Journal of Network and Computer Applications 183-184 (2021) 103074

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

A trustworthy and incentivized smart grid energy trading framework using distributed ledger and smart contracts

Ajit Muzumdar *, Chirag Modi, Madhu G.M., C. Vyjayanthi

National Institute of Technology Goa, India

ARTICLE INFO

Keywords:
Smart grid
Energy trading
Distributed ledger technology
Smart contract
Vickrey auction

ABSTRACT

The smart grid integrated with renewable energy sources (RESs) allows to perform peer to peer selling of energy via Local Energy Market (LEM). However, it faces the challenges of lack of transparency and verification of energy distribution, single-point failure in the energy data management, user's privacy, non-incentivized trading and lack of trust on the energy trading. To address these problems, we propose a trustworthy and incentivized framework for smart grid energy trading using distributed ledger technology and smart contracts. We propose different smart contracts *viz*; energy injection into smart grid, energy bidding to submit energy demand, energy trading and energy utilization. These contracts run on an ethereum blockchain platform with proof of stake (PoS) consensus mechanism to record energy trading related data. We have applied an iterative Vickrey–Clarke–Grove (Vickrey auction) method for the incentivized energy trading in context of both prosumers and consumers. The proposed framework offers trustworthy and incentivized trading of energy, participants' privacy, data transparency and no single point failure. The experimental results of the proposed framework are derived in terms of average cost of energy injection and bidding transactions, throughput and the incentivized trading by considering different test scenarios.

1. Introduction

The advancements in technologies like smart metering, communication infrastructure and energy storage allow to utilize Renewable Energy Sources (RESs) in traditional energy system (Joseph, 2015). Such developments have created new opportunities for consumers to generate energy from RESs, and therefore they are called as prosumers. Here, if a prosumer generates energy more than demand, he/she can sell excess energy. Otherwise, he/she can demand the required energy through bidding. The Government of India has taken an initiative to encourage participation of small RES in energy demand supply process. According to the electricity amendment bill, 2014, Ministry of Power, energy distribution license can be issued to one who is capable of energy supply and distribution. As per this bill, multiple licenses can be given in a region with at least one government energy supplier. It allows number of energy suppliers in a region and thus, the consumers have more options for purchasing the energy.

To participate in energy demand supply process, there are mainly three models *viz*; Feed-In Tariff (FIT), Net Metering Policy (NMP) and Energy Auction. In FIT model, a long-term contract exists between prosumer and state or national electricity board (Joseph, 2015). This contract pre-defines price of the injected energy into the power grid, which is fixed for the complete duration of the Power Purchase Agreement (PPA). In this model, a prosumer gets a low return on energy supply and the consumer has to pay a high amount for energy. NMP (Gustafsson, 2017) allows prosumers to supply energy to the power grid and to gain credits. Such credits can be later used to bridge the gap between energy demand and generation. In India, about eight states have already adopted the NMP (Lucas et al., 2013). In this model, prosumers get more incentives for excess energy than the FIT (Jenkins et al., 2015). The energy trading model is suitable for the microgrid. Here, local energy market (LEM) (Mengelkamp et al., 2017) allows prosumers to sell excess energy through trading and to gain incentives for excess. In addition, it allows a consumer to select energy supplier to fulfill the energy demand at an affordable rate.

In literature, few pilot projects on the distributed smart grid energy trading have been proposed. Piclo (2015) is a cloud-based energy trading system, a pilot project in the UK. It uses smart meter data, energy pricing and consumer's priority information to check imbalances in energy demand and supply. Grid Singularity (2018) provides an open, decentralized energy data exchange platform. It enables energy forecasting and grid management. It uses Proof of Authority (POA) consensus mechanism where authorities validate energy-related transactions. In Germany, Sonnen Community (2017) is aimed at providing

* Corresponding author.
E-mail addresses: ajitmuzumdar@nitgoa.ac.in (A. Muzumdar), cnmodi@nitgoa.ac.in (C. Modi), madhugm@nitgoa.ac.in (Madhu G.M.), c.vyjayanthi@nitgoa.ac.in (C. Vyjayanthi).

https://doi.org/10.1016/j.jnca.2021.103074
Received 21 September 2020; Received in revised form 26 January 2021; Accepted 5 April 2021
Available online 13 April 2021

smart grid functionalities. Members of sonnen community share surpass energy generation information. There is an intelligent battery storage system which connects people who can generate, share, and use energy. India has started its first smart grid project at Puducherry with the target of installing around 87000 smart meters (Jha et al., 2014). As a promising technology, the smart grid can address energy delivery limitations and energy outage problems.

The existing frameworks for smart grid energy management lack in providing transparency in energy trading process. Here, transparency can help in achieving the trust among participants and trading outcome. Energy consumers and prosumers depend on the trading services for securely handling of their energy related data and financial data. Attacks such as black hat may halt the working of trading services (Anon, 2019a). Providing user privacy and transaction transparency at the same time is also a major challenge in smart grid energy exchange (Kappagantu and Daniel, 2018). To overcome these challenges, blockchain can be an effective solution as investigated in (Nakamoto, 2008; Anon, 2014; Fortino et al., 2020).

In this paper, we propose a framework for smart grid energy management to offer trustworthy and incentivizing trading environment, users' privacy, transparency, and no single point failure. We propose different smart contracts *viz*; excess energy injection into smart grid, bidding, energy trading and utilization to ensure distributed trustworthy environment and the incentivized energy trading. We deploy the proposed smart contracts on the ethereum blockchain platform (Wood, 2014) which records energy trading and financial transaction data with append only feature. For the incentivized energy trading in context of both prosumers and consumers, we use an iterative Vickrey auction method (Vickrey, 1961). The proposed framework is analyzed in terms of average cost of transactions, throughput and the incentivized trading by considering different test scenarios.

The rest of this paper is organized as follows: Section 2 discusses the blockchain and its feasibility in the smart grid energy trading. In addition, it investigates the existing smart grid energy trading frameworks and their challenges. A detailed discussion on the proposed framework is given in Section 3. Section 4 analyzes the proposed framework through different experiments. Section 5 concludes our research work followed by the references.

2. Blockchain and smart grid energy trading frameworks

2.1. Blockchain platforms and consensus mechanisms

The blockchain/Distributed Ledger Technology (DLT) is a distributed database (ledger) that is practically immutable, maintained by decentralized Peer-2-Peer (P2P) network using consensus mechanism, cryptography and back referencing blocks to order and validate the transactions (Nakamoto, 2008; Eyal et al., 2016; Zyskind et al., 2015). In order to preserve identity of the peers, each peer is assigned with cryptographic pseudo identity using which he/she can initiate a transaction. The transactions initiated by users are visible to all peers and clubbed under one block. Such block of transactions is cryptographically verified by peer nodes based on the distributed consensus. Once the block is verified, it is added to the chain maintained at each mode and thus, it is nearly impossible to modify that block. A smart contract in blockchain is an agreement which binds the participants as per the defined policies. It has its own private storage and is associated with its predefined executable code which is triggered when a message is sent to its address.

The well known blockchain/DLT platforms are ethereum (Wood, 2014), hyperledger (Anon, 2019b), and IOTA (Anon, 2019c). The ethereum is a permissionless blockchain platform which provides a fully transparent environment where all participants have equal rights to append data on blockchain. It supports smart contracts written in solidity, which adds business regulation to the application (Leonhard, 2016). Hyperledger is a permissioned blockchain, which is more suitable for business to business applications. It applied role-based access. Hence, the transactions are confidential from the unauthorized access. It supports pluggable consensus mechanism for transaction validation (Anon, 2019b). The IOTA platform (Anon, 2019c) is based on a directed acyclic graph (DAG) data structure known as tangle. It is designed to support IoT devices with high scalability. It does not require transaction mining; Here, each transacting device has to validate a few recent transactions. However, IOTA platform is still under testing phase. Table 1 shows a comparison of the existing blockchain platforms.

In the proposed framework, we use ethereum blockchain as it is fully decentralized, permissionless, and transparent, and thus it is more suitable for the customer to customer applications such as smart grid energy trading. Ethereum supports proof of work (PoW) or proof of stake (PoS) consensus mechanism for transaction validation. In PoW based permissionless blockchain (Nakamoto, 2008), every node arranges all the verified transactions in a block using the Merkle tree data structure. Merkle root, previous block hash value, timestamp, and nonce value are applied to the SHA-256 hash function. If the output of hash function is less than the current difficulty value, then the puzzle is solved, else this process needs to be executed several times with the different nonce value. A node which solves the puzzle, broadcasts the result to all nodes, which gets verified and a block is added to the blockchain after 51% confirmations from the nodes. PoW method faces the challenges of wastage of energy, majority attack and other security threats (Chaudhry and Yousaf, 2018). PoS (Nguyen and Kim, 2018) consensus states that instead of wasting energy to solve the cryptographic puzzle as in PoW, a node can be selected to generate a new block based on its wealth. The PoS is highly energy efficient than PoW. In PoS, the stake of users decide block creation possibility. Stake denotes a user's asset share, i.e., the share of cash token or network transaction unit. The user with a higher stake is eligible for new block creation. The fundamental idea of PoS is that one having a maximum asset share will not perform any fraudulent activity. PoS is more scalable than PoW (Gervais et al., 2016; Anon, 2014). As PoW requires enormous energy for the processing, Siano et al. (2019) have recommended PoS as a consensus mechanism for the smart grid energy exchange. In addition, it offers high fault tolerance compared to other consensus mechanisms. Therefore, we have considered PoS in the proposed framework.

2.2. Existing frameworks for smart grid energy trading

There have been many frameworks reported till date for smart grid energy trading without considering blockchain. Few conceptual frameworks have been proposed to use a blockchain in smart grid trading.

Jimeno et al. (2011) have proposed an architecture of smart grid energy market management system based on a multi-agent system. Here, software agents maintain synchronization between energy generation and energy demand. Control systems are implemented using multi-agent system. Secondary control system keeps track of all bids and submits it to the trading agent. Here, cooperation of agents is required to achieve maximum utilization of available resources.

Lamparter et al. (2010) have proposed an agent-based local energy trading market in the smart grid. Here, software agents maintain the demand–supply mechanism. Here, an information layer collects the market information. A knowledge layer combines previously collected information with contract rules, while behavior layer is responsible to take action of each trading iteration.

Rathnayaka et al. (2012) have presented a smart infrastructure for the implementation of smart grids. In this framework, Virtual Power Plant (VPP) handles energy trading and energy distribution. Passive concentrator nodes collect the readings of smart meter from different prosumers and send them to the central data processing system in VPP. These nodes calculate energy generation and demand statistics which

Table 1
Comparison of different DLTs.

DLT platform	DLT type	Consensus	Smart contract language	Identity management	Transparency	Access restriction
Ethereum	Permissionless	PoW/PoS	Solidity	Anonymous	Transparent	No
Hyperledger	Permissioned	Pluggable framework	Go, Python, Javascript	Membership services	Partial transparent	Yes
IOTA	Not specified	PoW	Not supported	IAMPASS technology	Transparent	Yes

are used by the energy market. To achieve higher collective energy, a group of prosumers having mutual energy behavior and interest is formed in an ad-hoc manner, which leads to the unhinged association. Therefore, a robust grouping technique is required.

Mengelkamp et al. (2018a,b) have implemented a virtual energy trading system on top of the conventional grid. In this model, a centralized control handles the market mechanism. The demand–supply and financial transactions are stored on the blockchain. This system uses double price auction technique, where a consumer submits energy demand bids, and a prosumer submits energy generation bids to the auctioneer. Then, auctioneer selects value p randomly. All the energy bids above the p are selected, and all prosumers whose expected amount is less than p are selected for auction. This model rejects all other bids, and thus, winner percentage is less.

Dimitriou and Karame (2013) have focused on maintaining privacy in energy reporting and energy trading. Here, a utility provider interacts with smart meters to exchange the expected biding price and energy-related data. Report server maintains the reports related to energy generation, energy demand and trading process. Utility provider differentiates tasks and outsources them. A task contains location information of the querying smart meter. It uses a group signature mechanism to validate a new task. Group signature mechanism authenticates smart meter by assuming at least k members holds the same key to ensure k-anonymity of smart meter. After the successful completion of auction, it exchanges money using a centralized system, and thus it requires further verification of transaction and immutability of auction data.

Iria et al. (2018) have proposed an optimized aggregator model to collect demand–supply bids and scenario-based programming to handle the uncertainty of demand–supply bids conducted by prosumers. It attempts to minimize the cost of energy buying and selling in the day-ahead market. Zhou et al. (2015) have proposed a randomized auction to regulate demand–supply mechanism in energy trading. However, this is a centralized process and thus, there is a chance of single point of failure. In addition, data security needs to be improved.

In above presented approaches, there is a need of addressing issues such as prosumer's privacy, data transparency, immutability, availability and trustworthy trading. To address these problems, a blockchain with the required smart contracts needs to be incorporated.

Mannaro et al. (2017) have proposed a crypto trading system as a conceptual energy trading mechanism, which aims at addressing deficiencies of a regional energy distribution system using blockchain and smart contracts. Here, smart contracts handle the energy trading and distribution by considering European energy market.

Hwang et al. (2017) have presented a business model for prosumers. It is concluded that the increasing number of energy prosumers leads to the price competitiveness of the distributed power sources and gives options to the consumers for further reducing the energy cost. Myung and Lee (2018) have proposed an automated energy trading algorithm. It uses english auction strategy, where the highest bidder wins the auction and pays the same bid amount. In this approach, prosumer or bidder cannot get any incentive for participating in the trading process.

Gao et al. (2018) have presented a blockchain based smart grid monitoring. It includes smart contracts to monitor the consumer's energy usage and achieves non repudiation on usage. As shown in Fig. 1, trading agreements are converted into smart contracts which keep a track of trading. All the transactions are stored on blockchain which interact with a data center and energy center for data backup.

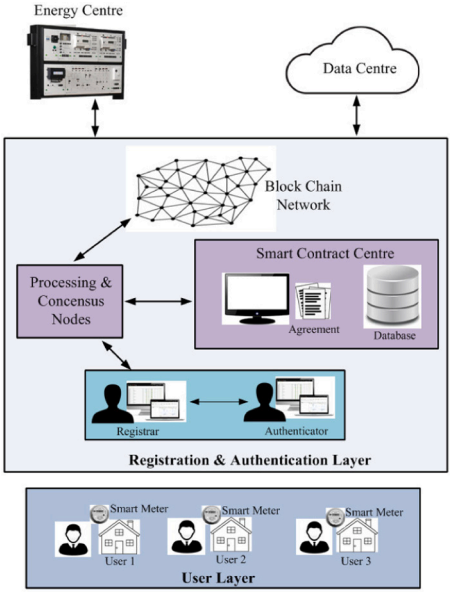


Fig. 1. Smart grid monitoring system (Gao et al., 2018).

Here, smart meter offers data integrity and blockchain provides data immutability.

Bergquist et al. (2017) have proposed a conceptual model to maintain transaction and communication anonymity in energy distribution and trading. It hides actual and predicted energy usage pattern and personal information. To achieve transaction anonymity, onion routing based crypto note algorithm is used. This model depends on Distributed System Operator (DSO) for controlling energy distribution and trading. It allows DSO to regulate trading securely and to enforce security rule.

Aitzhan and Svetinovic (2018) have proposed a messaging system to maintain security and privacy in the distributed energy trading system. It addresses two types of trading *viz*; full ownership of energy tokens and partial ownership over a micro payment channel. It prevents the double spending of energy tokens from the consumer side and the prosumer side using ownership locks which are managed by DSO (Hahn et al., 2017). However, this system lacks in offering the incentivizing trading.

Li et al. (2019) have used blockchain for the decentralized energy management. Authors have exploited blockchain to provide secure, reliable, and efficient energy exchange. It uses four different blockchains for energy exchange. However, the use, maintenance, and synchronization of four blockchains are cumbersome.

Saxena et al. (2019, 2020) have shown that a blockchain can improve the regulation policy, transparency and trust for smart grid voltage regulation. The reputation of energy resource is directly proportional to its involvement in voltage violation mitigation. This system does not offer peer to peer energy exchange.

Onyeka Okoye et al. (2020) have used a consortium blockchain for peer to peer energy trading. It is shown that a consortium blockchain can improve the scalability of the system. However, it is unable to handle concurrent transactions. In addition, peer to peer energy trading application needs full decentralization and transparency.

Kumari et al. (2020) have proposed an ethereum based energy trading scheme for the smart grid. It focuses on providing the privacy,

security and transparency to the transactions. For trading, first price auction is used, which is not incentive compatible.

Saxena et al. (2021) have proposed the residential energy trading system using permissioned blockchain-hyperledger fabric framework. It focuses on providing the scalable, decentralized, and self-governed network through permissioned blockchain. It uses the double auction mechanism for the trading, whereas a fuzzy bidding strategy distinguishes selfish and helpful participants. However, the double auction mechanism is not incentive-compatible which results into a high number of unsold bids. In addition, the use of permissioned blockchain puts restrictions on transparency.

From the literature, we have observed that there is a need of providing data transparency to the energy and auction related data in the existing approaches (Piclo, 2015; Sonnen Community, 2017; Jha et al., 2014; Jimeno et al., 2011; Lamparter et al., 2010; Rathnayaka et al., 2012; Dimitriou and Karame, 2013; Iria et al., 2018; Mannaro et al., 2017; Mengelkamp et al., 2018a,b; Gao et al., 2018; Aitzhan and Svetinovic, 2018; Li et al., 2019; Saxena et al., 2019; Onyeka Okoye et al., 2020; Saxena et al., 2021). The existing frameworks (Jimeno et al., 2011; Dimitriou and Karame, 2013) need to consider the prosumer's privacy. Peers need to be encouraged for energy trading within the microgrid by improving the trust and incentives. Incentivizing auction effort is not made yet in the existing frameworks (Piclo, 2015; Grid Singularity, 2018; Lamparter et al., 2010; Dimitriou and Karame, 2013; Iria et al., 2018; Zhou et al., 2015; Gao et al., 2018; Bergquist et al., 2017; Aitzhan and Svetinovic, 2018; Myung and Lee, 2018; Li et al., 2019; Saxena et al., 2019; Onyeka Okoye et al., 2020; Kumari et al., 2020; Saxena et al., 2021). The existing frameworks (Jha et al., 2014; Lamparter et al., 2010; Rathnayaka et al., 2012; Dimitriou and Karame, 2013; Iria et al., 2018; Zhou et al., 2015) lack in providing data immutability and thus, pose trust issues. Encapsulating these needs in a nutshell, there is a need of providing a secured, transparent, trusted and incentivizing platform for smart grid energy trading. Table 2 shows a comparison of the existing frameworks for energy trading in terms of fulfilling requirements such as: **R1**: Transparency, **R2**: Non-repudiation, **R3**: No single point of failure, **R4**: User's privacy, **R5**: Incentivized trading, and **R6**: Trust.

3. Proposed smart grid energy trading framework

3.1. Objective

The objective of the proposed framework is to achieve a trustworthy and incentivized energy trading for prosumers and consumers in smart grid, while fulfilling the following requirements:

Transparency: The information about excess energy injection, bidding, trading and supply to/from smart grid should be transparent.

Non-repudiation and no single point of failure: No participant should be able to deny about the performed transaction. The transactions should be recorded in a distributed manner to avoid single point of failure.

Prosumer's privacy: Participant's personal information, his/her energy utilization pattern, financial creditability etc. should not be revealed to any unauthorized entity. In addition, the source and destination of the energy supply should not be disclosed to the intermediate nodes.

Incentivizing energy trading and truthful bidding: The energy trading mechanism should be performed in a way that both prosumer and consumer can be benefited. In addition, it should make consumers to do truthful energy bidding instead of over/under bidding.

Distributed trustworthy environment: The proposed framework should create trust among peers on energy trading and data exchange, and thus distributed computing environment should be considered instead of involving only a third party/central authority. In addition, the trading process should be fully transparent to improve trust among the participants.

3.2. Design of the proposed framework

The Fig. 2 shows communication model of the proposed framework. Here, prosumers use advanced metering infrastructure (AMI) to monitor the injected excess energy (via energy transmission network) in the smart power storage. The smart power storage is the combination of grid energy storage and energy transmission network. On the other hand, consumers use AMI to place energy demand. Valid energy injection and bidding transactions are recorded on the blockchain which offers a distributed energy trading. The trading results are notified to the grid operator, responsible for actual energy release to the intended consumer via transmission network.

The proposed framework considers prosumers, smart power storage, distributed ledger technology (blockchain), smart contracts and consumers (bidders), as shown in Fig. 3. Prosumers have RESs like solar panel or wind turbine system to generate energy. They interact with blockchain through the smart meter. Each prosumer has a copy of the distributed ledger to maintain the energy data records with append only feature. We have considered ethereum blockchain to maintain energy data since it is fully decentralized, permissionless and fully transparent, and thus, it is more suitable for the customer to customer applications such as smart grid energy trading. Here, the blockchain has two transaction units *viz*; energy tokens and cash coin. The messages in the proposed framework are as follows:

1. Prosumer injects energy to the smart power storage
2. Data exchange between prosumers and energy injection contract which is called by prosumers to send energy generation information. Energy injection contract sends energy tokens (equivalent to amount of energy injected) to prosumer after transaction verification
3. Energy injection contract verifies prosumer's energy injection claim
4. Energy injection contract maintains the account of energy stock
   (a) Amount of energy available for the energy trading instance is submitted to trading contract
   (b) Verified energy injection transactions are stored on the DLT
5. Consumer sends energy demand and the expected amount as energy demand bid
6. Bidding contract organizes bid for the energy trading instance
   (a) Energy demand request for the energy trading instance is submitted to trading contract
   (b) Energy demand transactions are updated on DLT
7. Energy trading contract does the mapping of supply and demand based on iterative Vickrey auction method
   (a) Cash coins are issued to prosumer
   (b) Energy tokens are issued to consumer
   (c) Trading result is updated on DLT
8. Consumer calls energy utilization contract for energy usage
9. Contract verifies energy token ownership
10. Energy utilization contract burns energy tokens and instructs smart storage to release energy
    (a) Smart grid releases energy to the consumer
    (b) Energy tokens are surrendered and DLT updated accordingly

Above process is repeated after a fixed time interval to overcome multiple active auction processes at the same time. We have considered 30 min time interval system for energy exchange (Zhang et al., 2018). This interval can be changed as per the grid policies and regulations. During each interval, prosumers inject excess energy into the smart

Table 2
A summary of the existing smart grid energy trading frameworks in terms of fulfilling the requirements.

Author/Year	Approach/System	DLT	Smart grid energy management requirements					
			R1	R2	R3	R4	R5	R6
Lamparter et al. (2010)	Agent based Market for Smart Grids	None	✗	✗	✓	✓	✗	✗
Jimeno et al. (2011)	Microgrid Energy Management System	None	✗	✓	✗	✗	✓	✗
Rathnayaka et al. (2012)	Smart Grid Prosumer Management	None	★	✗	✗	✓	★	✓
Dimitriou and Karame (2013)	Multi Agent System	None	✗	✗	✗	✓	✗	✓
Jha et al. (2014)	Puducherry Smart Grid Pilot Project	None	✗	✗	✗	✓	✓	✗
Piclo (2015)	Piclo	None	✗	✓	✗	✓	✗	✓
Zhou et al. (2015)	Smart Grid Demand Response Model	None	✗	✗	✗	✓	✗	✗
Sonnen Community (2017)	Sonnen Community	None	✗	✓	✗	✓	✓	✗
Mannaro et al. (2017)	Crypto Trading System	Private Blockchain	★	✓	✗	✓	★	✓
Hwang et al. (2017)	Prosumer Business Model	Private Blockchain	★	✓	✗	✗	★	✓
Bergquist et al. (2017)	Transaction Anonymity Model	Private Blockchain	★	✓	✗	✓	✗	✗
Iria et al. (2018)	Optimized Aggregator Model	None	✗	✗	✗	✓	✗	✓
Mengelkamp et al. (2018b)	Blockchain-based Smart Grid	Private Blockchain	★	✓	✗	✓	✓	✓
Gao et al. (2018)	Smart Grid System Monitoring Model	Private Blockchain	★	✓	✗	✓	✗	✗
Aitzhan and Svetinovic (2018)	Distributed Energy Trading System	Private Blockchain	★	✗	✓	✓	✗	✓
Grid Singularity (2018)	Grid Singularity	Private Blockchain	★	✓	✓	✗	✗	✓
Myung and Lee (2018)	Automated Power Trading	Ethereum	✓	✓	✓	✗	✗	✓
Siano et al. (2019)	Transactive Energy Exchange	Permissioned Blockchain	✗	✓	✓	✗	✗	✓
Li et al. (2019)	Transactive Energy Management	Ethereum	✗	✓	✓	✓	✗	✓
Saxena et al. (2020)	Transactive Energy System	Permissioned Blockchain	✗	✓	✓	★	✓	✓
Onyeka Okoye et al. (2020)	Microgrid Energy Trading	Consortium Blockchain	✗	✓	✓	✓	✗	✓
Kumari et al. (2020)	ET-Deal	Ethereum	✓	✓	✓	✓	✗	✓
Saxena et al. (2021)	Residential Energy Trading	Hyperledger Fabric	✗	✓	✓	✓	✗	✓

✓: Fulfilled, ✗: Not Fulfilled, ★: Partially Fulfilled

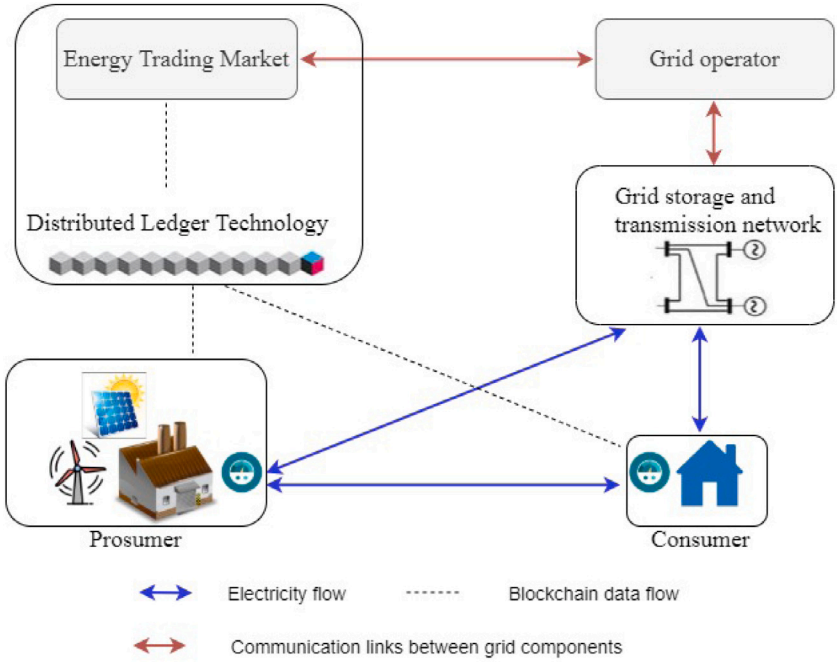


Fig. 2. Communication model of the proposed framework.

storage and get equivalent energy tokens. We define T_1 as time interval for energy injection and bidding. All prosumers supply their energy details in the prescribed time interval only. As shown in Fig. 4, a prosumer or consumer can supply or demand energy respectively by calling appropriate contract within prescribed time interval T_1.

Any entry after time interval T_1 cannot be considered for the current energy trading instance. A successful execution of energy injection contract claims the participation of the prosumer in auction iteration. Similarly, bidders have to supply their bid within time interval T_1 to confirm their participation in the energy trading instance. Energy trading process starts after the expiry of time interval T_1. Energy trading contract is also executed after every half an hour. Once a participant places bid, that bid is valid for all energy trading instances for the next 24 h. Consider, T_2 is a time interval for the validation of transaction committed at the closure of time interval T_1, execution of energy trading process and energy token allocation. Auction losers are also notified, in time interval T_2, and they have to settle as per FIT. For example, the time interval T_1 would be of 30 min from 10:15 AM to 10:45 AM for the energy exchange scheduled at 11:00 AM to 11:30 AM. All prosumers and bidders who wish to participate in the trading process can bid within this time interval T_1. In case any participant does not explicitly bid, his previous bid is considered. The allocation of energy to auction winner starts at T_2 after the expiry of T_1. All the bids are stored on the blockchain and thus, none of the participants can make any change to his bid and energy supply after the closure of T_1. A prosumer with the highest stake (i.e. amount of energy injected) in the previous auction instance is selected as a transaction validator and new block creator. In case, if such a prosumer is unavailable then

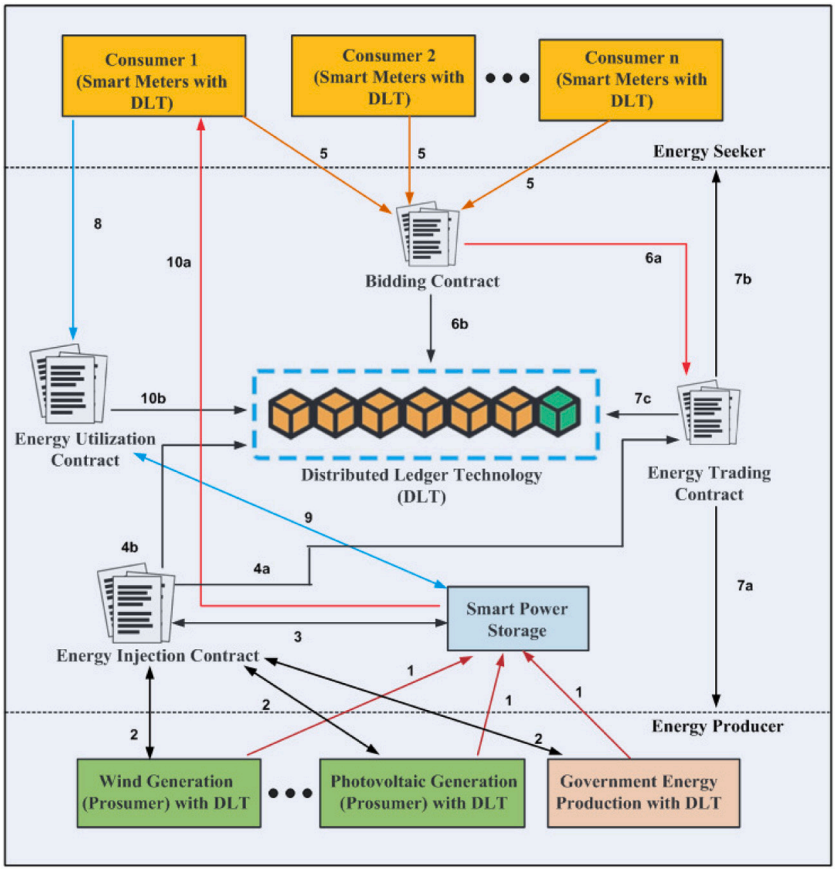


Fig. 3. Design of the proposed framework.

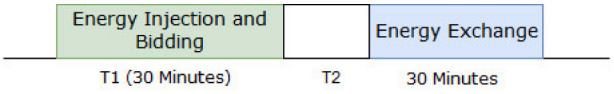


Fig. 4. Time sequence of trading process.

the prosumer having next highest stake is selected for the prescribed task and so on (Wood, 2014). Once a designated prosumer creates a new block of validated transactions, the new block is added into the blockchain. The proposed framework has mainly four modules *viz*, energy injection, bidding, energy trading, and energy utilization. The details of each module in the proposed framework are as follows:

3.2.1. Energy injection

As shown in Fig. 5, a prosumer calls energy injection contract to claim his/her participation in the energy trading process. The claimed transaction contains the energy injection information such as timestamp, the amount of energy generation (injected energy reading taken from smart meter is converted into a number of tokens) for the auction iteration and the expected value. The contract ensures ownership of energy generation and generates energy tokens accordingly. Then, it sends token information to the prosumer and updates same on DLT. The contract sends available energy generation for the energy trading instance.

Each prosumer creates a transaction to take part in energy trading, which is verified through PoS consensus mechanism and accordingly blocks of transactions are appended to DLT. The transaction format for energy injection is shown below:

na	*gas_price*	*gas_limit*	*to*	*injected_energy*	*expected_value*	*ts*

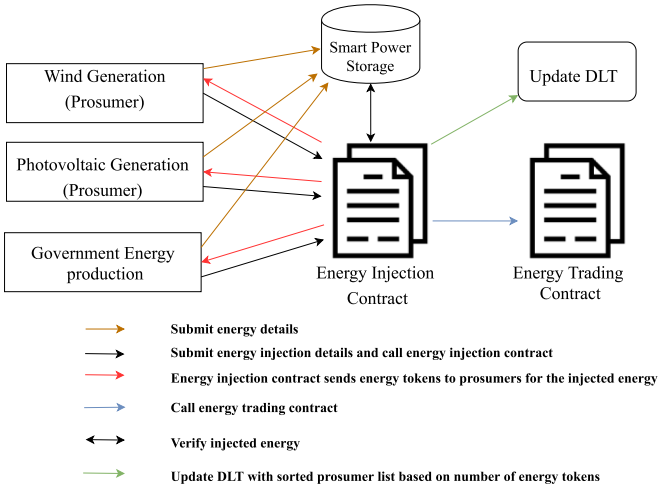


Fig. 5. Energy injection process.

Here, *"na"* indicates a count of the transaction initiated by the same prosumer. The *"gas_price"* is the maximum amount one can spend for per unit of gas. Gas is a computational step in the ethereum blockchain platform. *"gas_limit"* is the maximum amount one can spend as transaction amount. "*to*" is the contract account address of energy injection smart contract. *"injected_energy"* is amount of energy injected by prosumer into the grid. *"expected_value"* is the amount which prosumer is expecting for the injected energy. The "*ts*" indicates the time of energy injection. It prevents double spending of the same energy or cash coins. A prosumer signs transaction using elliptic curve based digital

signature algorithm (ECDSA) (Koblitz, 1987). This helps in achieving the non-repudiation of the submitted transaction.

Energy injection contract sends energy tokens to prosumers for defining the ownership of the injected energy. It sends the ownership (prosumer's digital identity) and energy token information to the energy trading contract. An algorithm for energy injection contract is given in *Algorithm 1*. Here, each prosumer initiates energy injection contract by submitting energy injection information, timestamp and expected value as an input. Each energy injection message is verified based on the time stamp and owner. The verified energy units are converted to the tradable energy units known as energy tokens. The generated energy tokens are given to prosumers based on the injected energy as an acknowledgment of their participation in the energy trading instance, and the sorted list of energy tokens is stored on the DLT as well. Then, available energy tokens, ownership and expected value in context of each prosumer are sent to the energy trading contract.

Algorithm 1 Energy Injection Contract

1: **for** each received message from prosumer **do**
2: Verify energy injection message based on timestamp
3: Generate $energy\_tokens = injected\_energy\_unit$
4: Send energy tokens to prosumer
5: Sort $ownership(n)$ for n prosumers in decreasing order based on the issued energy tokens
6: *available_energy_tokens* = Sum of all *energy_tokens [n]*
7: Insert verified message to DLT *(ownership [n], energy_tokens [n], expected_value[n], ts)* through PoS consensus method
8: Send *(available_energy_tokens [n], ownership [n], expected_value [n], ts)* → Energy trading contract
9: **end for**

Energy injection contract calls energy trading contract to initiate the trading process by sending a message as given below:

na	gas_price	gas_limit	to	available_energy_tokens[n]	ownership[n]	expected_value[n]	ts

3.2.2. Energy bidding

A consumer who seeks energy can place his/her demand by calling bidding contract, as shown in Fig. 6. This contract allows a energy seeker to set bid for his/her energy demand. A consumer places bid by specifying energy demand and the maximum amount which he/she can pay. During the bidding request, the bidder's balance is also verified. If a bidder is not having sufficient balance, then contract marks that bid as invalid and restricts such bidder from taking part in that auction iteration. At the end, bidding contract summarizes total demand along with bidding value and submits these information to the energy trading contract. The consumers use following transaction format for bidding, where "*to*" field denotes the contract address of the bidding contract.

na	gas_price	gas_imit	to	energy_demand	bid_ value	ts

As shown in *Algorithm 2*, the consumers call bidding contract by submitting energy demand, bid value, and timestamp. This contract verifies realistic energy demand, i.e., energy demand should be nearly equal to consumers average energy utilization. This prevents the system from a single consumer energy concentration. This helps to satisfy more number of bids. In addition, consumer's account balance is verified to make a bid. Finally, all valid bids are sorted and submitted to energy trading contract, and DLT is updated accordingly through PoS consensus method.

The transaction message format for sending energy demand and bid value to energy trading contract is given as follows:

na	gas_price	gas_limit	to	consumer_wallet_address [c]	energy_demand [c]	bid_value [c]	ts

Algorithm 2 Energy Bidding Contract

1: **for** each bid iteration Consumer **do**
2: Consumer *(consumer_wallet_address, energy_demand, bid_value, ts)* → Biding Contract
3: **for** each consumer c **do**
4: **if** ($consumer[c].energy\_demand$ <= $average\_energy\_utilization$ + $margin$) **then** // Margin indicates energy demand deviation for a consumer
5: **if** ($consumer[c].account\_balance > consumer.bid\_value[i]$) **then**
6: mark bid as $valid$
7: **end if**
8: remove consumer [c]
9: **end if**
10: **end for**
11: **end for**
12: Sort all valid bids in descending order based on *bid_value* and insert *Consumer_wallet_ address* and bid value to DLT through PoS consensus method
13: Send *(consumer_wallet_address* [c], *energy_demand* [c], *bid_value* [c], *ts)*→ *Energy Trading Contract*

3.2.3. Energy trading

In literature, English and double price auction are the preferred multi unit homogeneous mechanisms. However, English auction results into many unsatisfied bids as it is seller centric method. This results into unwillingness of consumer's participation. The double price auction is not an incentive compatible (Kwasnica and Sherstyuk, 2013). A Vickrey auction (Vickrey, 1961) is more suitable than other auction mechanisms as it is computationally efficient, incentive compatible, and fair to consumers as well as sellers. We propose energy trading contract based on vickrey auction method (Vickrey, 1961). The vickrey auction (Vickrey, 1961) is fundamentally designed for selling a single product where the bidder with highest bid gets the product at the end of the auction. Here, the bidder with highest bid is considered as winner, but a winner has to pay an amount equal to the second-highest bid. We have modified the vickrey auction to satisfy c consumers' energy demand with n prosumers' energy generation.

As shown in Fig. 7, trading contract receives two inputs *viz*; one from energy injection contract specifying energy available for the auction iteration and another from bidding contract specifying total energy demand. A consumer who has the highest bid wins the auction and as an incentive, he/she has to pay an amount equal to the second highest bidder's bid. Then, ownership of energy tokens is updated and tokens are assigned to the auction winner. Now, winner is detached from the auction process and available energy is also reduced by won energy tokens. The auction is recursively carried out for the available energy and bidders without changing their bid value. This process is continued till either all demands are satisfied or available energy becomes zero. The loser of the auction can get energy from the government energy generations at a FIT rate. A prosumer whose energy is unsold in auction can directly sell energy to government as per FIT.

As shown in *Algorithm 3*, energy trading contract receives two inputs for energy trading instance *viz;* energy available and energy demand. Energy trading instance runs for multiple iterations until all energy tokens are sold or demands are satisfied. In the first iteration, the consumer with the highest bid is elected as a winner and he/she gets the required energy tokens. This contract calculates a cost for the assigned energy tokens. The calculated cash coins are deducted from winner's account and credited to prosumer's account. Ownership of energy tokens is changed to winner consumer, and DLT is updated with the two transactions viz; ownership transfer of energy tokens and cash coin transaction through PoS consensus method. At the end, loser consumers and prosumers are notified.

In the proposed framework, consider, a consumer's payoff can be denoted by u_i, set of bidders in any auction is $i = (1, 2, 3 \ldots c)$, v_i is

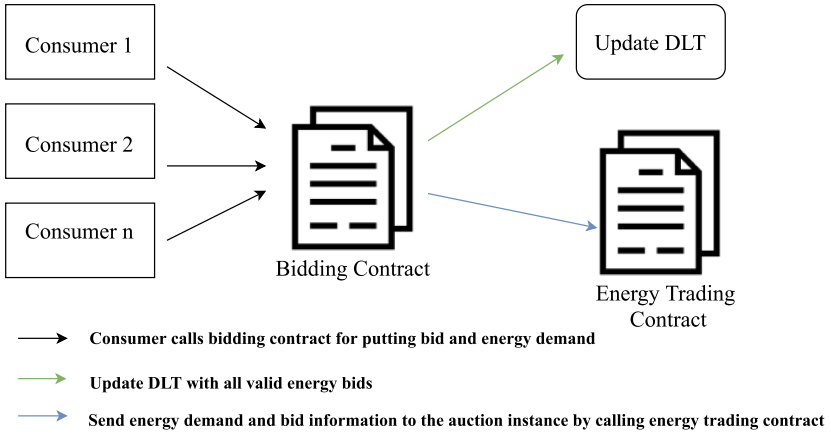


Fig. 6. Energy bidding process.

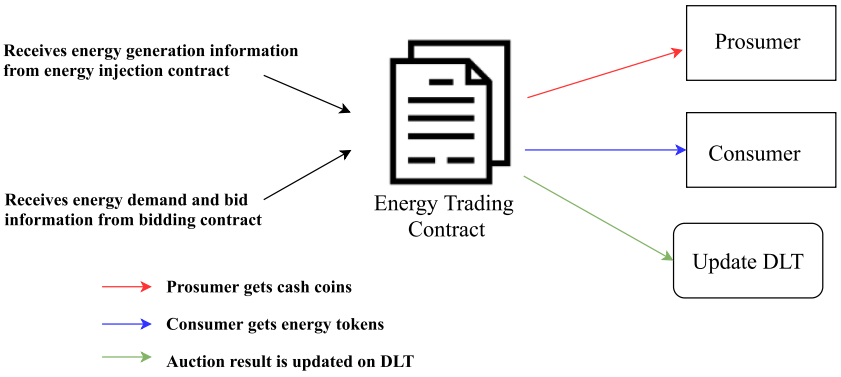


Fig. 7. Energy trading process.

Algorithm 3 Energy Trading Contract

INPUT: from Energy Injection Contract: *available_energy_tokens* [*n*], *ownership* [*n*], *expected_value* [*n*], *ts*[*n*]
INPUT: from Bidding Contract: *energy_demand* [*c*], *consumer_wallet_address* [*c*], *bid_value* [*c*], *ts* [*c*]

for each Vickery auction iteration **do**
  while *energy_tokens* > 0 **do**
    for each consumer $i = 1$ to $i = c - 1$ **do**
      Assign required energy tokens to *consumer*[*i*] at consumer [*i* + 1].*bidvalue*
      cost = *consumer*[*i* + 1].*bid_value* × *number of energy_tokens issued*
      consumer[*i*].*account_balance* = *consumer*[*i*].*account_balance* - *cost*
      Owner (Prosumer) gets cash coins in exchange of its *ownership* and cash coin transaction appended in a DLT
      Ownership of the issued *energy_tokens* is changed to the *consumer*[*i*]
      Add a new transaction about *ownership*, *energy_tokens* in a DLT
    end for
  end while
end for
Notify consumer and prosumer loser (if any)
Consumer loser can follow FIT contract or can take part in next bidding to purchase energy

the energy valuation of *i*th prosumer, b_i is a bid of *i*th consumer. A consumer has three options *viz*; $b_i = v_i$, $b_i > v_i$ and $b_i < v_i$.

$$u_i = \begin{cases} v_i - b_i & \text{if } b_j < b_i, for\ \ all\ \ j \neq i \\ 0 & \text{if } b_j > b_i, for\ \ some\ \ j \neq i \end{cases} \quad (1)$$

Here, if a consumer bids equal to the valuation and wins auction, then he gets 0 payoff. If a consumer bids higher than valuation and wins auction then he gets the negative payoff and if a consumer bids less than valuation and wins the auction then he gets the positive payoff. At the end of auction iteration, prosumers get cash coin for their sold energy and the consumer gets ownership of the energy tokens.

3.2.4. Energy utilization

As shown in *Algorithm 4*, a consumer winner in the auction calls energy utilization contract by sending the earned tokens with a timestamp. Contract matches user's ID with energy tokens ownership. After positive verification of the ownership, contract converts energy tokens back to equivalent energy amount. Then, it instructs smart storage to release amount of energy equivalent to energy tokens for the prescribed time interval. Smart grid transmission and distribution network takes care of actual energy delivery to the consumer. Energy tokens are surrendered to avoid double-spending, i.e., utilization of energy tokens to avail energy more than once. The ownership of such token are made NIL and updated to DLT using PoS consensus. Fig. 8 represents the energy utilization process.

Algorithm 4 Energy Utilization Contract

Consumer *(energy_token, ts)* → Energy Utilization Contract
if *consumer_wallet_address* = *energy_token.ownership* **then**
  Convert *energy_tokens* into equivalent *energy_units*
  Surrender *energy_tokens* to release energy
end if
Release Energy *(energy_units, consumer_wallet_address, ts)*→Smart power storage

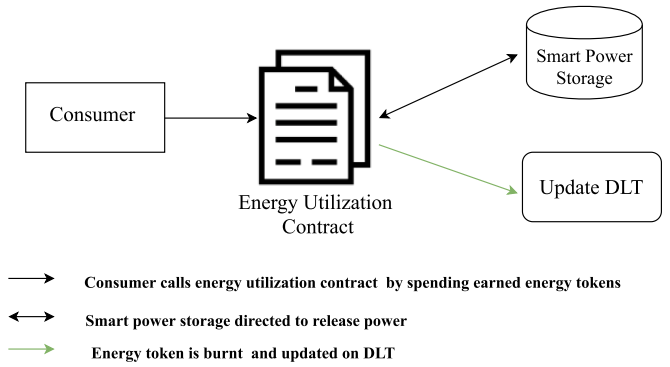


Fig. 8. Energy utilization process.

Energy utilization contract sends a message to smart power storage as given below. Here, "*to*" field points towards smart power storage. The "*energy_tokens*" indicates the amount of energy smart power storage has to release. "*ownership*" helps to derive account where energy needs to be released.

na	*gas_price*	*gas_limit*	*to*	*energy_tokens*	*ownership*	*ts*

3.3. Overall workflow of the proposed framework

A workflow of the proposed framework is shown in Fig. 9. Here, prosumer initiates energy injection process by calling energy injection contract. Prosumer sends excess energy information to the energy injection contract which issues energy tokens for the injected energy to the prosumer. Energy injection contract accumulates the available energy and submits it for the auction (trading) iteration by calling energy-trading contract and updates the distributed ledger. Consumer calls bidding contract and initiates energy bidding process. Consumer places a bid with the affordable amount. Bidding contract collects bids from all consumers, updates ledger and submits bid and energy demand for auction iteration.

Energy trading receives two inputs, energy supply information from energy injection contract and demand information from bidding contract. Energy trading contract performs an iterative Vickrey auction as per the energy supply and bids to declare a winner in each iteration. Consumer winner gets energy tokens, prosumer gets cash coin and trading iteration details are stored on the distributed ledger.

At the end, consumer winner initiates energy utilization contract and submits energy tokens by calling energy utilization contract. This contract confirms ownership of tokens and converts tokens to energy amount. Energy utilization contract informs smart storage to release the energy to the claimant.

4. Experimental results and analysis

4.1. Experimental setup

For the performance validation of the proposed framework, we have setup ethereum blockchain network testbed at NIT Goa as shown in Fig. 10. It includes 32 servers as nodes; each has $8GB$ RAM, Intel core $i7$ processor and Ubuntu 18.04 operating system. We have installed ethereum geth node and created random accounts 50 accounts on each node. We have written the required smart contracts in solidity and validated them using remix solidity IDE.

To evaluate the proposed framework in terms of auction winner percentage, we have considered energy demand data based on energy consumption dataset for buildings in British Columbia (Makonin, 2018). This dataset consists of energy consumption record of consumers from different background. We have selected 80 consumers' energy usage profiles randomly as per the dataset. This dataset consists of the simulated solar energy generation in different seasons (Makonin, 2018). We have considered 70 prosumers' energy generation profiles for the auction. For testing the performance of the proposed framework, we have considered different combinations of consumers and prosumers energy profiles with seasonal and temporal data during energy trading iteration. A percentage of winners in the proposed framework in compared with the existing auction methods such as double price (Mengelkamp et al., 2018b) and English auction method (Myung and Lee, 2018). The percentage of auction winners is calculated using Eq. (2). In addition, the proposed framework is evaluated in terms of average time required for energy injection, bidding and trading process in the interval of 15 and 30 min, throughput with varying rate send rate (i.e. 10 tps to 100 tps) of transactions and nodes, while performing 10000 transactions of energy injection and bidding.

$$Winner\_percentage = \frac{Number\_of\_satisfied\_participants}{Total\_number\_of\_participants} * 100 \quad (2)$$

4.2. Results and analysis

Fig. 11 shows that the proposed framework satisfies more number of bids than the existing methods such as double price (Mengelkamp et al., 2018b) and English auction method (Myung and Lee, 2018). This encourages more number of participants to take part in energy trading process and thus, increasing the utilization of RESs.

To analyze the effectiveness of the proposed framework in terms of incentivized trading, we have considered different types of bidding strategies *viz*; over bidding, under bidding and truthful bidding. In over bidding, bidder puts higher bid than actual valuation. In this case, even though bidder wins the auction, he/she gets the energy at a higher price than the valuation and thus, his/her payoff becomes 0. In under bidding, bidder bids less than the valuation and thus, the auction winning percentage is reduced. In truthful bidding, bidder bids as per actual valuation and if he/she wins, gets a higher payoff, i.e., the difference between his/her bid and next highest bid.

For better understanding of the incentivized bidding, consider a consumer can follow one of the three possible strategies, while bidding:

Strategy 1: Truthful bidding
Strategy 2: Over bidding
Strategy 3: Under bidding

As shown in Fig. 12, if a consumer chooses strategy 1, he/she gets 0 payoff for auction defeat and higher payoff for winning the auction as he/she bids as per expected value. In strategy 2, there are three possible scenarios: Scenario 1, where ith consumer loses auction and his/her payoff will be 0 due to over bidding. In scenario 2, ith consumer wins the auction and the second highest bid is less than the valuation then the payoff is positive. In scenario 3, ith consumer wins the auction but second highest bid is greater than valuation, payoff is negative. Here strategy 1 weakly dominates strategy 2 because of scenario 2. In strategy 3, bidder chooses under bidding. Here, consumer gets positive payoff only in scenario 2. Hence, strategy 1 dominates strategy 3. Nash equilibrium for this auction is strategy 1, i.e., all consumers can get the highest payoff if they choose truthful bidding.

We have considered an energy trading instance consisting of 20 consumers and 19 prosumers. As shown in Fig. 13, prosumer *P1* chooses over bidding and puts the highest value as an expected value. Prosumer *P1* loses auction as none of the bidding value matches to his/her expectation value. On the contrary, prosumer *P19* chooses under bidding and puts the lowest value for energy token and still loses the auction. A prosumer *P5* selects truthful bidding and expects 48 cash coins per energy token. At the end of the auction iteration, *P5* gets an average rate of 48.8 cash coins per energy token.

Fig. 14 shows incentives for the consumers for their different bidding strategies. In order to win an auction, a consumer *c1* overbids as 58 cash coins per energy token. Even though after winning the auction, he/she gets energy tokens at much higher rate than the expected value,

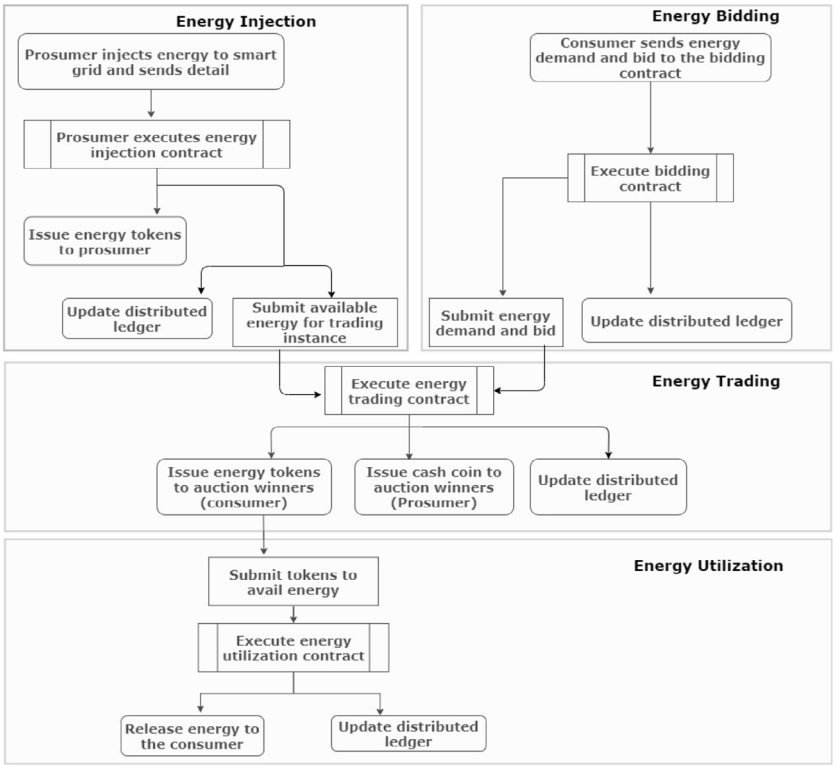


Fig. 9. Workflow of the proposed framework.

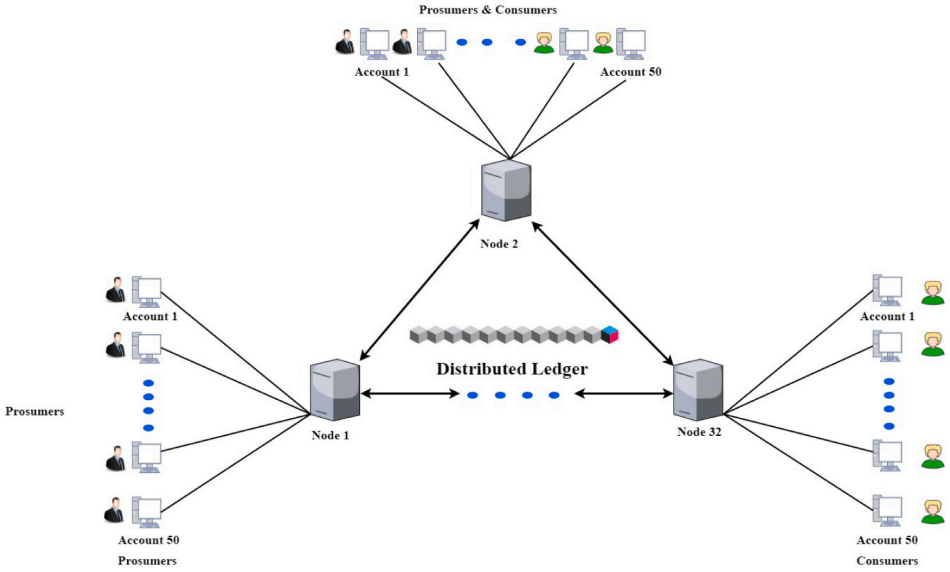


Fig. 10. Experimental setup.

and thus, his/her payoff is zero. Consumer *C20* loses auction due to his/her under bidding strategy and receives zero payoff. Consumer *C4* chooses a truthful bidding strategy and for his/her demand of 36 energy tokens, puts a bid of 50 cash coin per energy token. At the end of the auction iteration, *C4* wins the auction and gets energy at a rate of 48 cash coins per energy token. Hence, he gets 2 cash coins as an incentive per energy token. These scenarios indicate that the proposed framework forces to do truthful bidding as truthful bidders are auction winners and get a better deal than FIT. Truthful bidders get higher payoff than other bidders at most of the times.

An average latency of the transactions in the proposed framework is shown in Fig. 15. The time required for energy injection process, i.e energy injection transaction latency in context of number of prosumers participating in the trading iteration and different trading intervals is given in Fig. 15(a). It takes on average 11 s for energy injection transaction, its validation, execution and commitment on the distributed ledger. Fig. 15(b) shows the average transaction time required, i.e bidding transaction latency for bidding with respect to the number of consumers participating in the trading iteration as a bidder and different trading intervals. It takes approximately less than 12 s for performing a bidding transaction, its validation, execution and commitment on the distributed ledger. The energy trading transaction time in context of different number of participants and different trading intervals i.e energy trading transaction latency is shown in Fig. 15(c). It

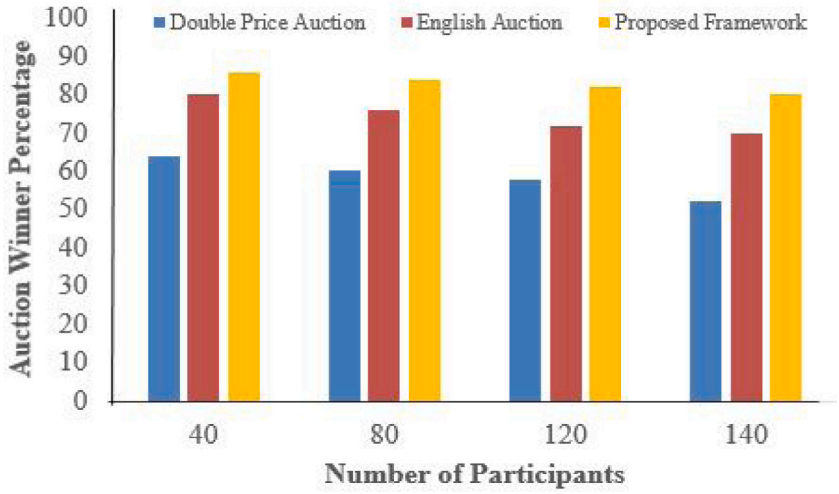


Fig. 11. Winner percentage in the proposed framework and the existing methods.

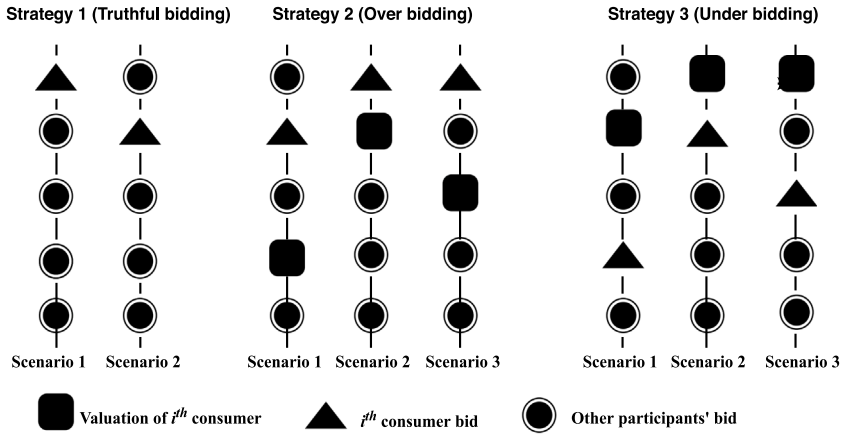


Fig. 12. Strategies for bidding.

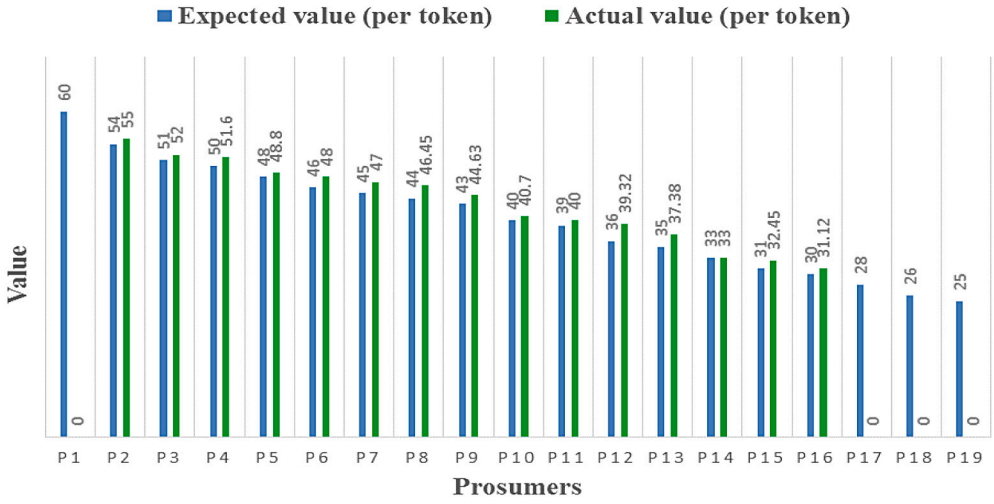


Fig. 13. Results on incentives for the prosumers in the proposed framework.

is a sum of trading process execution time, time required for prosumer and consumer settlement. It is dependent on number of participants (consumers and prosumers) participating in the trading iteration. The proposed framework requires on average 34 s for trading process among 150 participants.

Transaction throughput of the proposed framework depends on two factors, i.e., transaction send rate (transactions per second) and number of nodes. We have performed 10000 energy injection and bidding transactions at different send rates (10 tps to 100 tps) in the proposed framework as these transactions are directly related to blockchain state

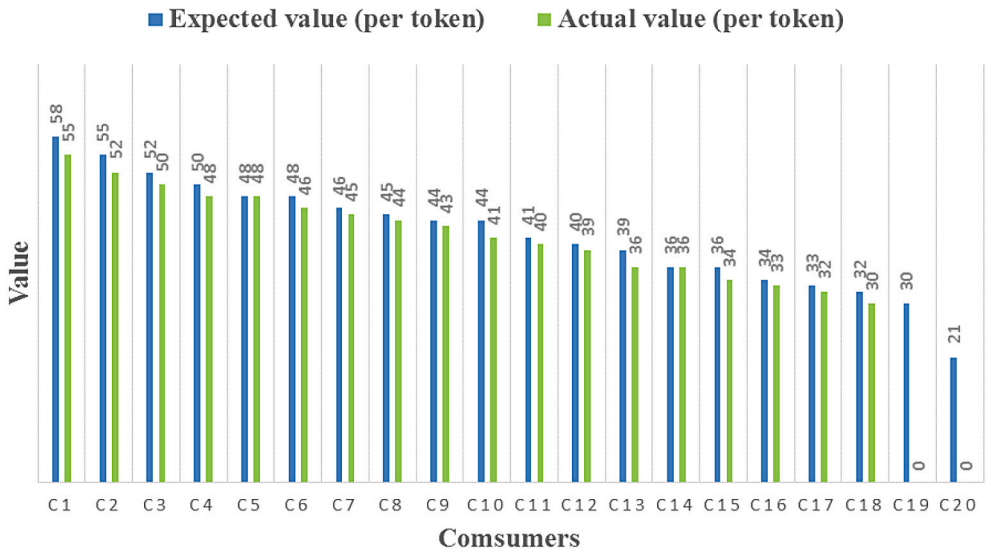
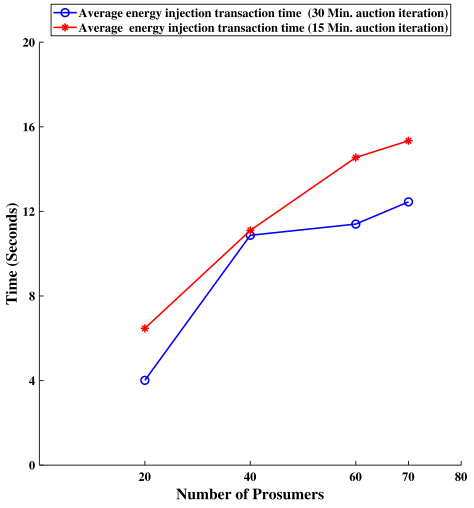
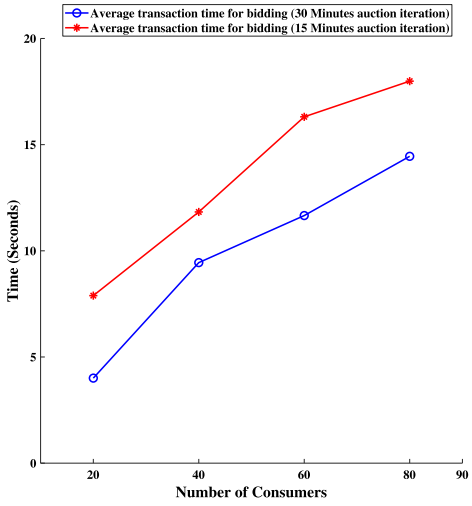


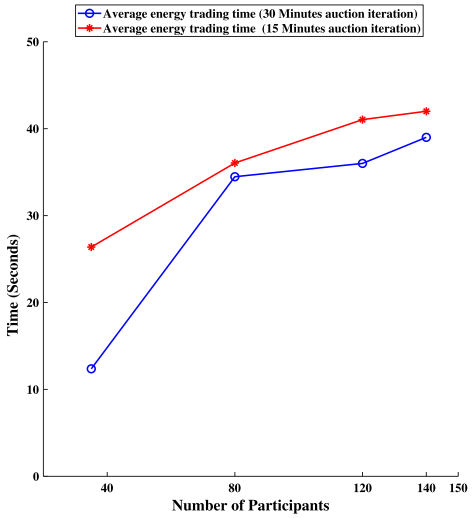
Fig. 14. Results on incentives for the consumers in the proposed framework.



(a) Average latency during energy injection.



(b) Average latency during energy bidding.



(c) Average latency during energy trading.

Fig. 15. Average latency of the transactions in the proposed framework.

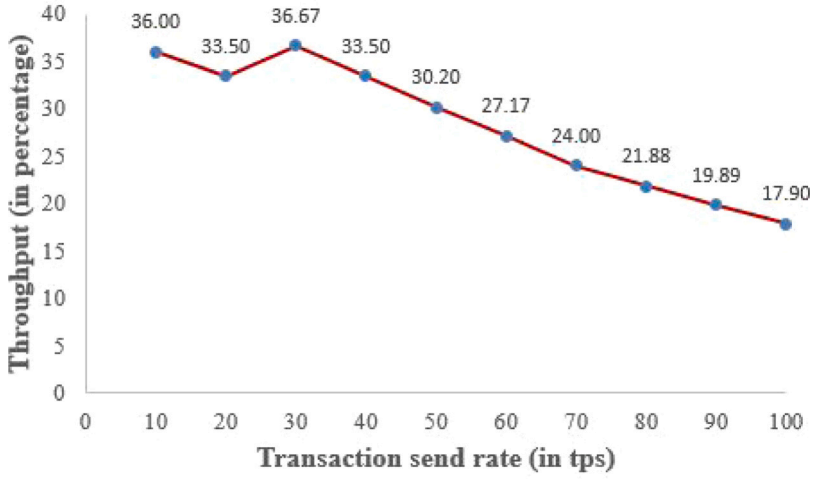


Fig. 16. Percentage throughput of the proposed framework with different send rates of transactions.

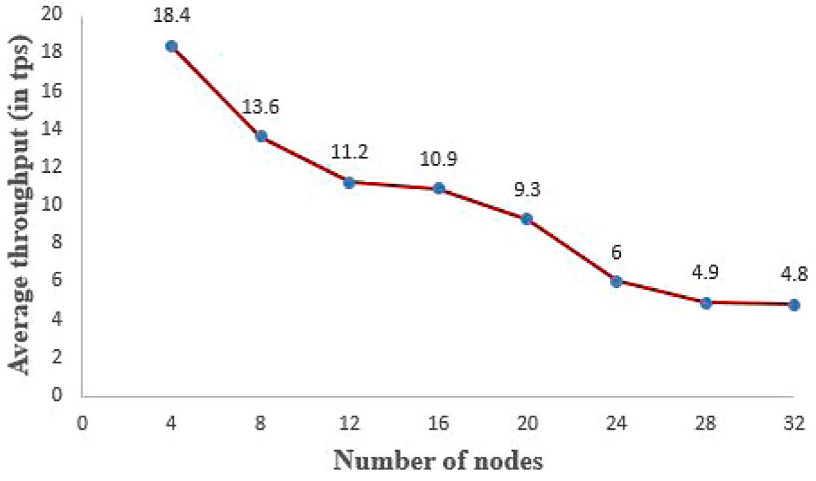


Fig. 17. Average throughput of the proposed framework with varying number of nodes.

updates. The percentage throughput of the proposed framework with different send rates of the transactions is shown in Fig. 16. For 10 tps send rate, the proposed framework achieves 36% throughput. It indicates that 3.6 transactions per second are successfully executed at 10 tps send rate in the proposed framework. We have observed that the proposed framework achieves throughput on average 13.6 tps.

An average throughput of the proposed framework with varying number of nodes, i.e., 4 to 32 nodes is shown in Fig. 17. It is observed that the throughput of the proposed framework is decreases with the increasing number of nodes. This causes a scalability issue which is due to the PoS consensus mechanism considered in the proposed framework. However, the PoS helps in achieving the higher fault tolerance compared to other consensus mechanisms. In future, this issue can addressed by increasing the block size and by considering the improved consensus mechanism.

4.3. Requirement analysis

The proposed framework offers data transparency and immutability, No single point of failure and non-repudiation, user's privacy, incentivized auction and distributed trustworthy environment.

4.3.1. Data transparency and immutability

Distributed ledger preserves the transparency of the transactions. Transactions are recorded on distributed ledger as append only feature

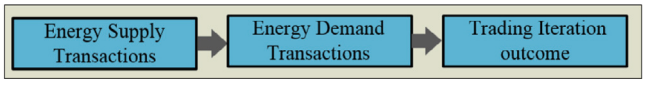


Fig. 18. Sample structure of the distributed ledger in the proposed framework.

only after the validation, and thus a block consists of valid transactions. All participants of the distributed ledger in the proposed framework have read access to all previous transactions on the ledger. For each trading iteration, distributed ledger creates three logical sub blocks like energy injection transaction responsible for storing energy supply related information, bidding transaction and trading transaction stores outcome of an auction instance. Once a block is added to the blockchain. A sample structure of the distributed ledger for auction iteration is given in Fig. 18.

4.3.2. No single point of failure and non-repudiation

The proposed framework overcomes single point failure problem unlike in the centralized system by storing all the transactions of energy-related data and trading data on a distributed ledger. All participants of the system has their own updated copy of the ledger. A node can get the updated copy of the ledger from peers, after recovery from any failure or offline mode. Ethereum blockchain allows a user to

decide a transaction amount that he can spend on particular transaction. No third party is involved to validate the transaction. Hence, user is sovereign entity who has all the rights to select lowest transaction amount. A transaction is digitally signed by initiator hence no one can deny its ownership.

4.3.3. User's privacy

The user's privacy requirements in energy trading are as follows:

1. No participant should learn a prosumer's energy generation share
2. No prosumer should learn a particular consumer's energy demand bid
3. Except a winner, no one should know who has purchased energy

The challenge in the distributed environment is that participants should not be able to identify initiator and beneficiary of the transaction even though they have access to all transactions. In the proposed framework, we use blockchain to mask every participant's original identity with pseudo identity, i.e., Externally Owned Account (EOA) address as digital identity of the participant. Here, ECDSA (Koblitz, 1987) generates keypair (pr,pu) for the user. Any number between 1 to 2^{256-1} is considered as a valid private key. Public key *pu* is derived using Eq. (3).

$$A_{pu} = G * A_{pr} \tag{3}$$

Public key A_{pu} for a user A is generated using elliptic curve multiplication. Here, G is the predetermined generator point on the curve and A_{pr} is a private key. As per the discrete logarithmic problem, computing A_{pr} from A_{pu} and G is very difficult (Johnson et al., 2001). Now, the generated public key is hashed using Keccak-256 hash function which generates 32-byte hash value as an output to generate account address, as given in Eq. (4).

$$Address = H(A_{pu}) \tag{4}$$

From these 32 bytes, last 20 bytes are considered as EOA address, and thus, each prosumer and consumer has unique EOA to perform the transactions in the proposed framework. All transactions are received at EOA address. In addition, EOA is used to define ownership of the energy tokens in the proposed framework.

The smart contracts in the proposed framework are also identified by their 32 bytes contract address. This address for each contract is generated after successful deployment of smart contract on the blockchain. The prosumers and consumers call a particular smart contract using contract account address, and thus proposed framework achieves user's privacy.

Here, each calling participant signs transaction using his/her private key. This transaction is verified using public key of the calling participant, and thus, EOA and contract account address provides anonymity to participants and smart contracts and preserves their privacy.

4.3.4. Incentivized auction

As discussed in Section 4.2, the proposed framework offers incentivized trading for the truthful bidders. In addition, winner percentage is more in the proposed framework than the existing frameworks.

4.3.5. Trustworthy distributed environment

The proposed framework builds trust among the participants using PoS consensus method. The assumption in PoS is that one having a maximum asset share would not perform any fraudulent activity. A designated peer is selected from prosumers having highest energy share during each trading instance. A designated peer creates a block of valid transactions. This block is added to the blockchain as append-only manner, i.e., once a block is added to the blockchain, it is nearly impossible to tamper that block. Hence, all peers are assured that all transactions on the blockchain are valid and non-tampered. As all nodes have read-only access to all transactions in the blockchain, the trading mechanism becomes transparent. Incentivized trading encourages consumers and prosumers to participate in the distributed energy trading. PoS consensus method, transparent nature of the blockchain, and incentivized trading offer a trustworthy distributed environment for the energy trading.

5. Conclusions

Smart grid improves the energy demand and supply process, where users can sell or purchase energy as per their interest instead of relying on net metering policy and fixed rate policy. However, current implementations of smart grid energy trading face the problems of user's privacy, transparency and immutability of energy related data, single point of failure, data repudiation, non incentivized auction and lack of trust on the energy distribution process. To address these problems, we have proposed a trustworthy and incentivized framework using distributed ledger technology and smart contracts. We have proposed different smart contracts *viz*; energy injection into smart grid, bidding, energy trading and utilization. The energy trading is performed by these contracts in peer-to-peer network of participants. The transactions performed by the participants for energy injection and bidding are recorded on a distributed ledger technology, ethereum blockchain platform and through PoS consensus mechanism. The proposed framework helps in maintaining the user's privacy through pseudo identity, data transparency and immutability using distributed ledger, resistance to single point of failure through decentralized data management, non-repudiation using elliptic curve based digital signature algorithm, and incentivized trading through Vickrey auction method. The analysis of the proposed framework is very encouraging to make smart grid energy management, a secured and trusted platform for distributing energy as per demand. In future, the scalability of the proposed framework can be further improved by increasing the block size and the improved consensus mechanism. In addition, energy forecasting can be implemented using feasible machine learning techniques to avoid energy crisis and for better preparedness.

CRediT authorship contribution statement

Ajit Muzumdar: Conceptualization, Design of study, Methodology, Software, Funding acquisition, Analysis and/or interpretation of data, Formal analysis, Validation, Writing - original draft, Writing - review & editing. **Chirag Modi:** Conceptualization, Design of study, Methodology, Software, Funding acquisition, Analysis and/or interpretation of data, Formal analysis, Validation, Writing - original draft, Writing - review & editing. **Madhu G.M.:** Conceptualization, Design of study, Methodology, Software, Funding acquisition, Analysis and/or interpretation of data, Formal analysis, Validation, Writing - review & editing. **C. Vyjayanthi:** Conceptualization, Design of study, Methodology, Software, Analysis and/or interpretation of data, Formal analysis, Validation, Writing - original draft, Writing - review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work is a part of the research project titled "Developing Smart Controller for Optimum Utilization of Energy and Trustworthy Management in a Micro Grid Environment [IMP/2019/000251]" with funding support under IMPRINT 2C.1 from Science and Engineering Research Board (SERB), Department of Science and Technology, Government of India. All authors approved the version of the manuscript to be published.

References

Aitzhan, N.Z., Svetinovic, D., 2018. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans. Dependable Secure Comput. 15 (5), 840–852.

Anon, 2014. Assessing blockchain's future in transactive energy. https://www.smartenergyportal.ch/assessing-blockchains-future-in-transactive-energy.

Anon, 2014. Blockchain scaling in pos. https://medium.com/coinmonks/pos-blockchain-scaling-8f9c0c485c0d.

Anon, 2019a. Black hats attack popular Russian stock-trading software. https://www.theregister.co.uk/2013/04/18/online_broker_malware/.

Anon, 2019b. Hyperledger fabric – hyperledger. https://www.hyperledger.org/projects/fabric.

Anon, 2019c. The next generation of distributed ledger technology — IOTA. https://www.iota.org/.

Bergquist, J., Laszka, A., Sturm, M., Dubey, A., 2017. On the design of communication and transaction anonymity in blockchain-based transactive microgrids. In: Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers, pp. 1–6.

Chaudhry, N., Yousaf, M.M., 2018. Consensus algorithms in blockchain: Comparative analysis, challenges and opportunities. In: 12th International Conference on Open Source Systems and Technologies (ICOSST). IEEE, pp. 54–63.

Dimitriou, T., Karame, G., 2013. Privacy-friendly tasking and trading of energy in smart grids. In: Proceedings of the 28th Annual ACM Symposium on Applied Computing, pp. 652–659.

Eyal, I., Gencer, A.E., Sirer, E.G., Van Renesse, R., 2016. Bitcoin-NG: A scalable blockchain protocol. In: 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI), pp. 45–59.

Fortino, G., Messina, F., Rosaci, D., Sarné, G.M.L., 2020. Using blockchain in a reputation-based model for grouping agents in the internet of things. IEEE Trans. Eng. Manage. 67 (4), 1231–1243.

Gao, J., Asamoah, K.O., Sifah, E.B., Smahi, A., Xia, Q., Xia, H., Zhang, X., Dong, G., 2018. Gridmonitoring: Secured sovereign blockchain based monitoring on smart grid. IEEE Access 6, 9917–9925.

Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H., Capkun, S., 2016. On the security and performance of proof of work blockchains. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. In: CCS '16, ACM, pp. 3–16.

2018. Grid singularity. https://gridsingularity.com/.

Gustafsson, M., 2017. Challenges for decision makers when feed-in tariffs or net metering schemes change to incentives dependent on a high share of self-consumed electricity. In: 44th Photovoltaic Specialist Conference (PVSC). IEEE, pp. 2025–2030.

Hahn, A., Singh, R., Liu, C.-C., Chen, S., 2017. Smart contract-based campus demonstration of decentralized transactive energy auctions. In: Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1–5.

Hwang, J., Choi, M.-i., Lee, T., Jeon, S., Kim, S., Park, S., Park, S., 2017. Energy prosumer business model using blockchain system to ensure transparency and safety. J. Energy Procedia 141, 194–198.

Iria, J., Soares, F., Matos, M., 2018. Optimal supply and demand bidding strategy for an aggregator of small prosumers. J. Appl. Energy 213, 658–669.

Jenkins, N., Long, C., Wu, J., 2015. An overview of the smart grid in Great Britain. J. Eng. 1 (4), 413–421.

Jha, I., Sen, S., Kumar, R., 2014. Smart grid development in India - a case study. In: 18th National Power Systems Conference (NPSC). IEEE, pp. 1–6.

Jimeno, J., Anduaga, J., Oyarzabal, J., de Muro, A.G., 2011. Architecture of a microgrid energy management system. Eur. Trans. Electr. Power 21 (2), 1142–1158.

Johnson, D., Menezes, A., Vanstone, S., 2001. The elliptic curve digital signature algorithm (ECDSA). Int. J. Inf. Secur. 1 (1), 36–63.

Joseph, A., 2015. Smart grid and retail competition in India: a review on technological and managerial initiatives and challenges. Proc. Technol. 21, 155–162.

Kappagantu, R., Daniel, S.A., 2018. Challenges and issues of smart grid implementation: A case of Indian scenario. J. Electr. Syst. Inf. Technol. 5 (3), 453–467.

Koblitz, N., 1987. Elliptic curve cryptosystems. J. Math. Comput. 48 (177), 203–209.

Kumari, A., Shukla, A., Gupta, R., Tanwar, S., Tyagi, S., Kumar, N., 2020. ET-DeaL: A P2P smart contract-based secure energy trading scheme for smart grid systems. In: IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 1051–1056.

Kwasnica, A.M., Sherstyuk, K., 2013. Multiunit auctions. J. Econ. Surv. 27 (3), 461–490.

Lamparter, S., Becher, S., Fischer, J.-G., 2010. An agent-based market platform for smart grids. In: Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems: Industry Track, pp. 1689–1696.

Leonhard, R.D., 2016. Developing renewable energy credits as cryptocurrency on ethereum's blockchain. Soc. Sci. Res. Netw. Electron. J. 1–15.

Li, Z., Bahramirad, S., Paaso, A., Yan, M., Shahidehpour, M., 2019. Blockchain for decentralized transactive energy management system in networked microgrids. Electr. J. 32 (4), 58–72.

Lucas, H., Ferroukhi, R., Hawila, D., 2013. Renewable energy auctions in developing countries. Int. Renew. Energy Agency, Abu Dhabi 1–52.

Makonin, S., 2018. HUE: the hourly usage of energy dataset for buildings in British Columbia. http://dx.doi.org/10.7910/DVN/N3HGRN.

Mannaro, K., Pinna, A., Marchesi, M., 2017. Crypto-trading: Blockchain-oriented energy market. In: Proceedings of the AEIT International Annual Conference, pp. 1–5.

Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L., Weinhardt, C., 2018a. Designing microgrid energy markets: A case study: The brooklyn microgrid. J. Appl. Energy 210, 870–880.

Mengelkamp, E., Notheisen, B., Beer, C., Dauer, D., Weinhardt, C., 2018b. A blockchain-based smart grid: towards sustainable local energy markets. J. Comput. Sci. Res. Dev. 33 (1), 207–214.

Mengelkamp, E., Staudt, P., Garttner, J., Weinhardt, C., 2017. Trading on local energy markets: A comparison of market designs and bidding strategies. In: 14th International Conference on the European Energy Market (EEM), pp. 1–6.

Myung, S., Lee, J.-H., 2018. Ethereum smart contract-based automated power trading algorithm in a microgrid environment. J. Supercomput. 1–11.

Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. http://www.bitcoin.org/bitcoin.pdf.

Nguyen, G.-t., Kim, K., 2018. A survey about consensus algorithms used in blockchain. J. Inf. Process. Syst. 14 (1), 101–128.

Onyeka Okoye, M., Yang, J., Cui, J., Lei, Z., Yuan, J., Wang, H., Ji, H., Feng, J., Ezeh, C., 2020. A blockchain-enhanced transaction model for microgrid energy trading. IEEE Access 8, 143777–143786.

2015. A smart and flexible energy system. https://piclo.uk/.

Rathnayaka, A., Potdar, V., Ou, M.H., 2012. Prosumer management in socio-technical smart grid. In: Proceedings of the CUBE International Information Technology Conference, pp. 483–489.

Saxena, S., Farag, H.E.Z., Brookson, A., Turesson, H., Kim, H., 2021. A permissioned blockchain system to reduce peak demand in residential communities via energy trading: A real-world case study. IEEE Access 9, 5517–5530.

Saxena, S., Farag, H.E.Z., Turesson, H., Kim, H.M., 2019. Blockchain based grid operation services for transactive energy systems. CoRR abs/1907.08725.

Saxena, S., Farag, H.E.Z., Turesson, H., Kim, H.M., 2020. Blockchain based grid operation services for transactive energy systems in active distribution networks. IET Smart Grid 3 (5), 646–656.

Siano, P., De Marco, G., Rolán, A., Loia, V., 2019. A survey and evaluation of the potentials of distributed ledger technology for peer-to-peer transactive energy exchanges in local energy markets. IEEE Syst. J. 13 (3), 3454–3466.

2017. Sonnen - energy is yours. https://sonnenbatterie.de/en/start.

Vickrey, W., 1961. Counterspeculation, auctions and competitive sealed tenders. J. Finance 16 (1), 8–37.

Wood, D.D., 2014. Ethereum: A Secure Decentralised Generalised Transaction Ledger.

Zhang, C., Wu, J., Zhou, Y., Cheng, M., Long, C., 2018. Peer-to-peer energy trading in a microgrid. J. Appl. Energy 220, 1–12.

Zhou, R., Li, Z., Wu, C., Chen, M., 2015. Demand response in smart grids: A randomized auction approach. IEEE J. Sel. Areas Commun. 33 (12), 2540–2553.

Zyskind, G., Nathan, O., Pentland, A., 2015. Decentralizing privacy: Using blockchain to protect personal data. In: Security and Privacy Workshops. IEEE, pp. 180–184.

Ajit Muzumdar is currently working as a research scholar in the department of computer science and engineering at National Institute of Technology Goa (NIT Goa). He has received M.E. degree in computer engineering from University of Pune, India in 2013. He has a work experience as an Assistant Professor in Sanjivani College of Engineering, India. His research interest include Blockchain, Cryptography, Game Theory, Smart Grid and Data Mining. Apart from publishing good quality papers, he is an active researcher and member of smart grid and blockchain research Lab at NIT Goa.

Dr. Chirag Modi is an Assistant Professor of Computer Science and Engineering at National Institute of Technology Goa since 2014. He has obtained his Ph.D (2010–2014) and M.Tech (2008–2010) degree in Computer Engineering from National Institute of Technology Surat (NIT Surat), India and did his B.E in Computer Engineering from Sardar Patel University, India. His research interest includes Information Security and Privacy, Cryptography, Cloud Security, Network Security, Intrusion Detection and Privacy Preserving Data Mining. He has published many papers in reputed journals and international conference proceedings, which have good number of citations. He has received the Young scientist award in specialization of Cloud Computing (2015) from VIFRA, Chennai, India. He holds Best Review Paper Award (2015), from Journal of Network & Computer Applications (JNCA), Elsevier, San Diego, USA. He holds first Position in the "National level workshop and competition on Ethical Hacking", conducted by Wegillent Inc. in association with IIT Roorkee, at NIT Surat, 2013. He holds research funded project titled "Developing Smart Controller for Optimum Utilization of Energy and Trustworthy Management in a Micro Grid Environment (IMP/2019/000251)" with funding support under IMPacting Research INnovation and Technology-2 C1 (IMPRINT-2 C1) by Science and Engineering Research Board (SERB), Department of Science and Technology, Government of India. He has completed research funded project titled "Designing out of VM Monitoring based Virtual Machine Introspection Framework for securing virtual environment of cloud computing" from

the SERB, DST, GOI. He has established Cloud Computing and Security Lab, Smart grid and Blockchain Research Lab at NIT Goa.

Madhu G.M. is currently working as a research scholar in the department of electrical and electronics engineering at National Institute of Technology Goa (NIT Goa). He has received M.Tech degree in Power Systems degree from UBDT College of Engg. Karnataka, India in 2017. His research interest include Smart Grid, Internet of Things, Optimization Algorithm Development, MPPT and control of Grid Integrated PV, Wind and Battery System. He is an active researcher and member of smart grid and blockchain research Lab at NIT Goa.

Dr. C. Vyjayanthi is an Associate Professor in the Department of Electrical and Electronics Engineering at National Institute of Technology Goa since 2014. She has obtained her Ph.D in 2011 from Indian Institute of Science, Bangalore in the area of Power Systems, M.Tech in 2005 from Anna University in Power Systems and B.Tech in 2001 from JNTU Hyderabad in the area of Electrical and Electronics Engineering. Before joining NIT Goa, she was working in the capacities of Manager (R&D Team) and Sr. Manager (R&D Team) at Power Research and Development Consultants Pvt. Ltd., Bangalore, India from October 2010 December 2014. She worked as a lecturer at Auroras Engineering College, Hyderabad, India, July 2001November 2002. Her research interest includes Restructured Power Systems; Planning, Operation and Control of Power Systems; Electric Arc Furnace Operations; Smart Electric Grids; Flexible AC Transmission Systems; AC/DC Microgrids and Cyber Security. She has published many papers in reputed journals and international conference proceedings. She holds two research funded projects viz; (1) "Development of a Multipurpose Intelligent Controller for a Nano Grid Operation" from Ministry of New and Renewable Energy, India. (2) "Development of coordination control schemes for hybrid AC/DC micro grids for a stable and reliable system operation", Science and Engineering Research Board (SERB), DST, India. She is an active member of Blockchain Research Lab at NIT Goa. She is Co-Investigator of research funded project titled "Developing Smart Controller for Optimum Utilization of Energy and Trustworthy Management in a Micro Grid Environment (IMP/2019/000251)" with funding support under IMPacting Research INnovation and Technology-2 C1 (IMPRINT-2 C1) by Science and Engineering Research Board (SERB), Department of Science and Technology, Government of India.