IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

A Secure and Decentralized Blockchain based EV Energy trading model using Smart contract in V2G Network

Atif Iqbal[1], IEEE Senior Member, Arun Sekar Rajasekaran[2], GadilliSainikhil[3], Maria Azees[4]

[1]Department of Electrical Engineering, Qatar University, Doha, Qatar.
[2,3,4]Department of Electronics and Communication Engineering, GMR Institute of Technology, GMR Nagar, Rajam - 532 127, AP,India.

e-mail :([2]arunsekar.r@gmrit.edu.in, [3]sainikhil.g.9.7@gmail.com, [4]azeesmm@gmail.com)

Corresponding author: Atif Iqbal (e-mail: atif.iqbal@qu.edu.qa).

ABSTRACT In this work, a secure and decentralized Blockchain based energy trading model for electric vehicles (EVs) using Smart contract that achieves Peer-to-Peer (P2P) transactions between EVs in Vehicle to Grid networks is designed. The traditional energy trading model is a centralized structure based on trusted third parties, and there may an issue of single-point failure and leakage of privacy. In this way, a blockchain-based framework offers a secure, efficient and transparent trading model. Initially, the participating EVs and aggregator in the trading process should register at the trusted authority. Once the registration is successfully completed, both EVs and aggregator authenticate each other mutually in an anonymous manner. Moreover, only authorized EVs (charging and discharging EVs) participate in the contrary auction mechanism to exchange power/money based on their demand. Simulation conducted for the proposed scheme shows that our scheme has high speed (i.e., less computational time and execution time) which improves the market efficiency. In-addition, the transactions are non tamperable, when compared to the conventional scheme.

INDEX TERMS Bilinear pairing, Blockchain, Electric vehicle, Smart contract, Vehicle to grid.

I. INTRODUCTION

Vehicle to grid can be represented as “V2G”. It is a technology that allows energy to be transferred (returned back) from the battery of an electric car to the power grid or vice versa. It enables bidirectional flow of the electricity in electric vehicle i.e. both charging and discharging of EVs [1]. The V2G principle is similar to traditional intelligent charging, which allows us to control the electrical charge so that charging capacity is increased or decreased. Furthermore, this V2G represents a step forward in returning the remaining energy to the power grid. In addition, the V2G network has a major impact on the transportation industry. If the number of electric vehicles (EVs) on the road increases, the amount of carbon and other gases burned for fuel will decrease. Electric vehicles minimize emissions because they do not need fuel (petrol or diesel). Furthermore, the batteries used in electric vehicles are the most cost-effective for energy storage since no additional hardware is needed. Smart EV charging is a smart back-end (smart meter) mechanism that gathers real-time data from charging/discharging vehicles at charging stations [2].In the present world nearly 91% of vehicles are running by internal combustion engines i.e. by petrol, diesel etc. Non-renewable resources are potentially detrimental to society. As a byproduct of these resources, carbon dioxide is generated, which is trapped in the atmosphere and is the primary cause of health risks, air pollution, and other climatic changes. So, it is better to shift towards eco-friendly renewable sources in place of non-renewable sources i.e. to use electric vehicles. However, as the number of electric vehicle users increases, charging the vehicles at the charging station would become more difficult. Furthermore, in the vehicle-to-grid network, there are two types of electric vehicles (EVs): charging and discharging, making the exchange of charge and price at the charging station more complicated. As a result, in order to provide charge for charging EVs and collect charge from discharging EVs, the best solution for energy trading must be chosen. Although there are numerous energy trading methods currently in use in vehicle-to-grid networks, they are inefficient in terms of security, performance, and delay. As a result, the design of a new system, which is explored in this research article, was prompted. Despite the fact that there has been a lot of research on block chain-based EV charging transactions, we have proposed a new decentralized Block chain-based Energy trading model for EVs in this work, in which the transactions are stored in blocks in a safe manner. In addition, the authors have used an innovative contrary auction mechanism in which discharging EV quoting least price is matched with charging EV having more trading time (EV duration of time in the network). Moreover, in this contrary auction process dynamic pricing technique is used, where loser discharging EV in current round has more probability to win in the next round by changing his quoting price depending on the winning price quoted by aggregator. Thus, it not only benefits all participants but also increases market efficiency and social welfare. Hence this process is better than the existing methods discussed in related works where there is no such type of innovative contrary auction mechanism used. Moreover, only static pricing algorithm is used for selecting a discharging EV to charge the grid/charging EV. Since, we focused on dynamic pricing strategy, the charging EV is required to pay the minimum cost quoted. When compared to existing EV trading method, improvements have been made in our proposed method mainly in terms of performance and security analysis. Furthermore, when compared to traditional methods, our proposed algorithm has a shorter delay, particularly when there are more electric vehicles at the charging station. Moreover, after the charge/amount has been exchanged, the transactions are stored in a private block chain that is non-tamperable, safe, and private. The authentication node in the communication server is used to authenticate the EVs and the aggregator. In addition, both the aggregator and the EVs authenticate among themselves in an anonymous manner before communicating with each other during charging and discharging. These charging areas are connected to the cloud and can be used in various ways, such as charging/discharging electric vehicles and storing the energy value of the vehicle being charged or discharged in the cloud.

The novelty in this framework is the use of dynamic pricing algorithm which can benefit all participating discharging EVs to win in the auction. Current trading methods, on the other hand, have a static pricing algorithm that can't raise benefit for all discharging EVs. Moreover, the newly proposed algorithm reduces the delay of the charging EV as the number of EVs increases at the charging spot. Since, Block chain technology is used, there will be no third party. But, in our scheme trusted authority is present only at the time registration and authentication to give public and private keys to users. There will be no third party during the trading process. Moreover, the exchange of money will be directly done based on smart contract and transactions are stored in blocks which are transparent. So, our proposed system will take less time to complete total trading than traditional trading methods. As a result, there is no need to spend extra time for storing the data in the blocks before or after the process is completed. However, there will be a third party in the traditional system, it will take considerably more time for the trading process, and there will be double spending. In addition, unlike our proposed Block chain-based approach, there would be no security for transactions in the traditional method.

The main contributions of this work are mentioned as follows:

1) A secure and decentralized EV energy trading model in V2G network using block chain technology and smart contract is proposed.

2) It is mainly based on contrary auction mechanism in which all discharging EVs quote their prices for the charge provided by them to charging EVs.

3) Contrary auction mechanism is used, where dynamic pricing algorithm is implemented which allows sellers (discharging EVs) to adjust their quoting prices dynamically based on winning price to win in the auction.

4) The proposed energy trading model uses mutual authentication technique which allows both EVs and aggregator to authenticate with each other so that no malicious user can enter into the network.

5)Moreover, the transaction details of auction results (i.e. matched charging EV and discharging EV details) after each round are stored in private block chain network which ensures more privacy for the transactions.

The remaining part of this paper is organized as follows. Section 2 explains about the related works on energy trading with respect to blockchain and V2G. Section 3 enlightens about the entire system overview. Proposed scheme based on blockchain and smart contract is described in section 4. Experimental analysis and results are described in section 5 and section 6 concludes this paper

II. RELATED WORKS

Hassija *et al.* [3], proposed a directed acyclic graph based lightweight blockchain based protocol. The conciliation between the EV and the grid for the transfer of energy is based on game theory model. Though it supports micro transactions, the price fixed by the grid is constant and there is no compromise in the reduction of the cost for the energy supply. Smart contracts and edge computing are used in the work proposed by Zhou *et al.* [4] to make energy transactions efficient and stable. Though the computational problem of resource allocation is solved used stack elberg game and backward induction method, there is no defined solution for reducing the price which is fixed by the discharging EV or the grid. Thus, there is no set of procedure for the distribution of energy resources. H. Wang *et al.* [5] introduces anonymous recompense scheme for discharging EV. This approach is proposed to promote the involvement of large numbers of discharging EV in the energy transfer. For the EV that supplies energy to the grid, a certain amount will be awarded to facilitate their participation. However, the amount is not specified in this work as the award is given. In addition, no guarantee is provided that all vehicles will be in on-line before the energy transaction is completed. Liu *et al.* [6] takes into account of grid system stability and energy cost. Iceberg execution algorithm is used for scheduling the charging and discharging EV. Though the simulation proved to be effective, there is no reduction of cost for the energy in the successive rounds. Once the cost for the energy is fixed, it cannot be changed and continued till all the charging and discharging EV leaves the network. Moreover, in [6] authors proposed a distributed procedure for electric vehicle charging process to minimize the instant electricity variations in the power source and to minimize the total charging price for customers. They initially calculate the electricity variation level issue with the help of vehicle cell capabilities, charging rates and vehicle users charging pattern. And they used an algorithm called iceberg order management to optimize the EV charging and discharging demands and further scheduled time for charging and discharging. This process has less gas usage in the running process and therefore it enhances the efficiency. However, it is important to think about the stability between operating and non-operating chain complexity. Kang *et al.* [7], performed energy transfer in the localized manner. To avoid the complex transportation of energy to long distances, local peer to peer transaction is performed. Incentives provided to the discharging EV are fixed in nature. Since, the energy transfer takes place in the localized, if there is more requirement, then the local discharging EVs are not difficult to meet the demand. Though double auction method is used, there is no dynamic price fixation in this work. Z. Wang *et al.* [8], proposed a method of power management based on Artificial intelligence. Artificial neural network is used for predicting the amount of energy in EV. Though the amount of energy is predicted and the charging and discharging EVs are segregated, there is no method for the dynamic allocation of cost for the energy. Sun *et al.* [9] proposed fog computing architecture for the problem of welfare maximization. A new algorithm called delegated proof of work is designed by combining the advances in byzantine fault algorithm and consortium blockchain. The simulation performed based on the proposed algorithm proved to be effective in terms of energy pricing and optimal charging. But, the dynamic allocation of cost for the energy transfer is not discussed in this work. Various challenges in vehicle to grid network are discussed in this work by Musleh *et al.* [10], segregated network load variation is reduced in the paper by Y. Li and B. Hu [11] based on restrictions of energy flow. This work discusses the mixed integer problem and suggests a heuristic approach to solve this problem. The decentralized architecture of trade is built based on the consortium blockchain. The efficiency of this work is enhanced by the KH algorithm. However, this work does not talk about the costs of trading in energy. In [12] Su *et al.* proposed a work for the security enhancement by the implementation of permissioned blockchain with smart contract. The consensus algorithm used in this work is based on Byzantine fault tolerance problem. Based on the fixed number of discharging EVs in the charging spot, energy is allotted to the required charging EV. This method doesn't ensures the charge lacking mechanism. The EV has been provided with rewards based on blockchain methods proposed by X. Chen and X. Zhang [13]. Transactions are protected by bilinear pairing and cryptography of elliptical curve. In addition, digital signature guarantees data integrity and privacy. This encourages the EV to engage in the energy exchange as much as possible. However, this analysis does not obey the complex price allocation for the energy transaction. Sheikh *et al.* [14], power demand is satisfied based on the renewable energy resource. Energy trading process takes place based on consensus protocol. Moreover, integration of renewable and non-renewable energy sources are utilized to meet the energy supply demand. The various types of cyber-attacks are discussed in this work. In addition, based on the Byzantine system, the protection of data from vulnerable assault and threats is improved. Zhao *et al.* [15] proposed a method in which the intruders use data mining algorithm to get user's privacy details, especially when the user group is located in nearby geographic positions during energy trading. So, the authors proposed a consortium block chain based solution to solve the privacy leakage issue without reducing the trading functions. It enlightens the EV trading user's privacy in the smart grid and also it visualizes the distribution of energy sale of users who supply energy. To get rid of security issue because of distributed power transaction, a conceptual research based on block chain in energy internet is introduced by Yang *et al.* [16]. In addition, the authors presented a robust application of the block chain in future energy internet operation, which will make system with more safety, flexibility and price efficient. Luo *et al.* [17], proposed a decentralized power trading system to make P2P power sharing easier among buyers and sellers. It has two layers i.e. a collective envoy system is built to enhance the producer and consumer grid, and an envoy alliance procedure is made to allow the user to form alliance and arrange electricity trading. In this envoy alliance layer, a block chain based transaction agreement procedure is made to allow the credible and safe agreement of power trading transactions which are already made in the collective envoy layer. Wu *et al.* [18], used the core architecture of the initial block chain technology, and they combined the security of the open block chain technology and the efficiency of private block chain technology to build a new hybrid block chain storage mode to solve the poor efficiency problem of the initial block chain. It is introduced for the purpose of improving internet executing, achieving distributed supervision and facilitating safe and efficient performance of the energy internet in the storage of its huge data. Yu *et al.* [19], proposed a graded bidding and transaction architecture using block chain to build a local electricity market. In initial stage, micro grid will assess the approximate cost probability distribution (mixed with the multi-agents) of other micro grids by using a theorem called 'Bayesian", making its probability closer to the accurate probability. Moreover in final stage, to maximize the benefits of micro grid, this paper used the Nash equilibrium to find the optimal quotation. Table 1 shows the comparative analysis of related works.

TABLE 1: Comparative Analysis of related works

Related works	Objectives	Advantages	Disadvantages	Techniques
Hassija *et al.* [3]	To help regular transactions and maximize the throughput of the transactions performed in V2G.	Light weight based block chain is used which maximizes the transaction throughput. No need of excessive computation to add the transactions in the network.	The game theory model proposed in this work is not effective to perform the amount transfer in an efficient manner. When number of electric vehicles is increasing then there may be delay in processing of exchanging of charge/amount.	Directed Acyclic Graph-based V2G network (DV2G) technique. A tangle data structure is designed for the purpose of storing the transactions. A game theory model is exploited to finish the agreement between the grid and vehicles.
Zhou *et al.* [4]	A safer and efficientV2G power dealing structure by exploiting block chain, edge computing and theory of contract.	Secure energy trading mechanism is achieved using consortium block chain and incentive is provided through contract theory. The prosperous possibility of formation of block is enhanced by exploiting edge computing.	To choose the starting point for concurrence performance requires furthermore exploration. The private statistical data like history of transactions, type of EV will be revealed outside which effects the privacy of the EV.	Consortium block chain, convex concave algorithm techniques is used. Contract theory based mechanism is used to reduce information asymmetry. Edge computing is used for the purpose of block creation.
H. Wang *et al.* [5]	Compensation for the EV who are ensuring energy to the grid in an undisclosed manner through block chain.	The EV gets compensation without depending on their energy contribution. The proposed scheme is practically secure and efficient for V2G networks in the smart grid.	Compensation given for EV is constant and there is no incremental based on their charge delivering capability. There may be misuse of contract-based authentication.	Ring signature. aggregated signature and public key infrastructure
Liu *et al.* [6]	To reduce the power variation zone in smart grid and the total charging price for the Electric Vehicle owners.	Power fluctuation problem is completely removed. Overall charging costs are reduced.	The number of EV participating in the network is limited. Lack of equity between on and off chain complexity.	Iceberg order execution algorithm.
Kang *et al.* [7]	To purchase and provide the energy locally to the Electric Vehicle.	Ensuring incentives to the discharging EV	Electricity pricing method is constant.	Iterative double auction mechanism
Z. Wang *et al.* [8]	To use Artificial intelligence for the purpose of power management in grid	Exact prophecy of power consumption	More power fluctuation output level.	artificial neural-network and federated learning
Sun *et al.* [9]	To balance the charging and discharging problem and to increase the social welfare.	No need of third party as the operation is completely distributed.	No automatic mechanism is there to Incentive for the energy providing EV.	delegated proof of stake

Muslehet *al.* [10]	To describe the consequences faced in smart grid based on block chain technology.	Oneness and distributed nature of block chain.	High price is required for executing the block chain.	Aggregator based micro grid architecture. Block chain as a cyber layer.
Y. Li and B. Hu [11]	To design a continual 2-layer model to improve the charging and discharging trading of electric vehicles.	Distributed trading construction based on the consortium block chain ensures 2 way security and privacy.	Flow constraints are to be noticed.	krill herd algorithm
[12] Su *et al.*	To design a energy block chain based on block chain for safer EV charging in smart community.	Energy allotment mechanism is used for allotting the energy to the demand EVs	No encouragement like compensations has been given to the discharging EVs	Byzantine fault tolerance consensus algorithm
X. Chen and X. Zhang [13]	To design safer power dealing and stimulus settlement model depending on the elemental guidelines of china's electricity market.	Increases the power dealing capacity and also minimizes the delay taking by the system to do the dealing. The proposed framework achieves lower overhead in the communication. It can check and Validate similar type of signed messages in a lesser time.	Malicious vehicles can disturb the harmony of the framework but there are no punishment actions for intruder EVs to build the framework with more stability.	Elliptic curve bilinear pairing. Practical Byzantine fault-tolerant consensus algorithm.
Sheikh *et al.* [14]	To design a Byzantine based block chain consensus framework which throws a light on the power dealing flow among Electric Vehicles and distributed network.	Power consumption is less due to the usage of SHA-256 algorithm. Less prone to different attacks by the intruders at the time of information transformation. Here they used Byzantine fault tolerance which achieves Identity management of nodes, Consensus finality and Scalability.	No refinement in consensus algorithm. There is no valuation of performance with extra physical limitations of Distributed Networks and Electric Vehicles.	Byzantine fault tolerance pricing technique. SHA-256 for the purpose of hashing.
Zhao *et al.* [15]	To explore the privacy troubles of a consensus based distributed energy management model where both energy producers and customers cooperatively enhance the social welfare.	Both the proposed algorithms can preserve the privacy of both customers and generation units. Concurrence and flawlessness of final solution are preserved.	Private data of consumers is disclosed for a while before using secret function. Regional confidential function can be recognized by adjoining nodes.	Distributed energy management algorithm. A confidential function dependent privacy-protecting and privacy-preserving energy management algorithms
Yang *et al.* [16]	To contribute a tentative vision with	An effective method for data transferring	System become complex while	Cloud based energy management system.

	the potential of block chain technologies when applied to decentralized operations in an Energy Internet environment.	and model updating in a decentralized operational framework.	incorporating energy internet which could be interpreted as multiple energy like cooling, electricity, gas, transportation etc.	
Luo*et al.* [17]	To design a distributed electricity trading system to provide the peer to peer electricity transferring between producers and consumers.	There will be secure settlement of the contracts. Overall enhancement in the energy efficiency of the distribution network.	Not applicable, if there are larger number of consumers. Need of third party for auditing the trading contracts in large territories.	Multi agent coalition formation technique. Negotiation protocol technique. Final contract determination algorithm.
Wu *et al.* [18]	To design a modern hybrid block chain for storage application which is block static storage (BSS) for the purpose of improving overall efficiency of internet running.	Proposed system is Trustworthy, efficient and safer for energy internet in storing massive data.	Hashing algorithm used is not more secure.	Hash 1 and Hash 2 techniques are used for the purpose of hashing.
Yu *et al.* [19]	To build a block chain based transaction structure which is uses hierarchical quoting to find optimal cost.	Ensures more security to the transaction process and achieves irreversible modification of transactions stored in ledgers.	The transaction settlement cost is not accurate to the actual cost and it is not a dynamic pricing technique.	Bayesian theorem. Nash equilibrium technique.

III SYSTEM OVERVIEW

The system model, security and privacy objectives and bilinear pairing are briefly explained in this section.

A. SYSTEM MODEL

The System model for the decentralized energy trading scheme is demonstrated in Fig. 1. The system model consists of five major components namely Trusted Authority (TA), aggregator, Electric vehicles (EVs), power supply stations, and the crypto currency Bit coin.

Trusted Authority: The trusted authority (TA) plays a key role in our scheme, it will maintain the whole system details. It should contain the details of each aggregator and each EV in network such as their ID numbers, license plate numbers of EVs, private and public keys of both EVs and aggregator etc. The TA is assumed to be fully trusted and it is impossible for any intruder or opponent to compromise TA. Moreover, the trusted authority is also responsible for the registration of aggregators and EVs before the start of the trading process. In our scheme the entire vehicle to grid network is divided into several constituencies and each constituency has a TA. Whenever an EV moves from one constituency to another region then the EV is authenticated by TA at new constituency using the public value of TA of that particular constituency. At that time, both TAs in two constituencies will interchange their public values to validate the Electric vehicles in the case of EV roaming from one constituency to other. In Fig. 1, only one TA is illustrated for one region for our understanding. This TA is used to generate the IDs, public and private keys for aggregators and EVs after their successful registration. TA authenticate all EVs (charging/discharging) participating in the trading model by using the authentication node in the communication server. Based on the authentication, the amount is debited in the form of crypto currency called bitcoin to ensure their participation.

Aggregator: These are fixed infrastructures placed at the charging spot. Aggregator works as a power mediator and contribute energy to the EVs. EVs which require charge send their energy request to the aggregator in the charging spot. Aggregators will choose an optimal energy solution to the charging EVs by announcing their demand information to the EVs which are ready to discharge. These aggregators are assumed to be semi-trusted i.e. they may disclose the sensitive data about any EV to an adversary. So that EV also should authenticate aggregator before communicating to it. Moreover, if any aggregator is found to be compromised, then TA will revoke the identity of that particular aggregator.

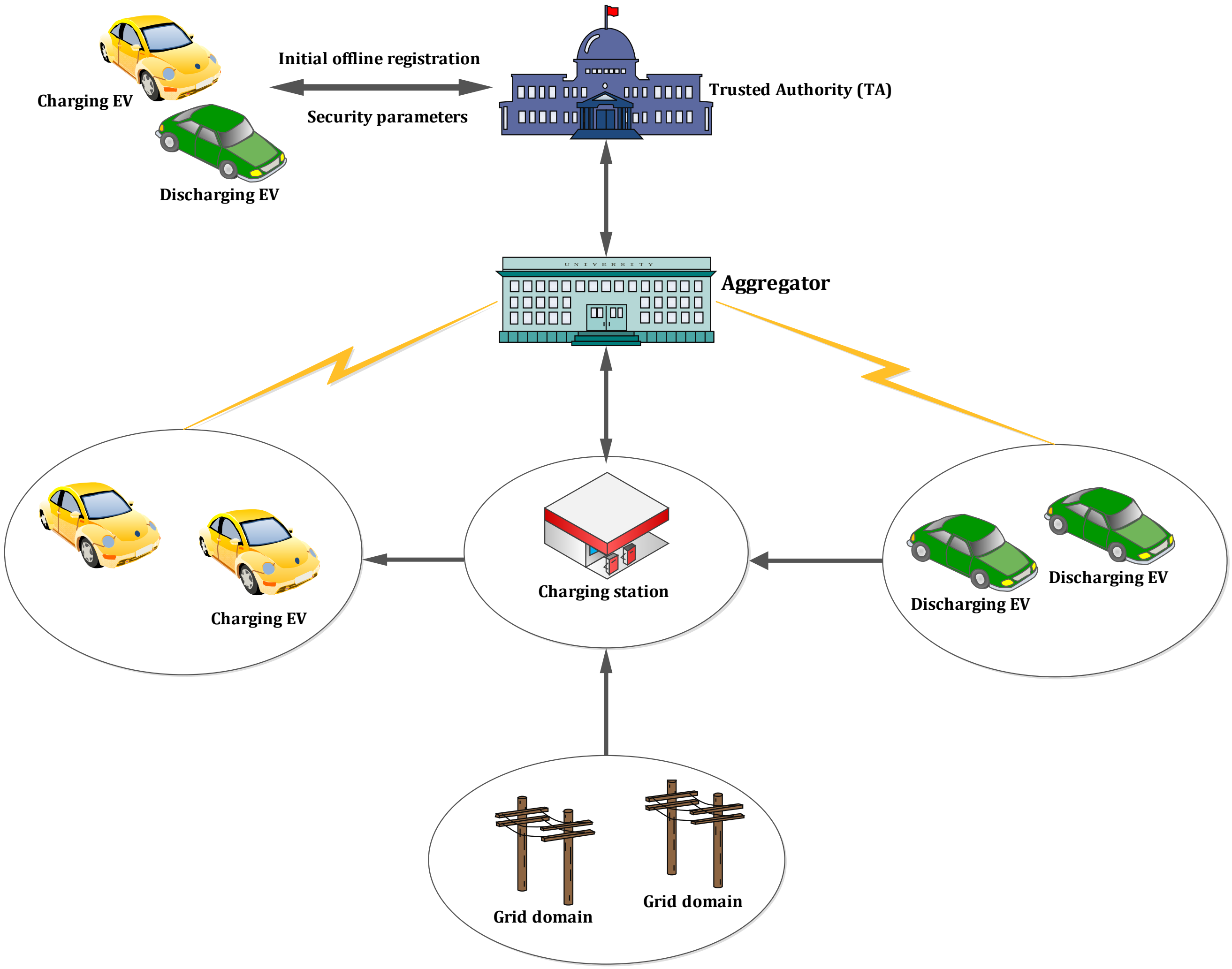

FIGURE 1.Schematic of Vehicle to grid architecture

Electric Vehicles: In the Vehicle to Grid network, EVs also play an important role in energy exchange, including charging and discharging. By using peer-to-peer trading method, the EV selects their belonging role. Each EV consists of an On Board Unit (OBU) which allows the EV to communicate with aggregator and other EVs to share messages. And each OBU has a TPD device which is known as Tamper-proof-device used to store the public and private keys information of that EV.

Power supply station: The power supply station provides the required power and power deal services for charging EVs incase if discharging EVs are not able to satisfy its criteria.

Crypo currency Bit coin: Bitcoin is one type of cryptocurrency used in this trading model. The charging EV

and discharging EV will pay some bitcoin to the aggregator during their initial registration and authentication. Once the energy transaction is successfully accomplished, the debited bitcoin amount will be transferred to the surplus EV based on smart contract. On the other hand, if the transaction is not successful, the advance amount collected from charging and discharging vehicles will be return back. Moreover, the energy transformation takes place through contrary auction mechanism.

The Fig. 1 depicts the decentralized and distributed Vehicle to grid architecture. Aggregator is connected to trusted authority in a wired manner. In addition, aggregator and power grid are connected to charging station in a wired manner. EVs are connected to aggregator in a wireless manner and at the time of offline registration, EVs will communicate with TA to get their public and private keys. The overall operation mechanism of V2G architecture is explained as follows. Initially, all EVs and aggregators register at trusted authority (TA) and then TA will generate public and private keys for both EVs and aggregator. When the EVs come to charging spot for the purpose of charging/discharging, aggregator and EVs authenticate mutually in an anonymous manner before the start of trading. Only, if the authentication is completed successfully, authorized vehicles are allowed to participate in the trading and the authorized EVs are indicated by status value of ‘1’ and unauthorized by '0'. In the beginning of trading, charging EVs will send their demand data to the charging station's smart meter or aggregator. Furthermore, the aggregator will receive details regarding the charging EV's power request and trading time. The aggregator then broadcasts the charging EVs demand data to the discharging EVs that have arrived at the charging station. Moreover, discharging vehicles send their power capacity and cost to the aggregator. Aggregator will match charging and discharging EVs for the purpose of exchanging of electricity and amount by using contrary auction mechanism. In each round aggregator will match one charging EV and one discharging EV by comparing the prices quoted by discharging EVs, then the charge from discharging EV is first transferred to charging station and the charge will be stored at charging station temporarily, then from charging station the charge will be transferred to matched charging EV. As a result, charging and discharging EVs will complete the energy transaction with help of the aggregator.

B. SECURITY AND PRIVACY OBJECTIVES

In this section, security and privacy analysis of our proposed method in terms of Anonymity, Authentication, Integrity and Transparency is discussed.

Anonymity: Rather than using the real identity, each Electric vehicle exploits a unique public key $\boldsymbol{Pu_{EV}}$ to communicate with aggregator, which prevents malicious users from discovering EV's identity. Moreover, an Electric Vehicle can alter its public key after each round by using updated private key $\boldsymbol{\alpha}$ sent by aggregator to avoid linking attack. This attack is the action of linking all data of the same EV together to discover the true identity of the EV.

Authentication: In this proposed method, mutual authentication technique is used, which allows both the EVs and aggregator to authenticate each other so that only the authorized users have the access in the network. Moreover, before the start of trading, the aggregator audits the quote of each EV whether it is true quote or not. As a result, no user on the network will compromise the authentication method.

Integrity: The transaction will be stored in a block in the block chain network after each round is completed, with each block containing its own hash as well as the hash of the previous block. Moreover, the copies of this transaction details in the form of public address will be available to all nodes in the network. As a result, an attacker cannot alter or modify any data in the block of any node in the network. However, the data inside the block is encrypted with asymmetric encryption techniques. Without a private key, decrypting the encrypted data is extremely expensive.

Transparency: The data in the block chain technology is visible to every node in the network i.e. any user/ software developer/ service provider in the network having the private key can access and monitor the transaction data inside the block without modifying it. Every node in the network saves a copy of data and it is transparent to all entities. As a result, any kind of malicious modification of the data can be easily detected and traceable. Even-though the transaction details are transparent, the privacy is preserved since the details are encrypted in the form of public address.

C. BILINEAR PAIRING

Assume $\boldsymbol{G_1}, \boldsymbol{G_2}$, and $\boldsymbol{G_T}$ indicate multiplicative cyclic groups of order $\boldsymbol{q}$, here $\boldsymbol{q}$ is a large prime number. The bilinear map $\boldsymbol{e} : \boldsymbol{G_1} \times \boldsymbol{G_2} \rightarrow \boldsymbol{G_T}$ obeys following properties;

Bilinearity: The mapping $\boldsymbol{e} : \boldsymbol{G_1} \times \boldsymbol{G_2} \rightarrow \boldsymbol{G_T}$ is called as a bilinear if $\boldsymbol{e(g_1^a, g_2^b)}$= $\boldsymbol{e(g_1, g_2)^{ab}}$,$\boldsymbol{g_1} \in \boldsymbol{G_1}$&$\boldsymbol{g_2} \in \boldsymbol{G_2}$ and $\forall \boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{Z_q^*}$, where $\boldsymbol{Z_q^*} = [\mathbf{1}, \dots, (\boldsymbol{q} - \mathbf{1})]$.

Non degeneracy: $\boldsymbol{e(g_1, g_2)} \neq \mathbf{1}_{\boldsymbol{G_T}}$.

Computability: we have an effective method to fluently calculate the bilinear map $\boldsymbol{e} : \boldsymbol{G_1} \times \boldsymbol{G_2} \rightarrow \boldsymbol{G_T}$.

IVPROPOSED SCHEME

Traditional Energy trading methods have no standard security precautions, which may allow unauthorized users to access the network without any security requirements. However, security is efficiently preserved in our proposed scheme through three steps: initialization, registration, and mutual authentication. Initially EVs and aggregator should register themselves to the trusted authority (TA). Then the trusted authority will generate public key and private key for each EV and aggregator for the purpose of mutual authentication at the time of trading. As a consequence, anonymity is accomplished by concealing the user's true identity. After receiving the public and private keys, both EVs and aggregator will authenticate each other mutually in an anonymous manner.

A. Initialization:

Initially TA will choose two keys namely private and public key as $\boldsymbol{Pr_T}$and $\boldsymbol{Pu_T}$ such that $\boldsymbol{Pr_T} : \boldsymbol{x} \in \boldsymbol{z_q^*}$ i.e. $\boldsymbol{x}$ is belonging to multiplicative group of prime number $\boldsymbol{q}$,such that$\boldsymbol{Pu_T} = \boldsymbol{e(g_1, g_1)^x}$.Moreover, TA will calculate the master key $\boldsymbol{k}$and$\boldsymbol{k_1}$. TA will choose another number $\boldsymbol{a}$ from the multiplicative group of $\boldsymbol{q}$ then it will compute Master key:$\boldsymbol{a} \in \boldsymbol{z_q^*}$ and compute $\boldsymbol{k} = \boldsymbol{g_1^a}$ and$\boldsymbol{k_1} = \boldsymbol{g_1^{x/(\propto+a)}}$. In addition, for aggregator TA will choose a large prime number i.e. $\boldsymbol{q}$ And Let $\boldsymbol{g_1}$ is the generator. Such that the private key for the aggregator is given by $\boldsymbol{Pr_A} = \boldsymbol{\alpha} \in \boldsymbol{z_q^*}$ and the public key of the aggregator is given by $\boldsymbol{Pu_A} = \boldsymbol{g^\alpha}$

B. Registration:

In registration process, TA need to provide private and public keys for EVs and aggregator.

For aggregator: First TA chooses a private key $\propto$ for aggregator such that, $\propto \in \boldsymbol{z_q^*}$ and also it will accommodate one Id for aggregator. And then compute public key $\boldsymbol{Pu_A}$ for aggregator such that $\boldsymbol{Pu_A} = \boldsymbol{g_1^{\alpha+a}}$. Then the TA will store($\propto$, $\boldsymbol{Pu_A}, \boldsymbol{Ts}, \boldsymbol{ID}$). And it will send $(\boldsymbol{k}, \boldsymbol{k_1}, \propto, \boldsymbol{Pu_A})$ to Aggregator securely, where $\boldsymbol{Ts}$ is the time stamp.

For EV: TA will choose a private key $\boldsymbol{\beta}$ for EV such that $\boldsymbol{\beta} \in \boldsymbol{Z_q^*}$ and then by using private key it will calculate the public key for EV as$\boldsymbol{Pu_{EV}} = \boldsymbol{g_1^{\beta + a}}$.And then($\boldsymbol{\beta, Pu_{EV}, Ts, license\ plate\ number}$)will be stored by TA. And finally TA will send ($\boldsymbol{\beta, Pu_{EV}, k}$) to the EV in a secure way.

C. Mutual Authentication:

After the completion of registration, EVs and aggregator will get their respective public and private keys from TA. They will use their public keys to transfer any information to other user at the time of trading. Before starting of trading when EVs came to charging spot EVs and aggregator will authenticate each other mutually in a secure manner i.e. in an anonymous manner. Initially, aggregator authenticates EV in an anonymous manner. For that, EV chooses random numbers $\boldsymbol{m_1, m_2} \in \boldsymbol{Z_q^*}$ and computes the random session keys as$\boldsymbol{S_1} = \left(\boldsymbol{g_1^{m_1+\beta}}\right)^{\boldsymbol{\alpha}}$,$\boldsymbol{S_2} = \left(\boldsymbol{g_1^{m_2+\beta}}\right)^{\boldsymbol{\alpha}}$,$\boldsymbol{S_3} = \boldsymbol{g_1^{\beta}}$ then from this it will compute C such that, $\boldsymbol{C = H(S_1||S_2||\ S_3||k).}$ Then EV will send $(\boldsymbol{L_1, L_2, C})$ to the aggregator where,$\boldsymbol{L_1} = \boldsymbol{g_1^{m_1\alpha}}$ and $\boldsymbol{L_2} = \boldsymbol{g_1^{m_2\alpha}}$.On receiving these parameters, aggregator will compute,$\boldsymbol{A_1} = (\boldsymbol{S_3})^{\boldsymbol{\alpha}}$,$\boldsymbol{S_1^1} = \boldsymbol{L_1.A_1}$,$\boldsymbol{S_2^1} = \boldsymbol{L_2.A_1}$. And then aggregator will compute $\boldsymbol{c^1} = \boldsymbol{H}(\boldsymbol{S_1^1}||\boldsymbol{S_2^1}||\boldsymbol{S_3}||\boldsymbol{k})$.If $\boldsymbol{c = c^1}$ holds, then aggregator will accept EV. Then, the aggregator sends $\boldsymbol{\gamma_1} = \boldsymbol{k} \oplus \boldsymbol{k_2}$&$\boldsymbol{\gamma_2} = \boldsymbol{k} \oplus \boldsymbol{k_1}$ to the EV, where$\boldsymbol{k_2} = \boldsymbol{g_1^{\alpha}}$. Then after receiving this, the EV calculates,$\boldsymbol{k_2} = \boldsymbol{\gamma_1} \oplus \boldsymbol{k}$,$\boldsymbol{k_1} = \boldsymbol{\gamma_2} \oplus \boldsymbol{k}$.Then, check the condition, $\boldsymbol{e(k_2.k, k_1)} = \boldsymbol{Pu_T}$.If this condition is satisfied, the aggregator is accepted by EV to communicate.So, in this way only authenticated users can participate in trading, so that security is preserved in our method.

D. Blockchain Technology In V2G Network:

Since the current EV energy trading system is centralized and relies on trusted third parties, there is a risk of user privacy leakage and single point failure. As a result, the protection and reliability of the trading system in the V2G network must be enhanced. Blockchain technology, which has the advantages of being decentralized, stable, and resilient, has recently been adopted for energy trading. After its promising implementation in the financial sector, Blockchain technology is now being used in all emerging technologies. Blockchain technology guarantees the safety of V2G power transactions for EVs [20-24]. As a result, using blockchain technology and smart contracts in a V2G network, it is possible to create autonomous and electrically driven trading between EVs. EVs with chargers will engage in this P2P [25] energy exchange in both directions. In addition, we use private blockchain to verify and audit transaction records between EVs based on aggregators. To achieve a balance between supply and demand in this V2G network, an adjustable mechanism is required [26]. To develop the energy trading model with dynamic pricing strategy and maximize the amount of energy exchanged between EVs, a method known as contrary auction is used.

E. Bitcoin Based Smart Contract Technology:

Smart contracts [27, 28] are an interesting feature of blockchain technology. Smart contracts are a type of code that runs on the blockchain and allows two parties to reach an agreement without the involvement of a third party. All smart contracts in blockchain technology are held publicly in blockchain nodes. Bitcoin is one of the cryptocurrencies used in blockchain technology. This bitcoin cryptocurrency is decentralized and offers excellent support for the growth of an EV-to-EV trading network. The amount will be debited/ credited in the form of bitcoin from charging EVs or to discharging EVs based on smart contract function. Charging EV will release their energy demand information while the discharging EVs will return their response information and price on the blockchain. Finally, the blockchain matches charging and discharging EVs automatically [29]. The smart contract for the trading model of EV energy is based on the contrary auction process.

F. V2G Energy Trading Using Smart Contract:

In a progressive order, energy transactions are split into three phases and they are as follows.

1) Succumb feature of demand:

During the initial demand registration process, authorized users in V2G may request the purchase of energy from the grid or from the discharging EV on the trading platform. In order to avoid the false requirements, bitcoin cryptocurrency should be released into the smart contract address during this registration stage. Smart contracts prioritize the application by referencing the time of registration.

2) Quotation function:

If the charging EVs have transferred the requisite charging details to the trading platform, it is made accessible to all registered users, and the auction process begins. The EV with excess energy submits a confidential quote and all required data to the trading platform, and the bidding process begins. The bidding process is divided into two stages:

Wrapped quotation phase: The surplus EV uses an irreversible hash function in the wrapped quotation process. It uses its true excerpt (real quote) with combined characters of characteristic strings and then hashes the cryptogram as a wrapped quotation stage. In order to avoid malignant bidding, the EVs need to transfer some amount of bitcoin to the smart contracts. The wrapped bid is given by*W*=*H(t,r)*.Here *W* is the wrapped quote; *H* is the algorithm based on hash; '*t*' is the true excerpt; '*r*' is the arbitrary data formed by combining characters personalized by the discharging EV.

Public quotation phase: In the public quotation phase, the surplus EV submits its own true power capacity and customized arbitrary string in advance. The smart contract checks if *H(t,r)* is persistent with the wrapped quotation *W* send by the surplus EV. If not, the quotation is represented as invalid. Each time a smart contract collects an accurate quote and it executes an auction method that is already accepted by all participants. Moreover, the initial price of every participant is recomputed based on the rules of contrary auction before the public offer span ends.

3) Transaction agreement method:

During the energy transmission time, an energy trading agreement is made between discharging and charging EVs. Once it is agreed and all the transactions are completed, the remaining margin will be repaid based on smart contract.

G. Constructing Distributed EV Energy Trading Model using the Proposed Contrary Auction:

The proposed blockchain-based contrary auction trading model is a dynamic allocation mechanism compared to the conventional EV driving model (static allocation mechanism). In the conventional model, the discharging EV arriving at first will provide their charge to the charging EV and there is no reduction in their original fixed cost. The charging EV should meet the demand made by the discharging EV. Moreover, the transaction is made under third party and there is no authentication of the EVs. In our proposed process, the discharging EV with the lowest cost will be chosen in the first round, and there is a probability of selecting the loser EVs based on dynamic allocation mechanism in the successive rounds. Aggregator plays a main role in this blockchain based mechanism, which chooses an optimal solution by integrating the time period and cost of the charging of EV. Initially, the EVs which require charge send their requests with digital signature to aggregator and then the authentication server authenticates the EV based on the digital signature and declares whether it is an authorized or unauthorized EV(i.e. in mutual authentication). In a variable named as “status”, if it returns ‘1’, then the EV is authorized otherwise it is unauthorized. Only authorized user will participate in contrary auction mechanism. Finally, the aggregator assess all candidates playing in the auction and chooses the discharging EV which is having the lowest starting price in the first round and declared as the winner.

Step 1: The charging EV sends details about its power demand to the aggregator. Priority is given depending on the time period, so if the time period is same, the aggregator will give priority to users who purchase more power.

Step 2: Similarly, the discharging EVs provide the aggregator with their respective power data. The priority is given based on the lowest quoting price &highest power delivering capacity of the discharging EVs.

Step 3: The authentication of charging EV and discharging EV are done at the authentication server through the communication server.

Step 4: If the authentication is successfully verified, it returns the value of “status” variable back to the aggregator via communication server.

Step 5: The control centre in the communication server sorts the received power information of charging EV and discharging EV and send backs to the communication server.

Step 6: The communication server sends this received demand power information of charging EV to the discharging EVs via aggregator.

Step 7: The contrary auction process takes place and the initial prices of all discharging EVs will be compared and the lowest initial price of the discharging EV will be chosen as the winner and prepared to match the charging EV.

Step 8: The results (only quoting price of winner) of the auction will be broadcasted, allowing the loser discharging EVs to help them change their initial price by reducing it by a certain amount. This method will increase the probability of the loser EVs to win in the next round.

Step 9: First a distributed ledger will be established based on Blockchain technology. After passing through the smart contract algorithm, an agreement will be concluded between charging and discharging EV.

Step 10: The Blockchain method further tests if there is a false quote between EVs being charged and discharged. If it happens, then transaction will be failed and smart contract process will pay the margin to other. i.e., if any false bidding is done at the charging side, then charging EV will be eliminated and the energy from the discharging EV will be transferred to the grid. On the other hand, if false bidding is done at the discharging side, then the corresponding discharging EV will be eliminated and the energy will be supplied from the grid to the charging EV. Otherwise, the transaction will be preceded in the normal way.

Step 11: The selected discharging EV through contrary auction will transfer energy to the charging EV. After each successful transfer; the bitcoin currency from the wallet of charging EV will be transferred to wallet of discharging EV using public key of both users wallet based on smart contract.

Step 12: The blockchain mechanism would refund the advanced sum back to the wallet of the charging EV if the transfer is not successful. If the first auction round is completed, the next auction round will be conducted by repeating all of the above steps until all charging EV transactions are completed.

The process can be explained by the following flow chart shown in Fig.2

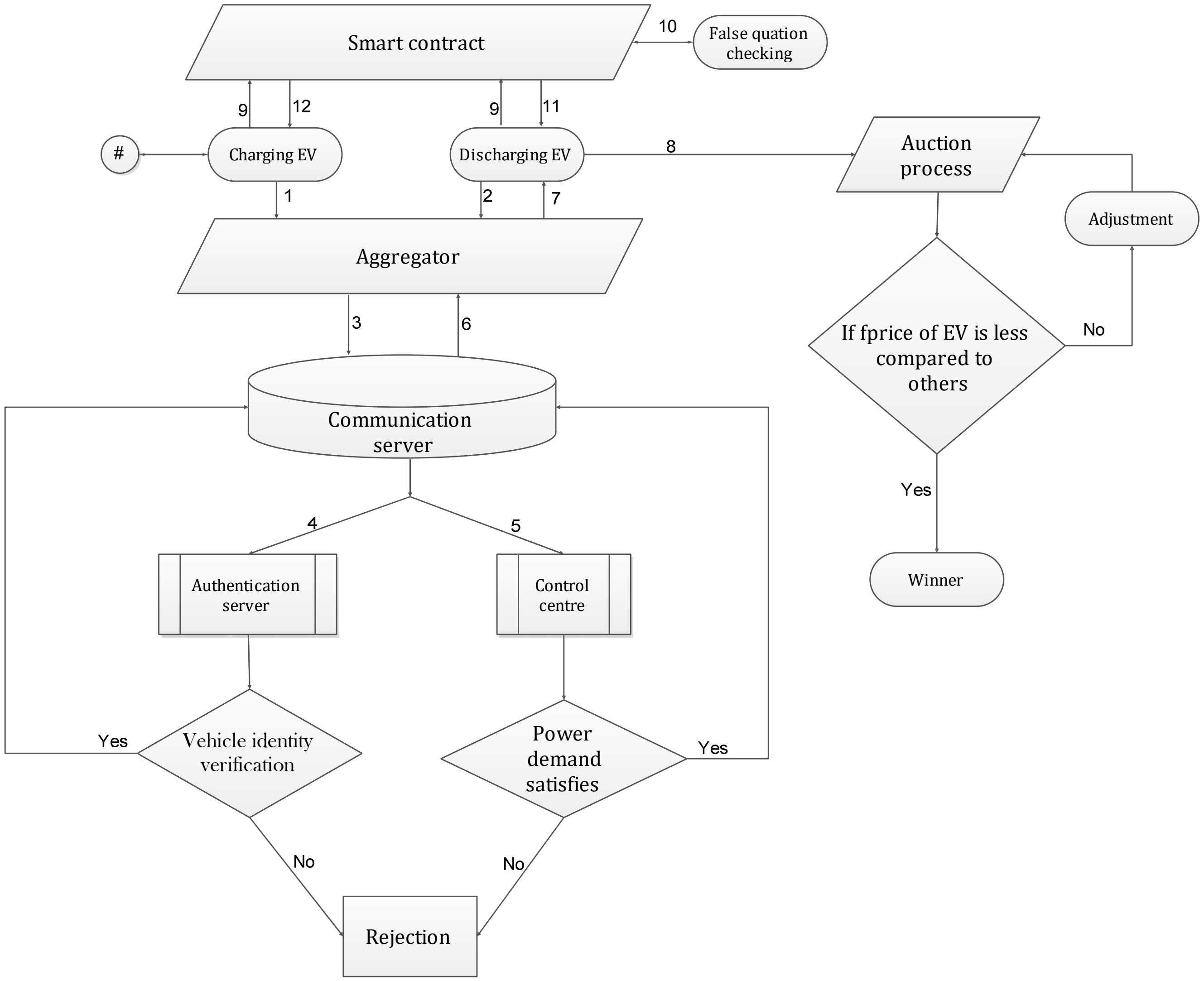

FIGURE 2. Flowchart showing the EV energy trading model using smart contract.

This trading scheme and settlement uses the consensus protocol of blockchain technology. In addition, all the information regarding transaction is stored in the distributed ledger in the block and the copy of block is broadcasted to every node in the block chain network. Any updation in the ledger will be updated simultaneously in the block and it is broadcasted to all the nodes. This dynamic pricing strategy has more advantages than the traditional static pricing strategy. Here, the price of electricity can be adjusted according to the transaction situation. i.e., if the discharging EV ('EV1') is winner in the first round of auction, then there will be nochange in its energy price. Else, its price is reduced by certain percentage but not less than the lowest price of that particular EV.

V EXPERIMENTAL ANALYSIS

A. Dynamic Pricing Algorithm using Contrary Auction:

The flowchart representing the contrary auction process is depicted in the Fig.3.

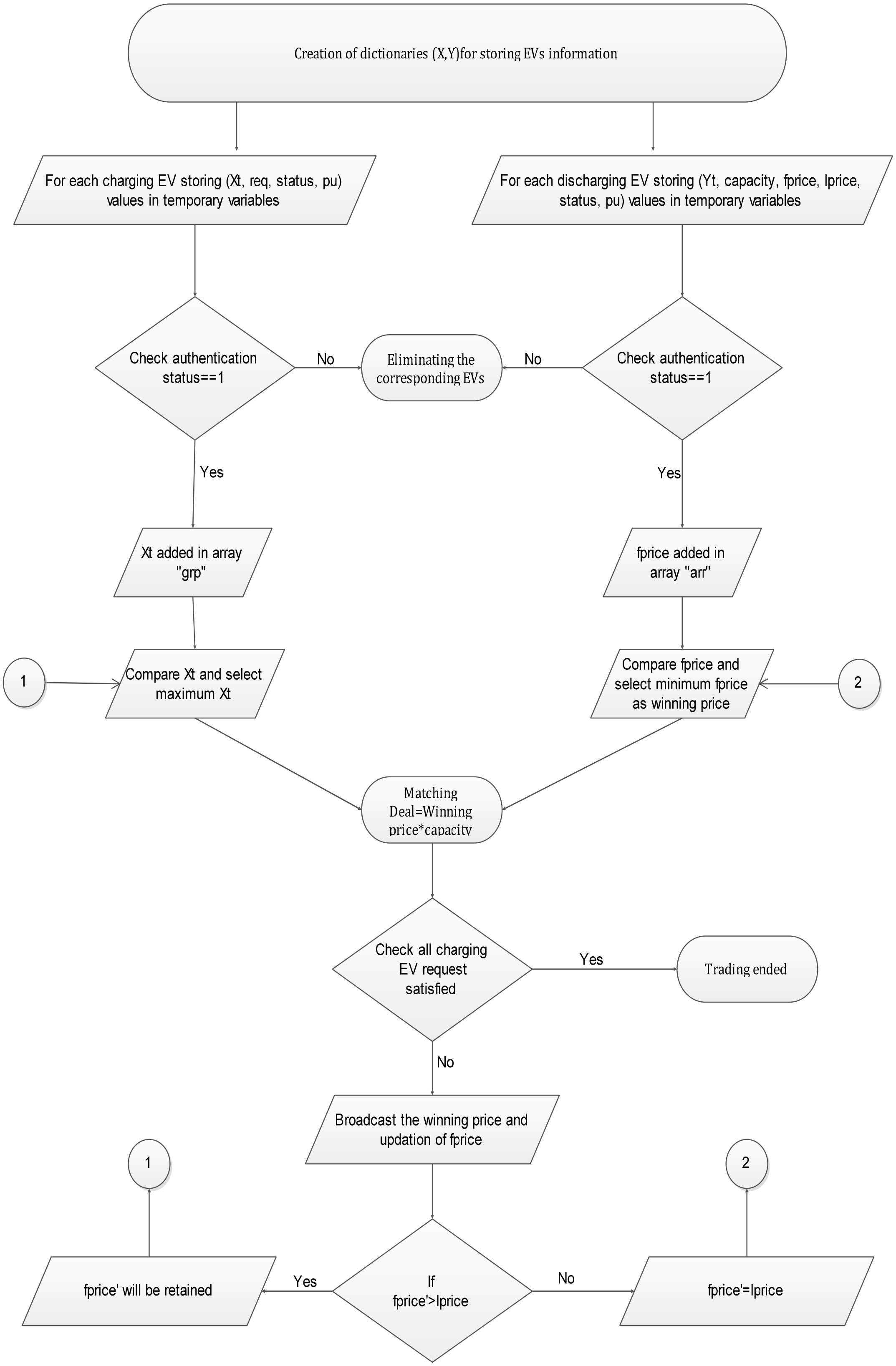
Creation of dictionaries (X,Y)for storing EVs information
For each charging EV storing (Xt, req, status, pu) values in temporary variables
For each discharging EV storing (Yt, capacity, fprice, lprice, status, pu) values in temporary variables
Check authentication status==1
No
Eliminating the corresponding EVs
No
Check authentication status==1
Yes
Yes
Xt added in array "grp"
fprice added in array "arr"
1
Compare Xt and select maximum Xt
Compare fprice and select minimum fprice as winning price
2
Matching Deal=Winning price*capacity
Check all charging EV request satisfied
Yes
Trading ended
No
Broadcast the winning price and updation of fprice
1
2
fprice' will be retained
Yes
If fprice'>lprice
No
fprice'=lprice

FIGURE 3.Schematic flow of contrary auction process in V2G network

Algorithm 1 Contrary Auction Algorithm

```
1: The aggregator forms a set of quad X= {($\boldsymbol{Xt_1}$ ,$\boldsymbol{req_1}$ ,$\boldsymbol{status_1}$,$\boldsymbol{Pu_1}$ )to ($\boldsymbol{Xt_n}$ ,$\boldsymbol{req_n}$ ,$\boldsymbol{status_n}$,$\boldsymbol{Pu_n}$ )}for each charging vehicle demand information. Then the information in X is arranged based on the trading time $\boldsymbol{Xt_i}$, if $\boldsymbol{Xt_i}$ is same, then the information is arranged based on demand $\boldsymbol{req_i}$ from large to small, $\boldsymbol{status_i}$represents authentication of $\boldsymbol{i^{th}}$ charging EV and $\boldsymbol{pu_i}$ contains the public key of the wallet of particular charging EV and 'n' denotes the number of charging EVs in the queue.
2:for i in range(n);
If int(status)==1:
          x[int(xt)]=[int(req),pu].
3: sorting the bid information of charging EVs based on their trading time:
          Sorted(x .keys ()) [: : -1].
4: adding the Xt to an array: grp=[]
5: Similarly, the aggregator forms a set Bids Y = {($Yt_1$, $Capacity_1$, $fprice_1$, $lprice_1$, $status_1$, $pu_1$), . .,($Yt_m$, $Capacity_m$, $fprice_m$, $lprice_m$, $status_m$, $pu_m$)} for each discharging EVs. Then the information is arranged according to trading time $Yt_j$, where $Capacity_j$ is the energy capacity of the discharging EV, $fprice_j$ is the starting setting price, $lprice_j$ is the minimum price, $status_j$ tells about the authentication of that particular discharging EV and $pu_j$ represents the public key of the wallet of that particular discharging EV and 'm' is the number of discharging EVs in the queue.
6:for j in range (m):
Ifint(status)==1:
          y[int(fprice)]=[int(Yt),int(capacity),lprice, pu]
7: Sorting the bid information of discharging EVs based on their initial price(fprice):
          Sorted(y.keys()).
8: Adding the initial prices of all discharging EVs to an array:     arr=[]
          for kiny.keys():
                    arr.append(k)
9:whilelen(x)!=0:
10:For each round the minimum of all initial prices of surplus EVs should be taken as winning price and at the same time one charging EV also should be selected for matching:
          Whilex[grp[0]][0]!=0:
                    Pay=min(arr)
                    M=min(x[grp[0]][0],y[pay][1])
                    deal=pay*M
11: charging EV & discharging EV bid update:
          y[pay][1]=y[pay][1]-M
          x[grp[0]][0]=x[grp[0]][0]-M
12: Before the beginning of next round the loser discharging EVs will update their initial prices by reducing fprice by some percentage( r ):
          Foriinrange(len(arr)):
                    r =((arr[i]-pay)/pay)
                    y[arr[i]-r]=y[arr]
                    del y[arr]
          sorted(y.keys())
          arr[i]=arr[i]-r
13:Therefore this process will continue until all charging EVs request (req) decrease to zero or all discharging EVs capacity is exhausted.
```

According to the contrary auction process, the buyer quotation queue (charging EV) would be matched by the respective seller queue (discharging EV) for transactions. When both the EVs are matched, there will be exchange of energy and the amount in the form of bitcoin will be debited/ credited from their wallet through smart contract mechanism. If the quotation queue of one of the buyer or seller is completed, then the matching between the two EVs will be stopped. If the discharging EV loses in one auction, they will be able to change their quotes in the next auction, increasing their probability of winning. As a result, it improves both social security and business productivity. The success rate is more when compared to traditional scheme.

B. SIMULATION SETUP

In order to store the transaction details in block chain network, it is necessary to get the details like amount, public key of the EVs wallet to transfer money, charge exchanged between charging and discharging EV for each round. Moreover, python 3.6.2 software is used for the practical experimental setup and algorithm is written in python code. The charging EVs information (transaction time, requesting charge, status, public key of the wallet of each charging EV) and discharging EVs information (transaction time, capacity of charge can be delivered by each discharging EV, initial quoting price of each discharging EV, lowest price of each EV below which no discharging EV should quote its price, status, public key of wallet of each discharging EV) are taken as inputs and if the data of charging EV matches with discharging EV, then the output is delivered after the completion of each round. Moreover, the algorithm will calculate the winning price and determines the winner of each round based on the Dynamic pricing strategy using contrary auction method i.e., the discharging EV that quotes the lowest price is considered as the winner of each round and all the loser discharging EVs will adjust their quotes for the next round based on the winning price and the process repeats. Simultaneously for each round, the charging EV to be matched is selected according to its trading time (in descending order) and also the time taken to complete total trading process is also noted.

The output for the selection of authenticated charging and discharging EVs, updation of fprice, iteration of successive rounds and winning EV are represented in the following tables. There are 9 charging EVs which are participating in the trading. The information (quote) of each charging EV will be in the form of"$\boldsymbol{Xtime}$: [$\boldsymbol{request}, \boldsymbol{status}, \boldsymbol{pu}$]". Table 2 shows the charging EV participating in the trading. Here, $\boldsymbol{Xtime}$represents the trading time for each charging EV, $\boldsymbol{request}$is the amount of electricity requested by the charging EV,*status* represents the integrity of an EV i.e. 1 represents authorized EV and 0 represents unauthorized EV,$\boldsymbol{pu}$represents the public key of wallet of EV.

TABLE 2: Total number of charging EV participating in trading.

S. No	Xtime	Request	Status	PU
1.	29	37	1	djfjdd7
2.	38	45	1	djdjdj7
3.	47	56	1	fhdhdh8
4.	25	39	1	fhdjok3
5.	40	60	1	kjhgdi2
6.	50	65	1	djlkop1
7.	35	51	1	ggkkio9
8.	60	70	1	fjigti5
9.	55	67	0	thuthn1

Table 3 represents the information of the charging EV after sorting according to their trading time. Here, the charging EV with more trading time is given the highest priority and the same is shown in the table 3.

TABLE 3: Total number of charging EV sorted according to their trading time.

S. No	Xtime	Request	Status	PU
1.	60	70	1	fjigti5
2.	50	65	1	djlkop1
3.	47	56	1	fhdhdh8
4.	40	60	1	kjhgdi2
5.	38	45	1	djdjdj7
6.	35	51	1	ggkkio9
7.	29	37	1	djfjdd7
8.	25	39	1	fhdjok3

Similarly, there are 9 discharging EVs participating in the trading model as shown in the table 4.The information (quote) of each discharging EV will be in the form of "*fprice:*[*ytime,capacity,lprice,status,pu*]".$\boldsymbol{ytime}$ represents the trading time for each discharging EV, $\boldsymbol{capacity}$ refers to how much energy the discharging EV can supply when it is fully charged.$\boldsymbol{lprice}$ & $\boldsymbol{fprice}$ are the lowest and initial prices quoted by discharging EV. Table 5 represents the information of discharging EV after sorting according to its initial price. From the table 5, it is clearly seen that the discharging EV having minimum initial price is given with highest priority.

TABLE 4: Total number of discharging EV participating in trading.

S.No	fprice	ytime	Capacity	lprice	Status	PU
1.	11	30	39	4	1	fhdjsd2
2.	9	39	41	5	1	ghdjsu3
3.	12	46	64	3	1	dkrihu4
4.	14	26	44	5	1	fhjiok5
5.	13	40	66	6	1	lkjhgf6
6.	16	51	27	2	1	mnbvcx2
7.	18	35	40	7	1	nbvhji8
8.	15	60	54	3	1	djkhil9
9.	20	66	77	4	1	kjiktf5

TABLE 5: Total number of discharging EV sorted according to their initial price.

S.No	fprice	ytime	Capacity	lprice	Status	PU
1.	9	39	41	5	1	ghdjsu3
2.	11	30	39	4	1	fhdjsd2
3.	12	46	64	3	1	dkrihu4
4.	13	40	66	6	1	lkjhgf6
5.	14	26	44	5	1	fhjiok5
6.	15	60	54	3	1	djkhil9
7.	16	51	27	2	1	mnbvcx7
8.	18	35	40	7	1	nbvhji8
9.	20	66	77	4	1	kjiktf5

Moreover, the table 5 clearly shows that the sorting operation is performed based on the initial lowest price quoted by the discharging EV. It does not depends on the total capacity of the charge that the EV possess nor on the trading time of the EV.As per simulation, the matched EVs information for each round are shown in table 6 (total 16 rounds). For each charging EV, the charge is delivered by the matched discharging EV or grid (if the matched discharging EV can't satisfy the charging EV or when the demand of charging EV is greater than the capacity of discharging EV). If the charge delivered is not sufficient, then the remaining demand charge for that particular charging EV will be provided by the next winning discharging EV or directly by the grid (when there is no more discharging EVs participating in trading). In our experimental setup analysis, table 6 shows, there are totally 16 rounds for charging and discharging process. In each round, the intermediate results are known to the aggregator and finally, the winning price should be broadcasted to all loser EVs. The loser discharging EV will adjust their quote to win in the successive rounds. This increases the winning probability of the losing discharging EVs. After the completion of the 16th round, all charging EVs requests are satisfied such that the trading is completed.

TABLE 6: Results of matched EVs after completion of each round.

Round	Matched charging EV				Matched discharging EV					
no.	Xtime	request	Status	PU	f price	ytime	capacity	lprice	status	PU
1	60	70	1	'fjigti5'	9	39	41	5	1	'ghdjsu3'
2	60	29	1	'fjigti5'	10.778	30	39	4	1	'fhdjsd2'
3	50	65	1	'djlkop1'	10.778	30	10	4	1	'fhdjsd2'
4	50	55	1	'djlkop1'	11.585	46	64	3	1	'dkrihu4'
5	47	56	1	'fhdhdh8'	11.585	46	9	3	1	'dkrihu4'
6	47	47	1	'fhdhdh8'	12.321	40	66	6	1	'lkjhgf6'
7	40	60	1	'kjhgdi2'	12.321	40	19	6	1	'lkjhgf6'
8	40	41	1	'kjhgdi2'	12.998	26	44	5	1	'fhjiok5'
9	38	45	1	'djdjdj7'	12.998	26	3	5	1	'fhjiok5'
10	38	42	1	'djdjdj7'	13.623	60	54	3	1	'djkhil9'
11	35	51	1	'ggkkio9'	13.623	60	12	3	1	'djkhil9'
12	35	39	1	'ggkkio9'	14.201	51	27	2	1	'mnbvcx7'
13	35	12	1	'ggkkio9'	15.279	35	40	7	1	'nbvhji8'
14	29	37	1	'djfjdd7'	15,279	35	28	7	1	'nbvhji8'
15	29	9	1	'djfjdd7'	16.285	66	77	4	1	'kjiktf5'
16	25	39	1	'fhdjok3'	16.285	66	68	4	1	'kjiktf5'

C. Computational Cost

In this section, the proposed scheme performance is evaluated in terms of computation cost. Here computational cost is the total cost incurred for signature verification and certificate verification process. The total verification time required for the single/*n* certificates and single/*n* signatures is called as Computational cost. This is mainly calculated to check the authenticity of the (charging and discharging) EVs that are arriving at the charging spot and to check the integrity of the information. The total verification time of the proposed scheme is compared with existing works like L.Li *et al.*[30], M.Azees *et al.*[31], Q.Feng *et al.*[32], J.cui *et al.*[33]. Let the time taken for performing the pairing operation, hashing operation, one point multiplication operation, single point addition operation and exponential operation are represented by *Tp, Th, Tm, Ta* and *Texp* respectively. For performing all the above operations, Type-A curve based pairing-based cryptography (PBC) library [34] is used. Moreover, 2GHz PC having 8-GB RAM with Cygwin version 1.7.35-15[35] is used for our executions. The time values for different operations such as *Tp, Th, Tm, Ta* and *Texp* are given by 1.6 ms (milliseconds), 2.7 ms, 0.6ms, 0.6ms and 0.7 respectively. Based on the timing parameters, the time taken for pairing operation and hashing operation is more in the calculation of computational cost.

TABLE 7: Computational cost for various schemes.

Schemes	For one vehicle	For $n$vehicles
L.Li et al.	$3T_P + 2\,T_m + 2\,T_h$	$3\,nT_h + 2\,n\,T_m + (1+2n)T_p$
M.Azees et al.	$2\,T_p + 4\,T_{exp} + 4\,T_m + T_h$	$(n+1)T_p + 4\,n\,T_{exp} + 4\,n\,T_m + n\,T_h$
Q.Feng et al.	$2\,T_p + 2\,T_h + 3\,T_{exp}$	$(n+1)T_p + 2\,n\,T_h + 3\,n\,T_{exp}$
J.cui et al.	$4\,T_m + T_p + 2T_h + T_a$	$4\,n\,T_m + (2n+1)T_p + (n+1)T_h + n\,T_a$
Proposed	$2\,T_h + 2\,T_{exp} + T_p$	$2\,n\,T_h + 2\,n\,T_{exp} + n\,T_p$

Table 7 clearly shows that our proposed scheme consumes less computational cost when compared to the existing schemes. Moreover, there is no single point multiplicative operation and single point additive operation in our proposed scheme. The time taken for verifying single certificate and single signature in our proposed scheme is only 8.4 ms. However, the computational cost is more than 10 ms for the single EV in the existing schemes.

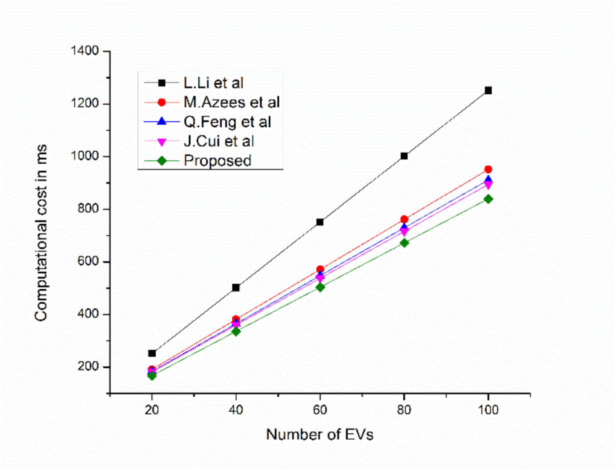

FIGURE 4. Comparison of computational cost of different schemes

Fig.4 clearly depicts our proposed scheme has less computational time in terms of both verification of signature and certificate. In addition, our proposed scheme requires, 840 ms is required as the computational time for verifying 100 EVs. Whereas, in the existing schemes, the computational cost is more than 900 ms for the same number of EVs.

TABLE 8: Execution time comparison of proposed with conventional method.

Number of vehicles	Time taken by our proposed method (in min)	Time taken by conventional method. (in min)	Time Gap (in min)
10	411	415	4
20	1104	1114	10
40	2957	2998	41
50	4222	4293	71
60	5653	5765	112
80	9128	9368	240
100	13,467	13,909	442

Total execution time is the time taken to complete the total trading process. The execution time taken by our proposed method and conventional method to complete the total process for different number of Electric vehicles is shown in the table 8.In order to calculate the execution time analysis, python 3.6.2 software is used for the practical experimental setup and algorithm is written in python code. The table 8 further highlights as the number of EVs increases, the time gap also increases between the proposed and conventional method. This clearly indicates that, energy trading is performed rapidly in our proposed method.

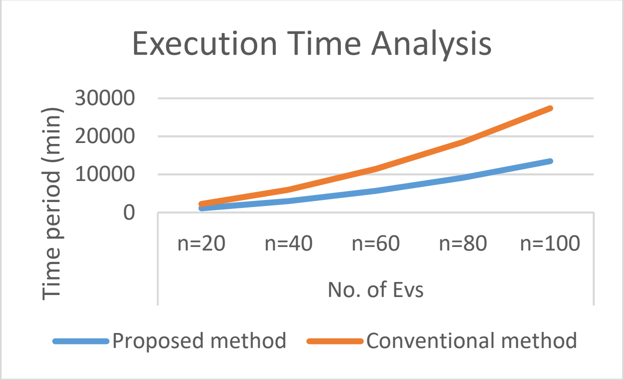

FIGURE 5. Execution time analysis based on number of EVs

When the number of EVs is low, there is no drastic difference between the two schemes (in terms of processing time), but as the number of EVs increases, there is a substantial time difference between the two schemes, as shown in Fig.5. As a result, our proposed scheme will take less time when compared to other traditional schemes to process the transaction.

VI CONCLUSION

In the recent years, applications and features of Blockchain made it wider popular and it can be applied to any platform as it provides security, trust and efficiency. Thus in this work, a system is proposed for Energy trading of Electric vehicles based on Blockchain technology and smart contract. Simulations are performed to compare the behaviour of the proposed scheme with the traditional scheme and the results showed that our proposed scheme takes 3.8% approximately less time compared to traditional scheme for processing the entire trading. This work can be further extended by applying Artificial intelligence (AI) and machine learning concepts to authenticate the electric vehicle as it approaches the charging spot for the purpose of charging/discharging. Moreover, AI can be used to detect and enforce penalties on malicious vehicles. In addition, Internet trading can be incorporated in the Energy trading process, where EVs send their bidding information to the nearby charging spot through online before arriving to the charging spot. This, further decreases the time taken to complete the total process.

Acknowledgement:

This publication, was made possible by NPRP grant # [13S-0108-20008] from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

The APC is funded by the Qatar National Library, Doha, Qatar.

REFERENCES

[1] K. Zhang, Y. Mao, S. Leng, Y. He, S. Maharjan, S. Gjessing, Y. Zhang, and D. H. K. Tsang, "Optimal charging schemes for electric vehicles in smart grid: A contract theoretic approach," *IEEE Transactions on Intelligent Transportation Systems,* vol. 19, no. 9, pp. 3046–3058, Sep. 2018.

[2] Wang, Y., Su, Z., Xu, Q., et al.: 'A novel charging scheme for electric vehicles with smart communities in vehicular networks',*IEEE Transactions on Vehicular Technology*., 2019, pp. 8487–8501

[3] V. Hassija, V. Chamola, S. Garg, D. N. G. Krishna, G. Kaddoum and D. N. K. Jayakody, "A Blockchain-Based Framework for Lightweight Data Sharing and Energy Trading in V2G Network," in *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5799-5812, June 2020, doi: 10.1109/TVT.2020.2967052.

[4] Z. Zhou, B. Wang, M. Dong and K. Ota, "Secure and Efficient Vehicle-to-Grid Energy Trading in Cyber Physical Systems: Integration of Blockchain and Edge Computing," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems,* vol. 50, no. 1, pp. 43-57, Jan. 2020, doi: 10.1109/TSMC.2019.2896323.

[5] H. Wang, Q. Wang, D. He, Q. Li and Z. Liu, "BBARS: Blockchain-Based Anonymous Rewarding Scheme for V2G Networks," in *IEEE Internet of Things Journal,* vol. 6, no. 2, pp. 3676-3687, April 2019, doi: 10.1109/JIOT.2018.2890213.

[6] C. Liu, K. K. Chai, X. Zhang, E. T. Lau and Y. Chen, "Adaptive Blockchain-Based Electric Vehicle Participation Scheme in Smart Grid Platform," in *IEEE Access*, vol. 6, pp.25657-25665,2018.

[7] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang and E. Hossain, "Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains," in *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3154-3164, Dec. 2017, doi: 10.1109/TII.2017.2709784.

[8] Z. Wang, M. Ogbodo, H. Huang, C. Qiu, M. Hisada and A. B. Abdallah, "AEBIS: AI-Enabled Blockchain-Based Electric Vehicle Integration System for Power Management in Smart Grid Platform," in *IEEE Access*, vol. 8, pp. 226409-226421, 2020, doi: 10.1109/ACCESS.2020.3044612.

[9] G. Sun, M. Dai, F. Zhang, H. Yu, X. Du and M. Guizani, "Blockchain-Enhanced High-Confidence Energy Sharing in Internet of Electric Vehicles," in *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 7868-7882, Sept. 2020, doi: 10.1109/JIOT.2020.2992994.

[10] A. S. Musleh, G. Yao and S. M. Muyeen, "Blockchain Applications in Smart Grid–Review and Frameworks," in *IEEE Access*, vol. 7, pp. 86746-86757, 2019, doi: 10.1109/ACCESS.2019.2920682.

[11] Y. Li and B. Hu, "An Iterative Two-Layer Optimization Charging and Discharging Trading Scheme for Electric Vehicle Using Consortium Blockchain," in *IEEE Transactions on Smart Grid,* vol. 11, no. 3, pp. 2627-2637, May 2020, doi: 10.1109/TSG.2019.2958971.

[12] Z. Su, Y. Wang, Q. Xu, M. Fei, Y. Tian and N. Zhang, "A Secure Charging Scheme for Electric Vehicles With Smart Communities in Energy Blockchain," in *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4601-4613, June 2019, doi: 10.1109/JIOT.2018.2869297.

[13] X. Chen and X. Zhang, "Secure Electricity Trading and Incentive Contract Model for Electric Vehicle Based on Energy Blockchain," in *IEEE Access,* vol. 7, pp. 178763-178778, 2019, doi: 10.1109/ACCESS.2019.2958122.

[14] A. Sheikh, V. Kamuni, A. Urooj, S. Wagh, N. Singh and D. Patel, "Secured Energy Trading Using Byzantine-Based Blockchain Consensus," in *IEEE Access,* vol. 8, pp. 8554-8571, 2020, doi: 10.1109/ACCESS.2019.2963325.

[15] Zhao, C., He, J., Cheng, P., & Chen, J. (2017), "Privacy-preserving consensus-based energy management in smart grid", *2017 IEEE Power & Energy Society General Meeting*. doi:10.1109/pesgm.2017.8274438.

[16] Yang, T., Guo, Q., Tai, X., Sun, H., Zhang, B., Zhao, W., & Lin, C. (2017)," Applying blockchain technology to decentralized operation in future energy internet", *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*. doi:10.1109/ei2.2017.8244418.

[17] Luo, F., Dong, Z. Y., Liang, G., Murata, J., &Xu, Z. (2019)," A Distributed Electricity Trading System in Active Distribution Networks Based on Multi-Agent Coalition and Blockchain", in *IEEE Transactions on Power Systems,* 34(5), 4097-4108. doi:10.1109/tpwrs.2018.2876612.

[18] Wu, L., Meng, K., Xu, S., Li, S., Ding, M., &Suo, Y. (2017)," Democratic Centralism: A Hybrid Blockchain Architecture and Its Applications in Energy Internet," *2017 IEEE International Conference on Energy Internet (ICEI)*. doi:10.1109/icei.2017.38

[19] Yu, Y., Guo, Y., Min, W., & Zeng, F. (2019), "Trusted Transactions in Micro-Grid Based on Blockchain" in *Energies*, 12(10), 1952. doi:10.3390/en12101952

[20] R. Zhang, X. Cheng, and L. Yang, "Energy management framework for electric vehicles in the smart grid: A three-party game," *IEEE Commun. Mag.,* vol. 54, no. 12, pp. 93–101, Dec. 2016.

[21] M. Andoni et al., "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renewable Sustain. Energy Rev.*, vol. 100, pp. 143–174, 2019.

[22] Z. Yang, S. Yu, W. Lou, and C. Liu, "P2: Privacy-preserving communication and precise reward architecture for V2G networks in smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 697–706, Dec. 2011.

[23] S. Garg, A. Singh, S. Batra, N. Kumar, and L. T. Yang, "UAV empowered edge computing environment for cyber-threat detection in smart vehicles," *IEEE Netw.*, vol. 32, no. 3, pp. 42–51, May/Jun. 2018.

[24] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, ''A blockchain-based smart grid: Towards sustainable local energy markets,'' *Comput. Sci.-Res. Develop.,* vol. 33, pp. 207–214, Feb. 2018.

[25] N. Liu, X. Yu, C. Wang, C. Li, L. Ma, and J. Lei, "Energy-sharing model with price-based demand response for microgrids of peer-to-peer prosumers," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 3569–3583, Sep. 2017.

[26] C. Zhao, J. He, P. Cheng, and J. Chen, "Privacy-preserving consensus based energy management in smart grids," in *Proc. IEEE Power Energy Soc.* Gen. Meeting, 2017, pp. 1–5.

[27] N. Z. Aitzhan and D. Svetinovic, ''Security and privacy in decentralized energy trading through multi-signatures, Blockchain and anonymous messaging streams,'' *IEEE Trans. Depend. Sec. Comput.,* vol. 15, no. 5, pp. 840–852, Sep./Oct. 2018.

[28] A. S. Yahaya, N. Javaid, M. U. Javed, M. Shafiq, W. Z. Khan and M. Y. Aalsalem, "Blockchain-Based Energy Trading and Load Balancing Using Contract Theory and Reputation in a Smart Community," in *IEEE Access*, vol. 8, pp.222168-222186,2020.

[29] Y. Li and B. Hu, "A Consortium Blockchain-Enabled Secure and Privacy-Preserving Optimized Charging and Discharging Trading Scheme for Electric Vehicles," in *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 1968-1977, March 2020.

[30]L. Li et al., "CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 7, pp. 2204-2220, July 2018, doi: 10.1109/TITS.2017.2777990.
[31]. M. Azees, P. Vijayakumar and L. J. Deboarh, "EAAP: Efficient Anonymous Authentication With Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks," in *IEEE Transactions on Intelligent Transportation Systems,* vol. 18, no. 9, pp. 2467-2476, Sept. 2017, doi: 10.1109/TITS.2016.2634623.
[32] Q. Feng, D. He, S. Zeadally and K. Liang, "BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad Hoc Networks," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4146-4155, June 2020, doi: 10.1109/TII.2019.2948053.
[33] J. Cui, D. Wu, J. Zhang, Y. Xu and H. Zhong, "An Efficient Authentication Scheme Based on Semi-Trusted Authority in VANETs," in *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2972-2986, March 2019, doi: 10.1109/TVT.2019.2896018.
[34] Pairing-Based Cryptography Library. [Online]. Available: http://crypto.stanford.edu/pbc/
[35] Cygwin: Linux Environment Emulator for Windows. [Online]. Available:http://www.cygwin.com/

ATIF IQBAL, Fellow IET (UK), Fellow IE (India) and Senior Member IEEE, Vice-Chair, IEEE Qatar section, DSc (Poland), PhD (UK)- Associate Editor, IEEE Trans. On Industrial Electronics, IEEE ACCESS, Editor-in-Chief, I'manager journal of Electrical Engineering, Former Associate Editor IEEE Trans. On Industry Application. Full Professor at the Dept. of Electrical Engineering, Qatar University and Former Full Professor at Electrical Engineering, Aligarh Muslim University (AMU), Aligarh, India. Recipient of Outstanding Faculty Merit Award academic year 2014-2015 and Research excellence awards 2015 and 2019 at Qatar University, Doha, Qatar. He received his B.Sc. (Gold Medal) and M.Sc. Engineering (Power System & Drives) degrees in 1991 and 1996, respectively, from the Aligarh Muslim University (AMU), Aligarh, India and PhD in 2006 from Liverpool John Moores University, Liverpool, UK. He obtained DSc (Habilitation) from Gdansk University of Technology in Control, Informatics and Electrical Engineering in 2019. He has been employed as a Lecturer in the Department of Electrical Engineering, AMU, Aligarh since 1991 where he served as Full Professor until Aug. 2016. He is recipient of MaulanaTufail Ahmad Gold Medal for standing first at B.Sc. Engg. (Electrical) Exams in 1991 from AMU. He has received several best research papers awards e.g. at IEEE ICIT-2013, IET-SEISCON-2013, SIGMA 2018, IEEE CENCON 2019 and IEEE ICIOT 2020. He has published widely in International Journals and Conferences his research findings related to Power Electronics, Variable Speed Drives and Renewable Energy Sources. Dr. Iqbal has authored/co-authored more than 420 research papers and four books and several chapters in edited books. He has supervised several large R&D projects worth more than multimillion USD. He has supervised and co-supervised several PhD students. His principal area of research interest is Smart Grid, Complex Energy Transition, Active Distribution Network, Electric Vehicles drivetrain, Sustainable Development and Energy Security, Distributed Energy Generation and multiphase motor drive system.

ARUNSEKAR RAJASEKARAN received his Bachelor's degree from Sri Ramakrishna Engineering College in 2008 and his Master's degree in VLSI Design in 2013 and his Doctorate of philosophy in Low Power VLSI design from Anna University, Chennai in 2019. He is currently working as an Assistant professor in the Department of Electronics and Communication Engineering at GMR Institute of Technology, Rajam, AndhraPradesh. He has nearly 12 years of teaching experiences. He had published more than 24 papers in International conferences and 15 reputed Indexed Journals. His areas of interest are Low power VLSI design, Network security, Body area networks and Image processing. He is a member of ISTE, IETE, ISRD and IEANG.

GADILLI SAI NIKHIL pursuing his 3rd year in Bachelor's degree in Electronics and communication engineering from GMR Institute of Technology. His areas of interests are IOT, Digital Electronics and Block chain Technology. And he is a member of IETE, ISTE.

MARIA AZEES received the B.E. degree in electronics and communication engineering and the M.E. degree in applied electronics from the St. Xavier's Catholic College of Engineering, Nagercoil, India, which is affiliated under Anna University, Chennai, India, in 2011 and 2013, respectively, and the Ph.D. degree in the faculty of information and communication engineering from Anna University, Chennai, in 2017. He is currently working as Senior Assistant Professor with the GMR Institute of Technology, Rajam, India. He has already published the research articles in some of the reputed journals, such as the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3081506, IEEE Access

IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, Cluster Computing (springer), and IET intelligent transport systems. His research interests include security in wireless sensor networks and VANETs.