A Consortium Blockchain-Based Energy Trading for Demand Response Management in Vehicle-to-Grid

Shubhani Aggarwal and Neeraj Kumar, *Senior Member, IEEE*

***Abstract*—In this paper, we propose a Peer-to-Peer (P2P) energy trading scheme between EVs and the SPs to manage the demand response in V2G environment. Unlike the traditional schemes, which consists of complex energy-transportation meshes, the proposed scheme achieves a balance between demand and response by providing incentives to EVs out of their self-interests. However, the online transactions security and privacy protection of EVs poses challenges with respect to confidentiality and integrity preservation. To cope up with the issues, we design a consortium blockchain-based scheme to ensure secure energy transactions between EVs and the SPs without trusted third-party intervention. Moreover, the energy pricing and the amount of traded energy problems for demand response are solved by a double auction mechanism to maximize the social welfare. Numerical results based on a real-time implementation on a private Ethereum network having smart contract demonstrated that the auction-based mechanism achieves social welfare maximization with privacy protection of online transactions between EVs and the SPs. The results obtained show that the rate of convergence, scalability metric average latency, and standard deviation of the energy transactions have been improved by approximately 18.18%, 15%, and 28.1%, respectively in comparison to the existing schemes. Moreover, security and privacy analysis of the proposed scheme shows that it improves the transaction security substantially in comparison to the existing state-of-the-art proposals.**

***Index Terms*—Vehicle-to-Grid, consortium blockchain, demand response management, double auction, social welfare maximization, privacy and security.**

I. Introduction

FROM the past few years, the power industry has gone through rapid changes which lead to various revolutions in smart grid, micro-grid, Vehicle-to-Grid (V2G). These technologies have provided an extraordinary transformation from the traditional power grids to smart grid with an integration of Internet and Information Communication Technologies (ICT). Also, digital technology allows bi-directional communication between the customers and service providers (SPs) alongwith sensing in transmission lines, which makes the power grid smart and is known as the *"Smart Grid"* [1]–[3]. It consists of smart homes, SPs, electric vehicles (EVs), smart appliances, smart meters, renewable energy, consumer engagement, distribution intelligence, operation centers, and plug-in hybrid electric vehicles (PHEVs) to control and manage the smart grid data. It is also defined as a network of transmission lines, substations, transformers, and distribute the electricity from one grid center to the smart homes, buildings, and industries [4]. It also provides an efficient way to transmit electricity to customers to reduce the peak demand of end-users, increases the integration of renewable energy resources, reduces operational and maintenance costs, and quick restoration after energy disturbances. Thus, it can be viewed as *"basic building blocks"* to support the energy requirements of both the industrial and residential users.

V2G is an emerging technology in the smart grid that supports energy exchange between EVs and the SPs. The power fluctuations by the diffusion of renewable energy resources in V2G is solved by EVs, which are being used in energy trading for demand response management [5], [6]. A large number of EVs absorb an excessive amount of energy during the off-peak time and get back the same energy to the grid during the peak time. They provide an efficient and effective solution to smooth the peak load and balance the demand-supply mismatch in V2G energy trading scenarios [7]–[9]. On the other hand, the widespread popularity of EVs among the consumers may impose a severe burden on V2G energy trading for demand response management. It is expected that by 2025, there will be around 8.4 million EVs on road globally [10]. Thus, there is a need for a reliable solution to furnish future energy requirements of industrial and residential users while supporting EVs' charging and discharging needs. Therefore, several research proposals have been put forward to study V2G energy trading for demand response management. For example, authors in [9] proposed a distributed coordination mechanism that enables charging and discharging operations on EVs. Similarly, authors in [11] proposed an architecture of a household user that enables energy transactions between the consumer and the load-server. They have used several smart devices like smart appliances, EVs for vehicle-to-home and V2G connections to reduce the electricity consumption and payment. In social hotspots like charging stations, EVs can trade energy in a localized Peer-to-Peer (P2P) manner (*e.g.,* vehicle-to-vehicle, V2G) [12]. Cao *et al.* [13] proposed an intermediate model to manage the EVs charging plan at charging stations for trip

Manuscript received February 1, 2021; revised May 14, 2021; accepted July 25, 2021. Date of publication July 29, 2021; date of current version September 17, 2021. This work was supported by the Cybersecurity Research Center, Prince Mohammad Bin Fahd University (PMU), Kingdom of Saudi Arabia with acknowledgement number (PCC-Grant-202119). The review of this article was coordinated by Dr. Mohammad Rastegar. *(Corresponding author: Neeraj Kumar.)*

Shubhani Aggarwal is with the Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, Patiala, Punjab 147004, India (e-mail: saggarwal20_phd17@thapar.edu).

Neeraj Kumar is with the Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, Patiala, Punjab 147004, India, with the Department of Computer Science and Information Engineering, Asia University, Taichung City 413, Taiwan, and also with the School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand 248007, India (e-mail: neeraj.kumar@thapar.edu).

Digital Object Identifier 10.1109/TVT.2021.3100681

duration and mobility uncertainty. This system model is based on third-party authenticator that may tamper and manipulate the data by using various malicious activities. Similarly, authors in [14] proposed a centralized system to manage, audit, and validate the energy transactions in the smart grid.

Despite the above-mentioned advantages, the wide-area deployment of V2G still confronts several challenges as follows. Firstly, there is lacking of a distributed security mechanism for V2G energy trading because traditional centralized mechanisms rely on a trusted third-party authenticator to manage and audit the energy transactions, which leads to a series of security threats such as denial of service attacks, data manipulation, and replay attacks. Secondly, there lacks an efficient V2G energy trading mechanism for demand response management. For example, authors in [8], [9], [15]–[17] proposed EVs charging and discharging scheme without considering security and privacy issues in V2G energy trading. They have announced the EV's private information to all the participants and have assumed that this information is known to everyone in energy trading for demand response management. With this, EV's long charging time and limited navigating range makes the V2G energy trading process more complicated. Without security and privacy concern in V2G environments, connected entities (EVs and the SPs) can be hacked and once hackers can gain control, they can tamper the functionality of these entities by stealing the energy data. This can affect the overall functionality of various appliances used in this environment. The data, energy, and information shared by EVs and other V2G entities, such as the local aggregator, communication and authentication servers, billing center, and control center, must be secured [18], [19]. So, there is a strong need to design a distributed security mechanism in V2G energy trading for demand response management, which can effectively maximizes the economic benefits of EVs and the SPs.

Recently, blockchain technology with advantages of decentralization, privacy, security, and trust management has been introduced in V2G energy trading for demand response management. It is a P2P distributed ledger technology (DLT), which enables energy trading to be executed in decentralized, transparent, private, and secure V2G market environments [20]–[23]. It stores the energy transactions securely on the network in a permanent way. A digital currency named *"NRGcoin"* based on blockchain was presented for renewable energy trading in smart grids. A demonstration platform for renewable energy exchange using NRGcoin was proposed in [24]. Similarly, authors in [12] used a blockchain with multi-signature to address the transaction security problems in decentralized smart grids.

Motivated from the aforementioned challenges and constraints, in this paper, we exploit the consortium (permissioned) blockchain to design a secure P2P energy trading for demand response management in a V2G environment. The consortium blockchain is a specific blockchain with multiple authorized nodes having Proof-of-Authority (PoA) consensus to establish the DLT with moderate cost. The energy transaction records between EVs and the SPs are uploaded to the nodes after encryption using cryptographic primitives [25]. Nodes of the blockchain network triggered the smart contract to audit the transactions and record them into the shared ledger [26]. This ledger is accessed by EVs and the SPs, which are connected as participants on the consortium blockchain. Moreover, the energy pricing and the amount of trade energy between EVs and the SPs needs to be optimized for demand response management in a V2G environment.

A. Motivation

V2G technology plays an important role in balancing the energy demand and supply between EVs and the SPs for demand response management. But, there are challenges of security and privacy preservation, data manipulation, transparency, in V2G environments. It may increase the gap between energy demand and supply. Hence, there is a requirement for an energy trading mechanism to stabilize the energy demand and supply. In literature, a lot of research proposals exist for demand response management between EVs and the SPs. However, only limited work has been done using a double auction mechanism having consortium blockchain in V2G environments for security and privacy preservation [27], [28]. Hence, we propose first-price reverse auction and double auction using game theory by considering private blockchain for social welfare maximization in V2G environments.

We also propose P2P energy trading to provide social welfare maximization for both EVs and the SPs. The proposed model maintains a balance between demand and the supply using blockchain technology in V2G environments. Thus, SPs submit sealed bids on blockchain network by requesting the energy by EVs. Using first-price reverse auction mechanism-based smart contract, EVs select the submitted bids having lowest price value. After the selection of EVs and the SPs, the problems of amount of traded energy and energy pricing are solved by a double auction mechanism to maximizes the social welfare in V2G environments.

B. Contributions of this paper

The major contributions of this paper are summarized as follows.

- A blockchain-based secure energy trading scheme for demand response management between the EVs and the SPs is presented.
- To optimize energy pricing and the amount of traded energy, a double auction mechanism is proposed between EVs and SPs to maximizes social welfare with privacy preservation.
- To validate the proposed scheme, we designed a framework for a private Ethereum network. The framework is based on lightweight virtualization and supports dynamic configuration of the network.
- We evaluated the proposed scheme using different performance evaluation parameters to test its efficacy in comparison to the existing state-of-the-art proposals.

C. Organization of the Paper

Rest of the paper is organized as follows. Section II elaborates the summary of related work. Detailed description of the system model is illustrated in Section III. The problem definition of the energy trading scheme for demand response management is discussed in Section IV and the solution is provided in Section V. Simulation results and analysis are discussed in Section VI and finally, Section VII concludes the paper.

II. Related Work

In this section, we review the P2P energy trading literature survey between the EVs and the SPs for demand response management in a V2G environment. Several research articles have been published, which explores blockchain in a V2G environment to handle the demand response management between the EVs and the SPs [29]. For example, Hassija *et al.* [30] proposed a blockchain-based V2G network for data sharing and energy trading. Authors used the game theory between the grid and the vehicles for the energy transactions at an optimized cost. Similarly, authors in [31] proposed a blockchain-based energy trading model for EVs to minimize the power fluctuations. Li *et al.* [32] proposed a P2P blockchain-based scheme based on a credit-based payment system, which reduces transaction latency. Garg *et al.* [33] presented a blockchain-oriented hierarchical authentication mechanism based on the elliptic curve cryptography (ECC) in V2G networks. They have classified the system model into four phases: (i) System Initialization, (ii) Registration, (iii) Hierarchical Mutual Authentication, and (iv) Consensus; wherein blockchain's distributed ledger has been employed for transaction execution in distributed V2G environments. Similarly, authors [34] proposed a DLT, which is used to maintain the network information between the vehicles and roadside units. They have used the ECC for mutual authentication and employed that the proposed scheme is lightweight and scalable for V2G networks.

Keeping in mind the extraneous load enforced by EVs on SPs in V2G environments, a secure demand response management scheme based on game theory may be beneficial to reduce the demand-supply issues [35]–[37]. In this, blockchain technology provides security and privacy to the EVs [38], [39]. For example, Su *et al.* [40] proposed a contract theory for energy trading among EVs. They have used the permissioned blockchain platform to allocate renewable energy for EVs. Similarly, Kumar *et al.* [41] proposed a secure technique for EVs-energy management based on the coalition game in V2G environments. All players in the game negotiate with one another for buying and supplying the energy and decide for energy exchange based on individual payoff function. This payoff function was used for preventing misuse of electricity consumption. On the similar lines, Xia *et al.* [42] used a bayesian game for optimal pricing scheme between the EVs in V2G energy trading. The pricing game has been implemented by the dedicated smart contract based on blockchain, which guarantees its trustworthiness, security, and reliability. The evaluation results show that the degree of approximation can reach up to 98% when the pricing ranges of buyers and sellers are close.

Kaur *et al.* [43] proposed a software-defined networking and blockchain-based cyber-physical privacy and security for EVs in the smart grid. They have designed a mutual authentication protocol based on ECC and also cost-efficient model in terms of communication and computation costs.

Tsao *et al.* [44] leveraged a blockchain in sustainable microgrids for real-time pricing in demand response system. They have used the fuzzy programming to provide equillibrium between the demand and the supply under uncertain conditions. Their case study evaluates that here is an increase of 1.68% and 2.61% of profitability and satisfaction percentage of customers, respectively and decrease of 0.97% impacts on environment.

Muzumdar *et al.* [45] proposed a Vickrey auction for energy trading using blockchain in smart grid. Authors used the proof of stake consensus on Ethereum to offer trust and privacy of participants and transparency in the system. Their experimental results show the better throughput, average cost of energy, and bidding transactions in comparison to existing ones. Anoh *et al.* [46] proposed a clustering method for energy trading among prosumers. Authors have used the Stackelberg game in virtual microgrids and optimize the utility for producers and consumers by formulation the Stackelberg Equilibrium. Similarly, Doan *et al.* [27] proposed a double auction based on P2P energy trading to maximize the social welfare for both sellers and buyers. They have formulated the model using Stackelberg game and find an optimal solution by evaluating Stackelberg Equilibrium. They have implemented their experiments on Hyperledger using chaincode. Kalakov *et al.* [28] used the double auction to create a decentralized-based transactive energy model with demand response. Their evaluation results show that the proposed energy model provides better privacy and security and minimize the loss in long transmission of energy. The comparison of the proposed scheme with the existing proposals is as shown in Table I.

From the literature survey, we have observed that the blockchain technology has not been widely used in V2G energy trading for demand response management. Therefore, we design a consortium blockchain-based secure energy trading scheme for demand response management in a V2G environment. The proposed scheme is based on a double auction mechanism that defines energy transactions between the EVs and the SPs. It provides a platform for balancing the demand-supply in V2G energy trading and ensures optimal service to the EVs and the SPs by maximizing the social welfare with privacy preservation.

III. System Model

A blockchain-based secure energy trading model between EVs and SPs in a V2G environment is as shown in Fig. 1. The interaction between the EVs and the SPs realizes V2G services through energy trading in demand response management. This system model consists of three main entities, *i.e.,* EVs, SPs with generator, and the blockchain network. Each node on the blockchain network has its own ledger with a wallet address that stores the energy transaction history and accepts the digital cryptocurrency at the time of energy trading for demand response management. The information stored on the blockchain network is transparent and immutable. So, no hacker or malicious activity can change the blockchain data because it has been secured by cryptographic hash primitives [47]. The functionality and speciality of each entity in which EVs represent the demand side and SPs represent the supply side are described as follows.

TABLE I
COMPARISON OF OUR SCHEME WITH THE EXISTING PROPOSALS

References	Detail Description	Model	Consideration of EVs	Network	Consensus Mechanism	Load Control	Social Welfare Maximization
[40]	Secure charging scheme for EVs in energy blockchain	Contract theory	✓	-	Delegated BFT	✓	✓
[41]	Secure energy management in V2G environments	Bayesian coalition negotiation game	✓	NS2	-	✓	×
[42]	Blockchain-based vehicle-to-vehicle energy trading scheme for Internet of vehicles	Bayesian game	✓	Fabric	PoA	✓	✓
[43]	Provides blockchain solution for EVs in smart grid	Elliptic Curve Cryptography	✓	Ethereum	-	✓	×
[44]	Provides sustainability for real-time price-based demand response programs	Robust Multi-objective Optimization	×	-	-	✓	×
[45]	Provides trustworthy smart grid energy trading	Vickrey auction	×	Ethereum	Proof of stake	×	×
[46]	P2P energy trading in virtual microgrids of smart grid	non-cooperative Stackelberg game	×	LoRaWAN	-	✓	×
[27]	Provides P2P energy trading	Double auction	×	Hyperledger Fabric	-	✓	✓
[28]	Provides blockchain-based transactive model with demand response	Double auction	×	JADE	-	✓	×
Our Proposed Work	Consortium blockchain-based energy trading for demand response management	First-price auction + Double auction	✓	Ethereum	PoA	✓	✓

A. Electric Vehicles

EVs play a vital role in a V2G environment. They have the capability of bi-directional energy trading. They can act as energy producers and provide electricity by discharging their battery during peak time. On the other side, they can also act as energy consumers by charging their battery with electricity during the peak-off time. They can adjust their charging and discharging nature and actively participate in a V2G energy trading to maximize their payoff. The interactions of the EVs with the grid realize V2G services through a two-way flow of energy, *i.e.,* energy flow from the EVs to the grid and the grid can send this energy to EVs at peak time. In this paper, as a consortium blockchain-based system, EVs can communicate to SPs for charging the batteries. Those EVs who need electricity services can determine their service demand to purchase the energy. They take energy services from those SPs, which have fewer energy prices on the blockchain network.

B. Service Providers

SPs with incorporated control of integrated communication resources and computing resources provide energy services to the EVs. To have an energy trading connection between EVs and SPs, SPs announce a reasonable price to the EVs for selling the services. EVs can drive their service demand for purchasing services based on the announced prices. Each SP has its own generator that generates the energy for energy trading during the peak timings. So, there is no need to charge the SPs as it has its own generator to produce energy from renewable energy resources.

C. Blockchain Network

The operation of the blockchain-based secure energy trading scheme for demand response management is described as follows. In the beginning, the nodes of the blockchain network register a request to the certifying authority for obtaining a public key (PU) and a private key (PK) using Public-key infrastructure (PKI) to ensure integrity and wallet security [48], [49]. These keys are generated and distributed by a legitimate authority. This authority provides a unique token to the nodes for identity through the registration information as shown in the Fig. 2. Nodes find the wallet address by adding them into the blockchain network for demand response management, which is described in the next section.

The blockchain network designs a scheme, which specifies the relationship between the EVs and the SPs, *i.e.,* amount of energy needed by EVs from the SPs and the reward, *i.e.,* payment to the

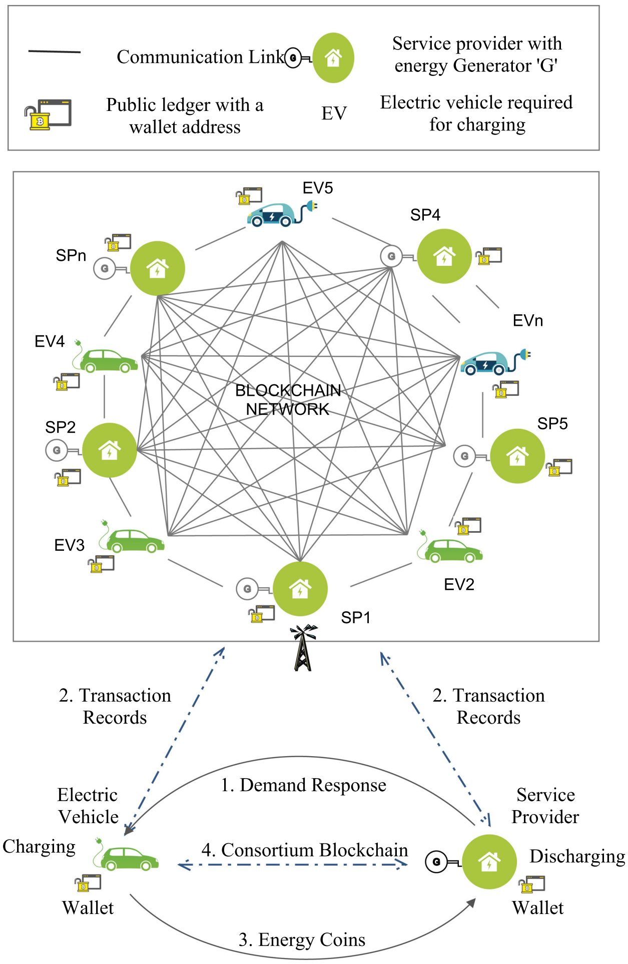

Fig. 1. System model.

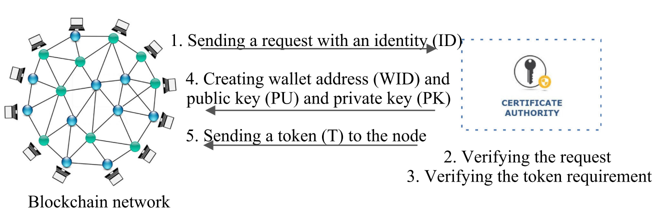

Fig. 2. Token registration of the nodes on blockchain network.

SPs in terms of energy coins [50]. Each node on the blockchain network has an account to store all transaction records, and the corresponding wallet for managing energy coins in the account. During P2P energy trading for demand response management, first EVs send request for energy demand on the blockchain network then, the corresponding SPs accepted an energy request and submit bids for selling the energy according to their supply. Nodes on the blockchain network act as energy brokers for EVs and the SPs to execute energy bidding and transaction through a double auction mechanism. The energy coins are transferred to the wallet address of SPs from the wallet address of the EVs. The authentication of the payment can be verified by checking the last block of the blockchain. The new transaction record is verified and digitally signed by the nodes then, only broadcasted on a consortium blockchain (Fig. 1).

All the transactions are done between the EVs and the SPs are collected and recorded within a certain amount of time. Then, these transactions are encrypted, digitally signed, and structured into blocks. Also, these blocks are broadcasted on the blockchain network for verification and validation, which is done by Proof of Authority (PoA) consensus mechanism. Fake and invalid transactions are discarded. PoA is one of the most mature versions of blockchain technology [51]. It is faster than other algorithms, more scalable, and does not depend on mining. Unlike proof-of-work and proof-of-stake, it does not require miners to be involved at all. The rights to generate new blocks are awarded to nodes that have proven their authority to do so, which is known as *Validators*. They need to confirm their real identities to approve their accounts. A node must be willing to invest money and put his reputation at stake. A tough process reduces the risks of selecting questionable validators and incentivize long-term commitment to the blockchain. The method for selecting validators must be equal to all nodes. The identity of validators must be verified to maintain the integrity of the blockchain. As a result, there is no need to spend vast amounts of resources to maintain the network's performance. The authority of the node is the guarantor of the transaction's validity. Therefore, such a network is protected against manipulation by the owners of richer nodes. Also, PoA validators must pass a series of checks to confirm the reliability of the system model.

IV. Problem Definition

In this section, we present the problem definition of energy pricing and the amount of energy traded between the EVs and the SPs to maximize the overall social welfare (i.e., the sum of nonlinear utilities). In any region, for establishing a real-time energy trading market for demand response management, a blockchain enriched smart contract can communicate with EVs and the SPs. Nodes of the blockchain network "$Node_n$" can facilitate energy trading between them and acting as an energy broker, which manages local EVs to execute energy trading operations for demand response management. A number of nodes (EVS and SPs) is denoted by n, where n $\in Node_n \triangleq$ (1,2,3..n). Let us denote a set of charging EVs in the blockchain network as $EV \triangleq (EV_i^n | i \in E, n \in Node_n)$, (E =0,1,2,3..I). The discharging SPs in the blockchain are denoted as $SP \triangleq (SP_j^n | j \in Z, n \in Node_n)$, (Z =0,1,2,3..J). $e_i^{n,min}$ and $e_i^{n,max}$ are the minimum and maximum energy needed for $EV_i^n \in Real$ on the blockchain network, respectively. So, the $Node_n$ must provide $e_i^{n,min}$ energy to EV_i^n for normal driving.

Here, e_{ij}^n is the energy demand of EV_i^n for discharging supply by SP_j^n in $Node_n$. The energy demand vector of EV_i^n is $E_i^n \triangleq (e_{ij}^n | j \in Z)$. In the blockchain network $Node_n$, the total energy demand of all the charging EVs is $E^n \triangleq (E_i^n | i \in E)$. The state of energy before charging the EVs' battery is SoC_i^n and the battery capacity of an EV_i^n is EV_i^{cap}. The satisfaction function

U_i of EV_i^n is :

$$U_i(E_i^n) = w_i \left[ln \left(\eta \sum_{j=1}^{J} (e_{ij}^n - e_i^{n,min}) + 1 \right) \right]$$
$$w_i = \sigma / SoC_i^n \quad (1)$$

where, w_i is the charging willingness of EV_i^n, η is an average charging efficiency from discharging, and σ is a constant.

For SPs, s_j^n is the amount of energy supply from SP_j^n to the EV_i^n in the $Node_n$. The energy supply for demand response management vector of SP_j^n is $S_j^n \triangleq (s_{ji}^n | i \in Real)$. In the blockchain network $Node_n$, the total energy supply of SP_j^n is $S^n \triangleq (S_j^n | j \in Z)$. The maximum energy supply is $S_j^{n,max}$. So, the cost function L_j of SP_j^n is:

$$L_j(S_j^n) = c_1 \sum_{i=1}^{I} (s_j^n)^2 + c_2 \sum_{i=1}^{I} (s_{ji}^n), \quad (2)$$

where c_1 and c_2 are cost factors and $c_1 \geq 0$.

Since the EVs want to maximize their utilities while the SPs try to minimize their cost, whereas $Node_n$ of the blockchain network not only tries to meet the demand of EVs and SPs, but also maximize energy allocation efficiency for demand response management. The blockchain network addresses the social welfare maximization problem (SWM) to allocate energy between the EVs and the SPs for demand response management. Here, the objective function of SWM problem is described as follows:

$$SWM : \max_{E_n, S_n} \sum_{i=1}^{I} U_i(E_i^n) - \sum_{j=1}^{J} L_j(S_j^n) \quad (3)$$

$$Subject\ to : e_i^{n,min} \leq \eta \sum_{j=1}^{J} e_{ij}^n \leq e_i^{n,max}, \forall_i \in E,$$
$$\sum_{i=1}^{I} s_{ji}^n \leq S_j^{n,max} \forall_j \in Z,$$
$$\rho s_{ji}^n = e_{ij}^n, \forall_i \in E, \forall_j \in Z,$$
$$e_{ij}^n \geq 0, \forall_i \in E, \forall_j \in Z, . \quad (4)$$

Here, ρ is an average energy transmission efficiency for demand response management between the EVs and the SPs. The objective function in Eq. (3) is concave with compact and convex constraints, so there exists a unique optimal solution using the method Lagrangian multipliers (non-linear programming solution technique) [51].

$$L_1(E^n, S^n, \lambda, \beta, \alpha, \gamma, \theta) = \sum_{i=1}^{I} U_i(E_i^n) - \sum_{j=1}^{J} L_j(S_j^n)$$
$$+ \sum_{i=1}^{I} \lambda_i \left(e_i^{n,min} - \eta \sum_{j=1}^{J} e_{ij}^n \right) + \sum_{i=1}^{I} \beta_i (\eta \sum_{j=1}^{J} e_{ij}^n - e_i^{n,max})$$
$$+ \sum_{j=1}^{J} \alpha_j \left(\sum_{i=1}^{I} s_{ji}^n - S_j^{n,max} \right) + \sum_{i=1}^{I} \sum_{j=1}^{J} \gamma_{ij} (\rho s_{ji}^n - e_{ij}^n)$$
$$- \sum_{i=1}^{I} \sum_{j=1}^{J} \theta_{ij} e_{ij}^n \quad (5)$$

Here, $\lambda_i, \beta_i, \alpha_j, \gamma_{ij}, \theta_{ij}$ are Lagrange multipliers for the constraints in (4). Hence, the optimal solution of *'SWM'* meets following conditions:

$$\nabla_{e_{ij}^n} L_1(E^n, S^n, \lambda, \beta, \alpha, \gamma, \theta)$$
$$= \frac{\eta w_i}{(\eta \sum_{j=1}^{J} e_{ij}^n - e_i^{n,min}) + 1}$$
$$- \eta \lambda_i + \eta \beta_i - \gamma_{ij} - \theta_{ij} = 0 \quad (6)$$
$$\nabla_{s_{ij}^n} L_1(E^n, S^n, \lambda, \beta, \alpha, \gamma, \theta)$$
$$= -2c_1\, s_{ji}^n - c_2 + \alpha_j + \rho \gamma_{ij} = 0 \quad (7)$$

For the SWM problem, it is necessary that the blockchain network has true and complete information of all EVs' utility and cost functions, and thus to solve the problem using Eqs. (6) an (7).

V. Auction Mechanism

In this section, we have used an auction mechanism to maximize the social welfare problem between the EVs and the SPs for demand response management. Initially, a sealed-bid first price reverse auction has been used to find the lowest bid from all the submitted bids by the SPs to charge the battery of the EVs. Then, a double auction has been used to find the final trading prices and the amount of traded energy for demand response management, which is useful and ensures information asymmetric of EVs. More specifically, each charging EV $'EV_i'$ mentions the required energy for charging with auction bid price $b_{ij} \geq 0$ on the blockchain network. In order to response EV_i, each SP_j submits a different bid price $p_{ji} \geq 0$ on the blockchain network. Here, blockchain having smart contracts acts as an auctioneer to perform a reverse auction according to buying prices from the EVs and selling prices from the SPs. After receiving these prices, the auctioneer solves the selection of *'SP'* problem, and thus allocates SP_j (having lowest-bid from all the submitted bids) to the EV_i for demand response management to achieve effective price market as described in the Algorithm 1.

A. *Different Roles in Auction Mechanism*

The nodes used in the blockchain network are working under the auction mechanism and their description is described as follows.

- *Electric Vehicles:* The bid price vector of EV_i^n to buy a energy for charging the battery from SPs on the blockchain network is $Bid_i^n = (b_{ij}^n | j \in Z)$. All bid prices of the EVs on the blockchain network are denoted as $B^n = (Bid_i^n | i \in E)$. So, EV_i^n needs to solve an optimal energy buying problem (EBP) by computing an optimal bid price

Algorithm 1: Selection of the Service Provider.

Input: N: The number of EV requests for charging the battery.
M: The number of SPs who have submitted bids for discharging the energy.
p_{ji}: represents the bids submitted by the SPs, where, *i* represents the bid for an i^{th} EV and *j* represents the SP_j.
Output: Selection of the SP_j used in energy trading for demand response management.

procedure FunctionN, M
  for $(i = 1; i \leq N; i++)$ **do**
    Select the EV_i
    Submit the auction bid price b_{ij} and required energy E_i by EV_i on the blockchain network
    for $(j = 1; j \leq M; j++)$ **do**
      Select the SP_j
      Submit the auction bid p_{ji} by the SP_j on the blockchain network
    end for
  end for
  if $(b_{ij} \geq p_{ji})$ **then**
    Calculate the Optimal_Prices for EV_i and SP_j as defined in Eqs. 15 and 16 ▷By Auctioneer
    $Optimal\_P.Value_1$ is used as $pay_i(Bid_i^n)$ for EV_i
    $Optimal\_P.Value_2$ is used as $Rew_j(P_j^n)$ for SP_j
  else
    No energy trading for demand response management.
    EV sends an energy request again on the blockchain network for demand response management.
  end if
end procedure

as follows:

$$EBP : \max_{B_i^n}[U_i(E_i^n) - pay_i(Bid_i^n)] \tag{8}$$

where $pay_i(Bid_i^n)$ is the payment function of EV_i^n given by the auctioneer.

- *Service Providers:* The bid price vector of SP_j^n for selling energy on the blockchain network is denoted as $P_j^n = (p_{ji}^n | i \in E)$. The bid price matrix of the SP_j^n is $SP^n = (P_j^n | j \in Z)$. So, SP_j^n solves an optimal energy selling problem (ESP) by determining optimal bid price:

$$ESP : \max_{P_j^n}[Rew_j(P_j^n) - L_j(S_j^n)], \tag{9}$$

where $Rew_j(P_j^n)$ is a reward function of SP_j^n given by the auctioneer.

- *Blockchain as an Auctioneer:* The auction bid prices are submitted by the EVs and the SPs to the blockchain network to perform a double auction mechanism. EVs and SPs solve their energy buying and selling problems, respectively to update the bid price vectors according to the auctioneer's newly calculated $Optimal\_Prices$ as demand and supply for EVs and the SPs, respectively. The blockchain network acts as an auctioneer by triggering the smart contracts on the nodes on the network. The auctioneer solves the allocation problem optimally 'OAP' to find the traded amount of energy as follows:

$$OAP : \max_{E^n, S^n} \sum_{i=1}^{I} \sum_{j=1}^{J} [b_{ij}^n ln e_{ij}^n - p_{ji}^n s_{ji}^n], \tag{10}$$

From Eq. (10), if the bid prices are known then, an auctioneer can solve the problem 'OAP'. Note that both Problems 'OAP' and 'SWP' have same subject to constraints as described in Eq. (4). So, here also we carry out constraint relaxation through Lagrangian method 'L_2'. To ensure that the optimal solution of one problem solves the other problem. Therefore, L_2 and L_1 have the same Lagrange multipliers as follows:

$$\nabla_{e_{ij}^n} L_2(E^n, S^n, \lambda, \beta, \alpha, \gamma, \theta)$$
$$= \frac{b_{ij}^n}{e_{ij}^n} - \eta\lambda_i + \eta\beta_i - \gamma_{ij} - \theta_{ij} = 0 \tag{11}$$
$$\nabla_{s_{ij}^n} L_2(E^n, S^n, \lambda, \beta, \alpha, \gamma, \theta)$$
$$= -s_{ji}^n + \alpha_j + \rho\gamma_{ij} = 0 \tag{12}$$

As the lagrangian multipliers are the same. Thus, from Eqs. (6), (7), (11), and (12), it is known that:

$$b_{ij}^n = \frac{\eta w_i e_{ij}^n}{(\eta \sum_{j=1}^{J} e_{ij}^n - e_i^{n,min}) + 1} \tag{13}$$
$$-s_{ji}^n = -2c_1\, s_{ji}^n - c_2 \tag{14}$$

B. Optimal Prices for EVs and SPs

The optimal price values of the EVs and the SPs allocated by an auctioneer is defined as follows:

$$pay_i(Bid_i^n) = \sum_{j}^{J} b_{ij}^n \tag{15}$$

$$Rew_j(P_j^n) = \sum_{i}^{I} \frac{(p_{ji}^n)^2}{4c_1} \tag{16}$$

Now, we calculate the pricing rules of the EVs and the SPs.

From the Eq. (8), we calculate:

$$\frac{\partial U_i(E_i^n)}{\partial b_{ij}^n} - \frac{\partial pay_i(Bid_i^n)}{\partial b_{ij}^n} = 0 \tag{17}$$

Hence,

$$b_{ij}^n = \frac{\partial U_i(E_i^n)}{\partial e_{ij}^n} e_{ij}^n = \frac{\eta w_i e_{ij}^n}{(\eta \sum_{j=1}^{J} e_{ij}^n - e_i^{n,min}) + 1} \tag{18}$$

Similarly, From the Eq. (9), we calculate:

$$\frac{\partial Rew_j(S_j^n)}{\partial p_{ji}^n} - \frac{\partial L_j(S_j^n)}{\partial p_{ji}^n} = 0 \tag{19}$$

Algorithm 2: Double Auction Mechanism.

Input: ξ, η, SoC^n, θ
Output: E^n, S^n, Bid^n, P^n
procedure Function$Double\ Auction\ Mechanism$
  Initialization: flag ←1, $t \leftarrow 0$, $Bid^{n(0)}$, $P^{n(0)}$
  while flag **do**
    if Participating EVs are not active or are not the nodes of the blockchain network **then**
      The auctioneer terminates the procedure and prepares to restart Algorithm 2.
    else
      Using $Bid^{n(t)}$ and $P^{n(t)}$, Auctioneer $\xrightarrow{\text{solves}}$ Problem OAP to get $E^{n(t)}$ and $S^{n(t)}$, and then broadcasts the optimized results to EVs and SPs, respectively.
      Based on $E^{n(t)}$ and $S^{n(t)}$, EVs $\xrightarrow[\text{optimal bid}]{\text{solves}} Bid^{n(t+1)}$ through solving EBP, and submit them to the *Auctioneer*.
      Based on $E^{n(t)}$ and $S^{n(t)}$, SPs $\xrightarrow[\text{optimal bid}]{\text{solves}} P^{n(t+1)}$ through solving ESP, and also submit them to the *Auctioneer*.
      $t \leftarrow t + 1$
      if RCB $< \xi$ and RCS $< \xi$ **then**
        flag $\leftarrow 0$
        $t \leftarrow t - 1$
      end if
    end if
  end while
end procedure

Hence,

$$s_{ji}^n = 2c_1\, s_{ji}^n + c_2 \tag{20}$$

From the Eqs. (18) and (20) shows that the optimal price values mentioned in the Equations. (15) and (16) satisfy the Eqs. (13) and (14) and ensures optimality.

According to the proposed mechanism and Algorithm 1, the auction bid prices EVs and the SPs are stored on the blockchain network. By using these bid prices, the auctioneer solves "OAP" to allocate the energy demand and supply. The auctioneer broadcasts a new prices solution to the EVs and the SPs. After that, they solve their own "EBP" and "ESP" problems to find optimal price for demand response management. Here, the termination condition is that the newest bid prices satisfy the convergence ξ condition (RCB $< \xi$ and RCS $< \xi$). If not, the algorithm repeatedly executes from the starting steps. EBP, ESP, and OAP can be solved through multiple iterations. Here, ξ determines the execution time and the accuracy of this algorithm. When ξ becomes small, the final values closer to the optimal values. More details on a double auction mechanism are given in Algorithm 2.

According to Eqs. (18) and (20), it is known that an EV and the SP will bid truthfully and maximize the utilities by solving EBP and ESP. Our proposed double auction satisfies the following properties:

1) *Individual Rationality (IR):* No node, *i.e.,* EVs and SPs in the blockchain network should loose from joining the auction.
2) *Weak balanced budget (WBB):* The auctioneer should not lose money while performing the double auction mechanism.
3) *Truthfulness (TF):* The dominant-strategy-incentive-compatibility (DSIC), which means that reporting the true value should be a dominant strategy for all nodes, *i.e.,* a node should not be able to gain by spying over other nodes and trying to find an *'optimal'* declaration which is different from true value.
4) *Economic efficiency (EE):* The social welfare should be the best possible after all energy trading in demand response management has completed.

The proposed double auction mechanism achieves an optimal energy trading solution in demand response management with social welfare maximization and privacy protection of EVs.

C. Demand Response Management

This subsection represents the energy transaction for demand response management between the EVs and the SPs on the network. In the blockchain network, all the authorized nodes need to audit and verify transactions and adds them in a new block by creating a consensus between them. It takes a certain time to finish the consensus process on the network. Then, the energy coins are transferred from the receiver's wallet address to the sender's wallet address. The step-wise detail description of energy trading transactions for demand response management between the requested EV and the selected SP is described as follows.

1) An EV EV_i (*i.e.,* energy buyer *i* with enough energy coins) can apply a request on blockchain network to buy a energy. Then, according to the price announces by the SPs, EV_i chooses the selected SP_i (, *i.e.,* energy seller *i*) using above-mentioned auction mechanism. Also. EV_i sends an energy request to a particular SP_i including the true identity 'ID_i,' wallet address 'WID_i,' current balance '$credit_i$,' namely as in the following (21),

$$EV_i \rightarrow SP_i : request_i = ID_i || WID_i || credit_i \tag{21}$$

2) After requesting '$request_i$,' the SP_i verifies the ID_i of an EV_i and check the funds in the given WID_i as per the requirements for energy trading transaction between them.
3) After the verification of EV_i by SP_i, it is allowed to obtain a token from the blockchain network for demand response management and fulfil the following demands.
   - There is enough wealth in EV_i's energy coin account or in a wallet address.
   - EV_i has a unique identity ID_i with an authenticated information. This ID_i of an EV_i should be in an encrypted form with its private key (PK_i) as mentioned

in the following (22).

$$ID_i = PK_i(Header||Content) \tag{22}$$

- All the other nodes on the network verifies the $ID_i = PK_i$ ($Header$ || $Content$) of an EV_i with its corresponding public key (PU_i). They calculate the $Verify_i = PU_i$ (ID_i). If the verification is true then, EV_i is an authenticated user otherwise not.

4) After the verification of EV_i, it receives a response '$response_i$' from the SP_i that includes token T_i and signature $SignToken_i$ as mentioned in the following (23).

$$SP_i \rightarrow EV_i : response_i$$
$$= T_i||SignToken_i||Timestamp \tag{23}$$

where as,
$T_i = credit_i$ || t || pre_record_i || $Timestamp$
$pre\_record_i =$ Hash (TX_i) where, i = 1,2,3...h
Here, T_i includes $credit_i$ that represents the current balance of EV_i, t represents verification of an EV_i, pre_record_i represents the previous record of the energy trading transactions of an EV_i, and $Timestamp$. EV_i should pay energy coins as a reward to SP_i when the transaction would successfully completed between them.

5) Further, EV_i sends T_i to SP_i for demand response management (DR_i) between them as mentioned in (24).

$$EV_i \rightarrow SP_i : DR_i$$
$$= T_i||SignToken_i||Timestamp \tag{24}$$

6) SP_i broadcasted the DR_i on the blockchain network (BN) with digital signatures on it. All the other nodes verifies the receiving T_i by comparing it with the original data present in the ledgers. If the T_i matches then, allow EV_i for demand response management otherwise not, as mentioned in the following 25.

$$SP_i \rightarrow BN : Verification\&Validation_i$$
$$= DR_i||SignToken_i||SignDR_i \tag{25}$$

7) Then, the energy transaction between EV_i and SP_i for demand response management will started and payment as energy coins will be transferred to the SP_i's wallet address from the EV_i's wallet address.
All the transaction information is audited and recorded in the ledgers of the blockchain, which can never be changed.

D. Complexity Analysis

1) Time Complexity: In Algorithm 1, the first *"for"* loop calculates b_{ij} for N number of EVs and the second *"for"* loop evaluates the p_{ji} run on blockchain for M number of CSs. The total time for both *"for"* loops is O(NM). The conditional operators used takes $O(1)$ time. Hence, the total computation time is of *O(NM) + O(1) = O(NM)* in the worst case.

In Algorithm 2, the conditional operators take $O(1)$ time. The bids submitted by EVs and the SPs *, i.e.,* B^n and P^n, respectively on a blockchain and then, auctioneer solves the E^n and S^n, which takes total time is of $O(n)$. After, EVs compute B^n by solving EBP based on the auctioneer results that takes $O(n)$ time. Similarly, SPs compute S^n by solving ESP based on the auctioneer results that takes $O(n)$ time. Hence, the total computation time of this algorithm is of *O(1) + O(n) + O(n) + O(n) = O(n)* in the worst case.

2) Space Complexity: In Algorithm 1, two lists are presented having *N* and *M* number of EVs and SPs, respectively. According to the insertion sort, these two lists take space complexity is of *O(NM)*. The rest of the algorithm takes *O(1)* space that uses conditional operators. So, the total space complexity of this algorithm is of *O(NM) + O(1) = O(NM)*.

In Algorithm 2, the conditional operators take $O(1)$ space. To calculate the value of E^n and S^n by the auctioneer on the basis of B^n and P^n bids submitted by EVs and SPs, respectively take the space complexity is of *O(n)*. Hence, the total space complexity of this algorithm is of *O(1) + O(n) = O(n)*.

VI. Performance Evaluation

In this section, we discuss the simulation results and security and privacy analysis of our proposed energy trading scheme for demand response management.

A. Numerical Settings

The performance of the proposed scheme is tested on a private Ethereum network. The experiments are performed on Intel Core i7 256 GB RAM, Ubuntu 18.04.5, 64core CPU and the algorithms are implemented using Solidity language [53]. For simulation, we considered a number of EV charging loads of 143 homes. The quantitative consumption data was supported by an online survey (83 respondents) and face to face interviews (13 respondents) with participants enrolled in the CLNR project based on a real dataset [54]. The charging energy demand of EVs range is [10, 60] KWh and the range of minimum price, EVs willing to buy the charging energy is [10, 60] units per KWh, whereas SPs range to discharge the energy is [50, 250] KWh with minimum selling price ranging from [5, 50] units per KWh. The cost factors used in the cost functions *, i.e.,* c_1 and c_2 is 0.01 and 0.015, respectively. The parameters η and ρ used in simulation are 0.8 and 0.9, respectively. η represents the average charging efficiency and ρ represents the average energy transmission efficiency. The threshold value of convergence ξ is 0.001. A summary of parameters used for simulation is described in the Table II.

B. Results and Discussions

The proposed scheme is compared with the existing state-of-the-art schemes [12], [16], [50], [55] and its performance is evaluated based on maximum social welfare, average converged iterations, scalability metrics: average throughput and latency, average buying and selling price, average transmitted and available energy, and standard deviation.

1) Impact on Social Welfare Maximization: Fig. 3 shows the convergence evolution of maximum social welfare achieved using Algorithm 2 in comparison to the existing algorithms discussed in [12], [50]. Note that the maximum social welfare

TABLE II
SIMULATION PARAMETERS

Parameters	Reference Value
η	0.08
ρ	0.09
ξ	0.001
Cost factors c1 & c2	0.01 & 0.015
EVs charging energy demand range	[10,60] KWh
Min. prices willing to buy by EVs	[10,60] units per KWh
SPs discharging surplus energy range	[50, 250] KWh
Min. prices by SPs range	[5,50] units per KWh
Network size	1, 5, 10, 20 sealers
Transaction sending rate	100, 200, 300, 500, 700, 1000 tx/sec
Workload	10,000 transactions
Consensus	Ethereum PoA (Clique)
Block Time	2 seconds
Geth	1.9.9 version
Simulation environment	Intel(R), 256GB RAM, Ubuntu 18.04.5, 64core CPU

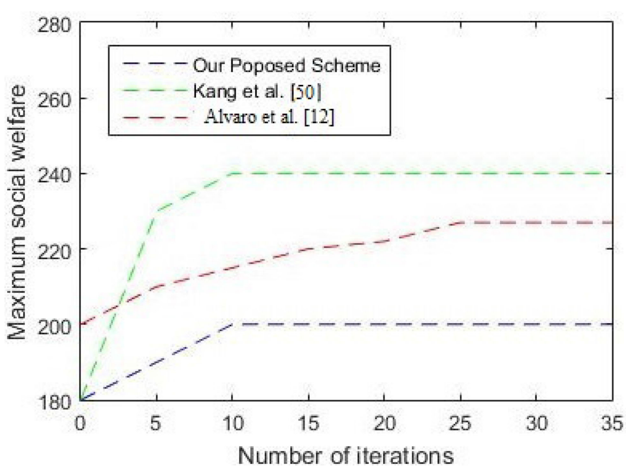

Fig. 3. Comparison of evolution of maximum social welfare.

rapidly converges close to the optimal value, *i.e.,* after 10 iterations whereas in the existing schemes [12], [50] converges after 25 and 12 iterations, respectively. Similarly, Fig. 4 shows the iteration convergence comparison between Algorithm 2 used for demand response management and the P2P energy trading algorithms discussed in [12], [50], [55]. After 10 000 experiments of energy trading with different energy demands by EVs, the average converged iterations of Algorithm 2 is 11, which is less than that of 11.9 in [50], 12.774 in [55], which is 37.5% less in comparison to [12]. From Fig. 4, it is clear that our proposed energy trading scheme for demand response management is faster than the existing P2P energy trading schemes.

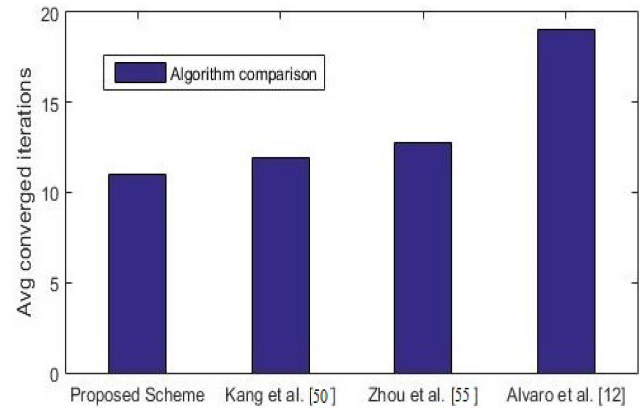

Fig. 4. Comparison between different algorithms.

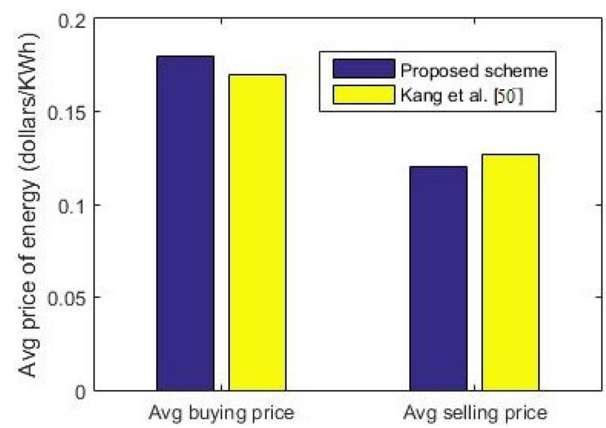

Fig. 5. Comparison of average buying and selling price.

2) Impact on Average Price and Amount of Energy: Fig. 5 shows the comparison between the proposed scheme and an existing energy trading scheme discussed in [50]. It clearly shows the comparison between average selling price and average buying price between the energy sellers and the energy buyers. In the existing scheme, authors described the electricity trading between the PHEVs. However, we focus on a P2P energy trading between EVs and the SPs. In addition, the proposed scheme achieves approximately 95% energy efficiency while trading or transmission whereas, the existing scheme in [50], the energy efficiency during electricity transmission is 90% approximately as mentioned in [56]. Similarly, the results in Fig. 6 shows that the proposed scheme in comparison to the existing scheme as discussed in [50] works better in transmitted energy to EVs and available energy at SPs. Hence, the proposed scheme has less energy loss and high energy utilization efficiency as compared to the existing trading scheme in [50].

3) Impact on Scalability: In order to evaluate the scalability metrics of the system model, we analyze average throughput and latency of our trading platform for demand response management on a private Ethereum blockchain. For this, we conducted several experiments under different workloads and network sizes. Six types of workload are used by sending the transaction rate is 100, 200, 500, 700, 1000, and 1200 transactions/sec. A blockchain with 1, 2, 3,.. upto 25 sealers are studied as a network

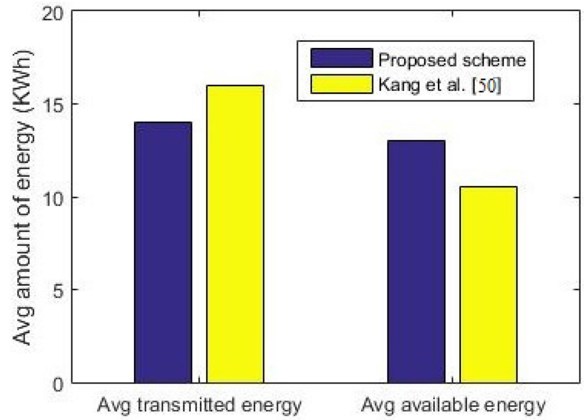

Fig. 6. Comparison of transmitted and available energy.

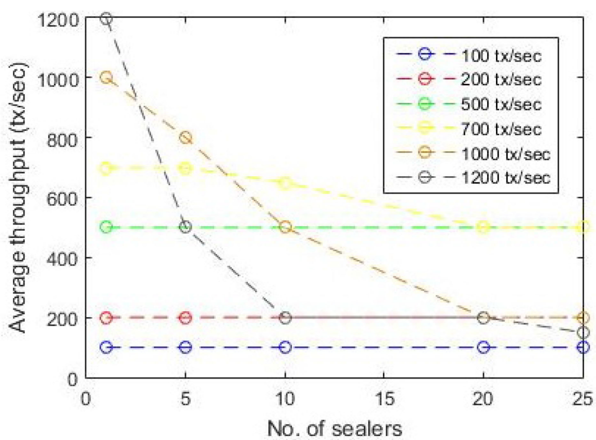

Fig. 7. Average throughput versus number of sealers.

size. The block time between two consecutive blocks is fixed and set to 2 seconds. The total number of transactions to be sent is also fixed and set to 10 000 as simulation parameters mentioned in Table II.

Fig. 7 shows the average throughput of the different transaction sending rates versus number of sealers. For moderate rates; 100, 200 and 500 tx/sec, the system achieves max throughput with all the transactions get processed and added to blockchain. For higher rates such as 700, 1000, and 1200. tx/sec, the throughput is automatically affected by the number of sealers, when scaling up to 25 sealers and drops below 50% of a sending rate of 1200 tx/sec. Similarly, Fig. 8 shows the average latency, which is inversely proportional to the throughput. For a moderate sending rate of a network size, the average latency of the different transaction sending rates is between 2.3 and 3 seconds. However, a higher sending rate and a bigger network size cause the latency to increase significantly up to 12 seconds. Fig. 8 clearly shows that the delay grows for handling of higher transaction rates because more time is needed to propagate the corresponding volume of data to all the sealers. Results also show that the maximum throughput is 500 tx/sec that supports the implementation platform.

4) Impact on Block Numbers: To show the limited computation power impact on the network size and time of the block,

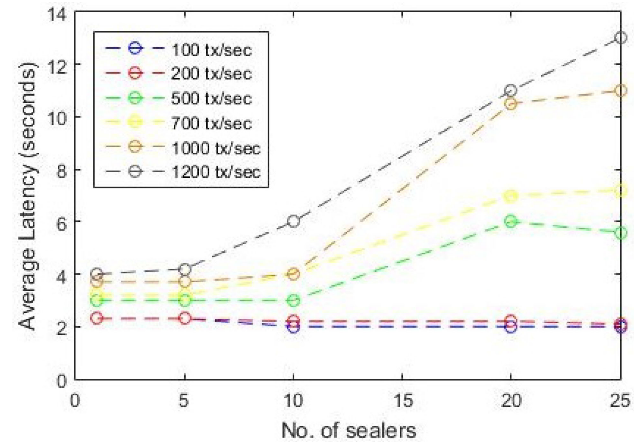

Fig. 8. Average latency versus number of sealers.

we observed the number of transactions per block by sending different transaction rates such as 200, 500 and 1000 (Fig. 9, 10 11). As shown in Fig. 9, the transaction sending rate is 200 tx/sec with 5, 10, and 20 sealers in Fig. 9(a),(b),(c) respectively. In Fig. 9(a), most of blocks are generated with uniform size and receive the same number of transactions, which is equal to the maximum throughput in block time of 2 sec. However, with an increase in the number of sealers and the transaction sending rate, the block sizes become more and more irregular as shown in Fig. 9, 10 11. To confirm this irregulation with respect to the increase in the number of sealers and the transaction sending rate, we plot the standard deviation of block sizes in Fig. 12. It clearly shows that the deviation from the mean grows higher but this deviation is lesser than the existing energy trading scheme in [16]. However, the higher transaction sending rates incur delay in the process and affect the generation time of new blocks.

The comparison between the proposed energy trading scheme and the existing schemes in simulation results is as shown in Table III.

C. Privacy and Security Analysis

In this subsection, we have discussed the privacy and security analysis of the proposed scheme.

- *No trusted third-party:* In this paper, the energy trading between the EVs and the SPs for demand response management has been done in a P2P manner. Thus, there is no need of third-party authenticator that makes the system more robust and scalable. We can also say that with the use of blockchain technology for demand response management in V2G environments, there is an elimination of trusted third-party.
- *Privacy protection:* To maximize the social welfare in V2G environments, we used double auction mechanism where EVs and SPs submit their prices on the blockchain network without any need of private information for energy trading known as *'Information Asymmetry'*. The energy coin accounts of each node on the blockchain are pseudonymous that protect its identity privacy and account security. EVs

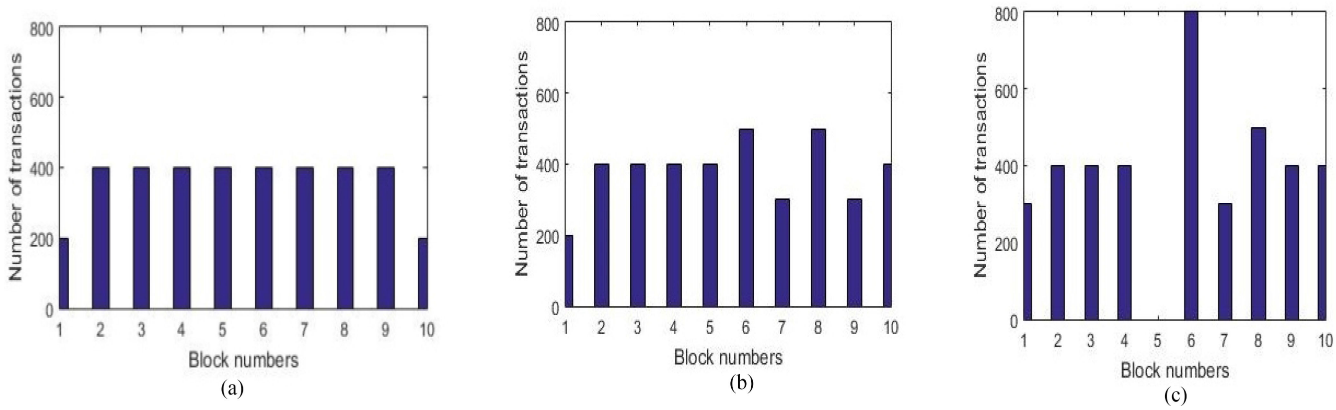

Fig. 9. Number of transactions within each block having sending rate 200 transactions/sec.

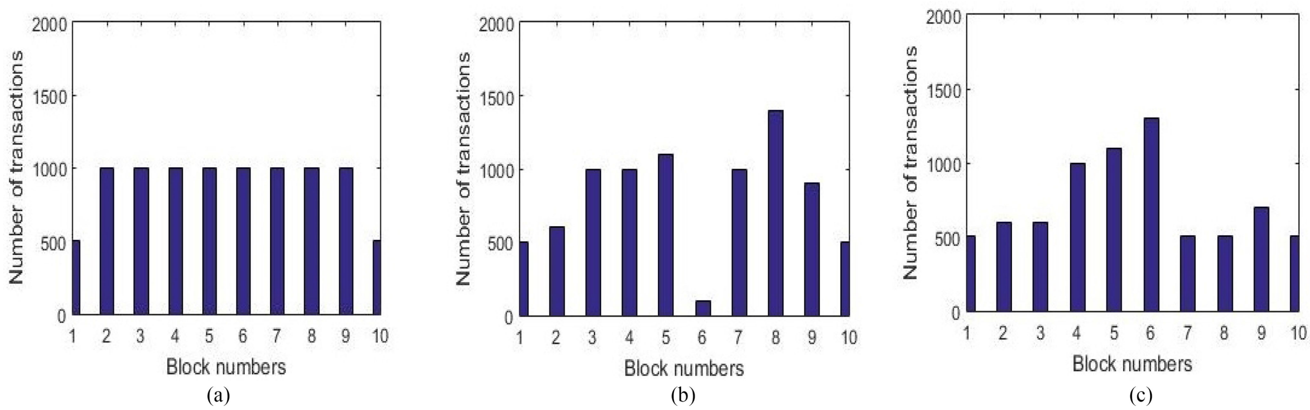

Fig. 10. Number of transactions within each block having sending rate 500 transactions/sec.

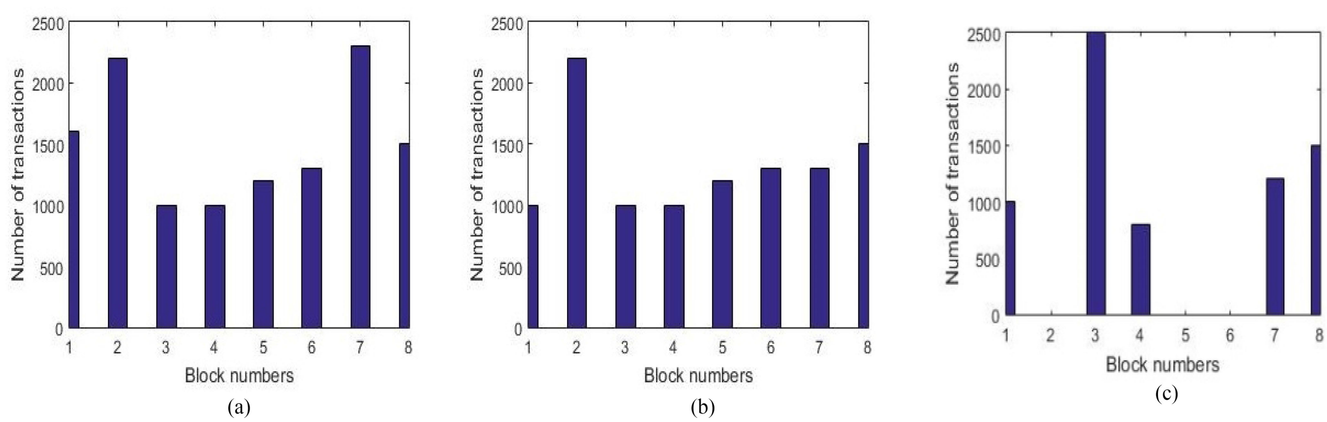

Fig. 11. Number of transactions within each block having sending rate 1000 transactions/sec.

prefer to use the public key for communicating with SPs rather than its true identity that prevents malicious attackers to hijack the private information of EVs.

- *Wallet security:* For the security of the wallet, the certification of the nodes is done using PKI infrastructure that provides the public and private keys to the nodes of a blockchain. Without knowing of corresponding keys and certificates, no-one can open a wallet of node and steal energy coins from the wallet on the blockchain network.
- *Transaction authentication:* All the energy transactions are validated and verified by an authority using PoA consensus in the proposed work. So, it is difficult for compromising all nodes due to the overwhelming cost of the blockchain network.
- *Data unforgeability:* The decentralized nature of consortium blockchain combined with cryptographic primitives ensures that an adversary cannot corrupt the energy transactions by taking the control over the blockchain system.

TABLE III
COMPARISON OF SIMULATION RESULTS OF THE PROPOSED SCHEME WITH THE EXISTING SCHEMES

Parameters	**Alvaro *et al.* [12]**	**Lasla *et al.* [16]**	**Kang *et al.* [50]**	**Zhou *et al.* [55]**	**Our Proposed Scheme**
Convergence reached	-	-	after 12 iterations	after 25 iterations	after 10 iterations
Average converged iterations	12.774 approx.	-	11.9 approx.	18.1 approx.	11 approx.
Maximum Throughput	-	350tx/sec	-	-	500tx/sec
Average latency	-	2.5-3.5seconds	-	-	2.3-3seconds
Standard deviation	-	600tx	-	-	450tx
Consensus Algorithm	-	PoA	Proof-of-Work	Proof-of-Work	PoA
Type of Blockchain	-	Private Blockchain	Consortium Blockchain	Consortium Blockchain	Consortium Private Blockchain

TABLE IV
PRIVACY AND SECURITY ANALYSIS COMPARISON OF THE PROPOSED SCHEME WITH THE EXISTING SCHEMES

Parameters	**Alvaro *et al.* [12]**	**Lasla *et al.* [16]**	**Kang *et al.* [50]**	**Zhou *et al.* [55]**	**Our Proposed Scheme**
Decentralized System	×	✓	✓	✓	✓
Privacy Protection	×	×	✓	✓	✓
Wallet Security	×	×	✓	×	✓
Transparency	×	✓	✓	✓	✓
51% attack	×	×	×	×	✓
Integrity	×	×	✓	✓	✓
DDoS	×	×	×	×	✓
Data Unforgeability	×	×	✓	×	✓
Transaction Authentication	×	✓	✓	✓	✓

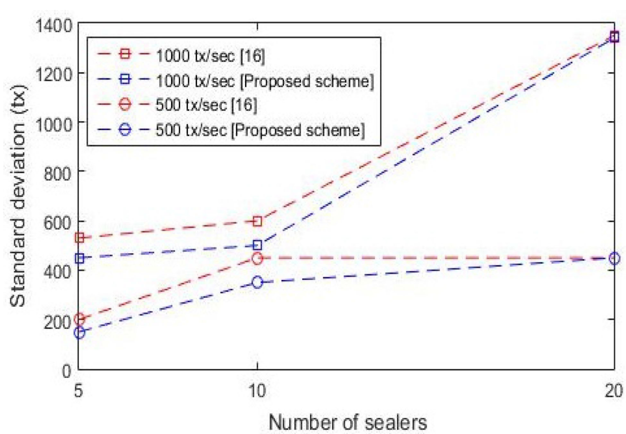

Fig. 12. Comparison of standard deviation with transaction sending rates.

- *Distributed Denial of Service (DDoS):* In this paper, we have used the PoA consensus to validate and verify the energy transactions done between EVs and the SPs. This mechanism makes it possible to defend against DDoS attack because the network nodes are pre-authenticated and verified. Therefore, block generation rights on a blockchain can be granted only to those nodes, which can withstand these type of attacks.
- *Integrity:* Once a block has been added into a blockchain, it includes the hash of the previous block, and its hash is stored in the next block. Therefore, it is difficult for a hacker to modify the block unless a hacker has a high amount of computational power. Moreover, the transactional data present in a block are secured by cryptographic primitives. So, it needs powerful resources to decrypt that data without knowing the private key.
- *51% attack:* In PoA consensus, 51% attack requires an attacker to obtain control over 51% of network nodes. This is different from 51% attack for the Proof-of-Work consensus types where an attacker needs to obtain 51% of network computational power. Obtaining control of the nodes in permissioned blockchain network is much harder than obtaining computational power. PoA consensus has a high tolerance of risk unless 51% of nodes acting maliciously.
- *Transparency:* Since the blockchain technology is DLT, so any participant node can have access to the blockchain and monitor the corresponding transactional data. Moreover, the transactional data is not saved on a single node and is transparent to all nodes. As a result, any malicious data modification can be traceable.

Hence, we have compared the proposed energy trading scheme with the existing schemes such as Alvaro *et al.* [12], Lasla *et al.* [16], Kang *et al.* [50], and Zhou *et al.* [55]. As Table IV, a comparison of the security features of above-mentioned schemes is listed. The comparison results show that the proposed scheme has better security features in comparison to the existing schemes.

VII. Conclusion

The exponential growth of energy demand in industrial and residential areas may increase the burden on the smart grid in the years to come. Moreover, the use and evolution of EVs in V2G energy trading are likely to increase the energy load many folds on the smart grid. It may result to load fluctuations at the grid center, thereby causing undesirable instabilities. The prime reasons for this behavior is due to the lack of security and privacy issues at various levels in a V2G environment. To resolve these issues, we proposed a consortium blockchain-based secure energy trading scheme for demand response management between EVs and the SPs in a V2G environment. In this scheme, a double auction mechanism has been used between EVs and the SPs to maximize the social welfare. The blockchain network works as an auctioneer to carry out the auction according to their bid prices, which does not require any private information of EVs. Numerical results based on a real-time implementation indicate that a double auction mechanism maximizes the social welfare. Thus, the simulation results clearly show that the energy trading scheme for demand response management is practical enough to be incorporated in a V2G environment. Privacy and security analysis show that the proposed scheme improves transaction security and provides transparency in energy trading between EVs and the SPs. In future, we will explore the resilience of the proposed scheme by increasing the workload and network size to analyze the network scalability.

Acknowledgment

Authors gracefully acknowledge the support from the Cybersecurity Research Center, Prince Mohammad Bin Fahd University (PMU), Kingdom of Saudi Arabia with acknowledgement number (PCC-Grant-202119)..

References

[1] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid the new and improved power grid: A survey," *IEEE Commun. Surv. Tut.*, vol. 14, no. 4, pp. 944–980, Oct.–Dec. 2011.

[2] H. Farhangi, "The path of the smart grid," *IEEE Power Energy Mag.*, vol. 8, no. 1, pp. 18–28, Jan.-Feb. 2010.

[3] V. C. Gungor *et al.*, "Smart grid technologies: Communication technologies and standards," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 529–539, Nov. 2011.

[4] J. B. Ekanayake, N. Jenkins, K. Liyanage, J. Wu, and A. Yokoyama, *Smart Grid: Technology and Applications*. Hoboken, NJ, USA: Wiley, 2012.

[5] Z. Zhou, J. Gong, Y. He, and Y. Zhang, "Software defined machine-to-machine communication for smart energy management," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 52–60, Oct. 2017.

[6] E. Zio and G. Sansavini, "Vulnerability of smart grids with variable generation and consumption: A system of systems perspective," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 43, no. 3, pp. 477–487, May 2013.

[7] Y. Xiao, D. Niyato, P. Wang, and Z. Han, "Dynamic energy trading for wireless powered communication networks," *IEEE Commun. Mag.*, vol. 54, no. 11, pp. 158–164, Nov. 2016.

[8] Z. Zhou, C. Sun, R. Shi, Z. Chang, S. Zhou, and Y. Li, "Robust energy scheduling in vehicle-to-grid networks," *IEEE Netw.*, vol. 31, no. 2, pp. 30–37, Mar./Apr. 2017.

[9] E. L. Karfopoulos, K. A. Panourgias, and N. D. Hatziargyriou, "Distributed coordination of electric vehicles providing V2G regulation services," *IEEE Trans. Power Syst.*, vol. 31, no. 4, pp. 2834–2846, Jul. 2016.

[10] J. P. Morgan, *Driving Into 2025: The Future of Electric Vehicles*, Accessed: Oct. 10, 2020. [Online]. Available: https://www.jpmorgan.com/insights/research/electric-vehicles

[11] S. Pal and R. Kumar, "Electric vehicle scheduling strategy in residential demand response programs with neighbor connection," *IEEE Trans. Ind. Informat.*, vol. 14, no. 3, pp. 980–988, Mar. 2018.

[12] R. Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens, "Peer to peer energy trading with electric vehicles," *IEEE Intell. Transp. Syst. Mag.*, vol. 8, no. 3, pp. 33–44, Fall 2016.

[13] Y. Cao, T. Wang, O. Kaiwartya, G. Min, N. Ahmad, and A. H. Abdullah, "An EV charging management system concerning drivers trip duration and mobility uncertainty," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 48, no. 4, pp. 596–607, Apr. 2018.

[14] W.-L. Chin, W. Li, and H.-H. Chen, "Energy big data security threats in IoT-based smart grid communications," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 70–75, Oct. 2017.

[15] Y. Wu, X. Tan, L. Qian, D. H. Tsang, W.-Z. Song, and L. Yu, "Optimal pricing and energy scheduling for hybrid energy trading market in future smart grid," *IEEE Trans. Ind. Informat.*, vol. 11, no. 6, pp. 1585–1596, Dec. 2015.

[16] N. Lasla, M. Al-Ammari, M. Abdallah, and M. Younis, "Blockchain based trading platform for electric vehicle charging in smart cities," *IEEE Open J. Intell. Transp. Syst.*, vol. 1, pp. 80–92, 2020.

[17] A. Jindal, M. Singh, and N. Kumar, "Consumption-aware data analytical demand response scheme for peak load reduction in smart grid," *IEEE Trans. Ind. Electron.*, vol. 65, no. 11, pp. 8993–9004, Nov. 2018.

[18] N. Saxena, S. Grijalva, V. Chukwuka, and A. V. Vasilakos, "Network security and privacy challenges in smart vehicle-to-grid," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 88–98, Aug. 2017.

[19] Y. Zhang, S. Gjessing, H. Liu, H. Ning, L. T. Yang, and M. Guizani, "Securing vehicle-to-grid communications in the smart grid," *IEEE Wireless Commun.*, vol. 20, no. 6, pp. 66–73, Dec. 2013.

[20] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.

[21] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K. R. Choo, and A. Y. Zomaya, "Blockchain for smart communities: Applications, challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 144, pp. 13–48, 2019.

[22] N. Kumar, S. Aggarwal, and P. Raj, *The Blockchain Technology for Secure and Smart Applications Across Industry Verticals*. New York, NY, USA: Academic Press, 2021, vol. 121.

[23] P. K. Sharma, N. Kumar, and J. H. Park, "Blockchain-based distributed framework for automotive industry in a smart city," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4197–4205, Jul. 2019.

[24] M. Mihaylov, I. Razo-Zapata, R. Rădulescu, S. Jurado, N. Avellana, and A. Nowé, "Smart grid demonstration platform for renewable energy exchange," in *Proc. Int. Conf. Practical Appl. Agents Multi-Agent Syst.*, 2016, pp. 277–280.

[25] S. Aggarwal and N. Kumar, "Chapter five—Signature primitives cryptographic primitives used in blockchain," in *Proc. Blockchain Technol. Secure Smart Appl. Across Ind. Verticals, ser. Adv. Comput.*, vol. 121, 2021, pp. 109–121.

[26] shubhani aggarwal and N. Kumar, "Chapter fifteen - blockchain 2.0: Smart contracts working model," in *Proc. Blockchain Technol. Secure Smart Appl. Across Ind. Verticals, Ser. Adv. Comput.*, vol. 121, 2021, pp. 301–322.

[27] H. T. Doan, J. Cho, and D. Kim, "Peer-to-peer energy trading in smart grid through blockchain: A double auction-based game theoretic approach," *IEEE Access*, vol. 9, pp. 49206–49218, 2021.

[28] A. Kalakova, A. Zhanatbekov, A. Surash, H. K. Nunna, and S. Doolla, "Blockchain-based decentralized transactive energy auction model with demand response," in *Proc. IEEE Texas Power Energy Conf.*, 2021, pp. 1–6.

[29] A. Jindal, G. S. Aujla, and N. Kumar, "Survivor: A blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment," *Comput. Netw.*, vol. 153, pp. 36–48, 2019.

[30] V. Hassija, V. Chamola, S. Garg, N. G. K. Dara, G. Kaddoum, and D. N. K. Jayakody, "A blockchain-based framework for lightweight data sharing and energy trading in V2G network," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5799–5812, Jun. 2020.

[31] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, and Y. Chen, "Adaptive blockchain-based electric vehicle participation scheme in smart grid platform," *IEEE Access*, vol. 6, pp. 25657–25665, 2018.

[32] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, “Consortium blockchain for secure energy trading in industrial internet of things,” *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.

[33] S. Garg, K. Kaur, G. Kaddoum, F. Gagnon, and J. J. Rodrigues, “An efficient blockchain-based hierarchical authentication mechanism for energy trading in V2G environment,” in *Proc. IEEE Int. Conf. Commun. Workshops*., 2019, pp. 1–6.

[34] K. Kaur, S. Garg, G. Kaddoum, F. Gagnon, and S. H. Ahmed, “Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure,” in *Proc. IEEE Int. Conf. Commun. Workshops*, 2019, pp. 1–6.

[35] B.-G. Kim, S. Ren, M. Van DerSchaar, and J.-W. Lee, “Bidirectional energy trading and residential load scheduling with electric vehicles in the smart grid,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1219–1234, Jul. 2013.

[36] N. Kumar, S. Misra, J. J. Rodrigues, and M. S. Obaidat, “Coalition games for spatio-temporal big data in internet of vehicles environment: A comparative analysis,” *IEEE Internet Things J.*, vol. 2, no. 4, pp. 310–320, Aug. 2015.

[37] N. Kumar, R. Iqbal, S. Misra, and J. J. Rodrigues, “Bayesian coalition game for contention-aware reliable data forwarding in vehicular mobile cloud,” *Future Gener. Comput. Syst.*, vol. 48, pp. 60–72, 2015.

[38] S. Thakur and J. G. Breslin, “Electric vehicle charging queue management with blockchain,” in *Proc. Int. Conf. Internet Veh.*, 2018, pp. 249–264.

[39] Z. Liu *et al.*, “A survey on applications of game theory in blockchain,” 2019, *arXiv:1902.10865*.

[40] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang, “A secure charging scheme for electric vehicles with smart communities in energy blockchain,” *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4601–4613, Jun. 2019.

[41] N. Kumar, S. Misra, N. Chilamkurti, J.-H. Lee, and J. J. Rodrigues, “Bayesian coalition negotiation game as a utility for secure energy management in a vehicles-to-grid environment,” *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 1, pp. 133–145, Jan./Feb. 2016.

[42] S. Xia, F. Lin, Z. Chen, C. Tang, Y. Ma, and X. Yu, “A Bayesian game based vehicle-to-vehicle electricity trading scheme for blockchain-enabled internet of vehicles,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 6856–6868, Jul. 2020.

[43] K. Kaur, G. Kaddoum, and S. Zeadally, “Blockchain-based cyber-physical security for electrical vehicle aided smart grid ecosystem,” *IEEE Trans. Intell. Transp. Syst.*, 2021.

[44] Y.-C. Tsao, V.-V. Thanh, and Q. Wu, “Sustainable microgrid design considering blockchain technology for real-time price-based demand response programs,” *Int. J. Elect. Power Energy Syst.*, vol. 125, 2021, Art. no. 106418.

[45] A. Muzumdar, C. Modi, G. Madhu, and C. Vyjayanthi, “A trustworthy and incentivized smart grid energy trading framework using distributed ledger and smart contracts,” *J. Netw. Comput. Appl.*, p. 103074, 2021.

[46] K. Anoh, S. Maharjan, A. Ikpehai, Y. Zhang, and B. Adebisi, “Energy peer-to-peer trading in virtual microgrids in smart grids: A game-theoretic approach,” *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1264–1275, Mar. 2020.

[47] J. Fisher and M. H. Sanchez, “Authentication and Verification of Digital Data Utilizing Blockchain Technology,” U.S. Patent App. 15/083238, Sep. 29, 2016.

[48] L. Axon, “Privacy-awareness in blockchain-based PKI,” *Cdt Tech. Paper Ser.*, vol. 21, pp. 1–17, 2015.

[49] L. Axon and M. Goldsmith, “PB-PKI: A privacy-aware blockchain-based PKI,” in *SECRYPT*, Jul. 2017, pp. 311–318.

[50] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, “Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains,” *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[51] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, “PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain,” 2018.

[52] M. Avriel, *Nonlinear Programming: Analysis and Methods*. Courier Corporation, 2003.

[53] S. Aggarwal and N. Kumar, “Blockchain 2.0: Smart contracts,” 2020.

[54] CLNR-L092: Insight Report Electric Vehicles, Aug. 2014, Accessed: Oct. 11, 2020, [Online]. Available: http://www.networkrevolution.co.uk/project-library/insight-report-electric-vehicles/

[55] Z. Zhou, B. Wang, M. Dong, and K. Ota, “Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing,” *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 50, no. 1, pp. 43–57, Jan. 2020.

[56] S. Li, P. Yi, Z. Huang, T. Xie, and T. Zhu, “Energy scheduling and allocation in electric vehicles energy internet,” in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf.*, 2016, pp. 1–5.

Shubhani Aggarwal received the B.Tech. degree in computer science and engineering from Punjabi University, Patiala, India, in 2015 and the M.E. degree in computer science from Panjab University Chandigarh, Chandigarh, India, in 2017. She is currently working toward the Ph.D. degree from the Thapar Institute of Engineering and Technology (Deemed to be University), Patiala. Some of her research findings are authored or coauthored in top-cited journals, such as the IEEE INTERNET OF THINGS JOURNAL, *Elsevier Journal of Network and Computer Applications*, *Computers and Security*, *Mobile Networks and Applications*, *Computer Communications*. Her research interests include blockchain, cryptography, Internet of Drones, and information security.

Neeraj Kumar (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from Shri Mata Vaishno Devi University, Katra, India. He was a Postdoctoral Research Fellow with Coventry University, Coventry, U.K. He is currently a Full Professor with the Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, Patiala, India. He has authored or coauthored more than 400 technical research papers in leading journals and conferences from IEEE, Elsevier, Springer, and John Wiley. He has also authored or coauthored four books from Springer and CRC Press. Some of his research findings are published in top-cited journals, such as IEEE TKDE, IEEE TIE, IEEE TDSC, IEEE TITS, IEEE TCE, IEEE TII, IEEE TVT, and IEEE ITS. He is an Associate Technical Editor of the ACM Computing Survey, IEEE TNSM, IEEE COMMUNICATION MAGAZINE, IEEE NETWORK MAGAZINE, *Elsevier Journal of Network and Computer Applications*, and *Computer Communications*. He is in the 2019, 2020 list of highly cited Researcher in WOS. He has won many prestigious awards from IEEE.