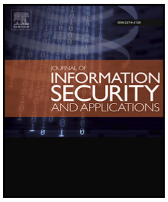
Journal of Information Security and Applications 63 (2021) 102998

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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



A consortium blockchain based energy trading scheme for Electric Vehicles in smart cities

Rabiya Khalid [a], Muhammad Waseem Malik [a], Turki Ali Alghamdi [b], Nadeem Javaid [a,c,*]

[a] *Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan*
[b] *Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Makkah 21955, Saudi Arabia*
[c] *School of Computer Science, University of Technology, Sydney, Sydney, Ultimo, NSW, 2007, Australia*

ARTICLE INFO

Keywords:
Consortium blockchain
Energy trading
Smart contract
Electric Vehicles
Smart cities

ABSTRACT

The real time Vehicle-to-Grid (V2G) and Vehicle-to-Vehicle (V2V) energy trading have ameliorated the smart city environment. Electric Vehicles (EVs) in smart cities have made it possible to balance the energy demand and supply without burdening the power grids. They also help in minimizing both the heap amounts of pollution and the greenhouse gas emissions. EVs not only charge their batteries from Charging Stations (CSs), but when the smart city faces energy deficiency, they supply their surplus energy to the power grids to fulfill energy demand as well. In addition, EVs also balance the energy demand and supply through energy trading at the local level during peak hours, which strengthens V2V energy trading. However, some issues, such as security threats and privacy leakage prevent EVs from participating in the energy trading process. In addition, the lack of incentives and knowledge about the cost of reaching the energy trading place within minimum time are also big challenges. Therefore, to solve the aforementioned challenges, a secure and efficient scheme for V2V and V2G energy trading is proposed in this paper. The proposed scheme also helps in promoting environmental friendliness and making the smart cities sustainable and reliable. In the proposed scheme, energy trading transactions are secured using consortium blockchain, wherein the Local Aggregators (LAGs) are selected as authorized nodes. LAGs perform their role as energy brokers and are responsible for validating the energy trading requests using Proof of Authority (PoA) consensus mechanism. Moreover, a solution to find accurate distance with required expenses and time to reach the charging destination is also proposed, which effectively guides EVs to reach the relevant CSs and encourages energy trading. Besides, we propose a fair payment mechanism using a smart contract to avoid financial irregularities. An incentive provisioning mechanism is also given in the proposed work to prevent EVs from acting selfishly. The efficient power flow having minimized losses in the vehicular network is of much importance. Therefore, the energy losses incurred in both V2G and V2V are discussed in this work. Furthermore, Oyente is used for smart contract's security analysis and for testing Ethereum's resilience against different security flaws. Two attacker models are proposed and the security analyses of the models are also provided. The analyses show that the proposed system is robust against the double spending and Sybil attacks. Finally, the efficient performance of our proposed scheme is validated and analyzed. The simulation results proved that our proposed work outperforms existing work in terms of providing a secure and efficient energy trading platform for both V2G and V2V environments.

1. Introduction

A rapid increase in the awareness of efficient use of energy and tackling the increasing amounts of pollution has led to the demand for reliable, secure and sustainable power grids. The demand further leads to the evolution of the traditional grids into smart grids [1]. With the advancement in information and communication technologies, the smart grid gets the benefit of the two-way flow of electricity and information. Smart grids generate energy using renewable energy resources [2], which are of intermittent nature. Therefore, energy management plays a very important role in maintaining the sustainability and reliability of the smart grid. Electric Vehicles (EVs) are considered an integral part of energy management systems. They play a key role in balancing the demand and supply of energy in smart grids. They rely on the usage of electricity rather than conventional fossil fuels, which remarkably reduces environmental pollution and minimizes greenhouse gas emissions. The aforementioned factors help in making

[*] Corresponding author.
E-mail address: nadeemjavaidqau@gmail.com (N. Javaid).

https://doi.org/10.1016/j.jisa.2021.102998

Available online 23 October 2021

the cities smart, green and sustainable [3]. For energy trading, Vehicle-to-Grid (V2G) and Vehicle-to-Vehicle (V2V) energy trading systems have emerged drastically, which enable better utilization of energy in the presence of scarce energy resources [4]. EVs have the ability to act both as energy suppliers and energy consumers in the smart transportation infrastructure. This ability of EVs helps in fostering reliability and sustainability in smart cities [5]. EVs sense and transmit the data about their environment using different communication technologies in a smart transportation system [6]. The built-in On-Board Unit (OBU) allows EVs to interact with each other for information sharing [7]. EVs can transmit energy trading requests to other EVs for buying and selling energy, price prediction, load forecasting, and optimal energy consumption scheduling [5].

The development of EVs has led the masses towards the smart transportation sector as they are providing various benefits apart from the transportation services [8]. To balance energy demands in the smart city, energy trading systems need to be managed efficiently and EVs must practice self-sustainability in the smart city [8]. EVs not only get energy from Charging Stations (CSs), but also from other EVs to reduce load during peak hours through V2V energy trading [9] at the Parking Lots (PRKs). Moreover, they supply the surplus energy back to the CSs (V2G energy trading), when the smart city faces an energy deficiency [8,9]. However, there are various challenges in both energy trading environments, such as security threats and privacy leakage. Therefore, to address the security issues, authors in [2–12] have used blockchain technology. Blockchain is an emerging Peer-to-Peer (P2P) distributed and decentralized network [13] in which data is shared among network nodes. This technology has been widely used in different fields, such as Wireless Sensor Networks (WSNs) [14], Internet of Things (IoT) [15], Vehicular Ad-Hoc Networks (VANETs) [16,17], cloud environment [18], energy and smart grids [19,20], healthcare, agriculture [21], etc., for secure, distributed, transparent, immutable and auditable storage of transactions records.

Apart from the aforementioned issues, EVs with surplus energy are not motivated to participate as energy sellers in the energy trading environment due to the lack of incentive provisioning. It causes imbalance in energy demand and supply in the smart city. Therefore, motivating them for energy trading is a vital challenge. Zhou et al. [4] proposed an incentive mechanism using contract theory for V2G energy trading. In this scheme, EVs receive a higher reward to discharge their energy at CSs. Kang et al. [2] proposed a localized P2P energy trading model for local energy trading among EVs to achieve demand response and balance localized energy demand by providing an incentive mechanism using an iterative double auction method with a consortium blockchain. However, finding the nearest CSs' information (such as price, distance, time slot) for EVs remains an important issue, which needs to be tackled. Authors in [8] and [22] proposed energy trading models to address this issue. Jindal et al. [8] proposed a mechanism for EVs to find the nearest CSs. However, they used equal-sized blocks of the smart city, which are not suitable when dealing with random-sized blocks. Chaudhary et al. [22] proposed a blockchain-based secure energy trading scheme for EVs. The proposed schemes of [2,4,8,22] do not involve well-defined payment mechanisms and are prone to attacks.

Motivated by the aforementioned developed energy trading schemes, we develop such a V2V and V2G energy trading environment for EVs and CSs, which leverages consortium blockchain with Proof of Authority (PoA) consensus mechanism and smart contract for efficient energy trading. Consortium blockchain provides features of both the public and private blockchains. PoA mechanism requires less computational power as compared to Proof of Work (PoW) and has maximum throughput with less latency. In our scenario, four major entities are involved: Registration Authority (RA), EVs, CSs, and Local Aggregators (LAGs). Blockchain is deployed on LAGs to keep track of energy trading transactions of EVs and CSs.

1.1. Problem statement

Many researchers provide solutions to manage energy demand in smart cities by trading energy in V2V and V2G manner. In the V2G energy trading environment, EVs charge and discharge their batteries at CSs; whereas, in V2V, energy trading occurs among EVs locally. However, EVs and CSs face various challenges in energy trading environments, such as security threats, privacy leakage, finding the nearest energy trading place, and lack of incentives.

Trust and security have always been the biggest challenges in the transportation sector. In energy trading, it is very important to authenticate energy trading requests. In addition, the malicious attacks by the malicious nodes are also a challenge in this area because some adversaries modify the transactions for their benefits, which results in the financial loss of both the CSs and the EVs. In the literature, blockchain is widely used in WSNs, VANETs and smart grid network scenarios to address security, data tampering, and request tampering challenges. The authors in [8,22] proposed blockchain-based energy trading mechanisms for EVs. In [8], Jindal et al. proposed an edge-as-a-service framework for energy trading in the V2G environment to reduce delay in energy trading decisions taken at remote control centers. They also proposed a model to find the nearest CSs for an EV to save both energy and traveling time. Chaudhary et al. [22] proposed a blockchain-based secure energy trading and minimum distance finding scheme for EVs. However, both schemes failed to achieve accurate distance in the random-sized city blocks. In both schemes, the authors selected the EVs as miner nodes to validate the energy trading requests using the PoW consensus mechanism. However, EVs cannot perform the role of miners due to their limited resources [23]. Moreover, the PoW consensus mechanism also requires a huge amount of computational power. Apart from that, the proposed schemes do not involve well-defined payment mechanisms and are prone to attacks. Additionally, no incentive mechanism is provided in [22] to motivate EVs to sell their surplus energy to CS while meeting the energy demand. Kang et al. [2] proposed a localized P2P energy trading model for local energy trading among EVs to balance localized energy demand by providing an incentive mechanism using iterative double auction method with a consortium blockchain. In [2] and [22], Transaction Server Controller (TSC) aggregates the requests of energy sellers and buyers from the local server and selects the pairs of sellers and buyers based on the auction price. However, no mechanism is specified to determine the locations of buyers and sellers to check either they are requesting from the same area or from different areas. We have discussed solutions to the aforementioned challenges in Section 3.

1.2. Our contributions

Our contributions in this paper are summarized as follows:

- consortium blockchain is deployed along with PoA consensus mechanism on the LAGs for secure energy trading,
- smart contracts are designed to ensure fair payment between EVs. Moreover, an incentive mechanism is proposed to encourage EVs to participate in energy trading. Besides, a punishment mechanism is developed to prevent EVs from acting maliciously,
- an algorithm is developed for energy trading in which EVs find the list of the nearby CSs or PRKs with information about distance, required time and energy expenses to reach the destination in both V2V and V2G energy trading environments,
- the power flow in the vehicular network and the associated energy losses are discussed and
- this study designs two attacker models based on the double spending and Sybil attacks. Security analyses of the models show that the proposed system is robust against both attacks. Also, Oyente symbolic execution tool is used for smart contract's security analysis, which is able to test common and well-known latest security flaws of Ethereum with Ethereum Virtual Machine (EVM) byte code.

1.3. Organization

In Section 2, the literature review of existing work on blockchain based energy trading is discussed. Section 3 describes our system model and problem formulation. Whereas, security objectives and analysis, and attacker models are given in Section 4. Simulation and discussion of results are given in Section 5. Finally, the conclusion of this paper is presented in Section 6.

2. Related work

During the past few decades, researchers are actively working in the area of the intelligent transportation system in research with the development of smart cities. The major aim behind this research is to make the cities smarter and greener. Using electricity instead of conventional fossil fuels helps in cutting down the heap amounts of pollution and greenhouse gas emissions. It leads to reliability and sustainability of the cities. In the literature, many solutions are proposed related to traffic management and smart energy management. The usage of EVs in smart cities has made it possible to balance the demand for electricity without relying on the power grids [8]. EVs are able to exchange their energy with the smart grid and are also used as a carrier to fulfill the energy requirements in smart cities.

In literature, much work has been done on different aspects of promoting both V2G and V2V energy trading in the smart transportation sector. The fundamental aims behind such work are to make the cities greener, reduce pollution, minimize greenhouse gas emissions, promote reliability and sustainability, etc. Chaudhary et al. [22] proposed a secure and efficient energy trading scheme for EVs using blockchain technology in Software Defined Networking (SDN) enabled Intelligent Transportation System (ITS). In this scheme, the authors provided real time processing of the energy trading ecosystem. They also addressed conventional and centralized security issues. Wang et al. [23] addressed the external and internal adversarial attacks using the blockchain technique and developed a Proof of Reputation (PoR) consensus mechanism to improve selected validator's security based on trust and credibility computing. In [24], authors considered different charging infrastructures in which the EVs can be charged. These infrastructures are compared using various performance parameters, which prove that the proposed distributed infrastructure outperforms the other two. Moreover, three different charging strategies are also considered in the work in terms of load profiles and cost.

In order to balance and stimulate energy demands in the smart city through EVs, Kang et al. [2] proposed a localized P2P energy trading model for local energy trading among EVs. In this scheme, the authors achieved demand response by providing an incentive-based mechanism. The role of an aggregator at PRKs also needs further consideration. Keeping this in mind, authors in [3] discussed the multi EV charging scenarios in residential PRKs. The fast-charging services are further compared with slow-charging services in the proposed work. A real time planning approach being adopted by the EV users to alternate between slow-charging and fast-charging services is also discussed in a stochastic manner. Zhou et al. [4] proposed a secure energy trading framework for EVs, using consortium blockchain technology. In this scheme, the authors proposed a contract theory-based incentive mechanism to motivate EVs to participate in an energy trading environment. Gao et al. [5] proposed a blockchain-based payment mechanism for the V2G energy trading environment. They also introduced a registration scheme to secure users' sensitive information.

Jindal et al. [8] proposed an edge-as-a-service framework for energy trading using blockchain technology in the V2G environment. In this scheme, authors reduce delay and network overhead issues in communication using SDN. They also provided the nearest CS's location with its distance and required time from an EV's current location. Li et al. [9] proposed a blockchain-based energy trading scheme to achieve security and privacy and improve trust and transparency in energy trading environment. They also introduced credit-based payment and loan schemes to support fast and frequent energy trading in the industrial Internet of Things (IoT). Zhou et al. [25] proposed a V2G energy trading framework using consortium blockchain for providing efficient and secure energy trading transactions. They also proposed an incentive mechanism using contract theory for V2G energy trading environment. In this scheme, EVs gained higher rewards to participate in discharging their energy at CSs.

In [26], a decentralized security model is presented to ensure the security of energy trading between EVs in a P2P network. The work also aimed at scheduling the EVs' charging time in an efficient manner using a realistic infrastructure. Authors in [27] proposed a trust based scheme for VANETs. The proposed work ensured locational privacy and identity protection of EV users. The trust management method was devised based on Dirichlet distribution. The proposed scheme efficiently detected malicious EVs and removed them from the network. Dorri et al. in [28] proposed a blockchain based model for promoting the security of users and privacy of the vehicular network. The costs incurred due to the wireless software updates and EVs' insurance are also included and dealt with in the proposed work. The service quality linked with wireless software is used to illustrate the efficiency of the proposed model.

A V2G data trading and sharing method is proposed in [29]. To address the issues of high computations and high cost of mining for microtransactions, a new protocol based on directed acyclic graph network is proposed. The protocol is suitable for lightweight transactions between network nodes. The negotiation about data sharing and energy trading between EVs and the grid is carried out using a game theory based model. The model optimizes the cost of the negotiation, which makes the proposed method efficient. The authors in [30] present a survey on applications of blockchain in the energy sector. In the survey, a deep analysis is provided on how blockchain is used in the energy sector so far and what are its possible future applications. The authors discuss the applications of blockchain in energy trading between vehicles, V2G, vehicles, and CSs, prosumers, etc. The existing models are studied, and a detailed discussion is provided to make the reader aware of the security and privacy challenges of blockchain. It is concluded that the blockchain technology is revolutionizing the traditional energy trading mechanisms and it is playing a vital role in improving the power system. Apart from the positive aspects of blockchain, it also suffers from different types of attacks. Feather forking attack is one of them [31]. In this type of attack, a minor node refuses to mine a block containing a specific transaction. The Reason for a minor's this kind of behavior can be that it may dislike the transaction or the node who is involved in the transaction. So, by refusing to mine the block it tries to blacklist the node or transaction. In [31], the feather forking attack is handled.

All the aforementioned schemes have some limitations. The schemes are either based on the energy trading between EVs or the V2G trading system. The existing schemes and their limitations are given in Table 1. In this paper, we propose an energy trading mechanism for V2V and V2G environments to get better energy trading results in the smart city. The working of our proposed scheme is described in detail in Section 3.

3. System model

In this section, we describe the proposed system model in detail, as shown in Fig. 1.

3.1. Consortium blockchain for energy trading

Blockchain networks are of three different types, which are public, private and consortium. A public blockchain is also known as a permissionless blockchain where everyone joins the network and participates in generating the blocks. Whereas, private and consortium blockchains

Table 1
Literature review.

Techniques	Goals	Achievements	Limitations
Blockchain technology with PoW consensus mechanism [2]	Efficient localized P2P energy trading	Improve localized demand response in plug-in hybrid EVs	High computational power consensus is used
Aggregator of EVs at residential PRKs [3]	Lower the charging cost and select the best charging service	Real time stochastic planning approach is introduced for EV users	Time complexity
Consortium blockchain technology with contract theory [4]	Provide incentive mechanism to motivate EVs in Internet of EVs	Energy trading framework is designed for EVs	Security issues, and Sybil and Re-Entry attacks are ignored
Hyperledger blockchain technology using proof of concept consensus mechanism [5]	Privacy-preserving payment mechanism for V2G network	Privacy preservation of data, and reliable and efficient payment mechanism is achieved	Prone to differential attack
Blockchain with PoW, edge nodes and SDN [8]	Reduce delay and network overhead issue, decisions making and provide nearest CS with distance and required time	Provide trading decisions closer to EVs' location using edge nodes and SDN for decreasing network latency	Accurate distance measurement issue and not well defined payment mechanism is given
Blockchain using PoW consensus and SDN [22]	Real time processing for energy trading, overcome security risks and reduce latency	Increase the overall security, use SDN to transfer EVs request to global SDN controller	Wallet is not secure, EVs selection as miner to perform PoW is tedious
Blockchain with Proof of Reputation (PoR) consensus mechanism [23]	Safeguard against internal and external attacks, and awing to the selfishness EVs	Overcame security risks and provide incentive mechanism	Focus only on EVs' reputation
Different charging infrastructures for EVs [24]	Differentiate between various charging infrastructures	Superiority of smart charging is achieved over dumb charging	Time complexity and security issues are not handled
Blockchain with edge computing and contract theory [25]	An efficient and secure energy trading in V2G	Incentive-based V2G energy trading framework is provided	CPA and CCA attacks are not tackled
Blockchain technology in P2P environment [26]	Scheduling of EVs' charging	Enhanced security and efficient charging scheduling	Time complexity
Blockchain-enabled privacy protection scheme in VANETs [27]	Location privacy of EVs and trust management	Trust based location privacy protection scheme is developed	Security analysis is not performed
Blockchain based architecture in vehicular ecosystem [28]	Protect users' privacy	a secure vehicular architecture is established	Trust issues are not handled

are permissioned where no one can join the network without permission. Moreover, in a private blockchain, only a single organization has control over the entire blockchain network. Unlike private blockchain, the consortium blockchain provides some access rules to join the network. We select consortium blockchain in our proposed system because it inherits security features from public blockchain and its network access is similar to private blockchain.

In the blockchain, the consensus process is quite important and it is used to verify the transactions before adding them in the blocks. In this work, the PoA consensus mechanism is used in which a validator is selected to validate transactions on the basis of the reputation values. In our proposed scheme, all LAGs are selected as validator nodes. Moreover, PoA requires less computational power than PoW. A smart contract is a computer protocol that digitally facilitates and validates transactions and contract negotiations happening in the blockchain network. A smart contract allows the reliable execution of transactions without the involvement of a third party. We have used smart contracts in our proposed scheme to provide an efficient payment mechanism. By using the smart contracts, we first obtain the wallet addresses of energy sellers and buyers and then energy coins are transferred between them at a predefined energy price.

3.1.1. *The proof of authority consensus mechanism*

In the existing PoW consensus mechanism, a hash-based mathematical puzzle is solved by nodes with high computational resources. Moreover, the hash-based puzzle is formulated as [32]

$$\mathrm{SHA256}(\mathrm{SHA256}(h, s)) < \mathrm{target}, \tag{1}$$

where h is the content of the blockchain, s is the solution that solves the puzzle and "target" is the level of difficulty for block mining. Because of the high computational resources required to execute PoW consensus mechanism, it is not suitable for our proposed scenario. Therefore, in this study, a new PoA consensus mechanism based on the reputation of nodes is used. In PoA consensus mechanism, reputation of each node is calculated instead of solving the hash-based mathematical puzzle. The key idea of PoA consensus mechanism is that a node rates another node based on direct interaction. In the blockchain, each node has an asset known as Reputation Point (RP) that is needed before any transaction is completed. RP is dynamically determined based on the Computation Factor (CF) as

$$CF = \begin{cases} \frac{\theta}{\sum_{i=1}^{n} \theta_i}, & \text{if } \rho > \Phi, \\ 0, & \text{otherwise}, \end{cases} \tag{2}$$

where CF lies within 0 and 1. n is the total number of nodes in the network, θ is the number of computational resources each node has, which is determined by hash rate and $\rho \in [0, 1]$ is the defined threshold that regulates malicious activities of a node. It is also used as the threshold for determining the double spending and Sybil attacks. $\sum_{i=1}^{n} \theta_i$ represents the overall computational resources of the network and Φ is the defined reputation threshold (i.e., $\Phi \in [0, 1]$). If $CF > 0$, then it means that the node is eligible to rate another node and vice versa. Based on CF value, the reputation of each node is calculated as

$$\mathrm{Reputation} = \mathrm{CF} \times \mathrm{rate}, \tag{3}$$

$$\mathrm{rate} = \begin{cases} 1, & \text{if there is an honest interaction}, \\ 0, & \text{otherwise}. \end{cases} \tag{4}$$

The mining task of each node in the blockchain network is given as

$$\mathrm{SHA256}(\mathrm{SHA256}(h, s)) < \mathrm{Reputation} \times \mathrm{target}. \tag{5}$$

3.1.2. *Creation of blocks and selection of miners*

In the proposed blockchain, three types of nodes are considered: ratee, rater and validators. The ratee is any node that receives ratings; whereas, a rater is any node that rates other nodes. Both rater and ratee nodes accept and relay ledger data in the blockchain. Validators are nodes with high reputation values while a node with the highest reputation value is the leader of the blockchain. Before any data is

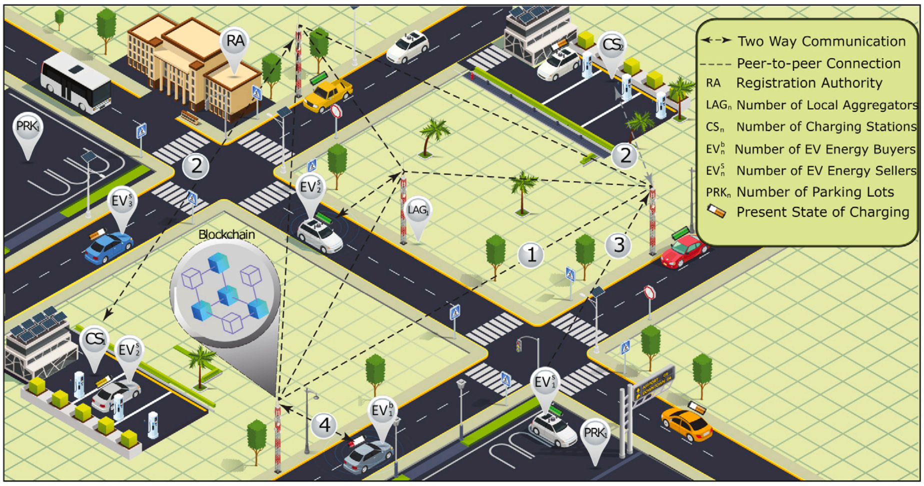

Two Way Communication
Peer-to-peer Connection
RA Registration Authority
LAG$_n$ Number of Local Aggregators
CS$_n$ Number of Charging Stations
EV$_n^b$ Number of EV Energy Buyers
EV$_n^s$ Number of EV Energy Sellers
PRK$_n$ Number of Parking Lots
Present State of Charging
RA
CS
PRK
LAG
Blockchain
EV
1
2
3
4

Fig. 1. Proposed system model for energy trading. ① LAGs are interconnected in a P2P manner, all energy trading transactions are stored, audited and verified by the authorized LAGs. ② CSs send the energy trading request to the LAGs. They reply back with the notification. ③ Seller EV sends the energy selling request form PRKs to LAGs. ④ Buyer EV gets the information of nearest energy seller with distance and required time and expenses.

recorded in the blockchain, it is digitally signed, hashed and encrypted by the leader of the network. The signed data is encapsulated as transaction in the blockchain. At any given time, all nodes have the same copy of the ledger and they become miners if their reputation values are greater or equal to Φ. Any node with reputation value less than Φ will not participate in the block mining and validation processes. Once the transactional data of a node is received by the leader, each validator verifies the signature by comparing it with the previous created block. If the verification is successful, then $K \in \mathbb{N}$ confirmation messages are broadcasted by validators. Afterwards, the leader provides the necessary services to the concerned node. A block is published if there are more than K confirmation messages received; otherwise, the block is not published. The theorems and proofs given in this study are used to validate the theoretical assumptions of the proposed model.

Theorem 3.1. *The proposed PoA consensus mechanism solves the miner centralization problem.*

Proof 3.1. The proof of Theorem 3.1 is given as follows. A miner centralization problem occurs when the same leader is selected at different polynomial time. Thus, the entire system is not secure. The proposed PoA consensus mechanism solves this problem based on CF, which means that at a given polynomial time t_1, the probability for selecting a leader is $\frac{1}{n}$. In subsequent polynomial time t_2, another leader will be selected with the same probability. It implies that CF of a leader changes on the basis of $\rho > \Phi$. Besides, θ of each node is different. Thus, the proposed PoA resolves the miner centralization problem.

Theorem 3.2. *There is no similar reputation value for different nodes when using the proposed PoA consensus mechanism.*

Proof 3.2. The proof of Theorem 3.2 is given as follows. A node is given high score when it engages in an honest interaction with other nodes and vice versa. Thus, the behavior of a node influences its reputation value. When a node behaves honestly, its rate value is 1; otherwise, it is 0. This means that the reputation of a node depends on CF and rate value. Moreover, no two nodes have the same CF, which means that θ values of the nodes are different. Thus, their reputation values can never be the same. Therefore, the proposed PoA consensus mechanism provides different nodes with reputation values that are not similar.

Theorem 3.3. *The proposed PoA consensus mechanism is robust against honest-but-curious nodes' behavior.*

Proof 3.3. From Proof 3.2, it is clearly proven that the behavior of a node influences its reputation. It implies that at a given time, a node behaves honestly and at other time, its behaves dishonestly in order to exploit the vulnerability of the proposed system. Based on the proposed PoA consensus mechanism, once a node has been detected to exhibit dishonest behavior, its gets the rate value of 0. Moreover, the defaulter node is penalized through reputation degradation and energy coin deduction. Thus, the proposed PoA consensus mechanism is robust against honest-but-curious behavior of a node.

3.2. Work flow of the proposed system

A typical scenario of our proposed model is illustrated in Fig. 1. There are four major entities in the proposed model, which are RA, CSs, EVs and LAGs. In our proposed scheme, CSs and EVs both act as energy sellers and buyers to participate in energy trading. RA is responsible for the registration of both EVs and CSs. Moreover, it also generates public (PK) and private (SK) key pairs to authenticate the nodes in the network. Both CSs and EVs register with RA to become bonafide nodes. As shown in Fig. 2, the step-wise flow of the proposed system model is described as follows.

Step 1: in the first step, a CS denoted as U_i, and an EV represented as V_j, with real identities ID_i and ID_j join the energy trading system. i and j are the indices of a CS and an EV, respectively. All LAGs are interconnected in a P2P manner to store, audit and verify the energy transactions.

Step 2: after joining the network, RA provides unique PK and SK key pairs to all participants for allowing them to participate in the energy trading environment.

Step 3: in this step, seller EV sends the energy selling request from PRKs to LAGs. In this manner, the surrounding EVs and other entities come to realize that which entities are available for energy selling.

Step 4: in this step, both U_i and V_j request for wallet addresses from the RA. RA generates a mapping list based on requests of both EVs and CSs, and provides wallet addresses to them.

Step 5: in this step, the coordinates of EVs and other charging entities are recorded, which further help in calculating the distance between different entities. Buyer EV gets the nearest charging entity's information with the required time, distance and expenses.

Step 6: after the energy transaction takes place, energy coins are stored in the wallets in this step. These wallets have specified addresses and are accessible through the smart contract during energy trading.

LAGs are considered as edge nodes with increased communicating and computing capabilities, which perform their role as energy brokers

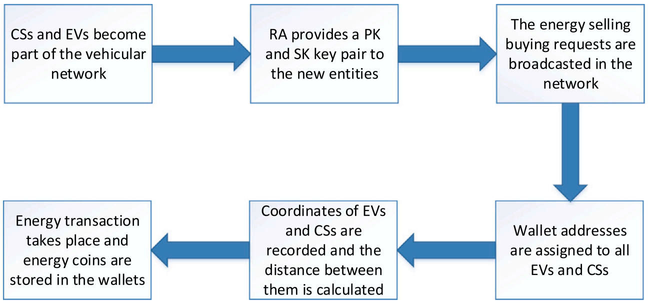

CSs and EVs become part of the vehicular network
RA provides a PK and SK key pair to the new entities
The energy selling buying requests are broadcasted in the network
Wallet addresses are assigned to all EVs and CSs
Coordinates of EVs and CSs are recorded and the distance between them is calculated
Energy transaction takes place and energy coins are stored in the wallets

Fig. 2. Workflow of the proposed system model.

to provide information about the nearby places where energy trading is to be performed. LAGs are interconnected in a P2P manner and blockchain technology is deployed on them. LAGs aggregate the energy trading requests from CSs and EVs to store, share and audit energy. Using the PoA consensus mechanism, trading transactions are verified and shared among LAGs.

In a smart city, CSs and PRKs are deployed at various locations. EVs need to travel some distance to reach any CS for charging or discharging their batteries. For this purpose, EVs want to know the required parameters, such as required distance ($Dist^{rq}$), required time (T^{rq}) and required expense (E^{rq}) to reach a destination for getting charged at better energy prices with maximum benefits [8]. Therefore, EVs send the request to LAGs to find the nearest CSs. LAGs then provide a list of nearest CSs with $Dist^{rq}$, T^{rq} and E^{rq}. An EV selects the preferable CS for energy trading according to the aforementioned parameters. LAGs carry the information of the pairs of energy sellers and buyers and send a notification to respective EVs and CSs regarding energy trading. During energy trading, smart contract calculates and records the energy amount in real time and then transfers coins accordingly. Finally, the buyer makes payment to the seller in response to the fulfillment of its requirement through the corresponding LAG.

In our proposed scheme, CSs and EVs are divided into two groups, which are sellers and buyers. The entire process of energy trading is described in Algorithm 1 where CSs and EVs select their roles according to the present State of Charging SoC^{pr}. Seller EV (EV^s), having surplus energy, sends the request to the nearest LAG for getting the list of nearest CSs. In Algorithm 1, the first two lines are for declaring $Input$ and $Output$. The request must be sent with ID_i, Role (R), Location (Loc^{cur}), SoC^{pr}, Battery Capacity (B^{cap}) and Time of Stay (T^{stay}). The lines 4 and 5 calculate Present Energy Units (E^{pr}_{kw}) and Available Energy (E^{av}_{kw}), respectively using Eqs. (6) and (7). While, line 7 calculates and Required Energy (E^{rq}_{kw}). Whereas, the lines 8 to 27 give the $Nested-if$ loop in which the energy prices given by different CSs are recorded and then EVs are informed with these recorded prices. A LAG verifies whether E^{av}_{kw} units are more than 10 kw or not. If E^{av}_{kw} are less than the required amount, then the energy request is discarded; otherwise, the Algorithm 1 moves to the next step. Lines 28 to 32 calculate the Energy Sale Price (P^s_i) using Eq. (8) [8], find the exact location and store the results in transactions pool. The last set of lines in the algorithm, i.e., lines 33 to 49 again present a $Nested-if$ loop, which first retrieves the energy requests from the transactions pool and then matches the EV with a preferable charging entity.

$$E^{pr}_{kw} = \left(\frac{SoC^{pr}}{100}\right) \times B^{cap}, \tag{6}$$

$$E^{av}_{kw} = B^{cap} - E^{pr}_{kw}, \tag{7}$$

$$P^s_i = a\left(\frac{B^{cap}}{E^{pr}_{kw} - E^{th}}\right), \tag{8}$$

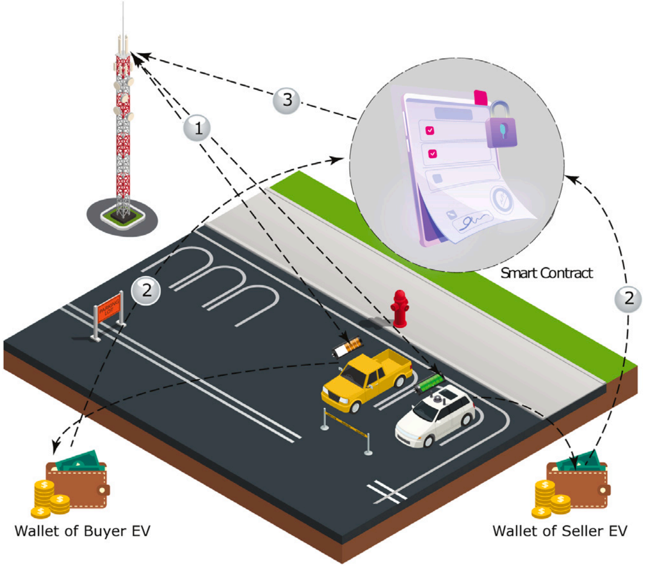


Fig. 3. Energy trading using smart contract. ① LAG sends the confirmed pair to the seller and buyer EVs. ② Smart contract runs and accesses addresses of both seller's and buyer's wallets. Smart meter calculates the energy amount and sends the recorded values to smart contract. ③ Smart contract transfers energy coins, and transaction stored and shared among LAGs.

where Eth is a threshold value. We select 30 percent constant value for Eth based on SoC for each EV's battery and a is used for constant price value, which is equal to \$0.32. However, Eth and a can be different in practice. In our proposed technique, we measure the Distance ($Dist$) using trusted third-party services, such as GPS, which provide accurate $Dist$ by calculating the road's length from EV's Loc^{cur} to CS's Loc^{cur}. LAG finds out the nearest CSs and broadcasts the EV's energy demand to CSs with P^s_i and E^{av}_{kw}. If any CS accepts the request, LAG creates the pair of EV and CS. After that, the smart contract is executed between the selected EV and CS. In Fig. 3, the execution of smart contract designed for payment method is shown.

The smart contract accesses and verifies the seller's and buyer's wallet addresses as given in Algorithm 2. Energy coins are provided to the seller according to the traded energy through the corresponding LAG using the smart contract. If energy coins are available, then the smart meter records the real energy amount and asks for the energy from the seller. The seller then transfers the energy to the buyer and gets required payment. The energy buyer also gives ratings to the seller for the fulfillment of its satisfaction. The LAG stores the validated transactions in the consortium blockchain ledger, which is shared by all LAGs.

CS also sends the energy trading request to the LAG with ID_i, R, Loc^{cur}, SoC^{pr}, B^{cap} and Present Time Slot (T^{slot}). If value of SoC^{pr} is up to SoC^{th}, then LAG performs PoA consensus mechanism to validate the transactions and store them in blockchain. Otherwise, LAG discards the energy request and sends the notification back to CS.

Consequently, we describe the buyer's energy trading process, when a buyer EV (EV^b) sends the request with required parameters to the LAG to find the nearest available CS or PRK. LAG verifies the energy trading request and calculates the distance from buyer's location to seller's location. After measuring $Dist$, LAG provides the list of nearest CS and PRK with $Dist^{rq}$, T^{rq}, E^{rq} and P^s_i to the EV.

$$Ex^{rq} = \left(\frac{Dist_{i,j}}{1000}\right) \times \left(\frac{P^s_i}{8.21}\right). \tag{9}$$

In Eq. (9), the calculated $Dist_{i,j}$ is given in meters, we divide it by 1000 to get values in kilometers and with the help of provided information by [33], we are able to estimate that an EV travels at least 4.0 km and maximum 8.21 km using energy of 1 kWh. The selected type of EVs and their properties for our proposed scheme are given in Table 2. Based on the provided information, we select the maximum energy consumption value that is 8.21 km.

Algorithm 1: Energy trading request

```
**Inputs:** $ID_{i,j}, R_{i,j}, Loc_{i,j}^{cur}, SoC^{pr}, B^{cap}, and\ T^{slot}$
**Output:** Confirmed Pair
$E_{kw}^{pr} = \left(\frac{SoC^{pr}}{100}\right) \text{x} B^{cap}$
$E_{kw}^{av} = B^{cap} - E_{kw}^{pr}$
//calculate the required energy by EV
$E_{kw}^{rq} = B^{cap} - E_{kw}^{pr}$
if $R^{type} := EV_i^s$ then
    $E^{th} = \left(\frac{30}{per}\right) \text{x} B^{cap}$
    if $E_{kw}^{av} > 10_{kw}$ then
        $Loc = Loc_i^{cur}$
        $P_i^s = a\left(\frac{B^{cap}}{E_{kw}^{pr} - E^{th}}\right)$
        //compute price
        $geocode(Loc)$
        // This function is called to get the nearest CSs.
        for $k$=1 to No. of nearest CSs do
            price announced to nearest CSs;
        end
        if CS select EV's Request then
            $i, j$ pair confirmed
        else
            request stored in transactions pool with $Loc_i^{cur}$ and $P^s$
        end
    else
        reply: present energy is very low
    end
end
if $R^{type} := CS_j^s$ then
    $P_i^s = a\left(\frac{B^{cap}}{E_{kw}^{pr} - E^{th}}\right)$
    $geocode(Loc)$
    request stored in transactions pool with $Loc_i^{cur}$ and $P^s$
end
if $R^{type} := EV_i^b$ then
    get requests from transactions pool with seller's $Loc_i^{cur}$ and $P^s$
    for $j$=1 to last 10 requests do
        $get\ Loc^s$ and $P^s$
        $Dist_{i,j}^{rq} = gmaps.distance\_matrix(Loc_i^b, Loc_{i,j}^s)$
        $Ex^{rq} = (Dist_{i,j}/1000)\text{x}(P^s/8.21)$
    end
    announce $Ex^{rq}, Dist_{i,j}^{rq}, T^{rq}\ and\ P^s$ to buyer EV
    if EV selects preferable CS or EV then
        buyer and seller pair is confirmed
        pair is sent to smart contract for energy trading
    else
        request discarded
    end
else
    send reply: select your energy trading role
end
```

In the proposed model, an EV selects the preferable energy trading place from the list of available energy selling places based on the distance. LAG creates the pair of both buyer and seller and sends the notification for energy trading. As we explained above, a smart contract is executed during energy trading and smart meter calculates and records the energy units and price. Smart contract accesses the wallet addresses of both seller and buyer and according to the smart meter's calculation, while coins are transferred from buyer's wallet to seller's wallet as shown in Fig. 3. Finally, smart contract is executed and transactions are stored and shared among LAGs. Table 3 shows 1–1 mapping of the limitations identified in this work with their proposed solutions. In the table, the limitations are denoted as *L.1–L.5*. While, the proposed solutions are referred as *S.1–S.5*.

Algorithm 2: Energy trading smart contract

```
**Inputs:** $ID_i^s, ID_i^b\ verify(ID_i^s)$
$verify(ID_i^b)$
$wallet^s\ =\ access\ wallet\ address\ according\ to\ ID_i^s$
$wallet^b\ =\ access\ wallet\ address\ according\ to\ ID_i^b$
$event\ Sent(from,\ to,\ amount)$
$transferEnergyCoin(wallet^s,\ wallet^b,\ P_{kw}^s,\ E_{kw})$ {
$amount^{payable}\ =\ P_{kw}^s$ x $E_{kw}$
if $amount^{payable}\ >\ balance[wallet^b]$ then
    insufficient balance please buy coins
end
$balance[wallet^b]\ -=\ amount^{payable}$
$balance[wallet^s]\ +=\ amount^{payable}$
$emit\ Sent(sender,\ receiver,\ amount^{payable})$
}
```

Table 2
Different type of EVs.

EVs type	Battery capacity	Range	Consumption
Type 1	42 kWh	345 km	8.21 km/kWh
Type 2	30 kWh	160 km	5.3 km/kWh
Type 3	90 kWh	360 km	4.0 km/kWh
Type 4	75 kWh	496 km	6.61 km/kWh

3.3. *Incentive provisioning and punishment mechanism*

In the proposed system model, EVs are provided with incentives based upon their reputation values. The aim of the incentive mechanism is to encourage the network node to participate in energy trading process. The reputation values of EVs further depend upon the credibility of the messages provided by the EVs. Moreover, the incentives are also given by the EVs to the charging entities upon efficient fulfillment of the energy requirements. The incentives ensure that no entity in the network act selfishly or maliciously. If any entity in the network act maliciously, it will not be given any incentive. Fig. 4 shows the flowchart of the incentive provisioning mechanism used in this work. The flowchart starts with the authorization verification of an EV. If an EV is verified, then the credibility of the message broadcasted by that EV is checked. Else, the EV is marked as malicious. Later, if the received message is found to be credible, then the EV is awarded with incentives; else, it is not awarded with an incentive.

In this study, each node in the blockchain network has different behavior orientations. It means that the node may behave selfishly for the purpose of endangering the network. A malicious node affects the stability and reliability of a network. It attempts to paralyze the network and also injects fake information. In a blockchain network, a malicious node tries to access and alter the information in an illegal way. Moreover, it creates fake transactions and flood the transaction pool with invalid transactions. As a result, the computational power and time of validator nodes is wasted. Additionally, several attacks are generated by malicious nodes in a blockchain network, 51% attack, double spending attack, selfish mining attack, sybil attack, replay attack, etc., which endanger the security, immutability, and decentralization of blockchain. If the number of malicious nodes increase in the network, the network is comprised. For example, if more than 50 percent of the blockchain nodes become malicious then 51% attack can be generated, and malicious nodes will take over the blockchain network. So, an efficient mechanism is required to discourage the malicious activities of nodes in the network. In the literature [34–36], malicious nodes detection and removal mechanisms are proposed. In [34,36], the vehicles are rated by other vehicles after providing the services. However, only service receivers rate the service providers. In case of a malicious service receiver, the honest service provider will

Table 3
Mapping of limitations with proposed solutions.

Limitation number	Limitation identified	Solution number	Proposed solution
L.1	Excessive resource consumption using PoW consensus mechanism	S.1	PoA consensus mechanism used
L.2	Accurate distance measurement	S.2	GPS used to measure the distance
L.3	Energy coin wallets not secured	S.3	Smart contract used to ensure security
L.4	Excessive time consumption by miners while selecting EVs	S.4	Mining performed by LAGs and EVs are selected
L.5	Robustness against attacks	S.5	Security analysis done using Oyente

suffer. In [36], when the reputation score of vehicles decreases a certain limit, they are excluded from the network. On the other hand, in [34], the vehicles are temporarily banned from the network; however, it is not mentioned how vehicles will rejoin the network. Moreover, in [36], the reputation of vehicles is not updated on each transaction. After a fix interval, the reputation values of all vehicles are computed. So, the reputations of those vehicles is also computed, which did not take part in the transactions. It wastes both the computational time and efforts of the validator nodes. Additionally, a malicious node detection and avoidance mechanism is proposed in [35]. Here, the vehicles are identified as malicious on the basis of their past encounter with other vehicles. The malicious vehicles are removed from the network. Keeping all these points in view, a new malicious vehicles identification mechanism is proposed.

In the proposed scenario, once a node is detected to commit fraudulent activities (i.e., malicious node), its Attitude Correction Factor (ACF) is degraded and a certain amount of coin is charged. In the strategy, an ACF is defined by the leader of the blockchain, which ranges between 1–10. The proposed system provides a way where the selfish or fraudulent nodes' behavior can be remedied through an attitude enhancement strategy, i.e., the selfish nodes are not removed from the network on their first malicious activity like [35]. It is necessary because an honest node may unknowingly commit a malicious activity and removing such node will not be fair. On a malicious activity, ACF value of the node degrades by 2 points and its reputation value becomes zero. Now it cannot take part in validation process; however, it can still participate in energy trading. With each valid transaction, the ACF score of the node increases by one point. When the ACF value of the node reaches 10, it means that the node's selfish behavior has been remedied; thus, its reputation value starts increasing. On the other hand, if the node keeps on committing malicious activities, its ACF score decreases by 2 points. If the ACF of the node becomes less than or equal to 1, it implies that the node's selfish behavior cannot be remedied; thus, the selfish node is blacklisted and its information is broadcasted over the network. Note that the ACF value is determined by the consensus of the leader and all validators. Therefore, a single validator or leader cannot manipulate the ACF value like [34,36]. When a nodes acts maliciously, its ACF is reduced by 2 points. However, when it acts normally its ACF is increase 1 points. In this way, a malicious node get chance to avoid the malicious activities.

3.4. Power flow in vehicular networks

In vehicular networks, efficient flow of information between different entities like EVs, CSs, Road Side Units (RSUs), etc., plays an important role. Moreover, lossless flow of power is also encouraged between EVs and other entities in vehicular networks. The charging of EVs in vehicular networks must be done in such a manner that minimum economic and power losses should be incurred [37]. Otherwise, serious economic impacts in terms of infrastructure degradation, excessive power loss, increased charging rates, etc., are to be faced. These losses are further comprised of many other losses like cable loss, transformer loss, hysteresis loss, I^2R loss, etc. These losses are not just confined to a certain strategy, scheme or area, they exist everywhere, and in both V2G and V2V environments.

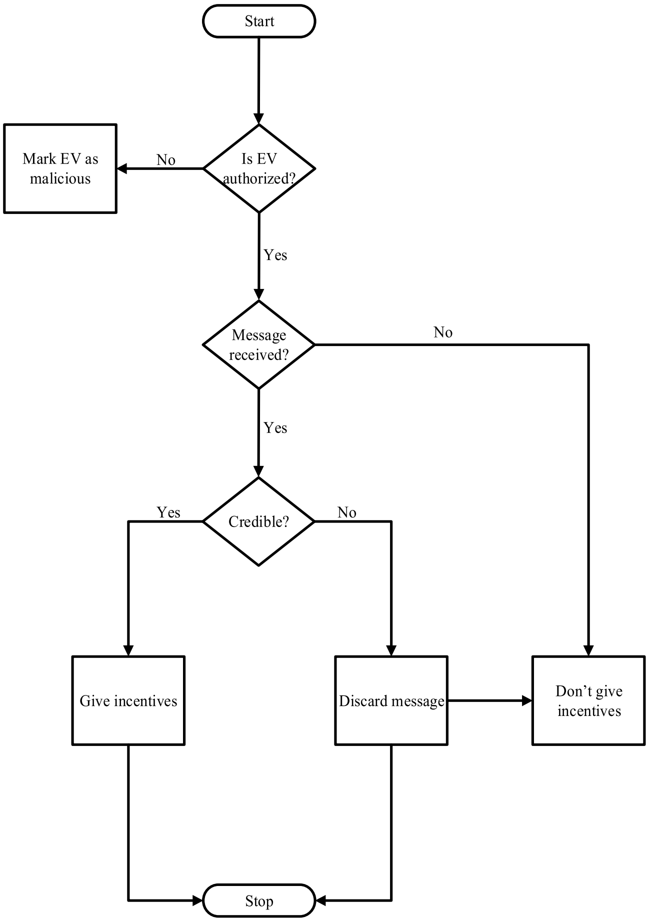


Fig. 4. Flowchart of incentive provisioning.

3.5. Associated energy losses

In Fig. 5 the energy losses associated with the charging of EVs using V2G and V2V energy trading environments are shown. There exist different types of energy losses, which are broadly classified into three main classes: Grid loss G_{loss}, Vehicle loss V_{loss} and Infrastructure loss I_{loss}. The grid losses comprise of all the faults, which occur at the CSs like transformer loss, circuit breaker loss, copper loss, I^2R loss, etc., [38]. Whereas, the vehicle losses include the ones, which occur in the EVs like battery loss, inverter loss, etc. The infrastructure loss includes the cable loss, current loss and those caused by severe weather effects.

3.6. Mathematical formulation of energy losses

In this subsection, the energy loss associated with the power flow in both V2G and V2V are mathematically formulated. As already discussed above that there exist three different types of energy losses, which are G_{loss}, V_{loss} and I_{loss}. All of these losses are summed up to provide us

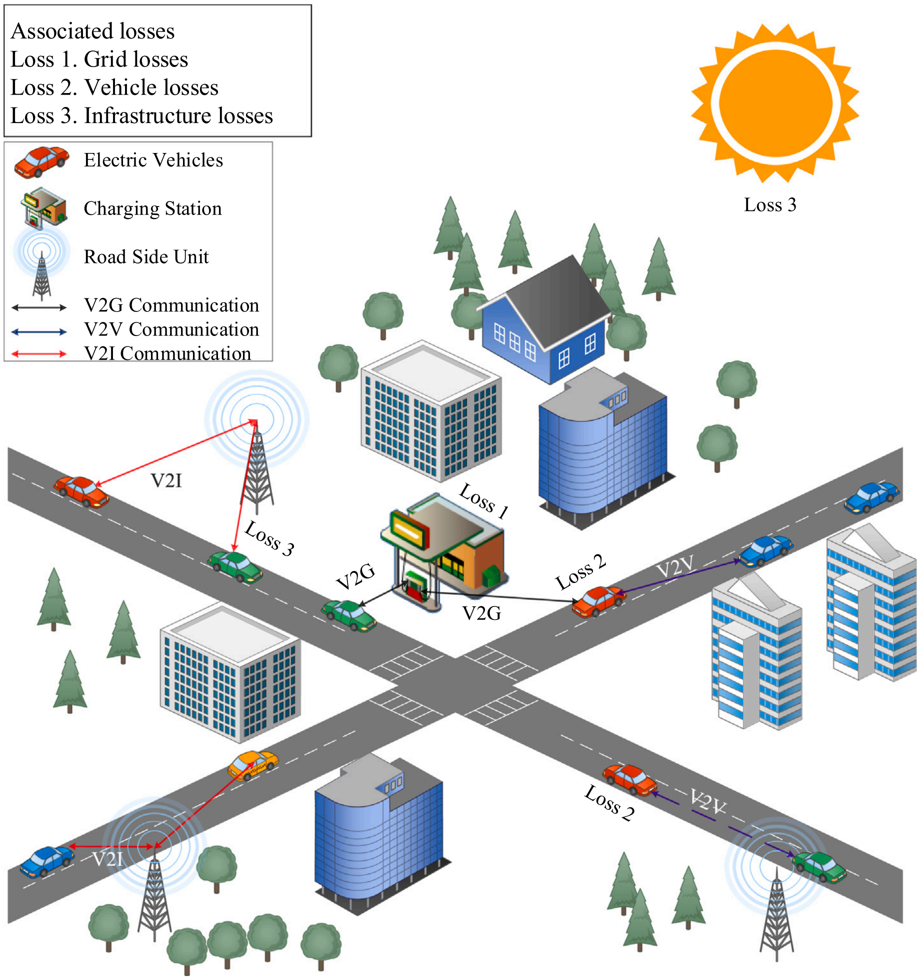


Fig. 5. V2G and V2V energy losses.

with the Total Power Loss P_{loss}^{total}, given in Eq. (10).

$$P_{loss}^{total} = G_{loss} + V_{loss} + I_{loss}. \tag{10}$$

These losses are individually formulated in Eqs. (11)–(13) below.

$$G_{loss} = transfomer_{loss} + line_{loss} + misc_{loss}, \tag{11}$$

$$V_{loss} = inverter_{loss} + battery_{loss}, \tag{12}$$

$$I_{loss} = cable_{loss} + current_{loss} + weather_{loss}. \tag{13}$$

During mathematical formulation of any phenomenon, the objective function and the subjected constraints must be kept in mind. Keeping this in view, the objective function is formulated to minimize the P_{loss}^{total}, given in Eq. (14). The objective function can be achieved using updated and efficient grid infrastructure, charging cables, vehicle inverters and batteries, increased insulation for protection against severe weather effects, etc.

$$Objective\ Function = \min(P_{loss}^{total}). \tag{14}$$

Subjected to constraints provided in Eqs. (15)–(20) .

$$16Amp \le I_t \le 32Amp, \tag{15}$$

$$0\% < transformer_{loss} \le 5\%, \tag{16}$$

$$0\% < line_{loss} \le 10\%, \tag{17}$$

$$0\% < inverter_{loss} \le 40\%, \tag{18}$$

$$0\% < battery_{loss} \le 30\%, \tag{19}$$

$$0 \le weather_{loss} \le 1. \tag{20}$$

The total losses occurred in both V2G and V2V energy trading environments are given below in terms of two Cases. Cases 1 discusses the energy losses in V2G, whereas Case 2 presents the losses incurred in V2V. The mathematical formulation is also provided below.

- **Case 1: Energy losses incurred in V2G** In V2G charging of EVs, the losses incurred are transformer loss, line loss and some miscellaneous losses like hysteresis loss, corona effect loss, I^2R loss, etc., [39]. The power losses incurred in V2G are calculated using Eq. (10).
- **Case 2: Energy losses incurred in V2V** The losses incurred in V2V include vehicle losses and infrastructure losses. However, it does not include the grid loss. As energy trading is done between two EVs, both equipped with energy inverters; therefore, the inverter inefficiencies will be added up [40]. Moreover, the battery loss is also incurred, which has a major contribution in accumulative power loss as well. Eq. (21) is used to calculate the power loss incurred in V2V charging of EVs.

$$P_{loss}^{total} = V_{loss} + I_{loss}, \tag{21}$$

where $G_{loss} = 0$.

4. Security objectives and analysis, and attacker models of the proposed system

In this section, we first discuss the security objectives of our proposed energy trading scheme. After that, we evaluate the security analysis of the proposed smart contract using the Oyente tool. Finally, two attacker models are formulated.

4.1. Security objectives

Unlike the traditional energy trading scheme's security and privacy protection, we use consortium blockchain in the proposed work. Instead of PoW, PoA consensus mechanism is used because only LAGs are selected as authorized nodes who validate the transaction data. While, EVs and CSs request LAGs for the buying and selling of energy. LAGs make a pair of the selected buyer and seller and then secure them using their identities. Likewise, all of the energy nodes (EVs, CSs and LAGs) are registered and permitted to join the energy trading network. The node must show its identity for getting permission to enter in the energy trading network. Thus, the energy trading network can be protected from both Sybil and double spending attacks.

4.1.1. Data auditability

Blockchain is used in our proposed scheme that keeps energy trading requests and payment records in an easily verifiable, timestamped and tamper-proof manner. It ensures that each node needs to get a license to join the network. Because of this, no adversary entity can become part of this network or add false blocks to the blockchain. Records in the blockchain network are tamper proof and there is a guarantee that data can be audited when required.

4.1.2. Wallet security

A smart contract is used for a fair payment system. The energy buyer requests LAGs for energy, which execute smart contracts and access the buyer's and the seller's wallet addresses. However, the wallet addresses are not shared publicly; therefore, without corresponding keys, no adversary can access the wallets and chances of stealing energy coins become zero.

4.1.3. Transaction authentication

Using PoA with blockchain, data of all transactions is validated by authentic LAGs. Therefore, it is impossible for the malicious nodes to compromise the system.

4.1.4. No transaction tampering

A financially-motivated attacker in an energy trading environment can tamper energy price or energy selling and buying requests. However, in consortium blockchain, the attacker cannot modify transaction because blockchain is tamper-proof.

4.1.5. Refusing to pay

In this attack, the malicious EV may pretend that it has not received any energy from the seller CS or EV and may also refuse to pay the cost of purchased energy [22].

4.1.6. Concurrency bug

This is a bug that arises when two functions are executed at the same time. This problem is often encountered while updating a data structure or a database. In the proposed model, PoA based consortium blockchain is used, so, only one block will be appended to the blockchain at a time. Besides, in blockchain, even if two blocks are created at the same time there would be a difference of micro seconds in their creation. So, the first block will be kept and second will be discarded.

4.2. Smart contract analysis

A smart contract allows a reliable transaction without the involvement of a third party. Therefore, it is very important to analyze the smart contract for possible bugs and loopholes. Oyente symbolic execution tool is used for smart contract's security analysis. It is developed by researchers from the National University of Singapore [41]. Oyente is able to test some of Ethereum's security flaws including EVM code coverage, integer underflow, integer overflow, parity multisig bug 2, callstack depth attack vulnerability, transaction-ordering dependence, timestamp dependency and re-entrance vulnerability bugs. The details of these bugs are given below. The smart contract used in our proposed scheme is analyzed by Oyente and results of security analysis are shown in Fig. 6 in which the result of all the above-mentioned attacks are seen as false.

4.2.1. Integer underflow and overflow

These bugs arise when the values of integers used in the smart contract exceed the predefined upper and lower limits. When the integer values exceed the set boundaries, the smart contract fails and whole system comes to a halt [42].

4.2.2. Parity multisig bug 2

This type of bug occurs when the attacker gets hold of multiple accounts and generate fake signatures for them. When a large number of such accounts are summed up, they cause the smart contract to stop, leading to the failure of the system [43].

4.2.3. Callstack depth attack vulnerability

This attack is also called a call depth attack. In this attack, the calling function fails if the call depth is equal to 1024 frames and it is only executed when its depth value is at most 1023 frames.

4.2.4. Timestamp dependency

In this attack, a miner manipulates the timestamp's conditions to favor himself during transaction mining. Every machine has its own physical time, called timestamp.

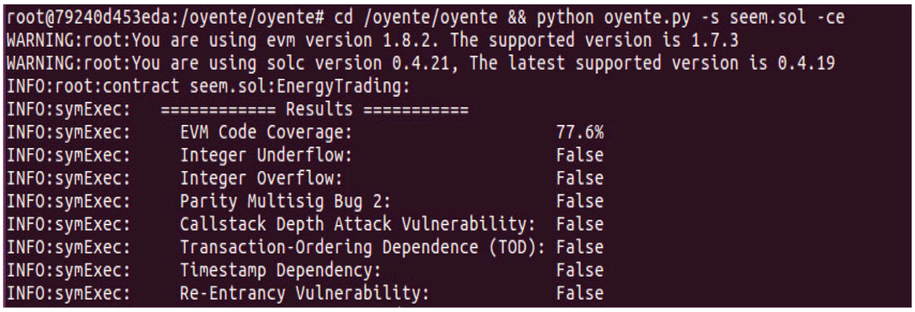
4.2.5. Re-entrancy vulnerability

In this vulnerability, the path condition is used and verified. For example, if one smart contract in Ethereum calls another smart contract, then the current transaction waits for that call to end and the use of the caller's intermediate state can cause problems.

4.3. Attacker models for blockchain

To design the attacker models, several assumptions and parameters are considered in this study. Moreover, the attacker can be any member of the network. In this study, we consider the double spending, Sybil attacks and feather forking attacks [31]. These attacks are more suitable for our proposed scenario, which means that once the attacks are prevented, other related attacks, such as refuse to pay attack [22,23], re-entry attacks [23], etc., cannot affect the proposed system.

In the energy trading environment, attacker nodes not only pose a threat to network security, but also cause financial loss to CSs and EVs. Apart from the aforementioned attacks, there are some other attacks and vulnerabilities, such as call stack attack, time dependency attack, concurrency bug and re-entrance vulnerability, which can damage the blockchain-based systems [44]. Similar attacks are discussed in [21] to analyze the security of their model. In the early stages of the development of Ethereum, there was a big case of Decentralized Autonomous Organization (DAO) hacking, which occurred in June 2016 and caused a loss of 3.6 million ethers [41].



```
root@79240d453eda:/oyente/oyente# cd /oyente/oyente && python oyente.py -s seem.sol -ce
WARNING:root:You are using evm version 1.8.2. The supported version is 1.7.3
WARNING:root:You are using solc version 0.4.21, The latest supported version is 0.4.19
INFO:root:contract seem.sol:EnergyTrading:
INFO:symExec:   ============ Results ===========
INFO:symExec:     EVM Code Coverage:                     77.6%
INFO:symExec:     Integer Underflow:                     False
INFO:symExec:     Integer Overflow:                      False
INFO:symExec:     Parity Multisig Bug 2:                 False
INFO:symExec:     Callstack Depth Attack Vulnerability:  False
INFO:symExec:     Transaction-Ordering Dependence (TOD): False
INFO:symExec:     Timestamp Dependency:                  False
INFO:symExec:     Re-Entrancy Vulnerability:             False
```

Fig. 6. Security analysis result of smart contract.

4.3.1. *Double spending attack model*

Double spending occurs when the same token is used twice for making payment. In the double spending attack, the attacker behaves as an honest node in the network. Here, the attacker propagates two payment transactions and publishes them over the network. This implies that the attacker can mine the two transactions along with the honest nodes in the network. Before the receiver node gets the payment, the attacker covertly releases the mined blocks for creating forks in the network. Once a fork is created, the transaction of the receiver node becomes invalid. It means that the request or response of the receiver node is discarded. In our scenario, we assume that the attacker is a malicious LAG and the receiver node is a CS. When an EV request for energy it makes pair of both buyer EV and seller CS. Now there are two cases, the attacker either pays himself or pays back to the EV, who got energy from the CS. In the first case, the CS will be befitted by getting money, while in the second case, it just performs a malicious activity to harm the energy trading process. Suppose, the LAG wants to pay himself, after energy trading, it creates two payment transactions: paying himself and paying the CS. Once the attacker succeeds in mining the former, then a block is continuously added to the blockchain and afterwards, an incentive is given to the attacker. This implies that the attacker has created a false branch in the network. If the false branch of the attacker is the longest in the network, then honest nodes must accept it as the valid branch [45]. At the end, CS provides energy to the EV without receiving any payment. In this study, a time based double spending model is developed, which is motivated from [45]. The existing model in [45] considers time advantage while the proposed model considers both time and computational advantages of the attacker. It means that the attacker has time and computational advantages to mine n blocks given that an honest node mines the mth block. Besides, in this study, the same branch length of both honest and attacker nodes are assumed along with different mining time t. In the proposed double spending model, the following parameters are considered.

1. The quantity $q \in [0,1]$ is the probability that an attacker mines a block before the honest node. q can also be defined as the percentage of computational power of an attacker to the total computational power of the network.
2. The quantity $\tau \in \mathbb{R}_{>0}$ is the expected time (seconds) that is required for mining a block.

This study defines a catch up function $C(q,z)$ as the probability of accomplishing the double spending attack where the branch length of the attacker is the longest given the initial disadvantage of z blocks. A potential process function $F(q,m,n)$ is the probability that an attacker mines exactly n blocks once an honest node mines the mth block. Nevertheless, $C(q,z)$ and $F(q,m,n)$ are required for formulating the probability of performing double spending attack $DS(q,K,t)$, which is derived as [45]

$$C(q,z) = \begin{cases} (\frac{q}{p})^{z+1}, & \text{if } q < \rho \wedge z > 0, \\ 1, & \text{otherwise}, \end{cases} \tag{22}$$

where $p = 1-q$ is the probability that an attacker has less computational resources.

$$F(q,m,n) = \begin{cases} 1, & \text{if } m = n = 0, \\ \binom{m+n-1}{n} q^n p^m, & \text{otherwise}, \end{cases} \tag{23}$$

where $\binom{m+n-1}{n} q^n p^m$ is the negative binomial distribution.

$$P(q,m,n,t) = \sum_{z=0}^{n} a(q,t,z)F(q,m,n-z), \tag{24}$$

$$a(q,t,n) = \begin{cases} 1, & \text{if } t = n = 0, \\ 0, & \text{if } t \leq 0, \\ \frac{(qt)^n}{n!} \exp^{-qt}, & \text{otherwise}, \end{cases} \tag{25}$$

where $P(q,m,n,t)$ is the probability that an attacker mines n blocks before the honest node mines the mth block. $a(q,t,n)$ is the probability of mining the n blocks in $t\tau$ seconds given q.

$$DS(q,K,t) = 1 - \sum_{n=0}^{K-n} \Big((P(q,K,n,t))(1 - C(q,K-n-1))\Big). \tag{26}$$

4.3.2. *Sybil attack model*

In the Sybil attack scenario, an attacker creates fake identities for deceiving honest nodes into rating him highly. The idea of the Sybil attack is obtained from [46]. This attack is necessary for the attacker as it receives high reputation during energy trading. This paper determines the probability of successful Sybil attack created by the attacker. We denote ns to be the number of successful Sybil identities and N to be the number of identities of honest nodes in the network. The total identities are $N + ns - 1$. Let w be the number of identities that are selected from $N + ns - 1$ at the initial stage. In each trial of the attack, the probability of successful Sybil attack is the number of Sybil identities created by the attacker, which is broadcasted over the network. The attacker fails to implement the Sybil attack if the number of Sybil identities are less than ρ. The probability $P[w]$ of selecting w Sybil identities randomly from $N + ns - 1$ identities in each trial is defined as

$$P[w] = \frac{\binom{ns}{w}\binom{N-1}{N-w}}{\binom{N+ns-1}{N}}. \tag{27}$$

Eq. (27) corresponds to a hypergeometric distribution where $\binom{ns}{w} = \frac{ns!}{w!(ns!-w!)}$ is a binomial coefficient.

4.4. *Feather forking attack*

A feather forking attack occurs when a miner refuses to mine a block because of the presence of a transaction, which it does not like. This attack is generated to blacklist an entity from the network. A miner node generates this attack when it becomes biased towards a node, and it does not allow its transactions to be added in the blockchain. In such a scenario, the attacker tries to involve other miners as well.

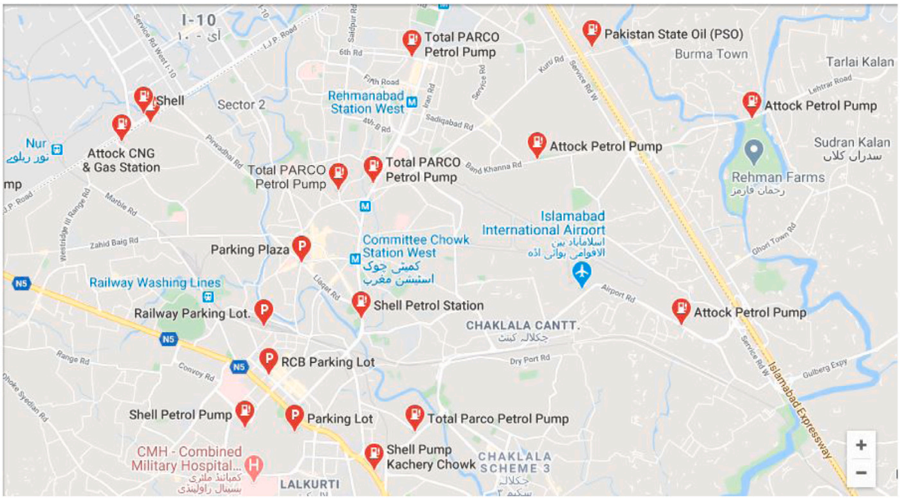


Fig. 7. Distribution of CSs and PRKs in the real map.

Table 4
Losses incurred in V2G.

Types of loss	SoC = 50%	SoC = 60%	SoC = 70%
Grid loss (%)	7.6%	6.5%	5.8%
Vehicle loss (%)	2.74%	2.50%	2.42%
Infrastructure loss (%)	3.5%	3.2%	2.95%
Total loss (%)	13.84%	12.5%	11.17%

Table 5
Losses incurred in V2V.

Types of loss	SoC = 50%	SoC = 60%	SoC = 70%
Grid loss (%)	0	0	0
Vehicle loss (%)	6.85%	6.25%	5.86%
Infrastructure loss (%)	3.72%	3.45%	3.38%
Total loss (%)	10.57%	9.70%	9.24%

The reason is that it needs 51% of the computational power of the whole network to blacklist a node. On the other hand, a victim node increases the transactional fee and pays other nodes more transactional fee to validate its transactions. In this way, it saves himself from being blacklisted from the network. The authors in [31] used this attack in their work. However, they have used it as a positive force. Using this attack, the energy providers who use non renewable energy resources for energy generation, pay more transactional cost. Besides, in our scenario, suppose a miner wants to blacklist an EV from the network and refuses to mine its transactions. On encountering such activity, other validators and miner nodes will reduce the ACF of the respective miner. So, if the miner will keep on refusing the transactions of an honest EV, after certain attempts, it will be declared malicious and removed from the network. However, if the miner starts working normally, its ACF value will be increased. Moreover, as we are using PoA consensus mechanism and miner node is selected on the basis of reputation value, so, a malicious node cannot become a minor. It will only refuse to validate the transaction or block, which contain the specific transaction.

5. Simulation results

In this section, the mathematical results are presented in tabular form. Table 4 gives the values of the losses incurred in V2G charging of EVs. Whereas, Table 5 provides the values of losses incurred in V2V charging. The results are obtained using three different values of SoC, i.e., 50%, 60% and 70%. The values are taken from [47] and [48]. It is observed that the loss values decrease with the increase in SoC values.

Table 6
Minimum hardware requirements to become a minor.

Hardware	Requirements
Disk space	350 GB
Download	500 MB/day
Upload	5 GB/day
Memory (RAM)	1 GB
System	Desktop, laptop, some ARM chipsets > 1 GHz
Operating system	Windows 7/8.x/10, Mac OS X, Linux

5.1. Experimental setup and results' description

A computer with a 1.61 GHz core m3-7y30 processor, 8 GB DDR4 RAM and Windows 10 operating system is used for simulations. The proposed model is implemented using Remix IDE, Ganache, MetaMask and Python 3.7. The hardware specification mentioned above are used for simulation purpose only. In real environment, the hardware specifications for LAGs will be different. Bitcoin is the common application of blockchain. The minimum system requirements to become a minor in bitcoin are given in Table 6 [49]. As the bitcoin uses PoW consensus algorithm, which is computationally more expansive than PoA; however, these are the minimum requirements. In our scenario, the required disk space and download and upload rates will vary because these parameters depend on the size of the network and amount of data being shared. The parameters given in Table 6 are presented to give the reader an idea of hardware requirements of LAGs in the real environment. However, the LAGs are not limited to these specifications.

The performance of our proposed model is analyzed using a real dataset in a real city area of the energy trading environment. The selected area is approximately 9.33 × 12.45 km^2 including 13 CSs, 7 PRKs and 50 EVs as shown in Fig. 7. The locations of the CSs shown in Fig. 7 are actually the locations of the real gas stations, which we have designated as CSs so that there is no problem of finding the distance from the EVs to the CSs. Real data has been used to calculate the accurate and efficient distance with the help of GPS when an EV traverses a fixed route from one place to another for energy trading. For instance, an EV wants to reach destination “D” from source “A”, it has to go through places “B” and “C” to reach destination “D”. Distances between all CSs are shown in Table 7.

As finding accurate distance is very important, so, we have used third-party services, such as GPS to measure the accurate distance. Besides, we have selected different types of EVs, which have different types of batteries. EVs and their battery specifications are shown in Table 2. However, SoC of the EV's battery is an important factor for

Table 7
Distance between CSs.

	CS_1	CS_2	CS_3	CS_4	CS_5	CS_6	CS_7	CS_8	CS_9	CS_{10}	CS_{11}	CS_{12}	CS_{13}
CS_1	–	3.9 km	4.1 km	2.9 km	6.5 km	7.8 km	14.6 km	11.4 km	13.5 km	14.4 km	16.1 km	15.3 km	17 km
CS_2	–	–	3.8 km	3.1 km	6.7 km	7.5 km	14.3 km	11.1 km	13.7 km	14.5 km	16.1 km	13.3 km	16.7 km
CS_3	–	–	–	3.1 km	6.7 km	4.4 km	6.1 km	5.6 km	6.9 km	8.9 km	8.8 km	7.4 km	13 km
CS_4	–	–	–	–	3.8 km	8.8 km	13.2 km	10 km	10.8 km	11.6 km	11.6 km	12.2 km	15.6 km
CS_5	–	–	–	–	–	10.5 km	9.2 km	11.8 km	7 km	7.9 km	9.5 km	13.6 km	15.1 km
CS_6	–	–	–	–	–	–	5.1 km	1.3 km	7.2 km	8 km	7.9 km	5.2 km	8.6 km
CS_7	–	–	–	–	–	–	–	3.4 km	6.2 km	8.2 km	8.1 km	3.9 km	11 km
CS_8	–	–	–	–	–	–	–	–	6.6 km	9 km	7.2 km	4.4 km	7.8 km
CS_9	–	–	–	–	–	–	–	–	–	3.6 km	3.3 km	4.5 km	10.1 km
CS_{10}	–	–	–	–	–	–	–	–	–	–	6.4 km	6.4 km	7.9 km
CS_{11}	–	–	–	–	–	–	–	–	–	–	–	6.4 km	7.9 km
CS_{12}	–	–	–	–	–	–	–	–	–	–	–	–	4.9 km

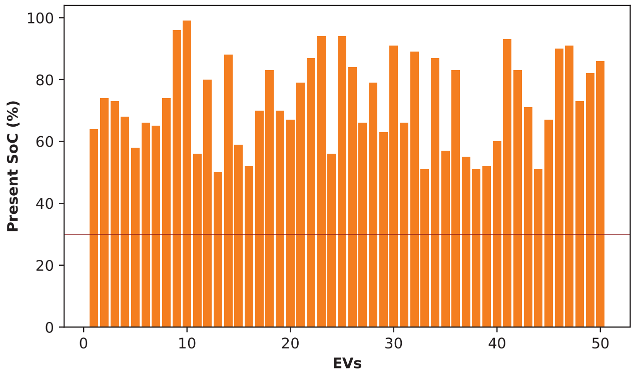


Fig. 8. Present SoC value of EVs.

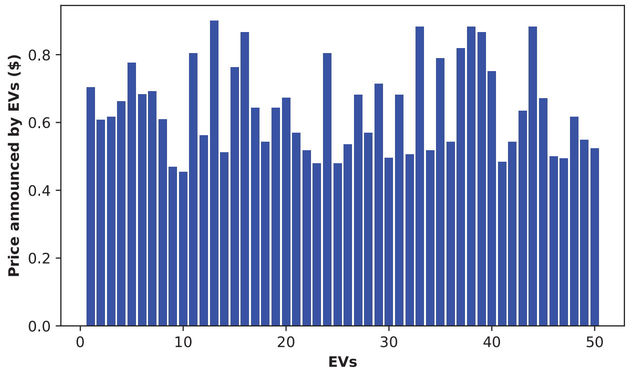


Fig. 10. Price announced by EVs.

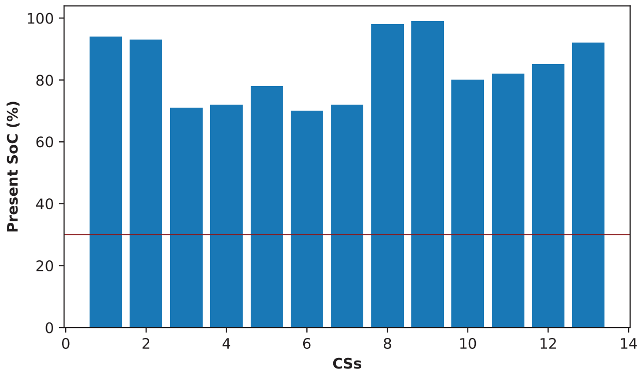


Fig. 9. Present SoC value of CSs.

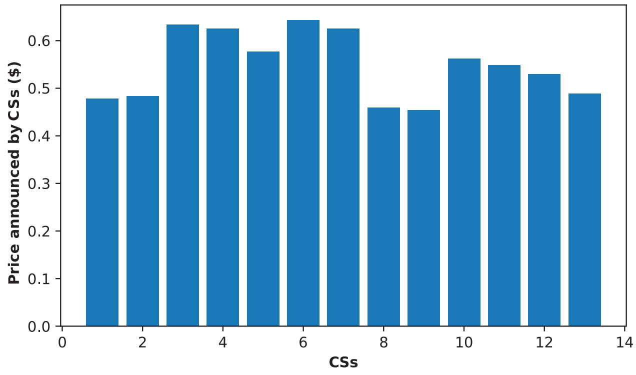


Fig. 11. Price announced by CSs.

Table 8
Coordinates of EV, CSs and PRKs.

EVs (Loc^{cur})	PRK_1 (Loc)	PRK_2 (Loc)	CS_1 (Loc)	CS_2 (Loc)	PRK_3 (Loc)
33.664344	33.6459273	33.6669018	33.6879759	33.6440546	33.6493211
73.1494082	73.1583868	73.1375861	73.1074905	73.1624118	73.1572385

selling and buying energy. Energy trading between an EV, who wants to sell surplus energy at a CS or a PRK and an EV, who wants to get energy from CS or another EV, is dependent on the value of SoC^{pr}. The values of SoC^{pr} for EVs' batteries are shown in Fig. 8 and for CSs are shown in Fig. 9.

The price of energy announced by EVs and CSs is a major influence in the energy trading environment. The energy price in our proposed scheme is determined by the formula given in Algorithm 1, which is derived from [8]. This formula uses the existing SoC^{cur}, B^{cap} and Eth values to determine the price. If the charging of the battery is full, the price would be $0.45, which is the current energy rate in the USA. Using this formula, the price of energy continues to increase as the level of charging decreases. The difference in price according to the level of charging for both EVs and CSs is illustrated in Figs. 10 and 11, respectively.

As we have explained earlier, EVs who participate in energy trading can charge and discharge their energies at any CS or any PRK based on energy requirements. The primary factor in the energy trading environment is the present SoC value in batteries, which decides about the buying and selling of energy. We have selected a 30 percent threshold value of SoC; however, the threshold value can be different in real energy trading practice. To verify the accuracy of computed distance between EVs, CSs and PRKs, five different locations of CSs and PRKs are selected as shown in Table 8. For a fair comparison, Scheme 1 [8], Scheme 2 [22] and our proposed scheme are executed using the same locations. Fig. 12 shows the results' comparison for the schemes used in [8,22] and our proposed scheme.

If we look at Fig. 12, we see that the result of the detected distance by all three schemes is very different. The reason is that, in [8], the

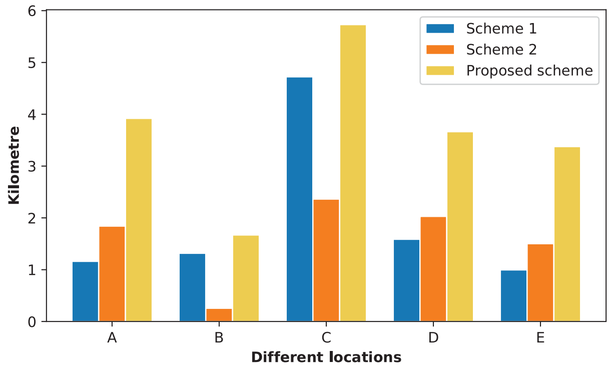


Fig. 12. Comparison for accurate distance measurement.

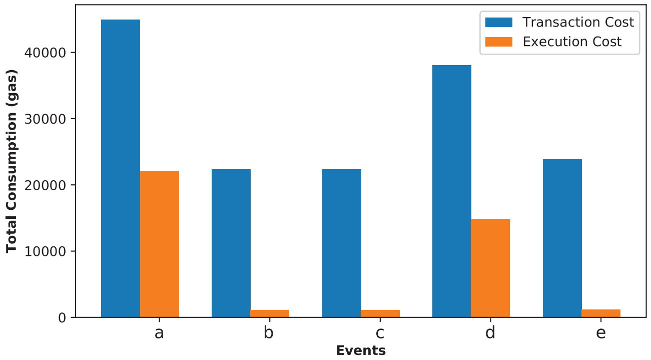


Fig. 13. Gas consumption cost.

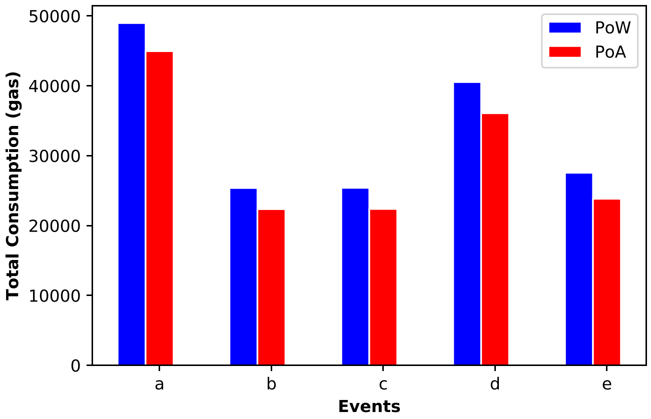


Fig. 14. Transaction cost comparison.

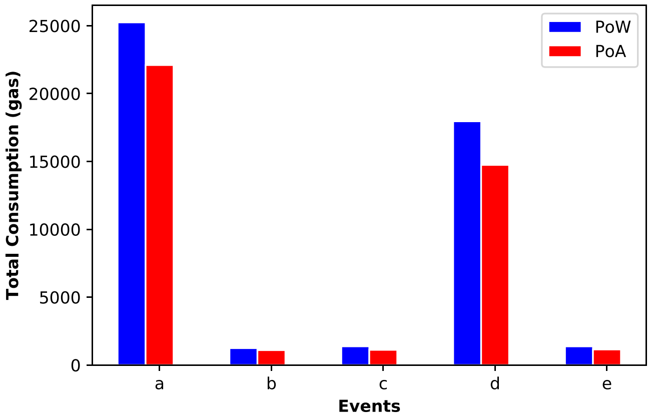


Fig. 15. Execution cost comparison.

city's geographical area is divided into equal-sized blocks, which is not applicable to the random sized geographical area. Moreover, in [22], an equation is used to find the distance between EVs to CSs with the help of latitude and longitude. However, in our proposed technique, the distance is calculated using third-party service.

In Ethereum, gas is a small unit of cryptocurrency. The unit is deducted from the users' accounts to perform a transaction in Ethereum. Fig. 13 shows gas consumption of smart contract's operations. There are five different functions in the smart contract that are used in the proposed work:(a) recharge wallet, (b) access buyer's wallet address (c) access seller's wallet address (d) transfer energy coin from one account to another account and (e) check current balance in the wallet. The gas consumption depends on the complexity of the smart contract. The deployment of a smart contract is an expensive operation in Ethereum. In Fig. 13, the transactional costs of the functions are shown. Moreover, Figs. 14 and 15 show the comparison of transaction cost and execution cost using PoW and PoA, respectively. It can be observe from both figures that PoA consume less cost as compared to PoW and hence, it is beneficial in implementing the smart contract. In Figs. 13–15, the functions used in the smart contract are labeled as *a*–*e*. These functions are get energy coins, get buyer address, get seller address, transfer amount and check balance. Table 9 represents the mapping of limitations to the proposed solutions and validations. The limitations identified in Section 1.1 and given in Table 3 are mentioned in Table 9 along with the proposed solutions and validation results, given in the 3rd and the 4th columns of Table 9, respectively.

5.2. Complexity analysis

The time complexity of our proposed Algorithm 1 is computed as follows. It runs n times for n requests of EVs and CSs, so, it takes $O(n)$ time to verify and transmit the requests. Finding the nearest energy trading place (CSs, PRKs) also takes n time because LAG selects the stored EVs and CSs from the transactions pool according to the buyer's requirements. Furthermore, remaining computations take $O(1)$ time to compute the energy trading request. Therefore, the whole time complexity of the proposed algorithm is $O(n)$.

5.3. Evaluation of security analysis

In this section, the evaluation results that analyze the double spending and Sybil attacks are provided. The computational resources of a node are calculated using gas values of the hash rate. Besides, the computational resources of an attacker are the proportion of its hash rate to the overall hash rate of the network. The block generation time and mining time and the random block disadvantage of [−5, 5] are considered for the analysis. This study considers different number of Sybil identities for the analysis. The parameters in this study are used for evaluating the effectiveness of the proposed system model and scenario. Moreover, the study is not limited to the above mentioned parameters, but can accept more parameters.

5.3.1. Evaluation of the double spending attack

The following parameters are used for analyzing the double spending attack: computational resources of the attack $q = 0.30$, number of confirmed messages $K = 20$, time advantage $t = 1$ and defined threshold $\rho = 0.25$. Fig. 16 shows the probability of successful double spending attack versus the number of confirmed messages. The proposed method is compared with existing method of [45] and the results show that the proposed method outperforms the existing method in terms of minimum probability of successful double spending attack.

Table 9
Mapping of limitations with validation results.

Limitation number	Limitation identified	Proposed solution	Validation results
L.1	Excessive resource consumption using PoW consensus mechanism	S.1	Figs. 14 and 15 show the cost comparison between PoW and PoA
L.2	Accurate distance measurement	S.2	Fig. 12 shows the comparison between accurate distance measurement using 3 different techniques
L.3	Energy coin wallets not secured	S.3	Algorithm 2 is used for energy trading, which also helps in securing the energy coin wallets
L.4	Excessive time consumption by miners while selecting EVs	S.4	No direct validation
L.5	Robustness against attacks	S.5	Fig. 6 shows the security analysis results using Oyente. Figs. 16–19 show the security results for double spending and Sybil attacks

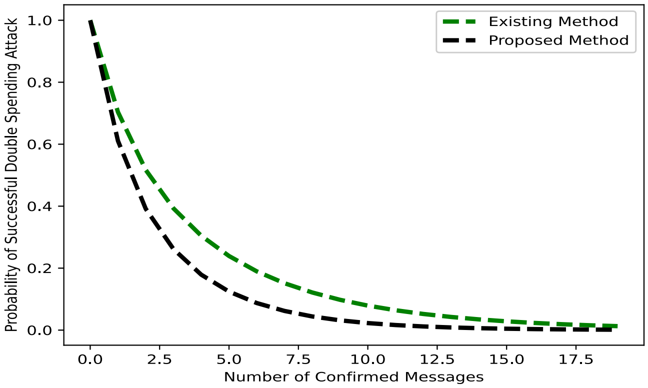


Fig. 16. Probability of successful double spending attack versus the number of confirmed messages.

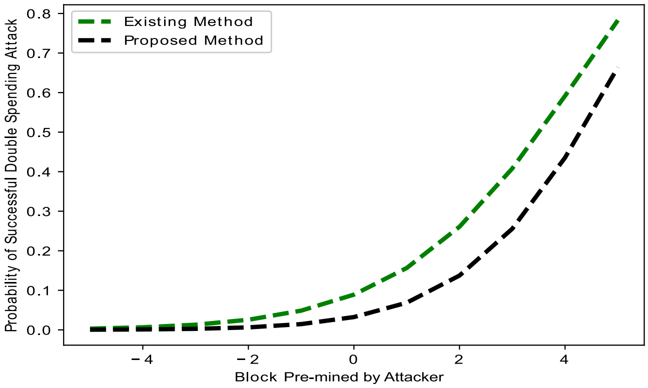


Fig. 17. Probability of successful double spending attack versus block pre-mined by attacker.

In this study, if the probability of successful double spending attack approaches 1, then the attacker is successful in launching the attack and vice versa. From the results in Fig. 16, it is observed that as the number of confirmed messages increases, the probability of successful double spending attack decreases, which implies that the proposed method prevents the attack because of the PoA consensus mechanism. Also, it means that the false branch created by the attacker is the shortest; therefore, honest nodes will reject the branch. It is also observed that the proposed method has the least probability of successful double spending attack as compared to the existing method. This means that the proposed method efficiently utilizes ρ for regulating the malicious activities of nodes in the network. Moreover, the proposed method considers both computational resource and time advantages instead of considering only time advantage like [45] for evaluating the double spending attack.

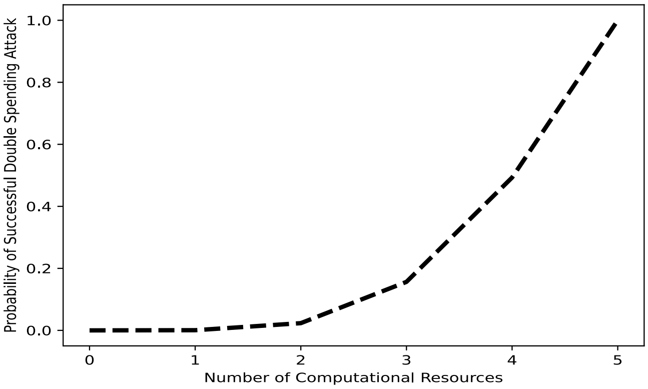


Fig. 18. Probability of successful double spending attack versus number of computational resources.

Fig. 17 shows the probability of successful double spending attack versus block pre-mined by attacker. It is observed from the figure that as the block pre-mined by attacker increases from −5 to 5, the probability of successful double spending attack increases. This shows the behavior of the attacker in a real life scenario. It also explains that if the attacker is successful in launching the attack with high computational resource and time, then it creates the longest branch in the network. It is also observed from the results in Fig. 17 that the proposed method has the minimum probability of successful double spending attack as compared to the existing method. This implies that the proposed method is more effective in preventing double spending attack in a real life scenario as compared to the existing method.

The advantages of computational resource of an attacker over the honest nodes in the network are analyzed and Fig. 18 shows the results. It is observed from the figure that the number of computational resources increases along with the probability of successful double spending attack. This means that if an attacker has high computing resources in real life scenario, it can control the entire network and can get more incentives. The proposed PoA consensus mechanism is used in this study to mitigate the double spending attack. In the PoA consensus mechanism, the reputation is considered instead of the computational resources of nodes. It means that if a node has high computational resources, but low reputation, then such a node cannot participate in the validation and mining processes. Generally, it is clearly shown from the evaluation results that the proposed system is robust against the double spending attack.

5.3.2. Evaluation of sybil attack

The parameters considered for evaluating Sybil attack are as follows: number of nodes $n = 200$, different Sybil identities $ns = 4$ and 8, and computational resources of an attacker $q = 0.3$. Fig. 19 shows the impact of different identities on the probability of a successful Sybil attack. It is observed from the figure that when the attacker

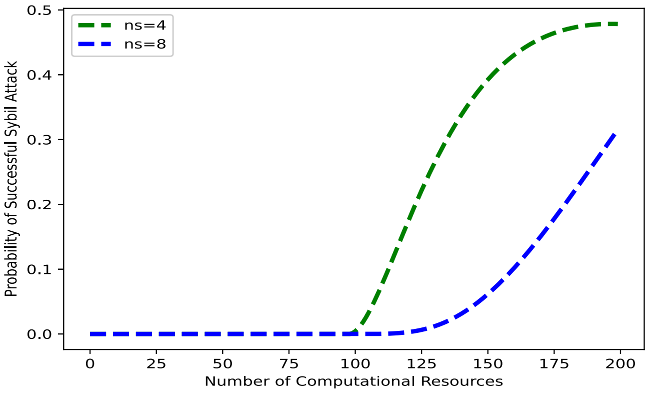


Fig. 19. Probability of successful Sybil attack versus number of computational resources.

creates 4 Sybil identities, the probability of successful Sybil attack is zero as the computational resources increase from 0–100. Afterwards, the probability of successful Sybil attack increases along with the computational resources, i.e., greater than 100. This implies that if the attacker increases the computational resources of the 4 Sybil nodes, then there is a high possibility of launching the Sybil attack. On the other hand, when the attacker increases the Sybil identities up to 8, the probability of successful Sybil attack is zero as the computational resources increases from 0–150. Although, the probability of successful Sybil attack increases when the computational resources are above 150. The analysis of 4 and 8 Sybil identities explains that as the attacker increases the Sybil identities in the network, the probability of successful Sybil attack remains zero while increasing the computational resources. The proposed PoA consensus mechanism mitigates the attack by considering the reputation instead of computational resources of nodes. It means that the nodes with high reputation can perform validation and mining tasks. Therefore, the proposed system is robust against the Sybil attack.

6. Conclusion

We have implemented V2V and V2G energy trading environments in a smart city using consortium blockchain and smart contracts for a fair payment mechanism where EVs and CSs can trade energy without reliance on the third party. Blockchain technology is deployed on authorized LAGs, which work as energy brokers to carry out the energy trading requests. We have used the PoA consensus mechanism instead of PoW because it uses less computational power as compared to PoW and provides maximum throughput with less latency. In our proposed scheme, an algorithm is proposed that provides accurate distance with the required time and minimum expenses to reach any CS and PRK for energy trading. The energy losses in both V2G and V2V energy trading environments are discussed in this work, which help in promoting efficient power flow in the vehicular networks. This study designs two attacker models based on the double spending and Sybil attacks. The evaluation of security analysis shows that the proposed system is robust against both attacks. Besides, We have used Oyente for smart contract security analysis, which can test common and well-known bugs including call stack depth attack vulnerability, transaction-ordering dependence, timestamp dependency, re-entrancy vulnerability, and DAO bugs. The experimental results and security analysis show that our proposed scheme improves transactional security and privacy. The results also show that the cost incurred using the PoA consensus mechanism is almost 25%–30% less than the cost incurred when using the PoW consensus mechanism. Moreover, the results also prove that our proposed scheme outperforms the existing schemes in terms of providing a secure energy trading environment for V2V and V2G charging of EVs. As a whole, the proposed scheme helps in making the smart cities reliable, sustainable, environment and user friendly and ensures energy efficiency.

CRediT authorship contribution statement

Rabiya Khalid: Conception and design of study, Writing – original draft. **Muhammad Waseem Malik:** Conception and design of study, Writing – review & editing. **Turki Ali Alghamdi:** Analysis and/or interpretation of data. **Nadeem Javaid:** Acquisition of data, 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.

Acknowledgment

All authors approved the version of the manuscript to be published.

References

[1] Amini MH, Moghaddam MP, Karabasoglu O. Simultaneous allocation of electric vehicles' parking lots and distributed renewable resources in smart power distribution networks. Sustainable Cities Soc 2017;28:332–42.

[2] Kang J, Yu R, Huang X, Maharjan S, Zhang Y, Hossain E. Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. IEEE Trans Ind Inf 2017;13(6):3154–64.

[3] Khalkhali H, Hosseinian SH. Multi-class EV charging and performance-based regulation service in a residential smart parking lot. Sustain Energy Grids Netw 2020;100354. http://dx.doi.org/10.1016/j.segan.2020.100354.

[4] Zhou Z, Wang B, Guo Y, Zhang Y. Blockchain and computational intelligence inspired incentive-compatible demand response in internet of electric vehicles. IEEE Trans Emerg Top Comput Intell 2019;3(3):205–16.

[5] Gao F, Zhu L, Shen M, Sharif K, Wan Z, Ren K. A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks. IEEE Netw 2018;32(6):184–92.

[6] Liu H, Zhang Y, Yang T. Blockchain-enabled security in electric vehicles cloud and edge computing. IEEE Netw 2018;32(3):78–83.

[7] Zheng D, Jing C, Guo R, Gao S, Wang L. A traceable Blockchain-based access authentication System with Privacy Preservation in VANETs. IEEE Access 2019;7:117716–26.

[8] Jindal A, Aujla GS, Kumar N. SURVIVOR: A blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment. Comput Netw 2019;153:36–48.

[9] Li Z, Kang J, Yu R, Ye D, Deng Q, Zhang Y. Consortium blockchain for secure energy trading in industrial internet of things. IEEE Trans Ind Inf 2017;14(8):3690–700.

[10] Aitzhan NZ, Svetinovic D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans Dependable Secure Comput 2016;15(5):840–52.

[11] Yahaya AS, Javaid N, Alzahrani FA, Rehman A, Ullah I, Shahid A, Shafiq M. Blockchain based sustainable local Energy Trading considering home Energy Management and demurrage Mechanism. Sustainability 2020;12(8):3385. http://dx.doi.org/10.3390/su12083385.

[12] Samuel O, Almogren A, Javaid A, Zuair M, Ullah I, Javaid N. Leveraging Blockchain Technology for secure energy trading and least-cost evaluation of decentralized contributions to electrification in Sub-Saharan Africa. Entropy 2020;22(2):226. http://dx.doi.org/10.3390/e22020226.

[13] Nakamoto S. Bitcoin: A Peer-to-Peer electronic cash system. 2019, Available online: https://bitcoin.org/bitcoin.pdf (accessed 13-December-2019).

[14] She W, Liu Q, Tian Z, Chen JS, Wang B, Liu W. Blockchain trust model for malicious node detection in wireless sensor networks. IEEE Access 2019;7:38947–56.

[15] Sultana T, Almogren A, Akbar M, Zuair M, Ullah I, Javaid N. Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices. Appl Sci 2020;10(2):488. http://dx.doi.org/10.3390/app10020488.

[16] Feng Q, He D, Zeadally S, Liang K. BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular Ad-Hoc Networks. IEEE Trans Ind Inf 2019.

[17] Javed MU, Rehman M, Javaid N, Aldegheishem A, Alrajeh N, Tahir M. Blockchain-based secure data storage for Distributed Vehicular Networks. Appl Sci 2020;10(6):2011. http://dx.doi.org/10.3390/app10062011.

[18] Zhu L, Wu Y, Gai K, Choo KKR. Controllable and trustworthy blockchain-based cloud data management. Future Gener Comput Syst 2019;91:527–35.

[19] Gai K, Wu Y, Zhu L, Qiu M, Shen M. Privacy-preserving energy trading using consortium blockchain in smart grid. IEEE Trans Ind Inf 2019;15(6):3548–58.

[20] Khalid R, Javaid N, Almogren A, Javed MU, Javaid S, Zuair M. A blockchain-based load balancing in decentralized hybrid P2P energy trading Market in Smart Grid. IEEE Access 2020;8:47047–62.

[21] Shahid A, Almogren A, Javaid N, Al-Zahrani FA, Zuair M, Alam M. Blockchain-based agri-Food Supply Chain: A complete solution. IEEE Access 2020;8:69230–43.

[22] Chaudhary R, Jindal A, Aujla GS, Aggarwal S, Kumar N, Choo KKR. BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system. Comput Secur 2019;85:288–99.

[23] Wang Y, Su Z, Zhang N. BSIS: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network. IEEE Trans Ind Inf 2019;15(6):3620–31.

[24] Sachan S, Deb S, Singh SN. Different charging infrastructures along with smart charging strategies for electric vehicles. Sustainable Cities Soc 2020;102238. http://dx.doi.org/10.1016/j.scs.2020.102238.

[25] Zhou Z, Wang B, Dong M, Ota K. Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing. IEEE Trans Syst Man Cybern: Syst 2019;50(1):43–57.

[26] Huang X, Xu C, Wang P, Liu H. LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem. IEEE Access 2018;6:13565–74.

[27] Luo B, Li X, Weng J, Guo J, Ma J. Blockchain enabled trust-based location privacy protection scheme in VANET. IEEE Trans Veh Technol 2019.

[28] Dorri A, Steger M, Kanhere SS, Jurdak R. Blockchain: A distributed solution to automotive security and privacy. IEEE Commun Mag 2017;55(12):119–25.

[29] Hassija V, Chamola V, Garg S, Krishna DNG, Kaddoum G, Jayakody DNK. A blockchain-based framework for lightweight data sharing and energy trading in V2G network. IEEE Trans Veh Technol 2020;69(6):5799–812.

[30] Bao J, He D, Luo M, Choo KKR. A survey of blockchain applications in the energy sector. IEEE Syst J 2020.

[31] Magnani A, Calderoni L, Palmieri P. Feather forking as a positive force: incentivising green energy production in a blockchain-based smart grid. In: Proceedings of the 1st workshop on cryptocurrencies and blockchains for distributed systems. Munich, Germany; 2018, pp. 99–104.

[32] Xu C, Wang K, Li P, Guo S, Luo J, Ye B, Guo M. Making big data open in edges: A resource-efficient blockchain-based approach. IEEE Trans Parallel Distrib Syst 2018;30(4):870–82.

[33] BU-1003: Electric vehicle (EV). 2020, Available online: https://batteryuniversity.com/learn/article/electric_vehicle_ev (accessed 19-March-2020).

[34] Xie L, Ding Y, Yang H, Wang X. Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs. IEEE Access 2019;7:56656–66.

[35] Yang YT, Chou LD, Tseng CW, Tseng FH, Liu CC. Blockchain-based traffic event validation and trust verification for VANETs. IEEE Access 2019;7:30868–77.

[36] Rathee G, Sharma A, Iqbal R, Aloqaily M, Jaglan N, Kumar R. A blockchain framework for securing connected and autonomous vehicles. Sensors 2019;19(14):3165.

[37] Abdolmaleki M, Masoud N, Yin Y. Vehicle-to-vehicle wireless power transfer: Paving the way toward an electrified transportation system. Transp Res C 2019;103:261–80.

[38] Load-no load losses of transformer-ECE Tutorials. 2020, Available online: https://ecetutorials.com/transformer/losses-of-transformer-noload-and-load/ (accessed 15-April-2020).

[39] Losses in distribution & transmission lines | electrical india magazine on power & electrical products, renewable energy, transformers, switchgear & cables. Electrical India magazine on power & electrical products, renewable energy, transformers, switchgear & cables. Available online: https://www.electricalindia.in/losses-in-distribution-transmission-lines/.

[40] Koufakis AM, Rigas ES, Bassiliades N, Ramchurn SD. Offline and online electric vehicle charging scheduling with V2V energy transfer. IEEE Trans Intell Transp Syst 2019.

[41] How to use oyente, a smart contract security analyzer - solidity tutorial. Medium; 2020, Available online: https://medium.com/haloblock/how-to-use-oyente-a-smart-contract-security-analyzer-solidity-tutorial-86671be93c4b (accessed 5-April-2020).

[42] Known attacks - Ethereum smart contract best practices. 2020, Available online: https://consensys.github.io/smart-contract-best-practices/known_attacks/ (accessed 5-April-2020).

[43] A postmortem on the parity multi-sig library self-destruct. Blockchain Infrastructure For The Decentralised Web; 2020, Available online: https://www.parity.io/a-postmortem-on-the-parity-multi-sig-library-self-destruct/ (accessed 5-April-2020).

[44] Ethereum smart contract best practices, known attacks. 2020, Available online: https://consensys.github.io/smart-contract-best-practices/known_attacks/ (accessed 5-April-2020).

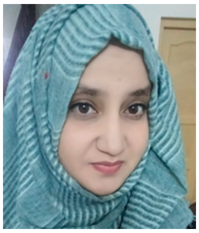
[45] Pinzón C, Rocha C. Double-spend attack models with time advantange for bitcoin. Electron Notes Theor Comput Sci 2016;329:79–103.

[46] Landa R, Griffin D, Clegg RG, Mykoniati E, Rio M. A sybil proof indirect reciprocity mechanism for peer-to-peer networks. In: IEEE INFOCOM 2009, Rio de Janeiro, Brazil; 2009, pp. 343–51.

[47] Apostolaki-Iosifidou E, Codani P, Kempton W. Measurement of power loss during electric vehicle charging and discharging. Energy 2017;127:730–42.

[48] Kriukov A, Gavrilas M. Energy/Cost efficiency study on V2G operating mode for EVs and PREVs. In: 2019 8th international conference on modern power systems (MPS). IEEE; 2019, p. 1–6.

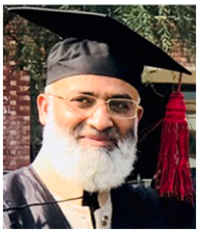
[49] Bitcoin core requirements and warnings. 2021, Available online: https://bitcoin.org/en/bitcoin-core/features/requirements (accessed 2-may-2021).



Rabiya Khalid received the M.C.S. degree from the Mirpur University of Science and Technology, Mirpur, Pakistan, in 2014, and the M.S. degree in computer science with a specialization in energy management in smart grid from the Communications Over Sensors (ComSens) Research Laboratory, COMSATS University Islamabad, Islamabad, Pakistan, in 2017, under the supervision of Dr. Nadeem Javaid, where she is currently pursuing the Ph.D. degree under the same supervision. She is also working as a Research Associate with the ComSens Research Laboratory, COMSATS University Islamabad. She has authored more than 20 research publications in well reputed technical journals and international conferences. Her research interests include data science and blockchain in smart/micro grids.

Muhammad Waseem Malik is currently pursuing the M.S. degree in computer science in the Department of Computer Science, COMSATS University Islamabad, Islamabad, Pakistan. He has five research publications in well reputed international journals and conferences. His research interests include data science, smart grid, blockchain, and financial market.

Turki Ali Alghamdi received the bachelor's degree in computer science from King Abdulaziz University, Jeddah, Saudi Arabia, the master's degree in in Distributed Systems and Networks from the University of Hertfordshire, Hatfield, United Kingdom, in 2006 and the Ph.D degree from the University of Bradfsord, United Kingdom, in 2010. He is a Professor in Computer Science Department, Faculty of Computer and Information Systems, University of Umm Al-Qura in Makkah (UQU), and the Founding Director of UQU Smart Campus Center (SCC). He has more than 15 years of research and development, academia and project management experience in IT. He has previously been Vice Dean of Technical Affairs for IT Deanship in Umm Al-Qura University and Dean of eLearning and IT in Taif university. He holds CDCDP and CDCMP certificates. He is passionate about developing the translational and collaborative interface between industry and academia. Turki's research, focusing on Wireless Sensor Networks, Energy and QoS Aware Routing Protocols, Network Security, IoT and Smart Cities.



Nadeem Javaid (S'8, M'11, SM'16) received the bachelor degree in computer science from Gomal University, Dera Ismail Khan, Pakistan, in 1995, the master degree in electronics from Quaid-i-Azam University, Islamabad, Pakistan, in 1999, and the Ph.D. degree from the University of Paris-Est, France, in 2010. He is currently an Associate Professor and the Founding Director of the Communications Over Sensors (ComSens) Research Laboratory, Department of Computer Science, COMSATS University Islamabad, Islamabad. He is also working as visiting professor at the School of Computer Science, University of Technology, Sydney, Australia. He has supervised 137 master and 24 Ph.D. theses. He has authored over 900 articles in technical journals and international conferences. His research interests include energy optimization in smart grids and in wireless sensor networks using data analytics and blockchain. He was recipient of the Best University Teacher Award from the Higher Education Commission of Pakistan, in 2016, and the Research Productivity Award from the Pakistan Council for Science and Technology, in 2017. He is also Associate Editor of IEEE Access and Editor of Sustainable Cities and Society journals.