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

Blockchain-based Energy Trading and Load Balancing using Contract Theory and Reputation in a Smart Community

ADAMU SANI YAHAYA[1], NADEEM JAVAID[1,*], MUHAMMAD UMAR JAVED[1], MUHAMMAD SHAFIQ[2,*], WAZIR ZADA KHAN[3], MOHAMMED Y AALSALEM[3]

[1]Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan
[2]Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, South Korea
[3]Farasan Networking Research Laboratory, Department of Computer Science & Information System, Jazan University, Jazan 82822-6694, Saudi Arabia

Corresponding authors: nadeemjavaidqau@gmail.com, shafiq@ynu.ac.kr

ABSTRACT The rapid deployment of Electric Vehicles (EVs) and the integration of renewable energy sources have ameliorated the existing power systems and contributed to the development of greener smart communities. However, load balancing problems, security threats, privacy leakage issues, etc., remain unresolved. Many blockchain-based approaches have been used in literature to solve the aforementioned challenges. However, they are not sufficient to obtain satisfactory results because of the inefficient energy management methods and time-intensiveness of the primitive cryptographic executions on the network devices. In this paper, an efficient and secure blockchain-based Energy Trading (ET) model is proposed. It leverages the contract theory, incentive mechanism, and a reputation system for information asymmetry scenario. In order to motivate the ET entities to trade energy locally and EVs to participate in smart energy management, the proposed incentive provisioning mechanism plays a vital role. Besides, a reputation system improves the reliability and efficiency of the system and discourages the blockchain nodes from acting maliciously. A novel consensus algorithm, i.e., Proof of Work based on Reputation (PoWR), is proposed to reduce transaction confirmation latency and block creation time. Moreover, a shortest route algorithm, i.e., the Dijkstra algorithm, is implemented in order to reduce the traveling distance and energy consumption of the EVs during ET. The performance of the proposed model is evaluated using peak to average ratio, social welfare, utility of local aggregator, etc., as performance metrics. Moreover, privacy and security analyses of the system are also presented.

INDEX TERMS Blockchain, Contract theory, Demand response, Energy, ET, EVs, Information asymmetry, Optimization, Reputations.

NOMENCLATURE

DR	Demand Reponse
DRM	Demand Reponse Management
DSM	Demand Side Management
ET	Energy Trading
EV	Electric Vehicle
ICT	Information and Communication Technology
LEA	Local Energy Aggregator
MWT	Model Without Trust
PoW	Proof of Work
PoWR	Proof of Work Reputation
PAR	Peak to Average Ratio
SDCR	Secure Discharging/Charging Ratio
SEM	Smart Energy Management
SDA	Shortest Distance Algorithm
SET	Smart Energy Trading
SoC	State of Charge
V2G	Vehicle to Grid
E_s^c	Current Energy Available within Suppliers
E_v^c	Current Energy Available within Demanders

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.2020.3041931, IEEE Access

C_s	Contract for Suppliers
C_v	Contract for Demanders
β_b	Dataset that has the Timestamp
DT	Direct Trust Value
$\phi(.)$	Exponential Decay Function
γ	Unit Cost of Energy Transfer
γ_L	Cost of Energy for LEA
D_{EV}	Energy Services by Honest LEA
D_{Total}	The Total Energy at t
θ_s	Entity Type for Energy Suppliers
θ_v	Entity Type for Energy Demanders
$Hash(.)$	Hash Function
$f(.)$	Puzzle Level
$m()$	Monotonic Function
α_b	Nonce Value
P_s	Probability Distribution of Suppliers
P_v	Probability Distribution of Demanders
Re_j	Reputation Values
Ra	Rating Values
V_i	Set of Validators
N	Set of Followers
J	Set of Candidates
$SW(.)$	Social Welfare Function
L_s	The Amount of Energy Supplied
L_v	The Amount of Energy Demanded
$E_j^{Savedtrl}$	The Energy Saved
D^{max}	Maximum Traveled Distance
$D_{y \longmapsto n}$	Distance Traveled from EVs to LEA
E_j^{rate}	The Rate of Energy Consumption
γ_d	The Difficulty Level
$E_{s,max}$	The Maximum Capacity of Battery Storage for Suppliers
$E_{v,max}$	The Maximum Capacity of Battery Storage for Demanders
R_s	The Reward for Energy Supplied
R_v	The Reward for Energy Demanded
τ_1 and τ_2	Threshold Values
$TEload(t)$	Total Energy Load with Respect to Time t
$U_L(.)$	Utility Function for Aggregator
$U^{EN}(.)$	Utility Function for Energy Entity

I. INTRODUCTION

A smart community integrates Information and Communication Technology (ICT) in an advanced way to elevate the living quality of its residents [1]. The rapid growth in the modern ICT has contributed to the increased accessibility of many services to customers within a specific time, for example, public administration, e-government, smart education, smart transport and Smart Energy Management (SEM) [2], [3]. Thus, making institutional, residential, business, etc., environments smart. SEM is one of the constituents of a smart community that efficiently monitors, controls and regulates the energy without affecting the comfort of energy users. An example of SEM is Smart Energy Trading (SET), which comprises of energy providers and consumers. The formers include utility companies and local energy prosumers while latter are found in all domains, i.e., commercial, residential, transportation and industrial [4]. Recently, the dramatic rise in the penetration of Electric Vehicles (EVs) in the transportation domain has increased the pressure on the power grids. It is because EVs are charged using electric power and the power grids have to fulfill their electricity demand [5], [6]. Besides, EVs play a very important role in balancing energy demand and supply as they can act as both energy carriers as well as energy consumers according to certain situations.

The energy provider and consumer entities establish an energy network where energy resources need to be managed efficiently to retain energy sustainability in the smart community. Therefore, it is a priority of power systems to manage energy generators efficiently. However, as the energy generation becomes scarce, efficient trading of energy becomes challenging in the smart community. It poses issues for SET [7], [8], such as the increased penetration of highly intermittent distributed renewable energy sources in the power systems, poorly coordinated EVs, load balancing problems, etc. The balance in energy demand and supply in a conventional system requires thousands of energy storage devices and centralized generators, which result in a huge investment in operational and capital expenditure [9]. Therefore, an alternative method is required to overcome the tremendous increase in demand for electricity that arises in the community [10]. Moreover,an Demand Response (DR) system is an option to manage energy at the demand side. It is the change in energy usage made by consumers from their regular electricity consumption patterns in response to the modifications in energy prices over a period of time [11].

The introduction of DR system with internet-connected EVs provides efficient methods to manage the huge electricity demand of EVs without increasing the number of energy storage devices and generators [12]. The benefits of integrating a DR system with EVs are structured into two perspectives, which are energy perspective and communication perspective [12], [13]. From the energy perspective, a number of EVs are used as backup energy sources when energy is critically needed. From the communication perspective, the internet of EVs facilitates the continuous collection of information from EVs for several purposes like to get information about driving behaviors, vehicle's conditions, energy states, route trajectories and road environment. This data collection is of great importance for traffic control in the smart communities [9].

Different SEM systems for DR Management (DRM) are deployed in the energy network of the smart city with the help of communication technologies. Therefore, these systems are vulnerable to different forms of attacks in which a malicious user may take advantage of the network security loopholes [14]. For instance, an attacker may maliciously alter the data to delay service provisioning in the network. In order to ensure security and privacy of Energy Trading (ET)

participants, a robust and safe energy management system is required. This system must ensure the user's privacy and network security in case of an adversary's attack. On the other hand, a single point of failure is another issue that is caused when a centralized ET model is used.

A new technology called blockchain has emerged as an effective solution to solve the security challenges and eliminate the dependency on the central system. This technology provides a way of storing transactions in a decentralized platform. It resolves the security challenges in a distributed and decentralized fashion. It also facilitates in many aspects, such as authentication, integrity and confidentiality of data. In the blockchain, network's nodes manage the executed transactions and keep their records in the form of blocks. Therefore, breaking the system's security is almost impossible as it requires compromising the miners that are responsible for managing the overall security of the system [6]. Miners are the blockchain users that secure, verify and add transaction into the blockchain ledgers. In a ledger, blocks are cryptographically secured and each block is connected with its previous block forming a chain. In this paper, miners and validators are used interchangeably. Despite the significant advantages of using blockchain to solve the security and a single point of failure issues in the ET system, the privacy leakage issue, high computational complexity, etc., remain unsolved. To efficiently resolve the aforementioned issues in ET systems, this study proposes a new model for SET and load balancing. The proposed model leverages contract theory, blockchain technology and reputation system to provide efficient ET and load balancing. Furthermore, in order to minimize the computational complexity and increase the system's reliability, a reputation based consensus mechanism is proposed. In the proposed model, the transactions are validated and audited publicly by the authorized nodes at a reduced cost.

The remaining part of the research paper is organized as follows. Section II and III discussed related work and problem statement, respectively. The description of the system model is given in Section IV. The proposed solutions are discussed in Section V, VI, and VII. The simulation results and discussion are presented in Section VIII. Finally, conclusion and future work are presented in Section IX.

II. RELATED WORK

A blockchain is a shared and distributed ledger, which has many benefits. It allows each executed transaction to be verified and stored permanently. It plays an important role in establishing a secure, transparent and distributed ET platform. It has undergone rapid changes from version 1.0 to 3.0 with applications in the fields of finance, education, health, energy, etc. [15]. The authors in [16] implement a reliable credit-based payment system by minimizing the waiting period of transaction confirmation delays. The authors carry out the implementation in a permissioned blockchain based on the industrial internet of things. This tends to make ET quicker and more frequent. Moreover, the authors apply an optimal pricing strategy to maximize the bank's utility of credit-based loans considering the idea of the Stackelberg game. However, trust evaluation for each node in the system and effective privacy mechanisms are not considered.

In [17], the authors present a distributed ET scheme to motivate peer to peer sharing of energy among prosumers. The proposed scheme has two layers. A coalition of prosumers is formed in the first layer to negotiate ET. In the second layer, blockchain technology is used as a medium to perform the monetary transactions. The work in [18] presents a distributed model to manage the DR mechanism. The model integrates blockchain technology with a power grid. This approach ensures the programmatic definition of the expected energy flexibility levels. It maintains the balance of energy demand and generation and also validates the agreements of DR through a smart contract. However, an effective and efficient approach to reach consensus is not considered. Furthermore, the privacy of transactions are also not resolved.

The work proposed in [19] smooths the lower level fluctuation of demand profile and also reduces the Peak to Average Ratio (PAR) of the energy consumption. The energy mismatch is caused as a result of supply constraints. Moreover, the work improves the blockchain model for a distributed microgrid platform. It also manages the payment system together with the sharing of energy information. In this model, the authors propose a non-cooperative theoretical game method for a Demand Side Management (DSM) scheme, which integrates storage battery system. In [20], authors introduce a blockchain framework, known as EnergyChain, to ensure secure ET between smart homes and smart grid. The proposed framework involves selection of miners, validation, block creation and transaction management. However, blockchain is not widely used in devices with less computational capabilities because higher computational cost is involved when creating blocks.

In [21], the authors propose a three-party smart grid framework incorporated with EVs. It involves flexible and complex interactions between EVs, energy grids and communities. The framework introduces two fascinating models based on the proposed three-party framework, which are EV-centered and smart community-centered. The framework also consist of a schedule-on-demand power management model. It incorporates both EVs and smart communities to achieve efficient and effective resource management in the energy generation network. The authors in [22] propose a new decentralized electronic currency, which is also known as the NRGcoin scheme. The proposed scheme allows the domestically produced energy to be purchased using the new digital currency. The currency obeys the renewable ET protocol in the power networks.

Gao *et al.* [23] propose a smart contract to execute the ET procedures amongst the participants, which provides trust within them. The authors in [24] implement a decentralized and secured ET model using an energy token that allows ET transactions to take place among participants. In this

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.2020.3041931, IEEE Access

model, anonymous energy price negotiation is applied using blockchain. In [25], the authors propose a zonal scheduling and hierarchical concept along with an iterative two-layer model. The model efficiently manages the discharging and charging energy of EVs. This model, therefore, minimizes the entire energy load variance of the distributed network under limited vehicle travel demand and power flows. Moreover, in the proposed model, a decentralized ET architecture is designed based on consortium blockchain technology. This architecture ensures the privacy and security of the bi-directional ET between the smart grid and EVs. The results of the system show that the proposed model can ensure privacy-preservation and security of both ET and the underlying system, in general. Authors in [6] present a secure blockchain-based DRM model, named GUARDIAN, to make secure ET decisions. It aims to efficiently manage the entire load profiles in the industrial, commercial and residential domains. In the proposed system, energy transaction validators are selected based on their processing capabilities and power consumption. The obtained results show the effectiveness of the system for securing DRM in the smart grid. Similarly, the authors in [26] present a secure ET framework based on blockchain and edge computing in Vehicle to Grid (V2G) ecosystem. The idea of approver nodes to secure trading of energy is used in this model. These nodes are selected based on a utility function and also serve to validate all the executed transactions. However, minimizing the confirmation latency of the transactions and block creation duration are not considered in the framework. The authors in [9] present a secure consortium blockchain-based ET model for EVs at a cheaper cost. The proposed model uses a contract theory based incentive method to encourage EVs to participate in DRM. The performance and security of the proposed model are validated and analyzed, respectively.

From literature review, it is observed that the proposed systems do not consider how to minimize the confirmation latency of both transactions and block creation. Also, none of the above works [6], [9], [26] consider minimizing routes and distance from the mobile entity to the Local Energy Aggregator (LEAG)'s location. In existing literature, it is observed that there are similar approaches [27], [28] to our proposed model. For clarification, we present their objectives and limitations. The authors in [27] implement an efficient and secure V2G ET model by exploring an edge computing system, contract theory and blockchain technology. In this model, consortium blockchain is used for securing ET between LEA and energy entities. The results of the proposed model are analyzed and validated using theoretical and numerical analyses. However, using edge computing can cause longer power or data outage time, potential data loss and expose the privacy of users. Furthermore, the cost of edge computing is very high, which also needs advanced infrastructure [29], [30]. The authors in [28] propose a secure and intelligent task offloading framework to address security and privacy challenges in vehicular fog computing. In this framework, smart contracts are used to facilitate fair task offloading and reduce security vulnerabilities. In addition, the authors design a subjective logic-based metric to construct a trustfulness assessment technique and quantify the possibility of task offloading success. However, edge computing devices expose users' privacy, have high operational expenditure and high deployment cost. Moreover, the development of a reputation system depends on a mathematical model to accumulate trust information and calculate reputation [31]. In literature [32], [33], reputation models are classified as probabilistic models [34], [35], flow-based models [36], summation and averaging models [37] and fuzzy matrices [38]. The study in [28] uses a subjective-based reputation that falls under probabilistic models, which is not suitable for our proposed scenario. In the proposed model, a summation and averaging model is used, which can be applied easily in a direct trust assessment to reduce computational complexity. As stated in [39], the choice of model type has an impact on the amount of trust information available and the procedure used to calculate the reputation values. In addition, routes' optimization from the mobile entity location to the stationary entity's location is not considered in [27] and [28].

III. PROBLEM STATEMENT

Several research domains use blockchain technology for authentication purposes [43]. Considering the potential benefits of blockchain, its applications in ET [20], [44], and DRM are increasing rapidly. It also enables the privacy provisioning of EVs in the transportation sector [45], [46]. Blockchain technology is one of the most effective technologies that serves as both security and crypto-currency solutions [41]. Its environment is reliable and cannot be compromised easily by a malicious entity [42].

In the literature, there exist few works that combine blockchain, ET and DRM considering the information asymmetry scenario in a smart grid, which leverage commercial, transportation, residential and industrial sectors. However, the studies in [6], [9], [27] and [28] do not consider how to efficiently minimize the confirmation latency of the transactions and the block creation time in a cost-effective manner. Moreover, the reduction in traveling costs and the distance from EV's current position to local aggregators are also not considered in these works. The penetration and deployment of EVs as energy carriers to manage energy demand encounter some problems in the smart community, such as privacy leakage, denial of service attacks, a single point of failure, etc. These challenges arise due to the lack of well-designed DR incentive mechanisms for the energy carriers and a secure ET process. To overcome the aforementioned problems, an efficient and secure DR system along with the ET model using consortium blockchain is proposed in this paper. Table 1 shows the comparison between the previous research works and the proposed work. The innovations and contributions of our proposed model are presented as follows.

- Based on consortium blockchain, an optimal and secure model for energy delivery in an immutable and verifiable manner is proposed.

TABLE 1. Comparison with Existing Work.

Features	[6]	[9]	[27]	[28]	[48]	[49]	[51]	Proposed Model
Consortium Blockchain	No	Yes	Yes	Yes	No	No	No	Yes
Weighted based Reputation System	No	No	No	No	Yes	No	No	Yes
Shortest-route Analysis	No	No	No	No	No	No	No	Yes
Trust Evaluation Mechanism	No	No	No	Yes	Yes	Yes	No	Yes
Contracts Theory	No	Yes	Yes	No	No	No	No	Yes
Privacy	No	Yes	Yes	Yes	No	No	No	Yes
Security	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

- A Proof of Work based on Reputation (PoWR) consensus mechanism for ET is proposed to efficiently meet consensus requirement and reduce the time complexity of a blockchain based system.
- A contract-based incentive mechanism is introduced, which helps to perform load balancing and ET using information asymmetry.
- We propose a route optimization algorithm, which reduces the traveling time and EVs' energy consumption cost. On top of that, the EVs arrive at their final destination with minimum monetary cost.
- To assess the effectiveness and efficiency of the proposed scheme, rigorous experimental simulations are performed.

IV. SECURE ENERGY TRADING USING CONSORTIUM BLOCKCHAIN

In this section, the overview of the proposed system model and its implementation are discussed.

A. PROPOSED SYSTEM MODEL

This subsection discusses a smart grid ecosystem scenario for DRM and ET, as shown in Fig. 1. The proposed system model is inspired by the studies done in [6] and [9]. It is an improvement of both works. For the improvement, a novel reputation based contract theory mechanism is implemented to preserve privacy and maintain trust of the users. Also, a shortest path algorithm is used to minimize EV's traveling distance, time and energy consumption to reach the charging location. There are four major energy domains in the proposed system model: the group of smart homes, industries, commercial buildings and EVs. Each domain has a local aggregator in the system. Moreover, EVs can either be mobile carriers that transport energy from one aggregator to another or consumers that manage energy demand load. The members of each domain directly communicate with their respective aggregator. It is assumed that each and every member's power line is connected to the aggregators. Similarly, each member has a smart meter that records energy information from the aggregator. In addition to the linkage with local members, the aggregators are connected to renewable energy sources to further balance the energy load, if necessary. With the power line connections between each aggregator and its members, a bidirectional energy transmission is achieved. The aggregators in the proposed system further provide services for ET and DRM. The services include continuous status monitoring, real-time data collection and coordination between energy demand and supply.

With the emergence of multi-directional trading in energy systems, ET with EVs became possible. In general, the entities involved in ET and DRM are all connected via consortium blockchain, where the transaction information is transmitted and verified. The ET between two entities, i.e., one that intends to purchase energy and the other, which tends to sell surplus energy, is explained below. In this scenario, the entities that want to buy energy send requests through their Local Energy Aggregators (LEAs) by selecting buying contract items. These requests are then sent to other LEAs for validation. After the validation test is passed, entities having surplus energy can trade their energy with those that have insufficient energy through their LEAs. Once the ET has taken place, the involved entities will receive dedicated payments for their contributions to the local demand-supply balance. This dedicated payment is in the form of energy coin, which is a kind of digital crypto-currency. Similar to the study done in [27], the aggregator in this model has three major components: an account server, a memory server and a transaction server. Digital wallet stores energy coins of each entity in the system. The privacy of participants is preserved by replacing the actual wallet addresses with the set of random pseudonyms (public keys). The transactional information that passes through the blockchain is permanently placed in the memory server. Moreover, all the transaction records of each participant are stored in the transaction account. Whereas, account server maintain the linking relationship between the transaction account and its corresponding random users' address. Furthermore, the transaction server is involved in designing the incentive mechanisms and coordinating energy supply-demand activities.

B. PRELIMINARY DISCUSSION

This subsection discusses the techniques and mechanisms used in this study for better understanding of the readers. The major techniques and mechanisms used in the proposed model are blockchain technology, contact theory and route optimization algorithm. The details are given below.

- Blockchain technology: To establish a secure, immutable and transparent ET system, blockchain technol-

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.2020.3041931, IEEE Access

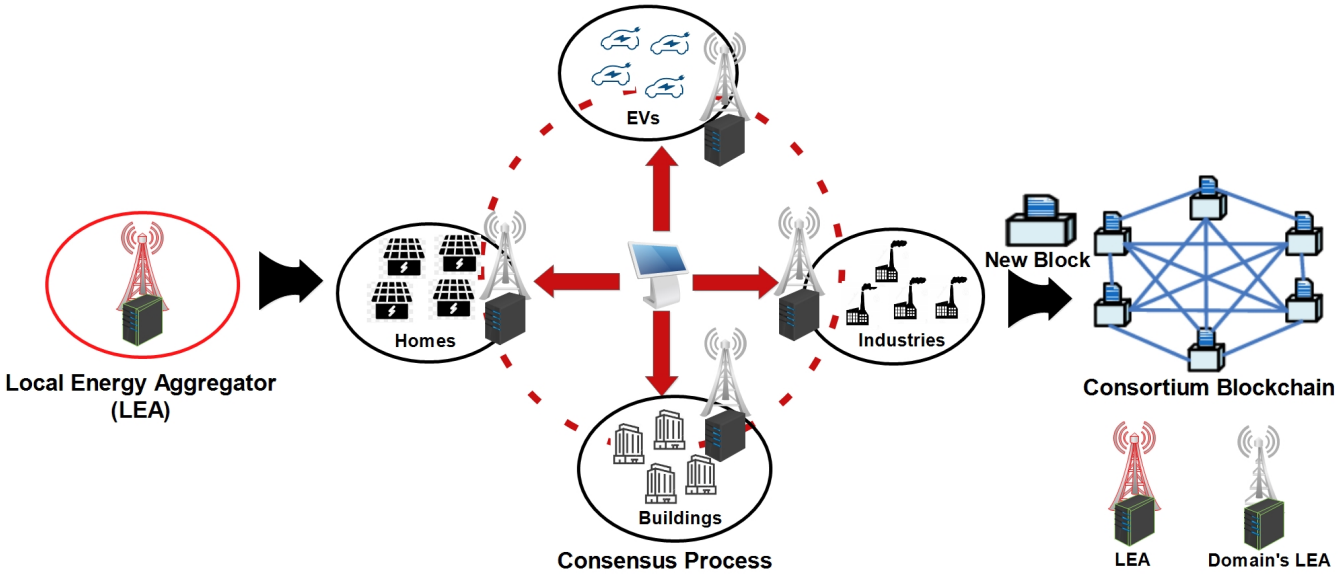


FIGURE 1. Proposed System Model: four different domains: smart homes, industries, commercial buildings and EVs, are shown in the figure. Each domain has an LEA, which sums up the total energy of the domain. The members in a domain communicate directly with their respective LEA, which is connected with both consumers and the renewable energy sources. The aggregated amount of energy is then aggregated by the main LEA (given in red color). After ET, transactions are added in the form of blocks that constitute the consortium blockchain.

ogy is introduced. The consortium blockchain based ET ensures distributed sharing of energy between entities. It also promotes security and privacy of the users.

- Contract theory: To provide an effective mechanism to address the incentive challenges using private asymmetric information of EV users, contract theory is introduced. Asymmetric information is a kind of information, where only the entity itself has full knowledge about it. The contract theory based incentive method encourages EVs to participate in DRM.
- Route optimization: EVs need energy to charge themselves and this energy comes mostly from the LEAs. Due to the rapid increase in the number of EVs and the scarcity of LEAs, route optimization has become a necessity. Different algorithms are used for this purpose (Dijkstra's algorithm is used in our case). Route optimization means finding the shortest distance to the nearest LEA and reducing both traveling time and cost.

C. IMPLEMENTATION

The proposed system operations of DRM and ET are similar to [9] and [27], which are discussed as follows. In the initialization of the system, existing cryptographic algorithms: SHA-256, Boneh-Boyen short signature and elliptic curve digital signature are used. Each entity from its domain has to register with an authorized node to get its private key, public key and a certificate. The certificate denotes a unique identity for each entity bound with its registered information. Entities of all domains have wallet addresses, which are obtained from the authorized nodes. At each transaction stage, every entity obtains the wallet address that is used by its LEA, which verifies the integrity of the wallet and retrieves data from the memory server.

All LEAs design a contract that specifies the relationship between the amount of energy provided or required by an entity and its corresponding payment (reward). The LEAs first broadcast contracts locally and each entity from that domain selects an appropriate contract item to maximize its profit. After the contracts are selected by the local entities, each LEA checks its available energy. If the contracts selected for buying energy are more than selling, then that particular domain is in energy deficit state. On the other hand, when the selling contracts of a domain are more than buying contracts, the domain has surplus energy. Otherwise, there is no demand-supply mismatch. In any case, the LEA broadcasts its status to other LEAs to trade energy in order to balance the demand load in the community. In a local demand or supply setting, when ET is performed successfully, every entity will either receives or transfers payment for the traded energy. The energy coins are forwarded to the wallet address of the LEA by an entity or vice versa depending on the transaction being performed. The payment authenticity can be validated from the last block in the blockchain.

The transaction information collected by the LEA in a given period is electronically signed, encrypted and then saved into blocks. Whereas, the energy transactions that are invalid are discarded, e.g., fake transactions. Validators build their local blocks concurrently, where every block is joined with the prior blocks using a cryptographic hash in the consortium blockchain. Every validator tries to find a solution, which is the same as in bitcoin before a new block is created. In the proposed model, a PoWR consensus mechanism is used, i.e., a hash value, to solve the cryptographic puzzles that satisfy some difficulty levels. The hash value

is computed using the nonce value α_b and the data set β_b that has the timestamp of the prior created block, its hash value and other necessary information. The valid nonce α_b must satisfy $Hash(\alpha_b + \beta_b) < \gamma_d$. Where γ_d denotes the difficulty level. The LEA that first finds a valid PoWR's hash value broadcasts the new block over the network. Then other LEAs verify and audit the transaction information received from the new block. After that, the LEAs decide to accept or reject the newly created block. If more than half of the LEAs accept the newly created block, then the block is added to the blockchain. Otherwise, it is discarded. The LEA that creates the new block is given a reward using the energy coins.

V. INCENTIVE MECHANISM BASED ON CONTRACT THEORY FOR ENERGY ENTITIES

This section discusses entity type modeling and contract formulation for information asymmetry and non-asymmetry. Similar works are also presented in the literature, for example, the authors in [9], [27] and [40] employ contract theory to design incentive mechanisms. However, trust evaluation among users is not considered. Whereas, our proposed method provides a reputation mechanism to enhance the trust of the users. Also, this paper considers the shortest path algorithm to minimize the traveling time and costs for energy buyers or sellers, which are not considered in [9], [27] and [40].

A. ENTITY TYPE MODELING

We utilize entity type to measure the independent choice of every entity to supply or request energy that is only known by the entity itself. The entity types are part of a set that belongs to finite and discrete space. An entity with a bigger type is much more willing to take part in DR and supplies or requests a huge amount of energy to get a higher reward. In this scenario, entities with bigger types are more relevant and preferable by the LEA. The entity type is formulated as given below.

Definition 1: A domain with S energy suppliers, and V energy demanders are considered in this model. These entities are grouped into S, and V types, and sorted in ascending order according to their preferences. Suppose the set of entity types is represented as $\Theta_s = \theta_1, \theta_2, ..., \theta_s, ..., \theta_S$, for energy suppliers, and $\Theta_v = \theta_1, \theta_2, ..., \theta_v, ..., \theta_V$, for energy demanders, then we have $\theta_1 < ... < \theta_s < ... < \theta_S$, where $s = 1, ..., S$, and $\theta_1 < ... < \theta_v < ... < \theta_V$, $v = 1, ..., V$. Also, $\Theta_s, \Theta_v \in \Theta$. To simplify the model, we assume that the number of supplied contract types, and the consumption contract types are the same, i.e., $S = V$.

The entity type is derived as follows. State of Charge (SoC) of an entity is the ratio of its available energy to maximum battery capacity [9]. SoC is used as the metric for calculating the condition of each energy entity's battery. SoC can be computed as given in Equation (1) and (2) by considering type θ_s entity for supplier and θ_v for demander [9].

$$SoC_s^c = \frac{E_s^c}{E_{s,max}}, \tag{1}$$

$$SoC_v^c = \frac{E_v^c}{E_{v,max}}. \tag{2}$$

Where E_s^c and E_v^c denote the currently available energy in entities s and v, respectively. The capacities of battery storage of entities s and v are represented as $E_{s,max}$ and $E_{v,max}$, respectively. Therefore, each entity can contribute not more than its available energy at time of trading, i.e., $\theta_v \leq E_v^c$ and $\theta_s \leq E_s^c$. Hence, the combined entity type, i.e., type $C\{\theta_s, \theta_v\}$ can be defined as given in Equation (3) [9].

$$C\{\theta_s, \theta_v\} = \begin{cases} SoC_s^c \times E_{s,max}, & if \ \ \theta_s \text{ is selected}, \\ SoC_v^c \times E_{v,max}, & Otherwise. \end{cases} \tag{3}$$

Where $C\{\theta_s, \theta_v\}$ means entity type for s or v. In the scenario of information asymmetry, LEA does not have knowledge about the exact type of Θ, however, it only knows the probability distribution of each Θ. In this model, it is assumed that LEAs have the idea of the total number of S for energy supply and V for energy demand. Also, the specific probability of each entity that belongs to types θ_s and θ_v are P_s and P_v, respectively. Where Θ is a set of θ_s and θ_v. The sum of the probability for all energy suppliers are $P_s = 1$ and demanders are $P_v = 1$.

B. CONTRACTS FORMULATION

In this model, we design a contract that consists of s contract items for s types of energy supplying entities and v contract items for v types of energy demanding entities. One contract item for each type is presented in this model to avoid providing the same contract item for entities with different types. The contract items' designs are given as follows: a contract for suppliers that contains S contract items and similarly, a contract for demanders that contains V contract items for S and V types are designed. For instance, the contract item designed for θ_s supply entity is represented as (L_s, R_s) and for demanding entity is denoted as (L_v, R_v). Where L_s and L_v denote the amount of energy supplied and energy demanded, respectively. R_s and R_v represent the reward in terms of digital coins for S and V, respectively. $C_s = \{(L_s, R_s), \forall s \in S\}$ is defined as a contract of energy supplying entity while $C_v = \{(L_v, R_v), \forall v \in V\}$ is defined as contract of energy demanding entity. Considering the S and V types of entities for supplying and demanding, the expected utility of the LEA based on energy supply is the total energy cost spent for all energy suppliers minus all the rewards [9], which is computed using Equation (4).

$$U_L(L_s, R_s) = S \sum_{s=1}^{S} P_s(\gamma_L L_s - R_s). \tag{4}$$

Similarly, the expected utility of the LEA energy demand is the total energy cost spent for all energy consuming entities minus all the rewards, which is computed using Equation (5).

$$U_L(L_v, R_v) = V \sum_{v=1}^{V} P_v(\gamma_L L_v - R_v). \tag{5}$$

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.2020.3041931, IEEE Access

Where γ_L is the cost of energy for each LEA. The utility function of types θ_s or θ_v that accepts the contract items (L_s, R_s) or (L_v, R_v) is the reward offered minus the cost of energy supplied or energy consumed [9], as given in Equation (6).

$$U_{s,v}^{EN}(L_{s,v}, R_{s,v}) = \begin{cases} \theta_s m(R_s) - \gamma L_s, & if \text{ energy is supplied,} \\ \theta_v m(R_v) - \gamma L_v, & \text{otherwise.} \end{cases} \tag{6}$$

Where γ is the unit cost of transferring energy to or from the energy storage. $\theta_s m(R_s)$ and $\theta_v m(R_v)$ represent the values of R_s and R_v for type θ_s and θ_v entities, respectively. The functions $m(R_s)$ and $m(R_v)$ are monotonically increasing with R_s and R_v, respectively. $m(R_{s,v})$ is defined as a quadratic function as given in Equation (7).

$$m(R_{s,v}) = \begin{cases} -\frac{x}{2}R_s^2 + yR_s, & if \text{ energy is supplied,} \\ -\frac{x}{2}R_v^2 + yR_v, & \text{otherwise.} \end{cases} \tag{7}$$

Where Equation (7) must satisfy $m(0) = 0$, $m^{'}(0) > 0$, and $m^{''}(0) < 0$. The symbols $m^{'}()$, and $m^{''}()$ represent first, and second derivative of $m()$. Here, x, and y are assumed to be constants. The total sum of the utility of all domains for energy supplied, and consumed is the social welfare that is given in Equations (8)-(10), which is a modified version of [9]. The social welfare for θ_s is given as the sum of Equation (4) and Equation (6).

$$SW_s(L_s, R_s) = U_L(L_s, R_s) + S\sum_{s=1}^{S} P_s U_s^{EN}(L_s, R_s), \tag{8}$$

the social welfare for θ_v is given as the sum of Equation (5) and Equation (6).

$$SW_v(L_v, R_v) = U_L(L_v, R_v) + V\sum_{v=1}^{V} P_v U_v^{EN}(L_v, R_v), \tag{9}$$

the aggregated social welfare is the sum of Equation (8) and Equation (9), which is given as

$$SW_s = SW_s(L_s, R_s) + SW_v(L_v, R_v). \tag{10}$$

To simplify the formulation process, we use the social welfare of supplying energy entities, i.e., $SW_s(R_s, L_s)$ only as the process is the same with the demanding energy entities $SW_v(R_v, L_v)$. The maximization problem for LEA social welfare under asymmetric information is shown in Equation (11) [9].

$$\max_{L_s, R_s} SW(L_s, R_s),$$

s.t.

$$C_1 : \theta_s m(R_s) - \gamma L_s \geq 0,$$

$$C_2 : \theta_s m(R_s) - \gamma L_s \geq \theta_s m(R_{s'}) - \gamma L_{s'},$$

$$C_3 : 0 < R_1 < ... < R_s < ... < R_S,$$

$$C_4 : L_s \leq \theta_s, \ \forall \ s, s^{'} \in S. \tag{11}$$

Where C_1, C_2 and C_3 denote individual rationality constraint, incentive compatibility constraint and monotonicity constraint, respectively. C_4 denotes the upper bound of the total energy supplied L_s. Equation (8) is the social welfare for supplying energy entities and Equation (9) is the social welfare for demanding energy entities. The aggregated social welfare for both supplying and demanding energy entities is shown in Equation (10). Individual rationality simply means that all contract types will get a nonnegative payoff. The incentive compatibility constraint ensures the self-revealing property of the contract. An energy entity gets maximum payoff, provided that it chooses the right contract item that belongs to its own type. Whereas, the monotonicity constraint means that the reward given to a contract with the higher type must be more than those with the lower type. According to the constraints given above, the following properties are derived.

Lemma 1: For each $s^{'} \in S$ and $v^{'} \in V$, if $\theta_s > \theta_{s'}$ and $\theta_v > \theta_{v'}$, then $R_s > R_{s'}$ and $R_v > R_{v'}$. $R_s = R_{s}^{'}$ and $R_v = R_{v}^{'}$ if and only if $\theta_s = \theta_{s'}$ and $\theta_v = \theta_{v'}$.

Lemma 2:

$$0 \leq R_1 \leq ... < R_s \leq ... \leq R_S,$$

$$0 \leq R_1 \leq ... \leq R_v \leq ... \leq R_V,$$

$$0 \leq L_1 \leq ... \leq L_s \leq ... \leq L_S,$$

$$0 \leq L_1 \leq ... \leq L_v \leq ... \leq L_V,$$

$$0 \leq U_1^{EN} \leq ... \leq U_s^{EN} \leq ... \leq U_S^{EN},$$

$$0 \leq U_1^{EN} \leq ... \leq U_v^{EN} \leq ... \leq U_V^{EN}. \tag{12}$$

The details of the similar proof can be obtained from [9].

C. INFORMATION ASYMMETRY DESIGN FOR OPTIMAL CONTRACT

The details on the information asymmetry design for optimal contract are given as follows.

1) Contract Feasibility

The necessary and sufficient conditions are first defined for the contract's feasibility. These are provided as $C_s = (R_s, L_s)$, $\forall S$ and $C_v = (R_v, L_v)$, $\forall V$. For simplification, we use energy supplying entities as examples to show the proofs. The proofs provided in this paper are similar to [47], which are obtained in the device to device wireless communication.

Proposition 1 (Necessary condition A): for any $s, s^{'} \in S$, $L_s > L_{s'}$ if and only if $R_s > R_{s'}$.

Corollary 1: for any $s, s^{'} \in S$, $L_s = L_{s'}$ if $R_s = R_{s'}$.

Proposition 2 (Necessary condition B): for any $s, s^{'} \in S$, $\theta_s > \theta_{s'}$ if and only if $R_s \geq R_{s'}$.

Combining *Proposition 1* with *Proposition 2*, we know that a higher contract type should contribute more energy.

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.2020.3041931, IEEE Access

The *proposition 2* shows the supplementary necessary condition for the contract feasibility. It shows that a higher contract type should be given more rewards. From *propositions 1 and 2*, it is concluded that for a feasible contract, all energy-reward combinations must satisfy Equation (13).

$$0 \leq L_1 \leq L_2 \leq ... \leq L_s, 0 \leq R_1 \leq R_2 ... \leq R_s. \quad (13)$$

With $L_s = L_{s+1}$ if and only if $R_s = R_{s+1}$. The above-mentioned propositions help in proving *Theorem 1*.

Theorem 1: The contracts for suppliers C_s and consumers C_v are feasible if the conditions stated below are satisfied. The conditions below is modified from [9].

- $0 \leq R_1 \leq ... < R_s \leq ... \leq R_S$; $0 \leq R_1 \leq ... < R_v \leq ... \leq R_V$, and $0 \leq L_1 \leq ... \leq L_s \leq ... \leq L_S$; $0 \leq L_1 \leq ... \leq L_v \leq ... \leq L_V$,
- $\theta_1 m(R_1) - \gamma L_1 \geq 0$,
- for any $s \in \{2, ..., S\}$ and $s \in \{2, ..., V\}$, $\theta_{s-1}[m(R_s) - m(R_{s-1})] + \gamma L_{s-1} \leq \gamma L_s \leq \theta_s[m(R_s) - m(R_{s-1})] + \gamma L_{s-1}$ and $\theta_{v-1}[m(R_v) - m(R_{v-1})] + \gamma L_{v-1} \leq \gamma L_v \leq \theta_v[m(R_v) - m(R_{v-1})] + \gamma L_{v-1}$.

The proofs of *Proposition 1* and *Proposition 2* are given in Appendix section.

2) Problem Transformation

To simplify the social welfare maximization problem that involves S individual rationality constraints and $S(S-1)$ incentive compatibility constraints, the following procedures are carried out:

Step 1: Individual Rationality Constraint Elimination.

Given type θ_s and θ_v for supplier and consumers entities, respectively, $s \in S$ and $v \in V$, where $s \neq 1$ and $v \neq 1$, we can derive

$$\theta_s m(R_s) - \gamma L_s \geq \theta_s m(R_1) - \gamma L_1 > \theta_1 m(R_1) - \gamma L_1, \quad (14)$$

$$\theta_v m(R_v) - \gamma L_v \geq \theta_v m(R_1) - \gamma L_1 > \theta_1 m(R_1) - \gamma L_1. \quad (15)$$

The individual rationality constraints of an entity with the higher contract types are automatically satisfied if and only if individual constraints of contract type θ_1 are true, i.e., $\theta_s > \theta_1$ and $\theta_v > \theta_1$.

Step 2: Incentive Compatibility Constraints Elimination. Incentive compatibility constraint is defined within contract types θ_s and $\theta_{s'}$ for suppliers entity and contract types θ_v and $\theta_{v'}$ for consumers entity, where $s' \in \{1, ..., s\}$ and $v' \in \{1, ..., v\}$, as downward incentive constraints. Similarly, an incentive compatibility between the contract types θ_s and $\theta_{s'}, s' \in \{s+1, ..., S\}$ for energy suppliers entity and also between contract types θ_v and type $\theta_{v'}, v' \in \{v+1, ..., V\}$ for energy consumers entity, are defined as upward incentive constraints. The downward and upward incentive constraints are reduced as follows. Note, to simplify the process, we consider the energy supply entity type reduction only.

Three adjacent entity contract types are considered, i.e., $\theta_{s-1} < \theta_s < \theta_{s+1}$ that satisfy Equations (16) and (17).

$$\theta_{s+1} m(R_{s+1}) - \gamma L_{s+1} \geq \theta_{s+1} m(R_s) - \gamma L_s, \quad (16)$$

$$\theta_s m(R_s) - \gamma L_s \geq \theta_s m(R_{s-1}) - \gamma L_{s-1}. \quad (17)$$

Where Equation (16) represents the downward incentive constraints between contract types θ_{s+1} and θ_s. While Equation (17) represents the downward incentive constraints between contract types θ_s and θ_{s-1}.

Considering $R_{s+1} \geq R_s \geq R_{s-1}$, we get Equation (18).

$$\theta_{s+1} m(R_{s+1}) - \gamma L_{s+1} \geq \theta_{s+1} m(R_{s-1}) - \gamma L_{s-1}. \quad (18)$$

Hence, the downward incentive constraints within θ_{s+1} and θ_{s-1} will hold, if downward incentive between contract type θ_{s+1} and θ_s holds. Moreover, the downward constraints incentive can be extended to the minimum contract type θ_1. In a similar way, it can be shown that if upward incentive constraints hold within the adjacent contract types, then automatically the other upward constraints will hold.

According to the analysis provided above, the S individual rationality constraints and $S(S-1)$ incentive compatibility constraints are reduced to 1 and $S-1$, respectively. Equation (11) can be rewritten as Equation (19).

$$\max_{\{L_s, R_s\}} SW(L_s, R_s),$$

s.t.

$$\begin{aligned} C_1 &: \theta_1 m(R_1) - \gamma L_1 \geq 0, \\ C_2 &: \theta_s m(R_{s-1}) - \gamma L_{s-1} \geq \theta_s m(R_s) - \gamma L_s, \\ C_3 &: 0 < R_1 < ... < R_s < ... < R_S, \\ C_4 &: L_s \leq \theta_s, \ \forall s = 2, ..., S. \end{aligned} \quad (19)$$

D. NON-INFORMATION ASYMMETRY DESIGN FOR OPTIMAL CONTRACT

If a selfish LEA knows the exact information about each entity's energy consumption or production, then it can increase the its profits as long as an energy entity accepts the contract item designed for its specific type. In the non-information asymmetry scenario, the LEA must guarantee the payment of each energy entity to be positive. Otherwise, the energy entity will have no benefit when the contract item is accepted. Conclusively, the contract item must satisfy the individual rationality constraints. Moreover, the contract item must meet the property given below.

Proposition 3: Any contract item $(L_s, R_s) \in C_s$ must meet $\theta_s m(R_s) = \gamma L_s$. This implies that the payment for the profit of each energy entity is zero.

Proof: We prove $Proposition\ 3$ by contradiction. Assuming an optimal contract item (L_s, R_s), if $\theta_s m(R_s) - \gamma L_s > 0$, then the LEA can further increase its utility by rising the amount of L_s up to $\theta_s m(R_s) - \gamma L_s = 0$. Therefore, this increment contradicts the assumption that the contract item (L_s, R_s) is sufficient.

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.2020.3041931, IEEE Access

So, by making the utility of every energy entity to be zero, the social welfare is now equal to the LEA's utility. The problem of optimization is generated, as shown in Equation (20) [9].

$$\max_{L_s,R_s} SW(L_s,R_s),$$

s.t.

$$C_1 : \theta_s m(R_s) - \gamma L_s = 0,$$
$$C_2 : 0 \leq R_1 < ... < R_s < ... < R_S,$$
$$C_4 : L_s \leq \theta_s, \ \ \forall s \in S. \tag{20}$$

To solve Equation (20), we need to find the solution of $\theta_s m(R_s) - \gamma L_s = 0$. Suppose that R_{s1} and R_{s2} are the two roots of the sth quadratic equation. Therefore, the optimal solution is shown in Equation (21).
$(L_s, R_s) =$

$$\arg\max_{R_s \in R_{s1}, R_{s2}} (SW(L_{s1}, R_{s1}), SW(L_{s2}, R_{s2})). \tag{21}$$

Proposition 4: For any energy supplying entity contract type θ_s, where $s \in S$; R_s is fixed regardless of θ_s. Similar proof can be found in [9].

VI. BLOCK CREATION AND VALIDATION

Because of the high cost of computation associated with the existing Proof of Work (PoW) based solution, an alternative solution is needed to solve the problem. In this research, a consortium blockchain is used to secure energy transactions with less computational efforts. In order to reduce gas consumption required for reaching consensus, minimize transaction confirmation latency in traditional PoW, we propose a new consensus mechanism, called as PoWR mechanism. Here, a direct trust rating is used, which is different from [48]. Furthermore, the proposed protocol combines consortium blockchain and reputation mechanism, which has the following steps.

A. VALIDATORS' GROUP FORMULATION AND BROADCASTING TRANSACTIONS

In the proposed model, we have four types of nodes: followers, candidates, proposers and validators. EVs and other energy entities serve as followers that can solely accept, relay and transfer ledger data. The LEAs in the proposed system act as candidates with the potentials of becoming validators. A validator is an approved node that participates in the process of consensus to agree on the creation of the next block based on its value of reputation. Candidates that have the highest reputation rankings in PoWR imply a higher degree of trust, and are assumed to perform their services excellently. A proposer is selected from the pool of validators, which is responsible for forwarding blocks' requests to the blockchain platform. The set of validators, followers and candidates are represented as Vi, N and J respectively.

In this blockchain, each legitimate node manages a copy of the reputation ratings of all candidates. The reputation rating of each candidate is computed at any given time. In the PoWR consensus mechanism, candidates that satisfy $Re_j \geq \tau_1$ establish a group of validators Vi, where $0 \leq \tau_1 \leq 1$ is the reputation requirement predefined in the network and Re_j is the reputation value. If a node is malicious, i.e., $Re_j \leq \tau_2$, then node j will be included into the pool of blacklisted nodes. This means that it will no longer be part of consensus nodes, where $0 \leq \tau_2 \leq \tau_1$ is a reputation threshold. For broadcasting transactions, we follow the same procedures as in [48].

B. BUILDING BLOCKS

In this work, the validator collects transactions independently and verifies them during the consensus period. All valid transactions are recorded in the blockchain memory pool, while the invalid transactions are discarded. Validators create their local blocks simultaneously and each block has a cryptographic hash connected to the prior block in the blockchain. To find the solution of a mathematical puzzle, the validator creates a new block, as given in Equations (22) and (24) [48]:

$$Hash(nonce||Hash(blockheader)) \leq \gamma_d, \tag{22}$$

$$\gamma_d = f(Re_{vi}) \times target, \tag{23}$$

$$f(Re_{vi}) = \begin{cases} w \log(1 + \frac{Re_{vi}}{\sum_{vi \in Vi} Re_{vi}}) + 1, if \ vi \in Vi, \\ 1, \qquad\qquad\qquad \text{otherwise.} \end{cases} \tag{24}$$

Where $w > 0$ is the adjustment factor coefficient, which makes it easier for the validators with higher reputation to find the nonce solution. From the above equations, the function for cryptographic hash value is $Hash(.)$. The $blockheader$ is the header of a block and the difficulty metric given by the system is $target$. The metric that determines the puzzle difficulty level is $f(.)$. The difficulty level of a mathematical puzzle is reduced for every validator as its reputation increases. Therefore, higher $f(.)$ means lower difficulty level. The function $f(Re_{vi})$ increases monotonically based on the value of a reputation Re_{vi}, as shown in Equation (24). Solving the puzzle becomes easier when the validator's reputation increases. Proposer is a validator that first finds the solution of the mathematical puzzles as given in Equation (22). Afterwards, the proposal message $ProMsg = (P||B||Sig_{SK_p}(H(B))||R_p||T_{stamp})$ is broadcasted to the entire network. B is the newly created block by the proposer P. All the validators check the correctness of the proposer result using Equation (22). They also verify the transactions in the collected block B. If all validators successfully verify the transaction, the consensus is reached. The new block B is added to the blockchain's local copy for each node. Every follower synchronizes the meta data of the validators' most recent blockchain.

C. EVALUATION OF REPUTATION

Energy entities share information with one another via the blockchain network to compute the degree of aggregator's

trust. The degree of trust value is used to select a reliable aggregator for energy transactions. In general, the method of selecting or trusting a user is divided into two types, i.e., indirect and direct trust [49]. The indirect trust degree also called the recommendation value is an estimation of services according to other entities' interactions or experiences. The entities can get more information about an aggregator, especially when they have less direct interactions. On the other hand, in direct trust, the energy entities get an aggregator trust from direct historical experiences and interactions. The reputation rating in energy system means that a legitimate node with a higher reputation rating gets higher chances to participate in the consensus mechanism and it also gets more rewards. Therefore, all LEA nodes in the energy network are encouraged to enhance their services for energy entities to improve their reputation ratings. After every service, the service provider is given a score by an energy entity.

In our scenario, we adopt the direct rating, i.e., energy entities providing rating to authorized nodes. The rating provided by an energy entity n to authorized node j is represented as $Ra^k_{j,n} \in [0,1]$ in kth interaction. Where $Ra^k_{j,n} = 1$ means that there is full service satisfaction and $Ra^k_{j,n} = 0$ means that service received is not satisfied. The local trust is generated from historical interaction between n and j. This local trust is directly related to the amount of energy traded, the rating of operation and the occurring time of each interaction [48]. In this research, an iterative method is used to reduce the computational complexity that finds the local trust degree. Let $N_{j,n} = \{1, , \aleph_{j,n}\}$ be the set of interactions between n and j from the initial time t to the time $t+1$. The direct trust degree of LEA n from j is the cumulative sum of all historical ratings that can be attained as given in Equation (25) [49].

$$DT_{j,n} = \frac{\sum_{k\in K} Ra^k_{j,n} \times \phi(\varpi_k)}{\sum_{k\in K} \phi(\varpi_k)}. \tag{25}$$

Where $\sum_{k\in K} \phi(\varpi_k)$ is the normalization factor and $\phi(\varpi_k)$ denotes the exponential time decay, which is defined using Equation (26).

$$\phi(\varpi_k) = e^{-\varrho(\varpi - \varpi_k)}. \tag{26}$$

Where ϱ, ϖ_k and ϖ denote the decay rate, the kth historical service time and the current service time, respectively. Therefore, the reputation score of the nth LEA node at time ϖ is computed using the $DT_{j,n}$ of the energy entity users that receive services from the nth LEA node n, as shown in Equation (27).

$$Re_{vi} = \begin{cases} DT_{j,n}, & if N_{j,n} \neq 0, \\ 0.5, & Otherwise. \end{cases} \tag{27}$$

We assume that every new user has an initial reputation score of 0.5.

VII. THE ENERGY MANAGEMENT

In this section, EVs Mobility and DRM managements are discussed.

Algorithm 1 Shortest Distance Algorithm

Input G, S, D

▷ Where G is Graph, S is Source and D is Destination

Output dis^*, S^*

▷ Where dis^* is optimal distance, S^* is optimal path

```
function FindShortestDist(G, S, D)
    for <each vertex V in G> do
        dis[V]=infinity, prev[V]= undefined
    dis[O]=0
    Q= the set of all nodes in G
                                ▷ Unoptimized nodes in G
    while Q is not empty do
        U= vertex in Q with smallest dis[]
        if dis[U] = infinity then
            break
        if U= D then
            break
        remove U from Q
        for <each neighbor V of U> do
            alt = dis[U] + costBetween(U, V)
            if alt < dis[V] then
                dis[V]= alt, prev[V]= U
                                ▷ Read the shortest path
    S= empty sequence, U=D
    while prev[U] is defined do
        insert U at the begining of S
        U= prev[U]
     return dis*, S*
```

A. THE MANAGEMENT OF ELECTRIC VEHICLES MOBILITY

In this research, we consider EVs as carriers of energy and trading partners that transport energy from one energy domain to another. Before the ET takes place between EVs and LEAs, their distances need to be considered as one of the primary factors for EV's participation. If the distance that an EV will travel is more than the distance that can be covered with current battery capacity, then the EV cannot go to LEA for ET [51]. Furthermore, if the EV has multiple routes to reach the LEA, then the EV selects the best route to maximize its profit. The distance between LEA and EV is represented as $D_{y \longmapsto n}$, where y is the current position of the EV and n is the LEA's position. $D_{y \longmapsto n}$ depends on the route that the EV has to follow from y to n. In this scenario, we use Dijkstra's shortest path algorithm [50] as our proposed Shortest Distance Algorithm (SDA). The algorithm for SDA to select the shortest path between the energy entity and the LEA is given in Algorithm 1.

B. SECURE AND PRIVACY-PRESERVED DEMAND RESPONSE MANAGEMENT

In this section, we discuss how ET is performed to transmit energy from one domain to another. It is assumed that all financial and information transactions are conducted via the blockchain. Using the blockchain makes the transactions secure. Moreover, the proposed contract theory based on reputation is used to preserve the privacy of the users. For ET,

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.2020.3041931, IEEE Access

an EV travels to the nearest buyer/seller that can be the LEA of smart homes, commercial buildings, or industries. After reaching the destination, the EV then connects with LEA to buy or sell energy. ET between energy domains and EVs (mobile entities) occurs when the energy transaction is validated, as explained in the previous sections (Secition IV). An EV travels from one location to another based on its energy requirement and the contract available (contract selected by EVs). So, in such a situation, two cases come up. In the first case, EVs act as energy consumers. Whereas, in the second case, EVs serve as suppliers of energy. These two situations, along with load balancing are discussed as follows.

1) EV as Energy Buyer

EVs serve as energy buyers when LEA (let say n) has surplus energy to sell. Similar to the local energy entity, EVs select contract items that fit their types θ_s for buying energy. The limit of energy that can be bought by an EV depends on its energy storage capacity, SoC level and the distance traveled. The energy that will be saved by an EV while traveling from source to destination is given in Equation (28).

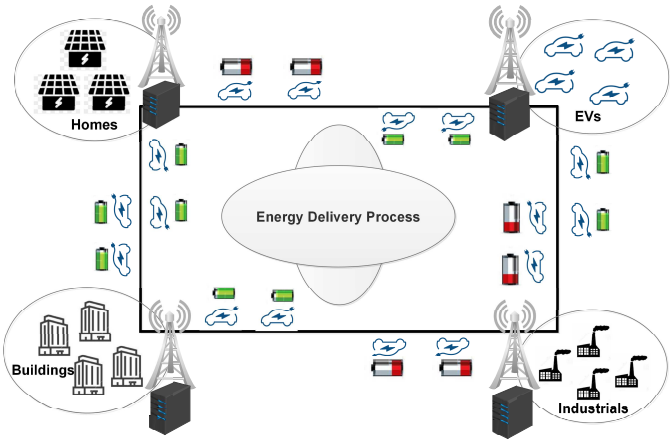


FIGURE 2. ET between Various Domains: four different energy domains, i.e., smart homes, commercial buildings, industrial sectors and EVs, are shown in the figure. Each consumer in the domain communicates with its respective LEA for fulfilling its energy requirements, i.e., selling or buying. ET is performed according to the selected contract items and after successful ET, energy coins are transferred to the respective wallets of the energy entities.

$$E_j^{Savedtrl} = (D^{max} - D_{y \longmapsto n}) \times E_j^{rate}. \tag{28}$$

Where D^{max} is the maximum traveling distance that can be covered by the EV when it is fully charged. E_j^{rate} is the rate energy consumption by the EV.

2) EV as Energy Seller

EVs serve as energy sellers when the LEA (let say n) has deficit energy. The EVs select contract items that fits their types θ_v for selling energy. The limit of energy to be sold by an EV depends on its energy storage capacity, SoC level and the distance covered. After the completion of ET, the energy coins are sent from one energy entity to another based on the current status of the energy entity. All the involved entities' wallet accounts are updated, as explained previously. A scenario of this ET is depicted in Fig. 2. In the figure, different energy domains belonging to smart homes, commercial buildings and industrial sectors willingly trade energy with EVs to manage their local energy demands. It is observed from the figure that EVs travel to different LEAs of a certain domain to either buy or sell energy according to the contract items selected and the requirements of the LEAs. Furthermore, the energy coins are then transferred to the respective wallets of the energy entities involved in the ET after energy is traded.

3) Load Balancing

Power grid stability is an important parameter that increases its reliability and sustainability. PAR is an essential factor and has a direct link with the grid's stability [52], [53]. The reliability of the utility increases when PAR decreases. Equation (29) is used to calculate PAR [53]. In the equation, $TEload(t)$ is the total energy load with respect to time interval t.

$$PAR = 24 \times \frac{\max\left(TEload(t)\right)}{\sum_{t=1}^{24} TEload(t)}. \tag{29}$$

VIII. RESULTS AND DISCUSSION

This section validates the proposed system through simulations. The analytical experiments are carried out on a desktop computer with the following specifications. The experimental environment configuration is AMD E1-6015 APU with a 1.4 GHz radeon (TM) R2 graphics processor, 4.00 GB RAM and Microsoft Windows 10 is the operating system. For performing the simulations, MATLAB2018a is used.

A. CONTRACT FEASIBILITY AND SOCIAL WELFARE ANALYSIS

In this research, 20 energy entities with one LEA are assumed for performing simulations. Each entity type follows the Gaussian distribution. For each energy entity, the capacity of energy storage is 24 kWh and the energy selling cost (γ) is 10 cents/kWh. The energy revenue for LEA (γ_L) is 13 cents/kWh. The numerical parameters used to show the simulation results for contract theory are obtained from [9]. For the purpose of comparison, we compare the proposed contract model without information asymmetry model.

The amount of energy sold and its corresponding reward are shown in Fig. 3 and Fig. 4, respectively. It is shown that both energy supply and the corresponding reward increase monotonically with the energy entity type. These increments in the energy supply and the respective rewards satisfy $Lemma$ 2. The numerical results further show that the proposed contract requires less amount of energy from energy entities and also gives reward according to the selected contract item. On the contrary to the contract with no information asymmetry, which requires more energy and gives the same reward to energy entities that supplied energy to the LEA. The utility of the energy entities is shown

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.2020.3041931, IEEE Access

in Fig. 5, while the utility of LEAs is shown in Fig. 6. The LEAs under no information asymmetry achieve higher utility than information asymmetry. The utility of each energy entity under no information asymmetry remains zero, while it is increased in the case of information asymmetry, which depends on the contract's item selected by the entity. Furthermore, the existence of the information asymmetry in the proposed model protects the energy entity from being exploited since the exact selected entity type is not known to the LEA. The relationship between the energy entity type and the social welfare is shown in Fig. 7. The results show that the contract with information asymmetry performs better than its counterpart. This is because under a no information asymmetry, the utility of any energy entity is precisely zero, which decreases the social welfare significantly.

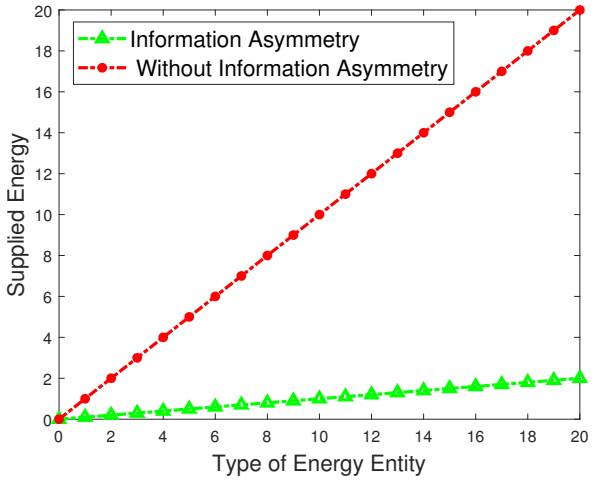


FIGURE 3. Contract Feasibility: Supplied Energy Vs Type of Energy Entity.

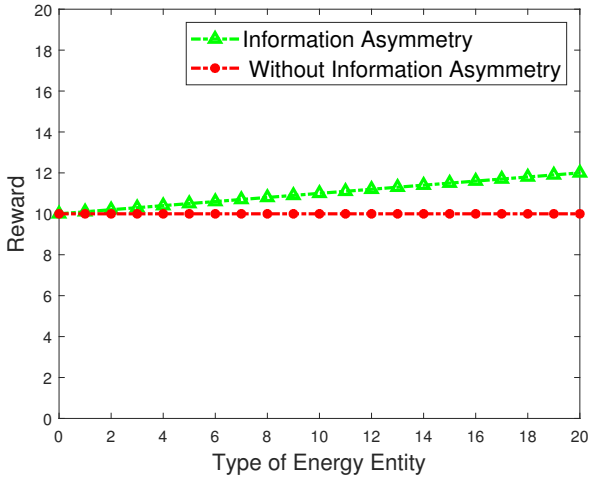


FIGURE 4. Contract Feasibility: Reward Vs Type of Energy Entity.

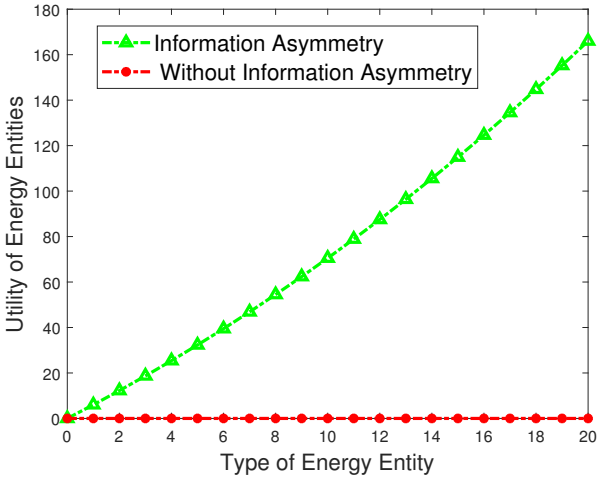


FIGURE 5. System Performance: Utility of Entities Vs Type of Energy Entity.

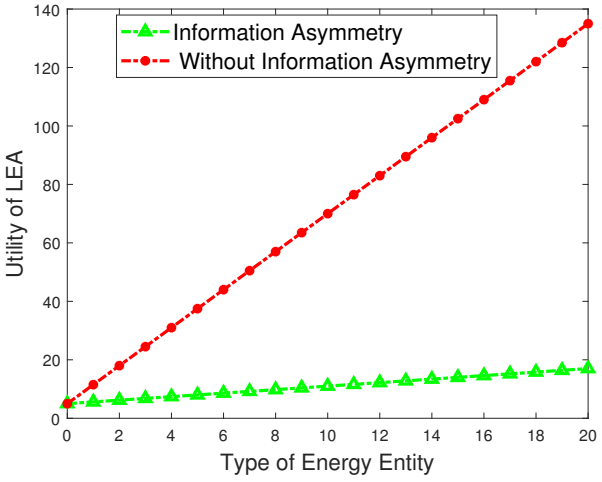


FIGURE 6. System Performance: Utility of LEA Vs Type of Energy Entity.

B. PERFORMANCE ANALYSIS ON TRUST MODEL AND REPUTATION

The performance of the trust model is evaluated using Secure Discharging/Charging Ratio (SDCR). It is the ratio of energy supply-demand that is provided by the honest LEA to the total energy supply-demand of all the EVs. In this research, the local energy supplied is not considered to determine the trust of an LEA. SDCR is defined as given in Equation (30) [49].

$$SDCR = \frac{D_{EV}}{D_{Total}}. \tag{30}$$

Where the sum of energy services by the honest LEA for EVs is D_{EV} and the total energy supply-demand of all EVs at a given time interval is D_{Total} . Our proposed model is compared with the Model Without Trust evaluation (MWT), in which each EV randomly selects an LEA to get energy services. Fig. 8 shows a comparison between MWT and 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.2020.3041931, IEEE Access

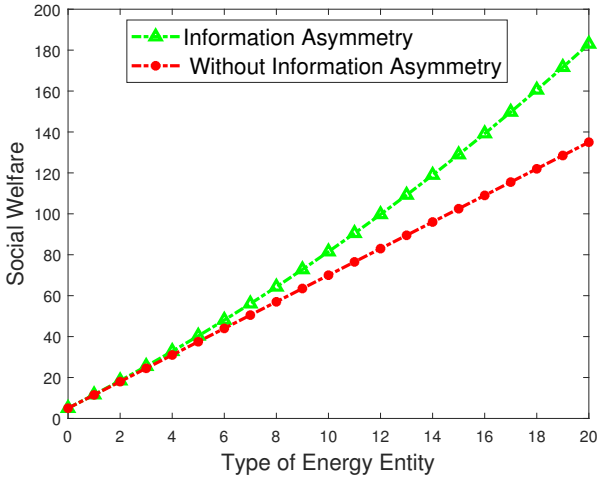


FIGURE 7. System Performance: Social Welfare Vs Type of Energy Entity.

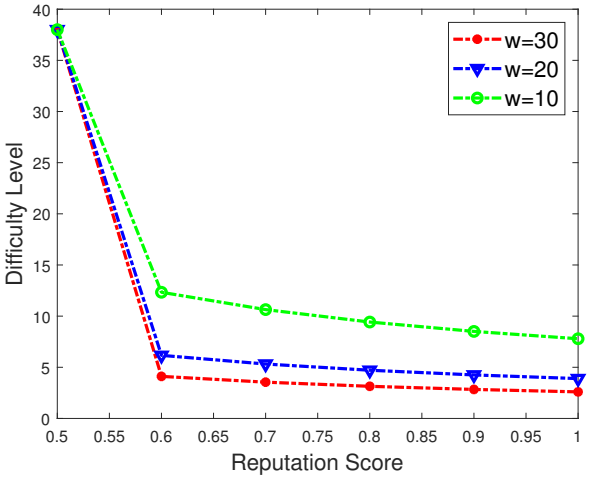


FIGURE 9. Difficulty Vs Reputation at Consensus Mechanism.

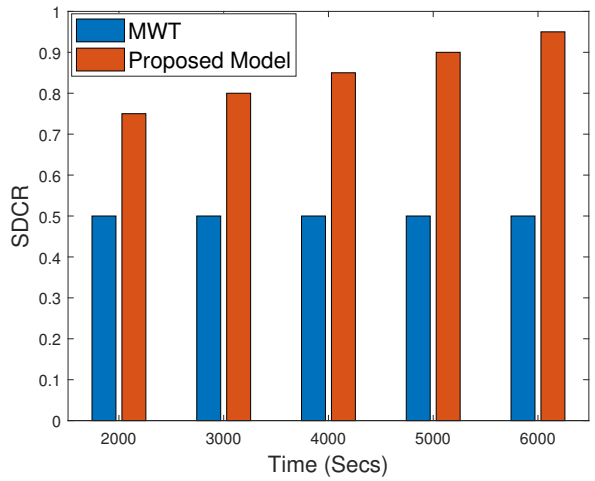


FIGURE 8. SDCR Vs Time of Simulation; the Ratio of Honest LEA is 0.5.

proposed model based on SDCR with variations in time from 2000 to 6000 secs. The result from the figure shows that the proposed model gives a higher SDCR than the MWT model when the time of simulation varies. In the MWT model, EVs randomly select the LEA for charging services, which causes the SDCR to become constant after multiple simulations. With the absence of trust evaluation, the services provided to the EVs by LEA can be malicious. On the other hand, in the proposed model, trust scores of the honest LEA increase with time while that of malicious LEA keeps decreasing. In the proposed model, every EV gets secure energy services from the LEA that has the highest trust score.

Fig. 9 shows the effect of reputation scores on the proposed consensus mechanism. The results show that an increase in reputation scores of the authorized node decreases the difficulty level of that node during the consensus process. Therefore, the delay in the consensus protocol is reduced, which also improves the efficiency of the system.

C. IMPACT OF LOCATION ON ELECTRIC VEHICLE'S ROUTING AND COST ANALYSIS

The impact of location on the EV's routing is investigated in this subsection. Fig. 10 shows multiple routes for an EV to reach LEA's location. In the figure, the routes between energy buyers and sellers are randomly generated within 100 km by 100 km square area. The red line in the figure shows the optimized paths from the buyer to seller. An EV's route is optimized using the proposed SDA, where the optimal route and distance are obtained. It is observed from Fig. 11 that when the distance between the EV's current location and the LEA decreases, the amount of energy saving increases, which further increases the profit of the EV user.

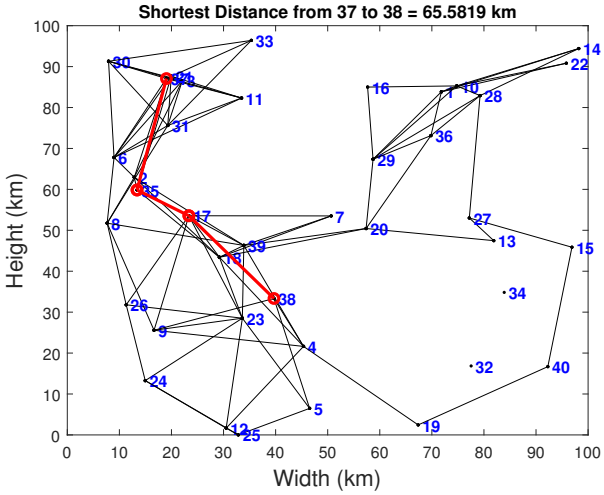


FIGURE 10. Shortest Routes and Distance Between EV and LEA.

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.2020.3041931, IEEE Access

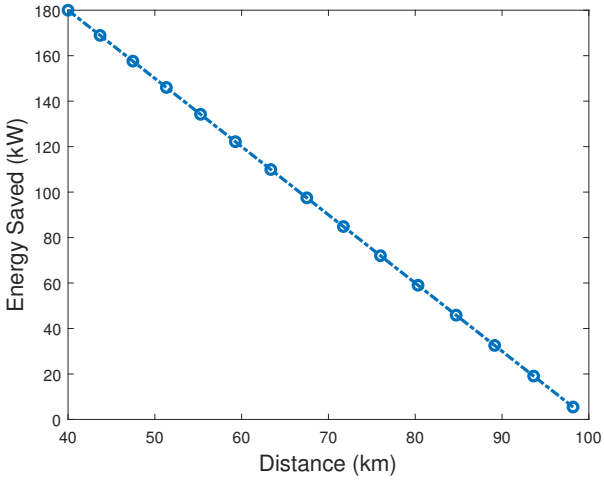


FIGURE 11. Effects of Optimal Route Analysis on EVs

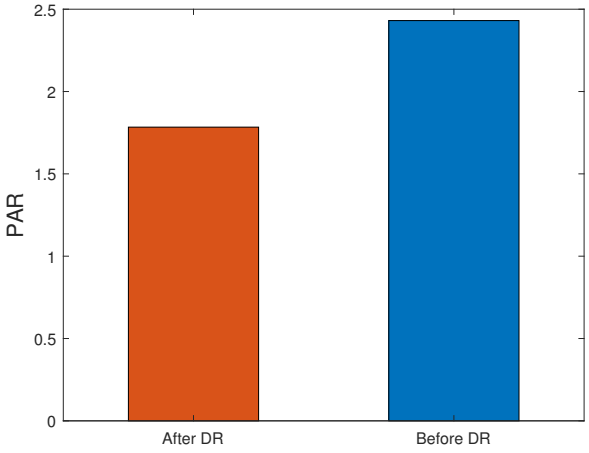


FIGURE 13. Comparison of PAR with DR and without DR scenario.

D. DEMAND RESPONSE MANAGEMENT NUMERICAL RESULTS

The proposed model having with 15 commercial buildings, 25 smart homes, 5 industrials buildings and 50 EVs is evaluated for ET. The load data of the commercial buildings, smart homes and industrial buildings are obtained from the US open energy information [54]. The EVs' load data is randomly generated between 12-36 kWh for simulations. Furthermore, the parameters used for the evaluation of DR are slightly similar to that of [6].

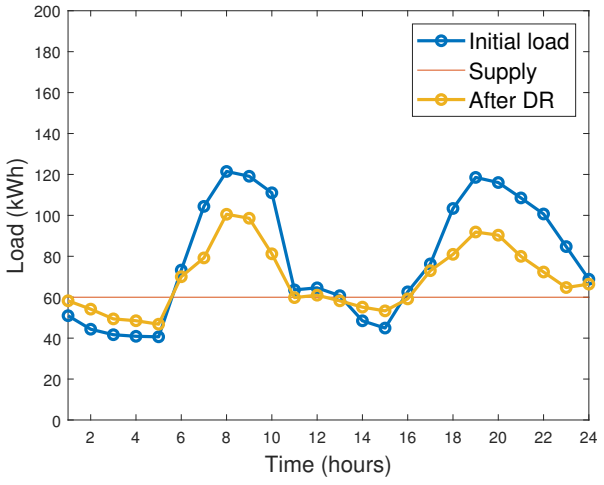


FIGURE 12. Effect of DR Management on Smart Homes Domain.

Fig. 12 shows the energy supply, initial load pattern of a smart home and its load pattern after applying DR. It is shown in the figure that the load demand in a community is greatly managed by the EVs in all the time slots. This also mitigates their reliance on the main power grid. Taking the smart homes domain as an example, Fig. 12 depicts the load consumption behavior of smart homes with a fixed energy of 60 kWh. The smart homes domain gives a room for EVs to select the buying contract item from 0000-0500 hours, when it has surplus energy after managing its own local demand. It also allows EVs to choose the selling contract item from 0500-1100 and 1700-2400 hours. When LEA wants to sell the energy to EVs, it serves as energy seller and vice versa. Fig. 13 shows the results of PAR, which is calculated using Equation (29). The result shows that the value of the PAR for the proposed model is lowered from 2.4309 to 1.7838 after DR is applied. It is a clear indication that the proposed model is beneficial for stability of the overall power system as the peak load reduces.

E. PRIVACY AND SECURITY ANALYSIS

The privacy and security analysis is discussed in this subsection.

1) *Authentication and Anonymity:* In the PoWR consensus mechanism, each energy transaction is authenticated and audited publicly by the authorized nodes. In this process, it is almost impossible for the adversary nodes to take control of more than 51% of the authorized nodes in the consortium blockchain network. The energy entities in this scenario use public keys to communicate with one another that prevents malicious users to trace the identity of an entity. Moreover, energy entity changes its used key after every transaction to avoid linking attacks.
2) *Transparency and Integrity:* Since the blockchain technology is an open source, everyone can access it. It also allows participants to track transaction. Moreover, this transaction is stored across all the nodes, which means that it is transparent to them. Therefore, any modification of data by a malicious user is traceable and noticeable.
   When a block is added to the blockchain ledger, it store the hash value of the previous block, which is passed

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.2020.3041931, IEEE Access

to the next block. With this structure, it is impossible to change the block unless more than 51% of the nodes are compromised. Furthermore, the data in the block is encrypted using asymmetric encryption technique, which take longer time and huge cost for the attacker to convert the encrypted data to its original form without the private key that generates the encryption.

IX. CONCLUSION

In this study, a blockchain based secure DRM model for ET and load balancing in a smart grid ecosystem is proposed. ET between energy entities and LEA is performed in a secure manner using consortium blockchain. Moreover, a contract theory based incentive mechanism is also introduced in this work to encourage energy users' participation. The proposed system also ensures privacy preservation of network nodes during ET. Furthermore, a reputation system is proposed in which the honest nodes are given positive reputation and malicious nodes are given negative reputation. It decreases the malicious activities during the consensus process as well as the block creation time. Furthermore, in the proposed model, the imbalance between EVs' energy demand and supply is tackled using efficient ET mechanism. Dijkstra's shortest path algorithm is further used to select the shortest route from an EV's current location to the LEA's location to minimize both traveling time and cost.

A. RESEARCH OUTCOME

Simulations are performed and results are obtained, which show that our proposed system achieves satisfactory results. The results of contract feasibility show that the contract with information asymmetry performs better as compared to the without contract information asymmetry. The former acquires less energy from energy entities as compared to latter and gives more rewards. Moreover, energy entities achieve a higher degree of social welfare and utility when information asymmetry is used as compared to without information asymmetry. Besides, it is observed that reputation score of an authorized node and its difficulty level of mining are inversely proportional, which implies that increase in reputation score decreases the difficulty level. PAR for the proposed model is also reduced from 2.4309 to 1.7838. It is a clear indication that the proposed model is advantageous to the overall power system. Moreover, the simulation results of the proposed system show its efficacy in terms of trust model, security, contract feasibility and energy saving costs.

B. FUTURE WORK

In future, we aim to investigate a more complicated scenario where knowledge about the probability distribution of the energy entity type is unknown. Machine learning techniques will be explored to get the corresponding knowledge. In addition, the storage and scalability issues blockchain will also be considered.

APPENDIX

Proof of Proposition 1: The proof is divided into two parts. In the first part, we show that if $L_s > L_{s'}$, then $R_s > R_{s'}$. While in the other part, we show that if $R_s > R_{s'}$, then $L_s > L_{s'}$.

In the first part, because of the incentive compatibility constraint in Equation (11), we have

$$\theta_s m(R_s) - \gamma L_s \geq \theta_s m(R_{s'}) - \gamma L_{s'},$$

i.e.,

$$\theta_s(m(R_s) - m(R_{s'}) \geq \gamma(L_s - L_{s'}),$$

since, $L_s > L_{s'}$, we say

$$\theta_s(m(R_s) - m(R_{s'})) \geq \gamma(L_s - L_{s'}) > 0,$$
$$\theta_s(m(R_s) - m(R_{s'})) > 0,$$
$$m(R_s) > m(R_{s'}).$$

In the second part, we prove that if $R_s > R_{s'}$, then $L_s > L_{s'}$, similarly to the incentive compatibility constraint, we have

$$\theta_{s'} m(R_{s'}) - \gamma L_{s'} \geq \theta_{s'} m(R_s) - \gamma L_{s'},$$
$$\gamma(L_s - L_{s'}) \geq \theta_{s'} m(R_s) - \theta_{s'} m(R_{s'}),$$
$$\gamma(L_s - L_{s'}) \geq \theta_{s'}(m(R_s) - m(R_{s'})),$$

Since, $m(R_s) > m(R_{s'})$, we say

$$\gamma(L_s - L_{s'}) > 0,$$
$$L_s > L_{s'}.$$

Proof of Proposition 2: To prove *proposition 2*, we use proof by contradiction. Suppose that there exists $m(R_s) < m(R_{s'})$ with $\theta_s > \theta_{s'}$, then we have

$$\theta_s m(R_{s'}) + \theta_{s'} m(R_s) > \theta_s m(R_s) + \theta_{s'} m(R_{s'}). \quad (31)$$

On the other extreme, the contract feasibility satisfies the incentive compatibility constraints for both the types θ_s and $\theta_{s'}$

$$\theta_s m(R_s) - \gamma L_s \geq \theta_s m(R_{s'}) - \gamma L_{s'},$$

and

$$\theta_{s'} m(R_{s'}) - \gamma L_s^{'} \geq \theta_s^{'} m(R_s) - \gamma L_s,$$

combining the above two inequalities, we get

$$\theta_s m(R_s) + \theta_{s'} m(R_{s'}) \geq \theta_s m(R_{s'}) + \theta_{s'} m(R_s),$$

where the result does not tally with Equation (31).

Proof of Theorem 1 (Sufficient and Necessary): to show the proof for *Theorem 1* and simplify the process, we consider only $C_s = \{(L_s, R_s), \forall s \in S\}$.

Proof for Sufficient Condition: Mathematical induction method is used to prove the theorem. Suppose $C_s(n)$ is denoted as the subset that contains the first n energy-reward combination in the contract C_s (i.e., $C_s(n) = \{(L_s, R_s), s = 1, 2, ..., n\}$). At the first step, we show that $C_s(1)$ is feasible. Because, it satisfies only one contract type; the contract is

feasible if it satisfies individual rationality constraint. This is true because of $\theta_1 m(R_1) - \gamma L_1 \geq 0$ in Theorem 1.

In the next step, we show that if contract $C_s(s)$ is feasible, we can develop a new contract $C_s(s+1)$ by adding new item (L_{s+1}, R_{s+1}). To attain this, the two results must be shown, i.e., R.1 and R.2.

R.1: The incentive compatibility and individual rationality constraints for type θ_{s+1} are

$$\begin{cases} \theta_{s+1} m(R_{s+1}) - \gamma L_{s+1} \geq \theta_{s+1} m(R_{s'}) - \gamma L_{s'}, \\ \forall s^{'} = 1, 2, ..., S, \\ \theta_{s+1} m(R_{s+1}) - \gamma L_{s+1} \geq 0, \end{cases} \tag{32}$$

R.2: For types $\theta_1, \theta_2, ..., \theta_{s-1}, \theta_s$ are contained in the contract $C_s(s)$, the incentive compatibility constraints are still satisfied after adding the new contract type θ_{s+1}.

$$\theta_{s'} m(R_{s'}) - \gamma L_{s'} \geq \theta_{s'} m(R_{s+1}) - \gamma L_{s+1}, \forall s^{'} = 1, 2, ..., S. \tag{33}$$

Note that the new contract $C_s(s+1)$ will satisfy the individual rationality constraints of all types from θ_1 to θ_s.

Proof of R1 in Equation (32): Initially, we prove the IC constraints for contract type θ_{s+1}. Since contract $C_s(s)$ is feasible, so, the incentive compatibility constraints for type $\theta_{s'}$ must hold, i.e.,

$$\theta_s m(R_s) - \gamma L_{s'} \leq \theta_s m(R_{s'}) - \gamma L_s, \forall s^{'} = 1, 2, ..., S.$$

Moreover, the right inequality of the third condition in *Theorem 1* is transformed to

$$\gamma L_{s+1} \leq \gamma L_s + \theta_{s+1}(m(R_{s+1}) - m(R_s)).$$

By combining the above two equations, we have

$$\theta_s m(R_{s'}) - \gamma L_{s'} + \gamma L_{s+1} \leq \theta_s m(R_s) + \theta_{s+1}(m(R_{s+1}) - m(R_s)), \forall s^{'} = 1, 2, ..., S. \tag{34}$$

We know that $\theta_{s+1} > \theta_s$ and $m(R_s) > m(R_{s'})$ from first condition in *theorem 1*, so, we have

$$\theta_{s+1} m(R_s) - \theta_{s+1} m(R_{s'}) \geq \theta_s m(R_s) - \theta_s m(R_{s'}).$$

Substituting this inequality into Equation (34), we have

$$\theta_{s+1} m(R_{s+1}) - \gamma L_{s+1} \geq \theta_{s+1} m(R_{s'}) - \gamma L_{s'}, \tag{35}$$

which is exactly the incentive compatibility constraint of type θ_{s+1}. The next step is to show the individual rationality constraints for the contract type θ_{s+1}. Since $\theta_{s+1} > \theta_{s'}$, for any $s^{'} \leq s$, then

$$\theta_{s+1} m(R_{s'}) - \gamma L_{s'} > \theta_{s'} m(R_{s'}) - \gamma L_{s'},$$

Considering equation (35), we get

$$\theta_{s+1} m(R_{s+1}) - \gamma L_{s+1} \geq \theta_{s+1} m(R_{s'}) - \gamma L_{s'}.$$

By combing the last two inequalities, we have

$$\theta_{s+1} m(R_{s+1}) - \gamma L_{s+1} \geq 0,$$

which shows that the individual rationality constraint is true.

Proof of R2 in Equation (33): Since contract $C_s(s)$ is feasible, so, the IC constraints for type $\theta_{s'}$ hold, i.e.,

$$\theta_{s'} m(R_s) - \gamma L_s \leq \theta_{s'} m(R_{s'}) - \gamma L_{s'}, \forall s^{'} = 1, 2, ..., S.$$

Also, we transform the left inequality of the third condition in *Theorem 1* to

$$\gamma L_s + \theta_s(m(R_{s+1}) - m(R_s)) \leq \gamma L_{s+1}.$$

By combing the above last two inequalities, we have

$$\theta_{s'} m(R_s) - \theta_s(m(R_{s+1}) - m(R_s)) \leq \theta_{s'} m(R_{s'}) - \gamma L_{s'} + \gamma L_{s+1}. \tag{36}$$

We know that $\theta_s \geq \theta_{s'}$, for any $s^{'} \leq s$ and $m(R_{s+1}) \geq m(R_s)$ in the first condition from *Theorem 2*. So, the result is

$$\theta_s m(R_{s+1}) - \theta_s m(R_s) \geq \theta_{s'} m(R_{s+1}) - \theta_{s'} m(R_s). \tag{37}$$

By combining inequalities (36) and (37), we generate

$$\theta_{s'} m(R_{s+1}) - \gamma L_{s+1} \leq \theta_{s'} - \gamma L_{s'}, \forall s^{'} = 1, 2, ..., S.$$

The result regenerated is exactly the same as IC constraints for contract type $\theta_{s'}$.

Proof for Necessary Conditions: It is easy to check that the sufficient conditions in *Theorem 1* are necessary for a feasible contract. In particular, the first condition in *Theorem 1* is the same as the conditions summarized in Equation (13). Whereas, the second condition is the same as the necessary individual rationality constraint for the lowest type θ_s, in a feasible contract. The left inequality of the third condition in *Theorem 1* is formulated from the incentive compatibility constraint for type θ_{s-1} in feasible contract. While the right inequality of the third condition in *Theorem 1* is formulated from the necessary incentive compatibility constraint for type θ_s.

REFERENCES

[1] Zhou, Suyang, Fenghua Zou, Zhi Wu, Wei Gu, Qiteng Hong and Campbell Booth. "A smart community energy management scheme considering user dominated demand side response and P2P trading." International Journal of Electrical Power & Energy Systems 114 (2020): 105378. DOI:10.1016/j.ijepes.2019.105378.

[2] Piro, Giuseppe, Ilaria Cianci, Luigi Alfredo Grieco, Gennaro Boggia and Pietro Camarda. "Information centric services in smart cities." Journal of Systems and Software 88 (2014): 169-188.

[3] He, Jianhua, Jian Wei, Kai Chen, Zuoyin Tang, Yi Zhou and Yan Zhang. "Multitier fog computing with large-scale IoT data analytics for smart cities." IEEE Internet of Things Journal 5, no. 2 (2017): 677-686.

[4] Maharjan, Sabita, Yan Zhang, Stein Gjessing and Danny HK Tsang. "User-centric demand response management in the smart grid with multiple providers." IEEE Transactions on Emerging Topics in Computing 5, no. 4 (2014): 494-505.

[5] Jindal, Anish, Neeraj Kumar and Mukesh Singh. "Internet of energy-based demand response management scheme for smart homes and PHEVs using SVM." Future Generation Computer Systems (2018): 677-687.

[6] Jindal, Anish, Gagangeet Singh Singh Aujla, Neeraj Kumar and Massimo Villari. "GUARDIAN: Blockchain-based Secure Demand Response Management in Smart Grid System." IEEE Transactions on Services Computing (2019): 1-13.

[7] Yahaya, Adamu Sani, Nadeem Javaid, Rabiya Khalid, Muhammad Imran and Mohsen Guizani. "A Blockchain-based Privacy-Preserving Mechanism with Aggregator as Common Communication Point." In ICC 2020-2020 IEEE International Conference on Communications (ICC), pp. 1-6. IEEE, 2020.

[8] Yahaya, Adamu Sani, Nadeem Javaid, Rabiya Khalid, Muhammad Imran and Nidal Naseer. "A Blockchain based Privacy-Preserving System for Electric Vehicles through Local Communication." In ICC 2020-2020 IEEE International Conference on Communications (ICC), pp. 1-6. IEEE, 2020.

[9] Zhou, Zhenyu, Bingchen Wang, Yufei Guo and Yan Zhang. "Blockchain and computational intelligence inspired incentive-compatible demand response in internet of electric vehicles." IEEE Transactions on Emerging Topics in Computational Intelligence 3, no. 3 (2019): 205-216.

[10] Wang, Kun, Huining Li, Sabita Maharjan, Yan Zhang and Song Guo. "Green energy scheduling for demand side management in the smart grid." IEEE Transactions on Green Communications and Networking 2, no. 2 (2018): 596-611.

[11] Albadi, Mohamed H. and Ehab F. El-Saadany. "Demand response in electricity markets: An overview." In 2007 IEEE power engineering society general meeting, (2007): 1-5.

[12] Zhou, Zhenyu, Changhao Sun, Ruifeng Shi, Zheng Chang, Sheng Zhou and Yang Li. "Robust energy scheduling in vehicle-to-grid networks." IEEE Network 31, no. 2 (2017): 30-37.

[13] Zhou, Zhenyu, Jie Gong, Yejun He and Yan Zhang. "Software defined machine-to-machine communication for smart energy management." IEEE Communications Magazine 55, no. 10 (2017): 52-60.

[14] Liang, Gaoqi, Steven R. Weller, Fengji Luo, Junhua Zhao and Zhao Yang Dong. "Distributed blockchain-based data protection framework for modern power systems against cyber attacks." IEEE Transactions on Smart Grid 10, no. 3 (2018): 3162-3173.

[15] Gatteschi, Valentina, Fabrizio Lamberti, Claudio Demartini, Chiara Pranteda and Victor Santamaria. "To blockchain or not to blockchain: That is the question." IT Professional 20, no. 2 (2018): 62-74.

[16] Li, Zhetao, Jiawen Kang, Rong Yu, Dongdong Ye, Qingyong Deng and Yan Zhang. "Consortium blockchain for secure energy trading in industrial internet of things." IEEE transactions on industrial informatics 14, no. 8 (2018): 3690-3700.

[17] Luo, Fengji, Zhao Yang Dong, Gaoqi Liang, Junichi Murata and Zhao Xu. "A Distributed Electricity Trading System in Active Distribution Networks Based on Multi-Agent Coalition and Blockchain." IEEE Transactions on Power Systems (2018): 4097-4108.

[18] Pop, Claudia, Tudor Cioara, Marcel Antal, Ionut Anghel, Ioan Salomie and Massimo Bertoncini. "Blockchain based decentralized management of demand response programs in smart energy grids." Sensors 18, no. 1 (2018). 162. DOI: 10.3390/s18010162.

[19] Noor, Sana, Wentao Yang, Miao Guo, Koen H. van Dam and Xiaonan Wang. "Energy Demand Side Management within micro-grid networks enhanced by blockchain." Applied energy 228 (2018): 1385-1398.

[20] Aggarwal, Shubhani, Rajat Chaudhary, Gagangeet Singh Aujla, Anish Jindal, Amit Dua and Neeraj Kumar. "Energychain: Enabling energy trading for smart homes using blockchains in smart grid ecosystem."+ In Proceedings of the 1st ACM MobiHoc Workshop on Networking and Cybersecurity for Smart Cities (2018):1-6. 2018.

[21] Zhang, Rongqing, Xiang Cheng and Liuqing Yang. "Energy management framework for electric vehicles in the smart grid: A three-party game." IEEE Communications Magazine 54, no. 12 (2016): 93-101.

[22] Mihaylov, Mihail, Sergio Jurado, Narcis Avellana, Kristof Van Moffaert, Ildefons Magrans de Abril and Ann NowÃl'. "NRGcoin: Virtual currency for trading of renewable energy in smart grids." In 11th International conference on the European energy market (EEM14),IEEE, (2014): 1-6.

[23] Gao, Jianbin, Kwame Omono Asamoah, Emmanuel Boateng Sifah, Abla Smahi, Qi Xia, Hu Xia, Xiaosong Zhang and Guishan Dong. "Gridmonitoring: Secured sovereign blockchain based monitoring on smart grid." IEEE Access 6 (2018): 9917-9925.

[24] Aitzhan, Nurzhan Zhumabekuly and Davor Svetinovic. "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams." IEEE Transactions on Dependable and Secure Computing 15, no. 5 (2016): 840-852.

[25] Li, Yuancheng and Baiji Hu. "An Iterative Two-Layer Optimization Charging and Discharging Trading Scheme for Electric Vehicle Using Consortium Blockchain." IEEE Transactions on Smart Grid vol. 11, no. 3 (2019): 2627-2637.

[26] Jindal, Anish, Gagangeet Singh Aujla and Neeraj Kumar. "SURVIVOR: A blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment." Computer Networks 153 (2019): 36-48.

[27] Zhou, Zhenyu, Bingchen Wang, Mianxiong Dong and Kaoru Ota. "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing." IEEE Transactions on Systems, Man and Cybernetics: Systems 50, no. 1 (2019): 43-57.

[28] Liao, Haijun, Yansong Mu, Zhenyu Zhou, Meng Sun, Zhao Wang and Chao Pan. "Blockchain and Learning-Based Secure and Intelligent Task Offloading for Vehicular Fog Computing." IEEE Transactions on Intelligent Transportation Systems (2020):1-13.

[29] Sonmez, Cagatay, Atay Ozgovde and Cem Ersoy. "Edgecloudsim: An environment for performance evaluation of edge computing systems." Transactions on Emerging Telecommunications Technologies 29, no. 11 (2018): 1-17.

[30] Zhang, Jiale, Bing Chen, Yanchao Zhao, Xiang Cheng and Feng Hu. "Data security and privacy-preserving in edge computing paradigm: Survey and open issues." IEEE Access 6 (2018): 18209-18237.

[31] Hoffman, Kevin, David Zage and Cristina Nita-Rotaru. "A survey of attack and defense techniques for reputation systems." ACM Computing Surveys (CSUR) 42, no. 1 (2009): 1-31.

[32] Kamvar, Sepandar D., Mario T. Schlosser and Hector Garcia-Molina. "The eigentrust algorithm for reputation management in p2p networks." In Proceedings of the 12th international conference on World Wide Web, pp. 640-651. 2003.

[33] Lempel, Ronny and Shlomo Moran. "The stochastic approach for link-structure analysis (SALSA) and the TKC effect." Computer Networks 33, no. 1-6 (2000): 387-401.

[34] Josang, Audun. "A logic for uncertain probabilities." International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 9, no. 03 (2001): 279-311.

[35] Josang, Audun, Ross F. Hayward and Simon Pope. "Trust network analysis with subjective logic." (2006): 85-94.

[36] Brin, Sergey and Lawrence Page. "Reprint of: The anatomy of a large-scale hypertextual web search engine." Computer networks 56, no. 18 (2012): 3825-3833.

[37] Huynh, Trung Dong, Nicholas R. Jennings and Nigel R. Shadbolt. "An integrated trust and reputation model for open multi-agent systems." Autonomous Agents and Multi-Agent Systems 13, no. 2 (2006): 119-154.

[38] Song, Shanshan, Kai Hwang, Runfang Zhou and Y-K. Kwok. "Trusted P2P transactions with fuzzy reputation aggregation." IEEE Internet computing 9, no. 6 (2005): 24-34.

[39] Vavilis, Sokratis, Milan Petkovic and Nicola Zannone. "A reference model for reputation systems." Decision Support Systems 61 (2014): 147-154.

[40] Zhou, Zhenyu, Haijun Liao, Xiongwen Zhao, Bo Ai and Mohsen Guizani. "Reliable task offloading for vehicular fog computing under information asymmetry and information uncertainty." IEEE Transactions on Vehicular Technology 68, no. 9 (2019): 8322-8335.

[41] Puthal, Deepak, Nisha Malik, Saraju P. Mohanty, Elias Kougianos and Gautam Das. "Everything you wanted to know about the blockchain: Its promise, components, processes and problems." IEEE Consumer Electronics Magazine 7, no. 4 (2018): 6-14.

[42] Bansal, Gaurang, Amit Dua, Gagangeet Singh Aujla, Maninderpal Singh and Neeraj Kumar. "SmartChain: a smart and scalable blockchain consortium for smart grid systems." In 2019 IEEE International Conference on Communications Workshops (ICC Workshops) (2019): 1-6. IEEE, 2019.

[43] Ranjan, Rajiv, Omer Rana, Surya Nepal, Mazin Yousif, Philip James, Zhenya Wen, Stuart Barr et al. "The next grand challenges: Integrating the Internet of Things and data science." IEEE Cloud Computing 5, no. 3 (2018): 12-26.

[44] Puthal, Deepak and Saraju P. Mohanty. "Proof of authentication: IoT-friendly blockchains." IEEE Potentials 38, no. 1 (2018): 26-29.

[45] Chaudhary, Rajat, Anish Jindal, Gagangeet Singh Aujla, Shubhani Aggarwal, Neeraj Kumar and Kim-Kwang Raymond Choo. "BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system." Computers & Security 85 (2019): 288-299.

[46] Karfopoulos, Evangelos L., Kostas A. Panourgias and Nikos D. Hatziargyriou. "Distributed coordination of electric vehicles providing V2G regulation services." IEEE Transactions on Power Systems 31, no. 4 (2015): 2834-2846.

[47] Duan, Lingjie, Lin Gao and Jianwei Huang. "Cooperative spectrum sharing: A contract-based approach." IEEE Transactions on Mobile Computing 13, no. 1 (2012): 174-187.

[48] Wang, Yuntao, Zhou Su and Ning Zhang. "BSIS: Blockchain based Secure Incentive Scheme for Energy Delivery in Vehicular Energy Network." IEEE Transactions on Industrial Informatics 15, no. 6 (2019): 3620-3631.

[49] Wang, Yuntao, Zhou Su, Qichao Xu, Tingting Yang and Ning Zhang. "A novel charging scheme for electric vehicles with smart communities in

vehicular networks." IEEE Transactions on Vehicular Technology 68, no. 9 (2019): 8487-8501.

[50] Santiago, Carlos, Bodhisattwa Gangopadhyay and JoÃčo Pedro. "Planning a urban Radio over Fibre network." In 2011 IEEE EUROCON-International Conference on Computer as a Tool (2011): 1-4.

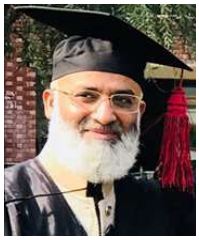
[51] Aujla, Gagangeet Singh, Anish Jindal and Neeraj Kumar. "EVaaS: Electric vehicle-as-a-service for energy trading in SDN-enabled smart transportation system." Computer Networks 143 (2018): 247-262.

[52] Yahaya, Adamu Sani, Nadeem Javaid, Fahad A. Alzahrani, Amjad Rehman, Ibrar Ullah, Affaf Shahid and Muhammad Shafiq. "Blockchain Based Sustainable Local Energy Trading Considering Home Energy Management and Demurrage Mechanism." Sustainability 12, no. 8 (2020): 3385.

[53] Khalid, Rabiya, Nadeem Javaid, Ahmad Almogren, Muhammad Umar Javed, Sakeena Javaid and Mansour Zuair. "A Blockchain-Based Load Balancing in Decentralized Hybrid P2P Energy Trading Market in Smart Grid." IEEE Access 8 (2020): 47047-47062.

[54] Open Energy Information, Available: http://en.openei.org/datasets/dataset/commercial-and-residential- hourly-load-profiles-for-all-tmy3-locations-in-the-united-states, [Accessed: April 2020].

ADAMU SANI YAHAYA received his B.S. degree in 2011 from Bayero University, Kano, Nigeria and received his M.S. degree in 2014 from Meliksah University (Erciyes University), Turkey. He is a lecturer with the Department of Information Technology, Bayero University, Kano, Nigeria. He is currently pursuing a PhD degree from the Communications over Sensors (ComSens) Research Laboratory, Department of Computer Science, COMSATS University Islamabad, Islamabad Campus under the supervision of Dr. Nadeem Javaid. He has authored research publications in international journals and conferences. His research interests include data science, optimization, security and privacy, energy trading, blockchain and smart grid.



NADEEM JAVAID (S'8, M'11, SM'16) received the bachelors degree in computer science from Gomal University, Dera Ismail Khan, Pakistan, in 1995, the masters 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 Campus. He has supervised 126 masters and 20 Ph.D. theses. He has authored over 900 articles in technical journals and international conferences. His research interests include energy optimization in smart/micro grids, wireless sensor networks, big data analytics in smart grids, blockchain in WSNs/smart grids, etc. He was a 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 the International Journal of Space-Based and Situated Computing and Sustainable Cities and Society.

MUHAMMAD UMAR JAVED received the bachelor's and master's degrees in electrical engineering from Government College University Lahore, Lahore, Pakistan, in 2014 and 2018, respectively. He is currently pursuing a PhD degree from the Communications over Sensors (ComSens) Research Laboratory, Department of Computer Science, COMSATS University Islamabad, Islamabad Campus under the supervision of Dr. Nadeem Javaid. He has authored 12 research publications in international journals and conferences. His research interests include smart grid, electric vehicles and blockchain.

MUHAMMAD SHAFIQ received the master's degree in information technology (IT) from the University of the Punjab, Gujranwala, Pakistan, in 2006, the M.S. degree in computer science from the University Institute of Information Technology, Arid Agriculture University, Rawalpindi, Pakistan, in 2010 and the Ph.D. degree in information and communication engineering from Yeungnam University, South Korea, in February 2018. He was with the Faculty of Computing and IT, University of Gujrat, Gujrat, Pakistan, as a Faculty Member, from 2010 to 2014 and formerly held the same position with the Department of Computer Science and IT, Federal Urdu University, Islamabad, Pakistan. His research interests include the Internet of Things (IoT); cognitive radio-based IoT networks-architecture and design; mobile ad hoc networks; wireless sensor networks, performance, management and security; 5G cellular networks, admission control and mobility management; device-to-device communications; medium access control protocols; Internet routing protocols; spectrum trading and auctions; information system, design and access control; and human-computer interaction

WAZIR ZADA KHAN (Senior Member, IEEE) received the bachelor's and master's degrees in computer science from COMSATS University Islamabad, in 2004 and 2007, respectively and the Ph.D. degree from the Electrical and Electronic Engineering Department, Universiti Teknologi PETRONAS, Malaysia, in 2015. He is currently working with the Farasan Networking Research Laboratory, Faculty of CS & IT, Jazan University, Saudi Arabia. He is also a Researcher with the Global Foundation for Cyber Studies and Research, which is an independent, non-profit and non-partisan cybersecurity think-tank based in Washington D.C. He has more than ten years of teaching/professional experience in Pakistan and Saudi Arabia. He has published over 75 research articles in the journals and conferences of international repute. His current research interests include wireless sensor networks, security and privacy, blockchain, the IoT, IIoT and reinforcement learning. He is a member of the technical program committee for many international conferences. He is serving as a Reviewer of many reputed journals.

MOHAMMED Y AALSALEM holds a PhD and master's degree in March 2009 from the University of Sydney, Australia, from the Faculty of Engineering and Information Technology and specializes in sensors networks, Internet of Things, Computer Networking, Network Security and Trust Management. Dr. Aalsalem is assistant professor at faculty of Computer and Information Technologies (Jazan University). He was the dean and Founder of the Deanship of E-learning and Distance learning at same university from 2009- 2014. He was the dean of the faculty of Computer and Information Technologies from 2014- August 2018.