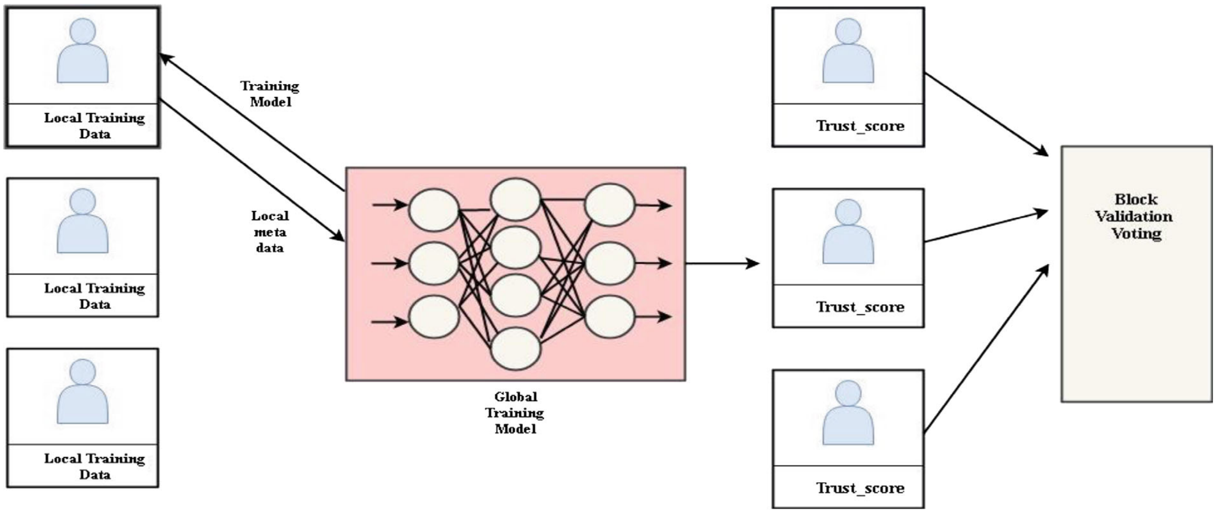


FIGURE 3 Architecture for trust_score calculation

assured with the numerous variants of the blockchain but to a certain extent the security factor in anonymous blockchain environment cannot be resolved well. In these solutions, the security of the system depends on the assumption of majority participation of honest nodes. Thus, the proposed research work presents a novel game theory based reliable PoS consensus mechanism. It aids to add more security automatically to existing PoS consensus with the help of federated learning by considering the behavior of the nodes. Along with adding more security to system, the proposed system also ensures the constant expected good behavior of the system through game theory without the intervenes of any third party. The proposed consensus based blockchain is used for crop insurance application for imparting the much-needed superfluous security to the system.

3 | PROPOSED RELIABLE POS CONSENSUS MECHANISM

In the light of issues discussed with PoS consensus algorithm, the proposed research work suggests to extend the PoS consensus algorithm with trust maintenance of validator nodes. Customarily, the trust maintenance mechanism can salvage the services of a third-party managing database services but it could lead to breach of security over the anonymity of nodes. Thus, before adding the new validator nodes, it has to undergo the trust_score calculation procedure using federated learning while preserving anonymity of nodes.

3.1 | Trust score computation

The conventional PoS consensus process is revised to integrate trust_score for each node along with net stake worth in decision making while voting procedure. The Figure 3 shows the architecture for trust_score calculation. Node n_i which wants the access to the network as validator node will proceed with Algorithm 1 for trust score calculation.

Algorithm 1. Calc_trust_score

```
Input: $T, \delta, \sigma_1$
Output: $TS_i$

for each node $n_i \in N$
invest stake $\delta$
register at cloud server
download the global model $\omega_0$
```

```
for each node $n_i \in N$
note the values of $T, \delta, \sigma_1$ for dataset
calculate NBA (next block approval) probability denoted by $\sigma_2$
    $\sigma_2 = T.\delta^2 + (\sigma_1/2)\,. \quad (1)$
at each node $n_i$
perform the local model training using the equation
    $\omega_{t+1}^{n_i} \leftarrow f\left(\omega_t^{n_i}\right). \quad (2)$
update the global model by aggregation at server.
    $\omega_{t+1} = \omega_t * \sum_{i=1}^{n} f\left(\omega_t^{n_i}\right). \quad (3)$
calculate the trust_score for each node using
    $TS_i = \sum_{i=1}^{t} \sigma 2_i + \gamma^t. \quad (4)$
for each node $n_i \in N$ :
if ( $TS_i > t1 ςς TS_i < t2$ )
$n_i$ = validator node
if ( $TS_i > t2$ )
$n$ $_{i=}$ validation leader node.
```

The aspiring validator node has to submit the validator fee. They are required to submit certain number of coins as their stake in the network. The magnitude of stake will decide their chances to be selected as the next block forging node.

The participant has to simultaneously register at the cloud server which will help in updating the global model variables. It stands clear that every node accesses cloud for model downloading where global model will be updated and sent back to the nodes. The neural network is used to predict the values of output variable. The central server is programmed to select the subset of participants as they have to perform local model training tasks. It initiates a neural network based global model ω_0 to each participant. Every node, n_i which registers at server, is required to maintain a dataset. For initial period of 10 days, data about node is collected by the interface. During this time period, the node n_i can only approve or disapprove the block initiated by some other leader node. The dataset collected contains T, δ, σ_1.

The data is collected in time series format. The parameters $X = [T, \delta, \sigma_1]$ will serve as the input parameters and the σ_2 is the parameter to be predicted for node n_i using the neural network-based training model. The $Y = \sigma_2$ will serve as the next block approval (NBA) probability for node n_i as depicted in Equation 1. These variables are collected and maintained locally in specific node with the help of local records.

$$Y \leftarrow f(X)$$

After the dataset collection phase is over, the training nodes selected will perform data analysis and then it gets added to the dataset values. To obtain an accurate next block approval probability, the local nodes will train the global model by using its own dataset which is being updated after every 10 days. The nodes work collaboratively to train the initialized global model which gets updated iteratively every fixed time period using Equation (2). The node $n_i \epsilon N$ where $N = \{n_1, n_2, \ldots, n_n\}$ with n number of participants in the network. The global model is updated iteratively by each single node. Every participating node uploads the local model over the centralized server which is averaged into a global updated model using federated averaging algorithm. The server uses the trained weights of generic neural network model to calculate the average of all these values and finally present the network with global neural network model.

Using the updated global model computed with the use of Equation (3), value of NBA will be calculated for each node and sent to the blockchain. For every node n_i, server will use the associated NBA value to find out the trust_score for node n_i using the Equation (4). Where TS is the trust_score, γ is aging parameter. We try to link more weight to older nodes. If $TS > t1$ then node n_i gets access to the network as validator node. The system will verify if $TS > t2$ only then in future the particular node n_i will be eligible to be selected as the leader node. The values of $t1$ and $t2$ depend on the system.

Meanwhile, every node in network broadcast the received transactions in the network. When ample number of transactions are collected, the nodes select the leader node based on the trust_score, which initiates the block creation. Every other node in network validates the block after authenticating the block. Every transaction in the block is executed and it is added to the blockchain. The leader node is rewarded for adding this block to blockchain.

3.2 | Integrating game theory in proposed PoS

A Game theoretic model is used to include self-sufficiency in the system to maintain a level of threshold trust score value for each participating node. The responsibility of maintaining the threshold value of trust score remains with the validation leader node selected in previous step. The different roles in proposed game theory model are:

a Validation leader: It creates, proposes and broadcasts to the network. It will be responsible to adjust the calculation metrics of trust score in certain cases where it seems right otherwise use the value calculated of trust score in previous step.

b Validators: It is responsible for validating the newly proposed block.

The validator node might attain a level of threshold just to enter the network with the objective of performing malicious activities and not maintain the required level of performance. It might lower the value of trust score after entering the network. Thus, it becomes the responsibility of the validation leader to maintain the optimum performance of the system. The validation leader will be rewarded for performing such task with efficiency. But it might also be punished for doing its duty.

Following are the players in the game:

Player 1 (P[x]): All validator nodes.

Player 2 (P[y]): Validation leader node.

Playing strategies:

It includes the set of actions defined for each specific category of players in the game theory. All the notations required for game theory model are mentioned in Table 3.

P(x): 1. It will try to maintain the specified threshold level of trust score This move is denoted by C.

2. It will not maintain the specified threshold level of trust score. This move is denoted by D.

TABLE 3 Notations used in algorithm

Notation used	Significance
δ	The net stake invested by node
T	The total time for which the node n_i is online
σ_1	The number of blocks approved by node n_i which were eventually added to the blockchain
σ_2	The number of blocks initiated by node n_i and eventually gets added to the blockchain
$t1$	Threshold value for node to be validator
$t2$	Threshold value for node to be validator leader

P(y): 1. It will use default trust score calculated. This move is denoted by M.

Y It will make the rules to calculate the trust score stricter (in order to make process more difficult). It will increase the threshold *t*2. It is denoted by N.

The expected payoff for player(y) for playing N is:

$$Exp(N) = \left[p.\left\{\left(P_y - m\right) - E_y\right\} + (1-p)\left(-E_y - m\right)\right]. \tag{5}$$

The expected payoff for player(y) for playing M is:

$$Exp(M) = \left\{p.R_y + (1-p).m\right\}. \tag{6}$$

So, player P(y) plays *N* (use strict rules) if

$$Exp(N) > Exp(M)$$

or

$$p > \frac{E_y}{P_y - R_y - m}. \tag{7}$$

Likewise, the expected payoffs for player P(x) are calculated.

$$Exp(D) = \left[(q.R_x - E_x) + \{(1-q).P_x - E_x\}\right] \tag{8}$$

and

$$Exp(C) = 0. \tag{9}$$

So, player P(x) plays “D” if

$$E_x(D) > E_x(C)$$

or

$$q > \frac{2.E_x - P_x}{R_x - P_x}. \tag{10}$$

Table 4 shows the strategic form of the given game theory model. Equilibrium can be achieved with Equation (7). The game matrix for different possible situations is represented in Table 5. If the player P(y) maintains a probability of playing “N” at the specified level indicated in Equation (7), then the other player P(x) has no incentive to deviate from its strategy. Similarly, if the player P(x) maintains the probability of playing “D” then other player P(y) has no incentive of deviating from its current strategy. Thus, P(y) will be punished in case the player P(x) is successful in making move “D” without being encountered.

4 | USE CASE: CROP INSURANCE

The main objective of current research work to deploy the above-mentioned consensus mechanism to reduce the current flaws of the financial systems like crop insurance for the social security of the farmers. The process of crop insurance can be made more automated, transparent and secure by channelizing federated learning based- blockchain in the crop insurance system. We propose a smart contract approach for registration of farmers, crop insurance and smart contract-based

TABLE 4 Game notations

m	A reward for player (y) reward “m”: If P(y) plays M and P(x) plays C If P(y) plays N and P(x) plays D punishment “m”: If P(y) plays M and P(x) plays D If P(y) plays N and P(x) plays C
E_x	Effort spent by P(x) to play D
P_x	The profit for P(x) for successfully playing D
R_x	The risk for P(x) if deterred by P(y)
E_y	Effort spent by P(y) to play N
P_y	The profit for P(y) for deterring a P(x)
R_y	The risk for P(y) if P(x) plays D and it plays N
p	probability for P(x) for playing D
q	probability for P(y) for playing M

TABLE 5 Game matrix

		Player, P(y)	
		M	N
Player, P(x)	C	$(0, m)$	$(0, -W_y -m)$
	D	$([P_x - E_x], R_y)$	$((R_x-E_x), (P_y -m)- E_y)$

authentication of insurance claims which leads to automatic claim redemption. The process of crop insurance is discussed in reference to following parameters:

4.1 | Stakeholders

A. Federal government: The role of government is crucial in paying a major portion of the premium for crop insurance according to the standard criteria set under insurance scheme. The government authorities initiate and deploy the smart contract for insurance of crops which save the assorted variables linked with insurance like the premium balance, claim history and so forth for particular farmers.

B. Empanelled insurance companies: These are the insurance companies and other financial institutes like commercial banks, co-operative banks along with their regulatory bodies which have been registered onto the government records. These entities have the means for processing the requests for insurance premium processing, claim processing and other detailed problem handling by the farmers registered onto the government records using the smart contracts.

C. Beneficiaries: The farmers satisfying the minimum eligibility criteria for availing the benefits of insurance scheme can register with the government through smart contract. This smart contract saves their details such as name, email and secret passphrase.

4.2 | Registration

The farmers send the request to register through the front end dapp which makes a contact with REG smart contract. It allows the farmer to provide his personal details like nation’s identity number and asks for a secret passphrase. The farmers are required to provide their preferences for crops, their locality. These details will be saved in offline database on cloud but the hash of the data will be saved on blockchain connected to overlay network. The personal data of farmers is

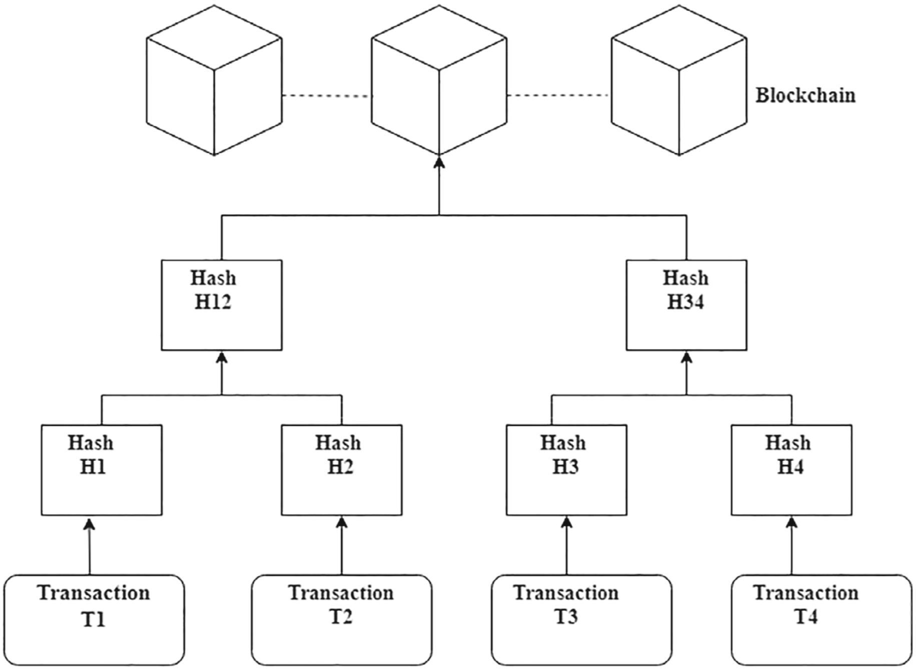


FIGURE 4 Merkle tree

accompanied with the digital signatures which are linked with the secret passphrase chosen by the farmers and a nation's identity number. While saving on the cloud, if the digital signatures are missing, the cloud server will discard the data. Cloud server will save the data in the form of merkle tree of identical size.[64] The data is grouped into identical block size which is converted to merkle tree. Figure 4 shows the Merkle tree architecture. The format of merkle tree provides the ease of generating a hash of the data using a function f. The hash function will take an input string of variable length but will generate an output string of identical length. This hash will be saved on the blockchain network.

4.3 | Insurance data sharing and claim payment

Once the farmers have registered successfully. They can pay the required amount of premium.

i. The farmer will visit one of the empanelled companies for crop insurance under the scheme.
ii. The insurance company will try to generate the hash using the same hash function by using the nation's identity number and the secret passphrase decided by farmer during registration.
iii. If the hash matches, the INS contract will change the status value to “accept” and it will trigger an event to government to make a contact with the third-party database for weather data fetching in real time using OAAS (Oracle as a service) since the smart contract cannot access the data from third party.
iv. After verifying data from both sides, the claim payment starts automatically. Figure 5 shows the flow of crop insurance system.

5 | INSCROPS: BLOCKCHAIN BASED CROP INSURANCE MOBILE INTERFACE

The abstract architecture described in Sections 3 and 4 are developed using a mobile application InsCrops which is provided to end users in proof-of-concepts based implementation. In this section, a mobile application for the aid of all stakeholders of the proposed system is discussed.

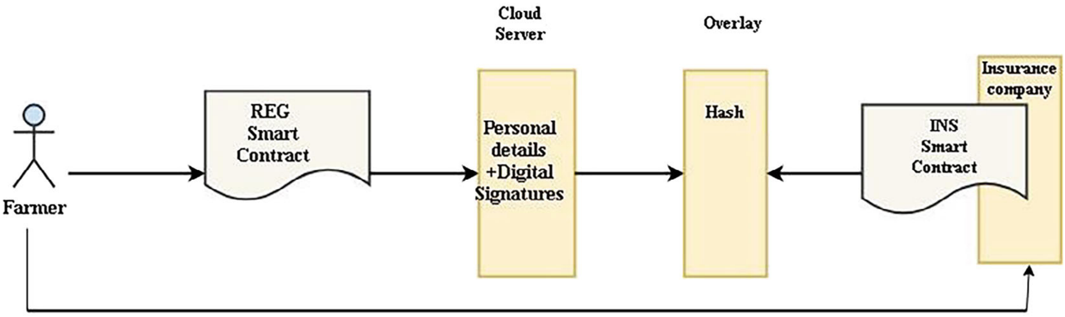
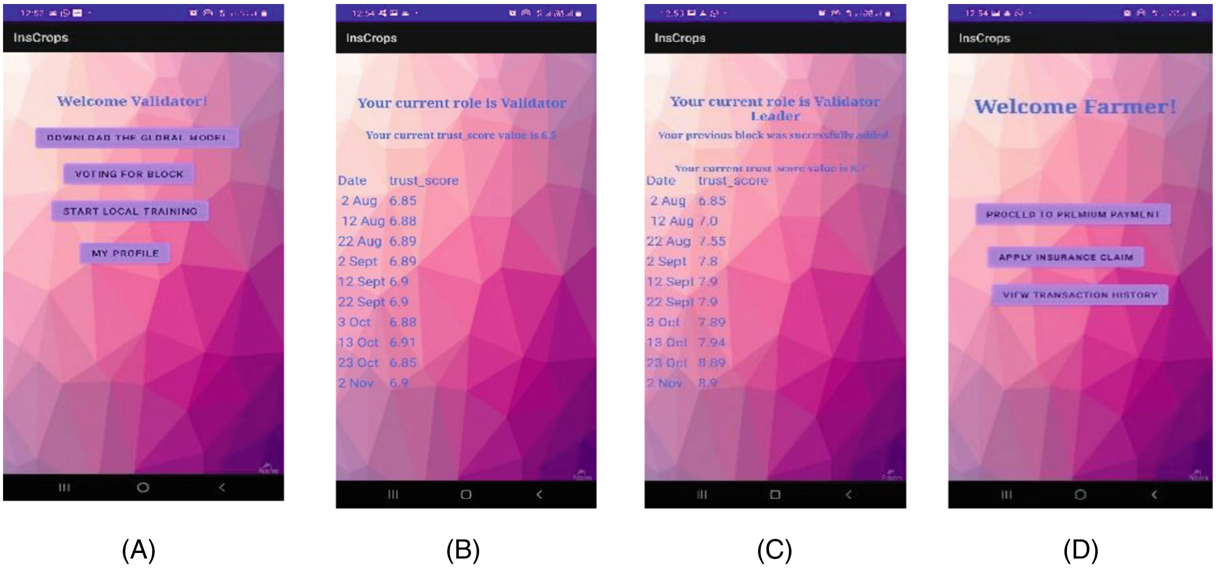


FIGURE 5 Flow of crop insurance system



Your current role is Validator

Your current trust_score value is 6.5

Date	trust_score
2 Aug	6.85
12 Aug	6.88
22 Aug	6.89
2 Sept	6.89
12 Sept	6.9
22 Sept	6.9
3 Oct	6.88
13 Oct	6.91
23 Oct	6.85
2 Nov	6.9

Your current role is Validator Leader

Your previous block was successfully added

Your current trust_score value is [illegible]

Date	trust_score
2 Aug	6.85
12 Aug	7.0
22 Aug	7.55
2 Sept	7.8
12 Sept	7.9
22 Sept	7.9
3 Oct	7.89
13 Oct	7.94
23 Oct	8.89
2 Nov	8.9

FIGURE 6 (A) Welcome page of validator node, (B) my profile for a validator node, (C) my profile for a validator leader node, (D) landing page for farmer node

The first step in the application is to choose among the category of participant among the various categories that is, validator, farmer and insurance company After selecting the role, the user lands up on specific page where he can proceed with the required actions as discussed in previous sections. The validator node [see Figure 6A] participates in federated learning procedure and thus has to download the global training model. Finally, the validator node participates in the voting procedure through the provided interface. The participating node is assigned a role according to its trust_score either as a validator node or as a validator leader node. Figures 6B,C show the further processing in both type of roles. The basic functionalities of insurance system are provided to the farmers such as premium payment, applying the insurance claim and checking his last transaction history [see Figure 6D]. Note that the premium payment module currently does not use blockchain but uses a third-party payment gateway. Once the farmer applies for insurance claim from the interface, he needs to visit the nearest empanelled insurance company. Whenever the insurance company tries to perform the specified operations, it will undergo the blockchain exclusive operations as discussed in Section 4.3 thus, leading to a secure pathway for crop insurance claim settlement.

6 | EXPERIMENTAL SET-UP

We implement the proof-of-concept based proposed system purely on a local cluster using solidity smart contracts and consortium blockchain system coded in python language. The python code aids in saving the transactions in batches with blocks, adding tamper-resistant digital fingerprints to blocks and finally to link blocks one by one. The consensus mechanism is modified using python programming language with federated learning framework designed on PySyft.[65]

Under Consortium blockchain, a selected group of users are granted the permission to participate in decentralized consensus procedure. It is generally used by some specific industrial groups such as financial sector.[66] There are two smart contracts, REG for registration of farmers and INS for insurance related functions. The local cluster implementation is performed in combination with the insurance application set-up scenario by using Chaquopy[67] (https://github.com/chaquo/chaquopy) plugin in android studio. The network size of 16 nodes for farmers, 2 nodes for insurance companies along with 50 validator nodes is set up. The genesis block extensively adds the stakeholder nodes in network. The blockchain nodes are setup in two labs. Lab1 consists of 35 validator nodes, 9 farmer nodes and 2 insurance companies. Lab2 contains the remaining nodes for the implementation.

The experiment is conducted on LAN deployment within the two labs. The AWS EC2 cloud services are used. The central server was implemented on a 1.6 Ghz i5 computing system with 8GB of RAM. The various PoS based protocols mentioned in section are also implemented for analysis of the proposed system in reference to the existing approaches. In Tendermint, the wait time is set to be 2 ms. In ouroboros and algorand, the epoch time is set to be 3 ms. The hyperparameters for federated learning are initialized as follows: the learning rate $\alpha = 0.01$, the total batches = 8 and local training epoch $\beta = 60$. The learning rate and the training loss for each batch is recorded and then the loss is plotted against learning rate as shown in Figure 7 which reveal that loss is minimum for learning rate $\alpha = 0.01$. Equivalently, the loss is minimum and accuracy is maximum for epoch $\beta = 60$ as demonstrated by Figure 8 and Figure 9, respectively.

The validator nodes dynamically collect data and perform the training simultaneously. The python code is extended to include the mathematically oriented game theory approach. The network has been simulated with assortment of both category of users performing their part in the game theoretic model. For the initializing the system processing, 2% nodes of system are already considered to be part of the approved validator nodes. The system is run through total 10 iterations which might acquire different validation leader in each iteration.

6.1 | Performance validation

In this section, we try to study and analyze the attack resistance capabilities of the proposed PoS consensus mechanism. For the purpose of evaluation, we estimate the intrusion accomplishment rate (IAR) which is defined as follows: the success rate of a malicious validator attacker trying to annihilate the performance of underlying system. It is assumed that the out of the total number of validator nodes, the proportion of attackers range from 10% to 30%. As depicted in Figure 10, the proposed consensus mechanism is less prone to the external data attacks. The proposed PoS mechanism is compared with standard PoS mechanism as well as the algorand, ouroboros, and tendermint implementation.

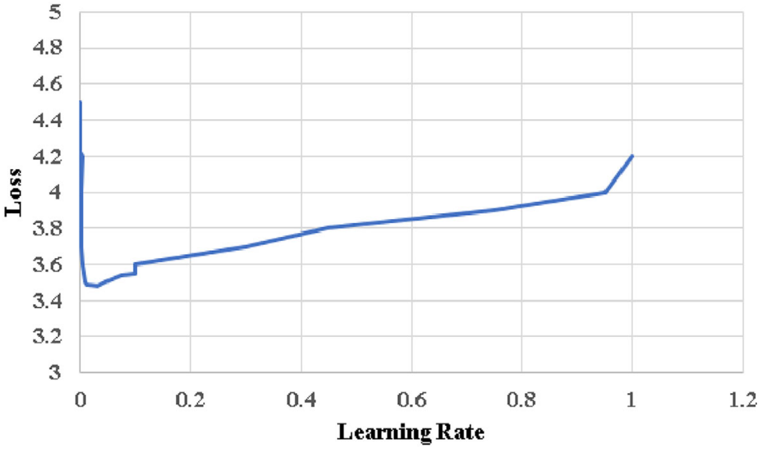


FIGURE 7 Loss vs learning rate

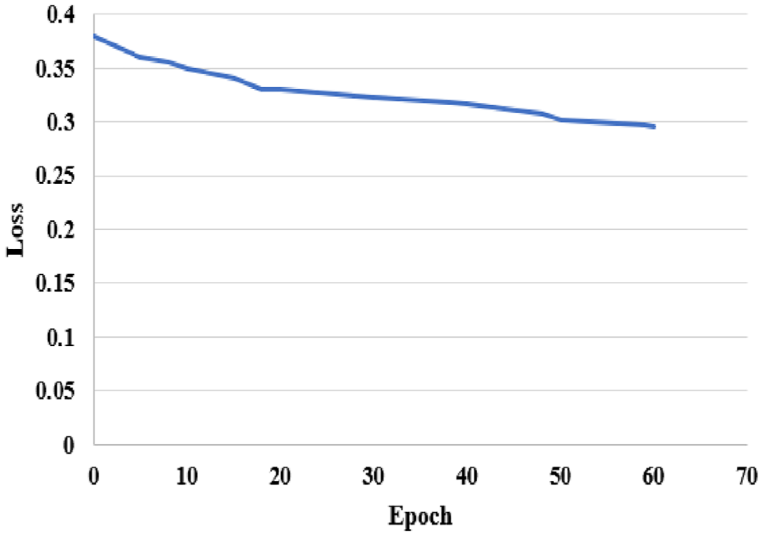


FIGURE 8 Loss vs epoch

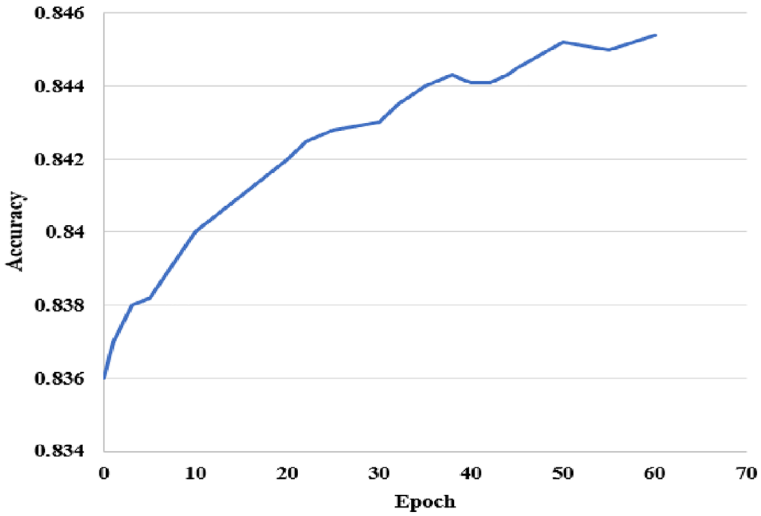


FIGURE 9 Accuracy vs epoch

The ouroboros algorithm relies only on the net stake owned by a node which increases the risk of malicious nodes in the network. The algorand algorithm works with slight variation in ouroboros algorithm. It does not reveal the final leader node without submitting the proof. But the randomness used in the input string selection process can be biased by some rival node. The tendermint consists of two step voting process. But it relies on majority participation of honest nodes.

Evidently, the proposed frameworks perform better due the incorporation of federated learning which does not require to move the data from users to central servers for data analysis whereas in PoS mechanism, the only criteria used is stake owned by the users and thus can be at times misleading.

Also, we compute the value of MAE (mean absolute error) using the Equation 11:

$$MAE = \frac{1}{n}\sum_{i=1}^{n} \mid x_i - x_p \mid, \tag{11}$$

where x_i is the observed σ_2 value and x_p is the predicted σ_2 value.

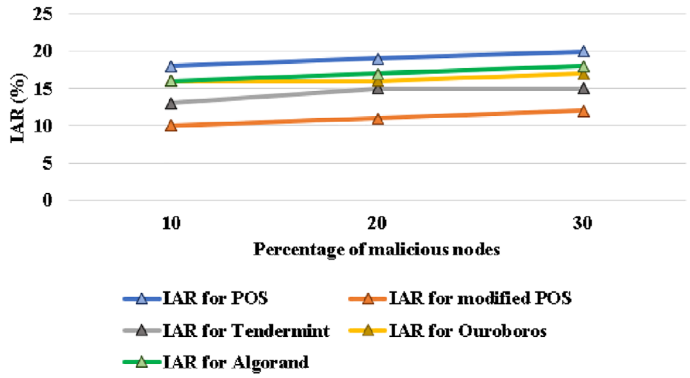


FIGURE 10 IAR analysis for proposed system

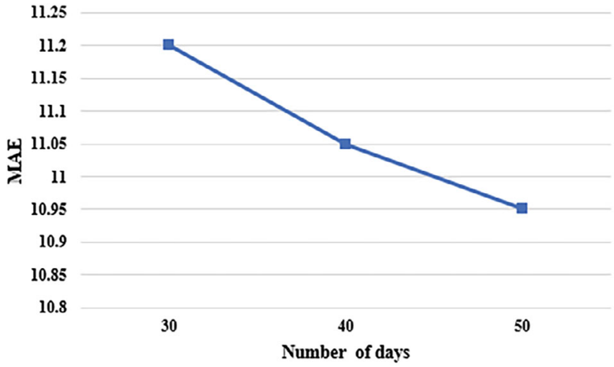


FIGURE 11 MAE analysis for proposed system

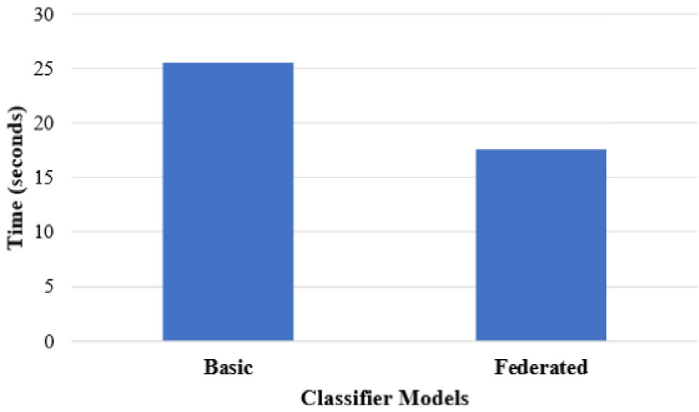


FIGURE 12 Time comparison for different classifier models

The MAE for given federated learning model is shown in Figure 11. The MAE value for proposed system decreases over time and shows constant value after some specific time. We compare the proposed system with basic neural network-based machine learning classifier. The essence of the model uses neural network for prediction of values.

The basic learning model is trained and assessed on whole dataset collected from all individual nodes. The dataset is transferred over the network to single local node for evaluation. Evidently the single node consumes more time for training over the model because of the limited computing capabilities of single node. Moreover, the dataset transfer over the network expends more time as well as bandwidth. It took 25.6 seconds to train the model and led to accuracy score of 86%. Figure 12 shows the training time taken by each node.

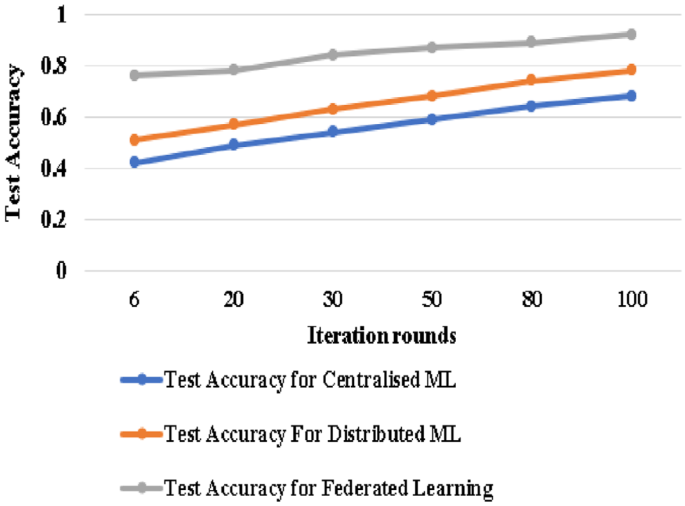


FIGURE 13 Analysis of learning mechanisms

In federated learning classifier, the nodes are trained locally isolated from the network on their own generated dataset. After fixed iterations, the weights are transferred to the server for accretion. As depicted by the features of federated learning models, the communication overhead due to data transfer is abridged. The average time taken by nodes for training on local node is 17.65 seconds with an aggregated accuracy of 84.5%. The system is compared with standard centralized learning procedures as well as distributed machine learning.

Figure 13 depicts the comparison between the 3 learning criteria. Federated learning outperforms the centralized learning as well as distributed learning.

For the purpose of evaluating the system, varying number of validator nodes are deliberately proposed to be the nodes which have an intention of performing malicious activity and will try to not maintain the threshold level of trust score after entering the network. Thus, these nodes will prefer to play the move “D” in game theoretic model.

6.2 | Modeled moves

This system is tested under varying combination of moves chosen by players of both categories. The moves of players are simulated and the performance of the system is evaluated under two major set of instances. The moves chosen by player P(y) play a significant role in deciding the overall performance of the system. The performance of the system will be superior when majority of the average trust score of the nodes in the system is above the threshold decided while setup of the system. The nodes which maintain their trust score value above the decide threshold value are considered to be the loyal nodes which will actually strive for the better performance of the system rather being involved in certain malicious activities.

Case 1. when player, P(y) makes move N.

The player P(y) is made to choose move N. The majority of the nodes maintain their average trust score value above threshold value if the probability, p of making move N is above the specified calculated value in Equation (7). Whereas the nodes maintaining their average trust score above threshold value become comparatively low in number when probability to make move N is less than the specified calculated value.

Thus, if the player P(y) actually makes move N when probability is above the calculated value, the performance of the system is superior and low otherwise. It is to be noted although the performance of the system will not be affected too much, but the player P(y) gets more punishment that being rewarded. This is illustrated in Figure 14A.

Case 2. When player, P(y) makes move M.

The player P(y) is made to choose move M. The majority of the nodes maintain their average trust score value below threshold value if the probability, p of making move N is above the specified calculate value. Whereas the nodes

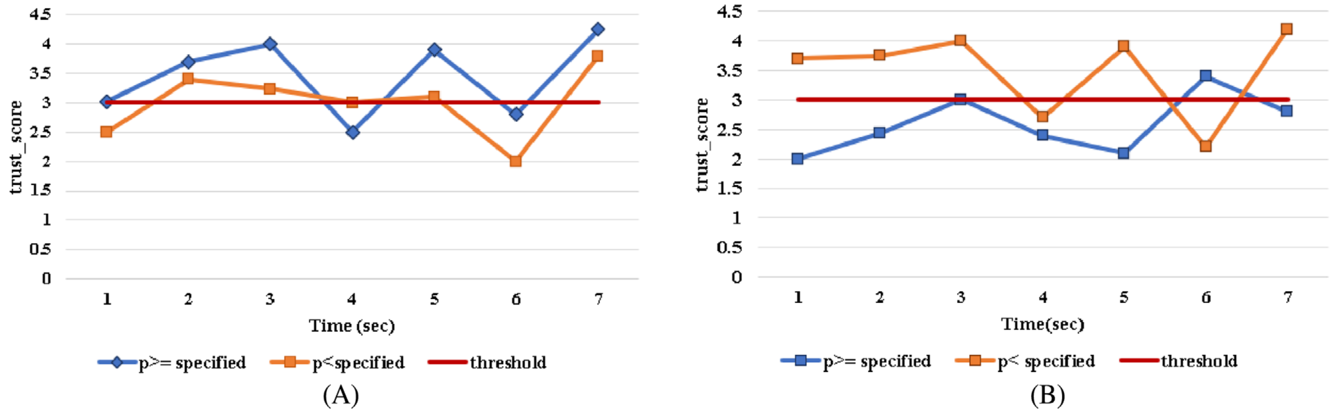


FIGURE 14 (A) Case 1 and (B) Case 2

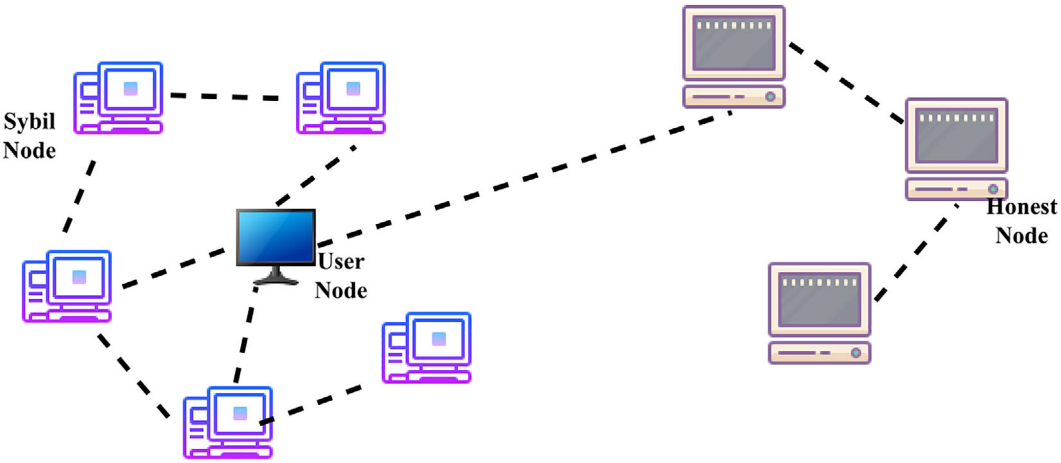


FIGURE 15 Sybil attack

maintaining their average trust score above threshold value become high in number when the probability to make move N is less than the specified calculated value.

Thus, if the player P(y) actually makes move M when probability of making move N is above the calculated value, the performance of the system is low and high otherwise. This is illustrated in Figure 14B.

Overall, it can be concluded that performance of the system is worst in case when the concept of game theory requires to make move N but the player P(y) chooses to make move M.

The significance of choosing to evaluate the system under varying modeled moves is to ensure the satisfactory level of performance of the system under almost all scenario since ultimately the system will be manged by anonymous users.

6.3 | Attacks prevention

In this section, we analyze the effectiveness of proposed PoS algorithm for resisting against various security attacks. The evaluation exhibits the efficacy of proposed PoS mechanism in combating the various security attacks which is the prime requirement in any application pertaining to finances, banking, and insurance.

6.3.1 | 51% Attack

There might be some scenario where the attacking nodes have acquired enough hashing power and stake to accomplish the 51% attack to put down the network. But the proposed PoS mechanism employs continuous monitoring through

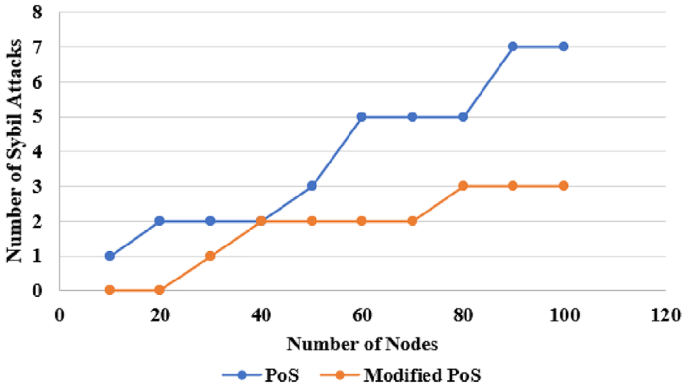


FIGURE 16 Sybil attacks comparison

federated learning which will be able to immediately detect any fault or slip in system. The federated learning allows to learn and grow simultaneously to avoid the 51% attack by associating a trust_score with every node which updated after specified time period.

6.3.2 | Sybil attack

In a blockchain network, an arbitrary challenger node can produce multiple simulated identities to take conquer the network. Such adversary nodes are called sybil nodes. Such attacker nodes can create an illusion of being the fully authorized node as shown in Figure 15. They can disconnect the genuine nodes from the network. In a blockchain network, the virtual sybil nodes will forward the block of only the malicious nodes in order to take charge of the network.[68] The proposed PoS consensus mechanism certainly aids to resist the sybil attack because before adding the new block by any random node requires its trust_score to be above a threshold value. Moreover, it is quite apparent to maintain a genuine trust_score.

In order to evaluate the performance of the system, few nodes in the system are deliberately coded as sybil nodes. The system with proposed PoS is able to counter more sybil attacks as compared to the system with conventional PoS consensus mechanism as depicted in Figure 16.

7 | CONCLUSION

The presented research work proposes a novel consensus mechanism that integrates federated learning and game theory with standard PoS mechanism. In an anonymous environment of blockchain, the proposed research work associates a trust_score with each validator node to enable the participants of network select the trust-worthy nodes. The trust_score is calculated using federated learning and maintained using game theory. The proposed mechanism uses game theory-based reward and punishment model to ensure only the trust worthy nodes survive in the system. The system has been analyzed under various experimental conditions. The proposed system is presented as an application for crop insurance involving farmers and the empanelled insurance companies. The choice of insurance sector for implementation is motivated out of needs of crop insurance sector is governed by high security requirements, timely transaction completion for farmers, tracking and traceability. The proposed system shows nearly consistent intrusion accomplishment rate under varying proportion of malicious nodes with an improvement of nearly 40% with respect to standard PoS consensus mechanism. Moreover, the mean absolute error of the learning model is reduced by nearly 30% over time. The proposes system also shows superior performance in terms of accuracy and training time incurred as compared to the basic machine learning classifier.

8 | FUTURE WORK

There are many mainstream consensus mechanisms for blockchain but they differ in terms of resource efficiency, scalability, computational complexity, security resilience. There is a constant requirement of improving the efficiency and performance of blockchain consensus mechanisms. In the same direction, the proposed research work presents a novel consensus mechanism for improving the consensus mechanism for improving the performance of existing consensus mechanism, that is, PoS.

However, there are few open areas in proposed research work. This proposed research work can be extended to enhance the scalability of the overall system. Since federated learning is involved, thus it becomes imperative to work toward the throughput performance of the system. Certain research efforts for improving the block generation time can further improve the applicability of the system. Detailed literature survey reveals that more research efforts are required for the efficient channelization of extreme potential of artificial intelligence models to do away the difficulties faced in blockchain. Future research goals should be focussed to address the technical aspects of the blockchain technology in combination with the specific social context of the insurance applications in general and financial applications in general. Also, the proposed research work makes the room for novel ideas in enhancing the fault tolerance of the insurance system by adjusting the learning parameters of the learning model.

CONFLICT OF INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

DATA AVAILABILITY STATEMENT

Research data are not shared.

REFERENCES

1. Wang B, Li Z, Li H. Hybrid consensus algorithm based on modified proof-of-probability and DpoS. *Future Internet*. 2020;12:122. doi:10.3390/fi12080122
2. Wang Y, Cai S, Lin C, et al. Study of blockchains's consensus mechanism based on credit. *IEEE Access*. 2019;1. doi:10.1109/ACCESS.2019.2891065
3. Chaudhry N, Yousaf M. Consensus algorithms in blockchain: comparative analysis, challenges and opportunities. Paper presented at: Proceedings of the 2018 12th International Conference on Open Source Systems and Technologies; 2018:54-63; Lahore, Pakistan: 10.1109/ICOSST.2018.8632190
4. Fekih R, Lahami M. Application of blockchain technology in healthcare: a comprehensive study; 2020. 10.1007/978-3-030-51517-1_23
5. Gatteschi V, Lamberti F, Demartini C, Pranteda C, Santamaría V. Blockchain and smart contracts for insurance: is the technology mature enough? *Future Internet*. 2018;10:20. doi:10.3390/fi10020020
6. Qi H, Wan Z, Guan Z, Cheng X. Scalable decentralized privacy-preserving usage-based insurance for vehicles. *IEEE Internet Things J*. 2021;8(6):4472-4484. doi:10.1109/JIOT.2020.3028014
7. Kamilaris A, Fonts A, Prenafeta-Boldú F.X.. The rise of blockchain technology in agriculture and food supply chains. *Trends Food Sci Technol*. 2019;91:640-652. doi:10.1016/j.tifs.2019.07.034
8. Bermeo-Almeida O, Cardenas-Rodriguez M, Samaniego-Cobo T, Ferruzola-Gómez E, Cabezas-Cabezas R, Bazán-Vera W. Blockchain in agriculture: a systematic literature review. Paper presented at: Proceedings of the International Conference on Technologies and Innovation; November 6, 2018:44-56; Springer, Cham. 10.1007/978-3-030-00940-3_4
9. Ayaz, Muhammad & Uddin, Ammad & Sharif, Zubair & Mansour, Ali & Aggoune, el-Hadi. (2019). Internet-of-things (IoT)-based smart agriculture: toward making the fields talk. *IEEE Access*. 7: PP. 1–10.1109/ACCESS.2019.2932609
10. Alam ASAF, Begum H, Masud M, Al-Amin A, Filho W. Agriculture insurance for disaster risk reduction: a case study of Malaysia. *Int J Disaster Risk Reduct*. 2020;47:101626. doi:10.1016/j.ijdrr.2020.101626
11. Kumar A, Sharma A. Socio-Sentic framework for sustainable agricultural governance. *Sustain Comput Inform Syst*. 2018;28:100274. doi:10.1016/j.suscom.2018.08.006
12. Kar A, Navin L. Diffusion of blockchain in insurance industry: an analysis through the review of academic and trade literature. *Telemat Inform*. 2021;58:101532. doi:10.1016/j.tele.2020.101532
13. Alghazo J, Kazimi Z, Latif, G. Cyber security analysis of internet banking in emerging countries: user and bank perspectives; 2017:1-6. 10.1109/ICETAS.2017.8277910
14. Ferdous MS, Chowdhury MJM, Hoque MA. A survey of consensus algorithms in public blockchain systems for crypto-currencies. *J Netw Comput Appl*. 2021;182:103035.
15. Wang W, Hoang DT, Hu P, et al. A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access*. 2019;7:22328-22370. doi:10.1109/ACCESS.2019.2896108
16. Fu X, Wang H, Shi P. A survey of Blockchain consensus algorithms: mechanism, design and applications. *Sci China Inf Sci*. 2021;64:121101. doi:10.1007/s11432-019-2790-1
17. Porat A, Pratap A, Shah P, Adkar V. Blockchain consensus: an analysis of proof-of-work and its applications; 2017.
18. Tosh D, Shetty S, Liang X, Kamhoua C, Njilla L. Consensus protocols for blockchain-based data provenance: challenges and opportunities; 2017:469-474. 10.1109/UEMCON.2017.8249088
19. Sun Y, Yan B, Yao Y, Yu J. DT-DPoS: a delegated proof of stake consensus algorithm with dynamic trust. *Proc Comput Sci*. 2021;187:371-376.

20. Hu Q, Yan B, Han Y, Yu J. An improved delegated proof of stake consensus algorithm. *Proc Comput Sci*. 2021;187(341–346):6-346.
21. Majumdar MA, Monim M, Shahriyer MM. Blockchain based land registry with delegated proof of stake (DPoS) consensus in Bangladesh. Paper presented at: Proceedings of the 2020 IEEE Region 10 Symposium (TENSYMP); June 2020:1756-1759; IEEE; Dhaka, Bangladesh.
22. https://news.bitcoin.com/study-finds-certain-proof-of-stake-networks-vulnerable-to-low-cost-attacks/.
23. Karaarslan E, Konacakli E. Data storage in the decentralized world: blockchain and derivatives; 2020. 10.26650/B/ET06.2020.011.03.
24. Becker M, Bodó B. Trust in blockchain-based systems. *Internet Policy Rev*. 2021;10(2). doi:10.14763/2021.2.1555
25. Zheng Z, Xie S, Dai HN, Chen X, Wang H. Blockchain challenges and opportunities: a survey. *Int J Web Grid Serv*. 2018;14(4):352-375.
26. Yang S, Chen Z, Cui L, Xu M, Ming Z, Xu K. CoDAG: an efficient and compacted DAG-based blockchain protocol; 2019:314-318. 10.1109/Blockchain.2019.00049
27. Salman T, Jain R, Gupta L. Probabilistic blockchains: a blockchain paradigm for collaborative decision-making; 2018. 10.1109/UEMCON.2018.8796512
28. Pilkington M. Blockchain technology: principles and applications; 2016.
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;7:118541-118555. doi:10.1109/ACCESS.2019.2935149
30. Lashkari B, Musilek P. A comprehensive review of blockchain consensus mechanisms. *IEEE Access*. 2021;9:43620-43652.
31. Bouraga S. A taxonomy of blockchain consensus protocols: a survey and classification framework. *Expert Syst Appl*. 2020;168:114384. doi:10.1016/j.eswa.2020.114384
32. Bou Abdo J, El Sibai R, Demerjian J. Permissionless proof-of-reputation-X: a hybrid reputation-based consensus algorithm for permissionless blockchains. *Trans Emerg Telecommun Technol*. 2021;32(1):e4148.
33. Bentov I, Lee C, Mizrahi A, Rosenfeld M. Proof of activity: extending bitcoin's proof of work via proof of stake [extended abstract] y. *ACM SIGMETRICS Perform Eval Rev*. 2014;42(3):34-37.
34. Yang J, Paudel A, Gooi HB, Nguyen HD. A proof-of-stake public blockchain based pricing scheme for peer-to-peer energy trading. *Appl Energy*. 2021;298:117154.
35. Niya SR, Schiller E, Cepilov I, et al. Adaptation of proof-of-stake-based blockchains for IoT data streams. Paper presented at: Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC); 2019:15-16; IEEE; Seoul, Korea (South).
36. Cheng Y, Hu X, Zhang J. An improved scheme of proof-of-stake consensus mechanism. Paper presented at: Proceedings of the 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE); 2019:826-8263; IEEE; Hohhot, China.
37. Platt M, McBurney P. Sybil attacks on identity-augmented proof-of-stake. *Comput Netw*. 2021;199:108424.
38. Ko S, Fan X, Zhong Z, Chai, Q. EMS: an extensible and modular staking architecture for proof-of-stake systems. Paper presented at: Proceedings of the 2020 2nd International Conference on Blockchain Computing and Applications (BCCA); November 2020:122-128; IEEE.
39. Kwon J. Endermint: consensus without mining. Draft v. 0.6, fall 1.11; 2014.
40. https://www.bigchaindb.com.
41. https://ethermint.zone.
42. Kiayias A, Russell A, David B, Oliynykov R. Ouroboros: a provably secure proof-of-stake blockchain protocol. *Advances in Cryptology – CRYPTO*. Lecture Notes in Computer Science. International Association for Cryptologic Research 2017; Vol 2017; 2017:357-388.
43. Gilad Y, Hemo R, Micali S, Vlachos G, Zeldovich N. Algorand: scaling Byzantine agreements for cryptocurrencies. Paper presented at: Proceedings of the 26th Symposium on Operating Systems Principles; 2017:51-68; ACM, New York, NY.
44. Abdulrahman S, Tout H, Ould-Slimane H, Mourad A, Talhi C, Guizani M. A survey on federated learning: the journey from centralized to distributed on-site learning and beyond. *IEEE Internet Things J*. 2021;8(7):5476-5497. doi:10.1109/jiot.2020.3030072
45. Asad M, Moustafa A, Ito T. Federated learning versus classical machine learning: a convergence comparison. ArXiv [CsLG]; 2021 10.48550/ARXIV.2107.10976
46. Chen Y, Chuang Y, Wu A. Online extreme learning machine design for the application of federated learning. Paper presented at: Proceedings of the 2020 2nd IEEE International Conference on Artificial Intelligence Circuits and Systems (AICAS); 2020:188-192; Genova, Italy. doi: 10.1109/AICAS48895.2020.9073802
47. Li T, Sahu AK, Talwalkar A, Smith V. Federated learning: challenges, methods, and future directions. *IEEE Signal Process Mag*. 2020;37(3):50-60.
48. Konečný, J., McMahan, H. B., Felix, X. Y., Richtárik, P., Suresh, A. T., & Bacon, D. (2016). *Federated learning: strategies for improving communication efficiency*. 6th International Conference on Learning Representations. ICLR 2018 Conference Track: Vancouver Convention Center, Vancouver, BC, Canada.
49. Dhar Dwivedi A, Singh R, Kaushik K, Rao Mukkamala R, Alnumay WS. Blockchain and artificial intelligence for 5G-enabled Internet of Things: challenges, opportunities, and solutions. *Trans Emerg Telecommun Technol*. 2021;e4329.
50. Hussain AA, Al-Turjman F. Artificial intelligence and blockchain: a review. *Trans Emerg Telecommun Technol*. 2021;32(9):e4268.
51. Bravo-Marquez F, Reeves S, Ugarte M. Proof-of-learning: a blockchain consensus mechanism based on machine learning competitions. Paper presented at: Proceedings of the 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON); 2019:119-124; IEEE; Newark, CA, USA.
52. Nguyen DC, Ding M, Pham QV, et al. Federated learning meets Blockchain in edge computing: opportunities and challenges. *IEEE Internet Things J*. 2021;8:12806-12825. doi:10.1109/JIOT.2021.3072611

53. An, Jian & Yang, He & Gui, Xiaolin & Zhang, Wendong & Gui, Ruowei & Kang, Jingjing. (2019). TCNS: node selection with privacy protection in crowdsensing based on twice consensuses of blockchain. *IEEE Trans Netw Serv Manag*. PP. 1, 10.1109/TNSM.2019.2920001, 16, 1267
54. Kim H, Park J, Bennis M, Kim SL. Blockchained on-device federated learning. *IEEE Commun Lett*. 2019;24(6):1279-1283.
55. Kim S. *Game Theory Applications in Network Design*. Sogang University, South Korea: IGI Global; 2014.
56. Gibbons, R. (1992). *A Primer in Game Theory*. MIT: Pearson.
57. Branzei R, Dimitrov D, Tijs S. *Models in Cooperative Game Theory*. Vol 556. Springer Science & Business Media; 2008.
58. Liu Z, Luong NC, Wang W. A survey on applications of game theory in blockchain. arXiv Preprint arXiv:1902.10865.
59. Bhuiyan BA. An overview of game theory and some applications. *Philos Progress*. 2018;59-60:111-128. doi:10.3329/pp.v59i1-2.36683
60. Brickley J, Smith C, Zimmerman J. An introduction to game theory and business strategy. *J Appl Corp Financ*. 2000;13(2):84-98.
61. Dey S. Securing majority-attack in blockchain using machine learning and algorithmic game theory: a proof of work. *Proceedings of the 2018 10th Computer Science and Electronic Engineering (CEEC)*. Colchester, UK: IEEE; 2018:7-10.
62. Rawat DB, Njilla L, Kwiat K, Kamhoua C. iShare: blockchain-based privacy-aware multi-agent information sharing games for cybersecurity. Paper presented at: Proceedings of the 2018 International Conference on Computing, Networking and Communications (ICNC); 2018:425-431; IEEE; Maui, HI, USA .
63. Schrijvers O, Bonneau J, Boneh D, Roughgarden T. Incentive compatibility of bitcoin mining pool reward functions. Paper presented at: Proceedings of the International Conference on Financial Cryptography and Data Security; 2016:477-498; Springer, Berlin, Heidelberg.
64. Yang X, Liu J, Li X. Research and analysis of blockchain data. *J Phys Conf Ser*. 2019;1237:022084. doi:10.1088/1742-6596/1237/2/022084
65. Ziller A, Trask A, Lopardo A, et al. PySyft: a library for easy federated learning. In: Rehman MH, Gaber MM, eds. *Federated Learning Systems. Studies in Computational Intelligence*. Vol 965. Cham: Springer; 2021. doi:10.1007/978-3-030-70604-3_5
66. Hölbl M, Kompara M, Kamisalic A, Nemec Zlatolas L, A systematic review of the use of blockchain in healthcare. *Symmetry*. 2018;10:470. doi:10.3390/sym10100470
67. https://github.com/chaquo/chaquopy
68. Swathi P, Modi C, Patel D. Preventing sybil attack in blockchain using distributed behavior monitoring of miners. Paper presented at: Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT); 2019; 2019:1-6, Kanpur, India. 10.1109/ICCCNT45670.2019.8944507

How to cite this article: Bala K, Kaur PD. A novel game theory based reliable proof-of-stake consensus mechanism for blockchain. *Trans Emerging Tel Tech*. 2022;33(9):e4525. doi: 10.1002/ett.4525