A Two-stage Privacy Preservation and Secure Peer-to-Peer Energy Trading Model using Blockchain and Cloud based Aggregator

ADAMU SANI YAHAYA\textsuperscript{1}, NADEEM JAVAID\textsuperscript{1,*}, AHMAD ALMOGREN\textsuperscript{2,*}, ABRAR AHMED\textsuperscript{1}, SARDAR MUHAMMAD GULFAM\textsuperscript{3}, and AYMAN RADWAN\textsuperscript{1}

\textsuperscript{1}Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan
\textsuperscript{2}Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia
\textsuperscript{3}Department of Electrical and Computer Engineering, COMSATS University Islamabad, Islamabad 44000, Pakistan
\textsuperscript{4}Instituto de Telecomunicacoes and Universidade de Aveiro, Aveiro, Portugal

Corresponding authors: *Nadeem Javaid (e-mail: nadeemjavaidqau@gmail.com); Ahmad Almogren (ahalmogren@ksu.edu.sa)

ABSTRACT Local energy trading has attracted the attention of many researchers as a result of its promising benefits. These benefits include minimizing gas emission, reducing power shortage, and establishing a competitive energy market. However, the energy trading between several prosumers causes trust, security, and privacy challenges in energy systems. On the other hand, a single point of failure and an increase in overall system cost occur when the energy system is managed using a centralized model. Therefore, to tackle the mentioned issues, this work proposes a two-layered secure Peer-to-Peer (P2P) energy trading model based on blockchain. The proposed model has two layers: authentication, and secure energy trading. In the authentication layer, in order to protect the proposed model from impersonation attacks, a mutual authentication process is implemented. In the energy trading layer, a new consensus mechanism is proposed to minimize the number of malicious validators. Afterwards, an incentive-punishment algorithm is introduced to motivate energy prosumers to contribute more energy in the model. Next, a dynamic contract theory based on supply-demand ratio pricing scheme is proposed. The purpose of the proposed pricing scheme is to solve the issues associated with the existing pricing schemes. It also preserves the privacy of the actual energy consumption behavior of the trading participants. Furthermore, a consensus mechanism validators’ selection model is proposed. The aim of the proposed work is to have an efficient and secure P2P energy trading platform. Simulations are executed to show the performance of the proposed model in terms of communication and computational costs, reputation, energy contributed, reward, and prices. The results for the authentication process show 7.45 ms computational cost and 1152 bits communication cost, which are better than the existing works. In the consensus process, 66.67% of the validators are selected to conduct the consensus for every transaction. This selection efficiently improves the consensus process and minimizes the number of malicious validators. In the proposed model, the increase in reward is observed for increased energy contribution, decreased non-malicious transactions and adjustment of energy consumption. The proposed model shows a satisfactory performance in terms of trust, security, and privacy.

INDEX TERMS Mutual Authentication, Blockchain, Contract Theory, Energy Trading, Privacy, Security.

I. INTRODUCTION

With the rapid increase in the number of distributed energy consumers and generators, Peer-to-Peer (P2P) energy trading has become important in a smart community [1]. P2P energy trading is a new paradigm for the operation of an energy system where prosumers in different places produce energy from renewable resources. The places include factories, offices, commercial buildings, and residential homes where energy is shared locally with one another. Prosumer is an energy user who can both consume and generate energy.

Energy trading is managed either using a centralized approach or in a decentralized and distributed manner. In the
centralized approach, an intermediary entity single-handedly manages, processes, and validates transactions between different users. However, this approach increases the risks of a single point of failure and the overall cost of the system. Furthermore, security and privacy related problems are also part of the centralized approach’s drawbacks. A significant electricity failure in the system may be disastrous for consumers if an alternate source of energy solution is unreachable. Therefore, distributed and decentralized energy systems are presented as an alternative method to the centralized approach. Blockchain technology is used to provide a convenient and distributed platform where prosumers control their transactions in a more secure manner [2].

In smart grids, distributed and decentralized energy transactions between consumers and producers can be performed with the support of the blockchain network [3]. All users in the network are directly connected to each other. The blockchain is a shared technology ledger, which places every transaction into a block. The blocks are arranged and linked together in a chronological order [4]. Furthermore, the blockchain solves the single point of failure and security problems associated with the central approach system. It is also used for many purposes, such as confidentiality, integrity, and authentication. Using blockchain, it is difficult to break the security of the system as the malicious users must compromise the validators. The validators are the network users that manage the network security [5] based on the rules given by a consensus mechanism. A blockchain consensus mechanism is a set of rules that allows untrusted users to concur on a global state of their network [6]. However, users’ privacy leakages, impersonation attacks, and internal security threats are not solved when using the blockchain model, which can limit its usage.

In addition, as many users join the distributed energy system, security problems related to transactions become more prominent [7]. Blockchain technology is a better option to solve the energy transaction security problem. Numerous researchers propose models that are based on blockchain to tackle this problem [8], [9]. However, the commonly used consensus protocols, i.e., Proof of Stake (PoS) and Proof of Work (PoW), are not suitable for two-layered energy trading scenarios. The energy trading management in distributed energy systems is commonly based on data forecasting. As a result of the existence of malicious users and negative factors in the energy systems, it is difficult to believe that most of the users can trade honestly. Thus, in the proposed two-layered energy trading scenario, it is a major problem to develop a robust and effective consensus mechanism. Furthermore, the local utilization of energy that is generated from decentralized and distributed energy sources through energy trading is more beneficial than forwarding it to the power system grid [10]. This helps to minimize the hazardous effects of high voltage on the residential homes’ appliances. Thus, a new model is required that manages the locally generated energy in the community. However, unstable energy prices and pricing regulations in the energy market have restricted the smooth implementation of local energy trading.

This research develops a two-layered P2P secure energy trading model to overcome the above mentioned issues. The proposed model provides mechanisms for mutual authentication, users’ privacy protection and privacy preserving dynamic pricing. The model is developed on a permissioned blockchain where the proposed consensus mechanism enables prosumers to perform energy trading transactions in a fair and privacy preserving fashion. The primary contributions of this research work are as follows.

- A two-layered efficient and reliable energy trading model using a permissioned blockchain is proposed.
- The study proposes an off-chain mutual authentication mechanism to prevent the system from impersonation, active, and passive attacks.
- A reputation based score mechanism is presented to tackle collusion and dishonesty between energy buyers (Bs) and sellers (Ss) in this study.
- An efficient privacy preserving dynamic pricing mechanism based on contract theory and Supply-Demand Ratio (SDR) is proposed. The pricing mechanism is proposed to solve the problems that are originated from auction, negotiation, and fixed pricing schemes.
- A monetary incentive mechanism is introduced that motivates users to contribute more energy in the proposed market scenario. Also, a consensus mechanism validators’ selection model is proposed.
- The effectiveness of the proposed energy trading model is shown by conducting simulations. Moreover, the privacy and security of the model are theoretically analyzed.

The rest of this research work is structured as follows. In Sections II and III, we present the related work and problem statement, respectively. In Section IV, the proposed model is discussed. The proposed solution is presented in Section V. In Section VI, simulation results and discussion are presented. The conclusion is given in Section VII.

II. RELATED WORK
Blockchain is a distributed and decentralized P2P network that allows communication between untrusted users in a verifiable fashion. Various research works use blockchain to decentralize complex energy markets and P2P trading networks. In [11], the authors propose a secure blockchain model that allows users to negotiate energy prices without involving a third party. The authors thoroughly discuss on strategies that make the energy system more secure. In this model, if the selling prosumer does not commit to the purchaser’s energy need within a stated period, the associated transaction is expired and considered as invalid. The robust verification scheme is used to make the model stand well against security attacks. The authors in [12] initially demonstrate a powerful blockchain based Internet of Things (IoT) combination across many industries. Afterwards, a list of secure blockchain energy trading models in the blockchain based Industrial-IoTs (IIoTs) is proposed. In [4], the authors...
propose an energy trading model based on blockchain. The purpose of the model is to manage and supervise the trading process in order to build a reliable trading platform as well as improve the quality of energy. The authors use anonymous authentication to safeguard the privacy of users. Also, a timed commitment scheme is developed to affirm verifiable fairness at the time of trading.

In [13], a three-party smart grid model that integrates Electric Vehicles (EVs) is presented. The model involves complex and flexible communication between power grids, EVs, and communities. Two intriguing domains for energy transaction are introduced: community-centered and EV-centered. The model combines both smart communities and EVs in order to provide efficient energy resource management in the power system. Moreover, a demand-on-schedule energy management model is proposed. In [14], the authors implement a decentralized and secure energy trading model using an energy token. The token is used to allow energy trading transactions to be executed between users. An anonymous blockchain based negotiation pricing scheme is used in the model. The authors in [15] propose a blockchain based smart contract model for energy trading between users. In the model, the proposed smart contract is used to provide trust between the users and to eliminate the reliance on a third party. In [16], a novel and decentralized digital coin model, named as NGRcoin model, is presented. In the model, energy users use the proposed digital coin to trade the locally generated energy. The proposed coin used in the network obeys the green energy trading protocols.

In [17], the authors present a lightweight blockchain based model, which is known as a directed acyclic graph based vehicle-to-grid network. In this work, a tangle data structure is adopted to store the transactions in scalable and secure manners in the network. Also, to perform negotiations between the vehicles and the grid at an optimal cost, a game theory framework is used. The proposed model does not require fees to conduct transactions and heavy computation. The authors in [18] develop a consortium blockchain model to address the privacy leakage issues without causing any hindrance in trading functions. The model mainly focuses on the privacy of users during energy trading in the smart grid. It also screens the distribution of energy sales of selling prosumers. The sales are derived from the fact that energy trading can be performed to detect their trading relationship with other information. For example, energy usage and physical location. The experimental evaluation has shown the effectiveness of the model.

The authors in [19] propose an efficient and secure energy trading model based on blockchain. The model is divided into two layers, which can protect users’ privacy and also achieve a power balance between demand and supply. Also, credibility based on an equity proof scheme is developed to improve the system’s availability in the energy internet. In [20], the authors propose a methodology for local P2P energy trading and power distribution network co-simulation systems. The simulator of the distribution system is interfaced with the P2P energy trading platform, which incorporates a distributed double auction technique based on blockchain. The system is demonstrated using a case study of a typical European suburban distribution network. In [21], the authors introduce a generic model for a blockchain network, which allows P2P energy trading in a nearby power market. The research work focuses on seeking energy matching pairs between demand and supply sides. It also motivates direct energy trading between consumers and generators. The developed multi-directional blockchain network implements a complete trading process. As smart contract executes payment and trading rules without the intervention of a third party, the fairness and security of the energy trading model are significantly improved.

The authors in [22] propose an energy trading model based on blockchain between EVs (generators) and critical load (consumers) in microgrids. Contrary to the conventional wholesale energy market where consumers buy energy from retailers, in this proposed model, the prosumers are directly connected to consumers to meet their temporary energy needs. Blockchain technology is introduced to create a reliable energy trading platform. Also, a prototype for energy trading is implemented to monitor the energy trading activities between consumers and generators remotely using a graphical user interface. In [23], the authors propose a consortium blockchain based energy trading framework using a PoS consensus mechanism. In the framework, the pre-selected validators are custodians for power losses compensations in distribution lines by energy transactions. The authors demonstrate the process of smart contract creation and blockchain establishment. Furthermore, another type of crypto-currency, called “eleccoin”, is developed in the P2P energy market, which is announced by the consensus process of the blockchain. The simulation results show effectiveness and feasibility of the framework in terms of security and efficiency.

III. PROBLEM STATEMENT
As the number of distributed energy generators and consumers increases, secure P2P energy trading becomes paramount in a smart community [24]. However, in a distributed energy trading model integrated with public blockchain technology, energy trading users can join or leave the trading network without permission at any time. This makes controlling and authenticating the network users difficult for the energy systems. It can also lead to possible impersonation, active, and passive eavesdropping attacks when an authentication mechanism is not implemented. Traditionally, centralized systems were used to ensure energy trading between entities. However, these systems exhibited several issues like lack of trust, security and privacy threats, single point of failure, etc. To tackle the issues, decentralized systems were introduced, which provided efficient solutions for the issues [25]–[27].

To overcome the vulnerabilities of centralized energy trading models, blockchain technology is one option [28].
However, blockchain alone cannot guarantee the successful delivery of energy and information from a sender to a receiver without collisions. Also, privacy and trust concerns restrict the implementation of the blockchain technology in many research domains. Furthermore, using a consortium blockchain, an authentication certificate is produced by a central authority [29], [30]. In this regard, a single point of failure can still occur. Therefore, developing efficient privacy preserving methods for an energy trading system based on blockchain can improve the effectiveness of the P2P energy trading platforms.

However, there still exist different issues in the energy systems such as price determination without the involvement of a trusted third party, which discourages P2P energy trading. The authors in [31] propose a P2P energy trading model in which the energy prices in the market are fixed. However, this model is inefficient and non-beneficial for prosumers as price of energy is more than the grid's pricing tariff. In another work, energy prices are determined based on auction or negotiation market approaches, which are the best approaches for solving the problem of fixed pricing determination [32]. However, both auction and negotiation approaches become complex and time consuming when the number of users grows. The auction approach takes more time for a matching process to converge. Whereas, the negotiation approach usually takes place through an arbitrator, which makes the approach to lack trust and transparency.

According to the above mentioned challenges, it is clear that applying blockchain alone in energy trading systems cannot provide a sustainable and efficient energy trading platform. Moreover, the studies discussed do not consider solving the lingering challenges in the existing pricing schemes. At the same time, protecting the system from impersonation and collusion attacks are not fully resolved. So, it is the motivation of this study. To tackle this issue, the proposed system comprising of blockchain technology, cloud system, reputation and incentive mechanism, and SDR pricing mechanism are introduced. Table 1 shows comparison of the proposed work and the existing works.

### IV. THE PROPOSED SYSTEM MODEL

The proposed energy trading system in Fig. 1 is divided into two layers. The first layer provides privacy preserving mutual authentication between the buying and selling prosumers. In the second layer, a secure P2P energy trading model for the prosumers in the permissioned blockchain network is implemented. The model consists of Autonomous cloud based Aggregator (Agr) and energy users (prosumers and consumers), which communicate via the permissioned blockchain, i.e., consortium blockchain. An energy user that locally generates energy and preserves its surplus energy for future use is called an energy prosumer. The prosumer has the ability to act as B or S at any given time based on the current energy status. In this model, the energy prosumers can be either Electric Vehicles (EVs), charging stations, commercial buildings or residential homes. Also, all prosumers have smart meters. The smart meter is a sealed tamper proof device that has the ability to resist injection or extraction of secret keying material by either the owner or an attacker [33]. It is used to record and monitor the energy consumed or transferred by the users. In addition, the data produced from the meters is stored in the blockchain. In Fig. 1, Agr is an autonomous system that is believed to be a trusted entity. It is mandatory for all of the energy users to register themselves with Agr before performing energy transactions. The registration process is discussed in Section V-A. The purpose of using cloud in the proposed model is that it solves data storage issue because large amount of data cannot be stored on blockchain. Moreover, it also provides high computing capability and increases the cost saving as multiple resources are not required to store data. The real identities of the users are only known by Agr and are discarded after each successful transaction, provided that no complaint is received. To preserve the privacy of the actual users’ energy consumption information at time of energy trading, Agr sets multiple energy contract types for every time slot. The contract type contains the amount of energy to be purchased or sold and the corresponding price. The fundamental principle of using contract theory is to hide the actual energy consumption pattern of users in the system. The price of the selected contract depends on the amount of requested energy and the availability of energy. Details on how to determine the price are discussed in Section V-C3. Furthermore, we assume that each prosumer selects the contract type that will not exceed its storage capacity. Moreover, the upper and lower thresholds of validators’ selection are set by Agr for validators and blacklisted users, respectively. In the proposed model, block mining is only performed by the Agr and the selected validators, which are assumed to have high computational resources.

Following the prosumers’ registration and mutual authentication level as well as setting up the trading parameters, the energy trading begins. The prosumers select their en-

| Papers | Permissioned Blockchain | Mutual Authentication | Validators' Selection Techniques | Reputation | Contract Theory | SDR |
|--------|--------------------------|-----------------------|----------------------------------|------------|----------------|-----|
| [4]    | Yes                      | No                    | No                               | No         | No             | No  |
| [8]    | Yes                      | No                    | No                               | Yes        | No             | No  |
| [9]    | Yes                      | No                    | No                               | Yes        | No             | No  |
| [31]   | Yes                      | No                    | No                               | No         | No             | Yes |
| [32]   | Yes                      | No                    | No                               | Yes        | No             | No  |
| Proposed model | Yes                      | Yes                   | Yes                              | Yes        | Yes            | Yes |
| Technique(s)                        | Objective(s)                                                                 | Research Achievement(s)                                                                 | Limitation(s)                                                                 |
|-----------------------------------|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Consortium blockchain and digital signatures [4] | To reduce trading payment delay and supervise trading process                  | An efficient payment system and secure trading model are achieved                        | Time complexity in consensus process is not considered                        |
| Private blockchain [5]            | To minimize the confirmation latency and block creation time                   | The effectiveness of the system for secure DRM is enhanced                               | Privacy is considered only during charging scheduling                           |
| Blockchain and smart contracts [11] | To improve energy management and scalability in P2P trading                   | Efficient energy management is developed and IoT scalability is achieved                  | User authentication and load balancing are not considered                       |
| Private blockchain and consortium blockchain [12] | To develop a secure and trusted energy trading system and to enhance system availability | Credible energy platform, load balancing, and secured energy trading system are proposed | Improvement on the system scalability is not achieved                           |
| Three-party game and schedule upon-request [13] | To minimize cost, and improve matching and searching of users                 | An efficient and effective resource management is achieved                               | Lack of privacy                                                                |
| Public blockchain, and encryption algorithms [14] | To provide a decentralized secure transaction system in smart grids using the blockchain technology | Privacy and security of the transaction system are enhanced                              | Efficient consensus and user authentication mechanisms are not considered        |
| Smart contracts and blockchain technology [15] | To provide trust between the users                                           | Trust and security in the system are enhanced                                           | Privacy and efficient consensus mechanisms are not considered                  |
| Blockchain technology and game theory framework [17] | To increase local energy generation and improve interaction between prosumers and power plants | Proposed a NRGcoin model that allows locally generated renewable energy to be sold using digital currency in the smart grid | Privacy preservation and mutual verification are not considered                  |
| Smart contracts, consortium blockchain [18] | To store transaction in a scalable manner and perform negotiations between vehicles and grid | Reduction in energy losses is achieved and negotiation between users is performed at low cost | Privacy and mutual verifiable fairness mechanisms are not considered            |
| Private blockchain and bidding techniques [19] | To improve energy demand and supply. Also, to provide protection during energy trading | The proposed system is successful in matching energy demand and supply at power grid level | Verifiable mechanism and less computational complexity for consensus mechanisms are not considered |
| Blockchain and double auction mechanism [20] | To develop a friendly and secure system for energy trading and also provide mechanism that protect users’ privacy | The system achieved a power balance between demand and supply | The problems of high energy consumption and computational power needed for consensus is still not resolved |
| Smart contract, blockchain and iterative double auction mechanism [21] | To improve trust, openness and transparency in energy trading                  | Trust, transparency and openness are achieved when blockchain is used                    | The system does not focus on better pricing scheme and the complexity of the consensus mechanism. Privacy of users is not considered |
| Review on blockchain based energy trading techniques [24] | To increase social welfare and balance demand and supply                      | Social welfare is increased and security is significantly improved                        | Privacy is not protected                                                       |
| Blockchain technology and edge computing [29] | To propose technical solutions for Brooklyn microgrid                         | Seven components of the energy market are identified and discussed                      | Lack in discussing the provisioning of efficient allocation and pricing mechanisms |
| Consortium blockchain, homomorphic encryption, and demurrage mechanism [32] | To achieve an efficient and secure system during consensus process            | The efficiency of the system is improved                                               | Confirmation latency and block creation time are not considered                 |

The efficiency of the system is improved

Privacy is considered only during charging scheduling

User authentication and load balancing are not considered

Improvement on the system scalability is not achieved

Lack of privacy

Privacy and efficient consensus mechanisms are not considered

Privacy preservation and mutual verification are not considered

Verifiable mechanism and less computational complexity for consensus mechanisms are not considered

The system does not focus on better pricing scheme and the complexity of the consensus mechanism. Privacy of users is not considered

Privacy is not protected

Lack in discussing the provisioning of efficient allocation and pricing mechanisms

Confirmation latency and block creation time are not considered

Verifiable mechanism and less computational complexity for consensus mechanisms are not considered
ergy contracts from the blockchain network. Agr matches B and S based on a first-come-first-serve scheme. In first-come-first-serve scheme, the user request that arrives first gets served first with the required energy. After the trading is completed, B deposits digital tokens to the S’s wallet account. The mechanism for transferring tokens is not in the scope of this research. Furthermore, the energy transaction information received through the blockchain is encrypted by an asymmetric technique and is cryptographically signed. The public key of the asymmetric technique is used for encryption and verification of signature while private key is used for decryption and generation of the electronic signature. The received transaction is placed into a transactions’ pool, which will subsequently be added to a block after validation. Therefore, valid transactions are stored while invalid transactions are discarded. New blocks are created in the blockchain by applying the proposed consensus and validators’ selection mechanism. Details of the consensus mechanism are given in Section V-C2. Each block is connected with its immediate block in the blockchain using a cryptographic hash value.

A. BILINEAR PAIRING
Suppose three (3) multiplicative cyclic groups of prime order q are denoted as $G_1$, $G_2$, and $G_T$. $m_1$ and $m_2$ represent the generators of $G_1$ and $G_2$, respectively. A represents isomorphism from $G_2$ to $G_1$ where $A(m_2) = m_1$. The bilinear map is represented as $e() : G_1 \times G_2 \rightarrow G_T$. The following are the properties of the bilinear map.

1) Non-degenerate: $e(m_1, m_2) \neq 1_{G_T}$.
2) Bilinear: $\forall m_1 \in G_1, m_2 \in G_2$ and $b, a \in \mathbb{Z}$, we have $e(m_1^b, m_2^a) = e(m_1, m_2)^{ba}$.
3) Computability: An efficient algorithm exists to calculate $e() : G_1 \times G_2 \rightarrow G_T$.

The proposed authentication method is designed based on the implementation performed in [34]. Different challenges were faced during the implementation of the proposed blockchain network. The major challenge was the resource management. Due to the resource constraint of the lightweight nodes, they cannot be applied in the mining process. Therefore, Agr and the validators (selected nodes) are used for performing the mining process.

B. COMMUNICATION MODEL
Conventional energy trading uses a centralized model. However, in a contemporary system, the prosumers may not require a central person to perform P2P transactions. In a power system where energy is transferred through a physical medium, prosumers can communicate with each other.
For instance, nearby residential homes can directly connect through a physical cable wire to transfer energy. At another instance, EVs can transfer energy to one another via wireless or wired mode whenever they meet at the same station or place without the involvement of a third party. In the proposed model, all of the prosumers are equipped with smart meters. As shown in Fig. 1, the nodes communicate via consortium blockchain to ensure successful energy transactions between users. It is assumed that prosumers have the physical medium for transferring energy during the trading period.

C. ATTACK MODEL

This section discusses the attack model and the design goals of the proposed system. The assumptions for attackers are given as follows. (i) The data of each node in the blockchain is tamper-proof and it is not possible to be compromised. (ii) Impersonation attack can occur in the absence of an authentication mechanism. (iii) Passive and active attacks can be launched when the transactional data is not encrypted. The major goal of the proposed system is to design a reliable and secure model. To achieve this goal, the identified security threats must be addressed. Thus, a secure and reliable energy trading platform is implemented using a permissioned blockchain, i.e., consortium blockchain. The identities of the prosumers must be kept private in the permissioned blockchain. The users should be authenticated to remove all those entities from the system that are not legally participating in energy trading. Moreover, the immutability of transactional data must be maintained. So that no energy entity can modify the given information. Also, all of the trading operations conducted must be verified and validated before being accepted by the network. The identities of the network nodes must not be linkable with their energy transactions and no energy node should know the identity of its counterpart. Privacy preservation of energy users is very important, whereby protecting their sensitive information is paramount. The traceability and integrity in the proposed system model must be adhered, so that the transactions should be easy to trace but difficult to tamper with. Also, the participants should not repudiate energy transactions and the transmitted information. Trust should be the foundation of trading energy between Ss and Bs. Energy trading must be conducted in a trustable and a fair fashion, so that the S receives the exact amount of energy cost from the B. Also, B receives the amount of energy he paid for.

D. PROPOSED SMART CONTRACT

The ledger and smart contract are the essential parts of majority blockchain platforms (Ethereum and Hyperledger Fabric). A smart contract states the executable codes that are compiled either by Solidity or by Go language supported by Ethereum or Hyperledger Fabric, respectively. Afterwards, the codes are stored in the blockchain as bytecode in the executed transactions. Moreover, the binary interfaces and defined functions are triggered via executing transactions and message call from different smart contracts. In the proposed model, a smart contract is used to record the users’ requests and respond accordingly in order to provide a reliable system and eliminate the third party. The energy trading mechanism is provided in Algorithm 1, energy trading process is performed. Before the trading begins, the proposed smart contract checks the B’s available balance to verify whether the B can afford to pay for the requested energy or not. If B has sufficient funds, the smart contract checks for the availability of the energy. If energy is available in the market, the proposed contract verifies whether the B has enough storage that can accommodate the purchased energy or not. If the conditions are true, the proposed contract allows the participant to trade energy. The smart contract invokes the proposed consensus mechanism that allows validators to verify and add transactions in the chain’s ledger before all transactions are stored in the blockchain. After the transactions are validated, the punishment-incentive mechanism is invoked where the users are rated positively and rewarded upon successful honest transactions. Otherwise, the users are rated negatively and no incentive is awarded, which may subsequently lead to add the users to the blacklist. The pseudocode of the energy trading’s smart contract is given in Algorithm 1.

V. PROPOSED SOLUTIONS

The proposed solutions are divided into three stages: 1) system initialization and registration, 2) mutual authentication, and 3) secure and trusted energy trading.
A. SYSTEM INITIALIZATION AND REGISTRATION

For each energy trading transaction, Agr selects two secretly preserved random numbers \( q, p \in \mathbb{Z}_q^* \) to compute public keys for Ss and Bs in an efficient manner. Afterwards, a cryptographic hash function is selected as \( H : \{0,1\}^* \rightarrow \mathbb{Z}_q^* \) by Agr. A selected its private key as \( S_{Agr} \in \mathbb{Z}_q^* \) and its public key is computed as \( U_{Agr} = m_1 S_{Agr} + q \). In the end, Agr allocates the system’s parameters to the participants as \( \text{parm} = (q, G_1, G_2, G_T, m_1, U_{Agr}, H, c(e)) \).

Initially, \( S \) with an index of \( i \), i.e., \( S_i \) is registered with Agr. After registration, \( S_i \) generates its private key as \( S_{Si} \in \mathbb{Z}_q^* \) and computes its public key as \( U_{Si} = m_1 S_{Si} + q \). Afterwards, Agr receives the public key from \( S_i \) through a secure channel. Likewise, \( B \) with an index \( i \), i.e., \( B_i \) randomly selects \( S_{Bi} \in \mathbb{Z}_q^* \) as a private key and produces its corresponding public key as \( U_{Bi} = m_1 S_{Bi} + q \). Subsequently, Agr receives the public key of \( B_i \) via a secure channel.

B. ANONYMOUS MUTUAL AUTHENTICATION

Authentication is a mechanism that proves users’ identities. It helps to avoid energy trading interactions of honest users with adversary users. Mutual authentication is the process where both communicating parties authenticate each other to make the system more immune from spoofing attack [35]. A spoofing attack is a situation where a malicious node successfully impersonates another node in a network by falsifying data in order to gain an illegitimate advantage [36]. The roles of blockchain technology are highlighted in resource constrained scenarios because of its beneficial properties, which include immutability, verifiability, and decentralization. The properties are advantageous for developing reliable, convenient, and secure resource constrained platforms. Therefore, various blockchain based authentication models with high confidentiality and anonymity are getting popular and increasingly available. However, the following problems are still faced by the blockchain based authentication models [37]. The anonymity property of blockchain can be suitable for smart homes and resource constrained devices to ensure participants’ privacy. However, in the systems, the behavior of the participants cannot be efficiently regulated, which can lead to impersonation attacks. In another words, an efficient technique that can trace the participant who performs malicious activities does not exist. Another problem is that all of the transaction requests are not encrypted, which can easily be collected and can statistically analyze the participant’s daily activities. Thus, compromising the participants’ privacy. Therefore, the need for an efficient and anonymous mutual authentication mechanism is required. However, as additional authentication mechanism is added, computational cost increases, which is the tradeoff of the proposed model. Though, the cost is still less than the existing models. The steps for mutual authentication are given as follows.

1) Energy Buyer to Seller Authentication

The authentication from \( B_i \) to \( S_i \) is conducted in this section to request for energy from the Ss. A one-time secret key is used for Ss’ verification by \( B_i \) in order to preserve their privacy. It means that validity of the authentication keys ends after performing energy transaction using the secret key. For a new energy transaction, a new authentication process is required. The following are the steps for \( B_i \) to \( S_i \) authentication.

a) If the expression above does not hold, then the request is rejected by \( S_i \).

b) \( S_i \) computes \( c = H(x_i m_1 H(R_{Bi})) \) and sends the request = \( (R_{Bi} | m_1 H(R_{Bi}) | T_B) \) to \( S_i \). \( T_B \) represents current timestamp of \( B_i \).

c) Once the request is received, \( S_i \) checks the freshness of \( T_B \) and validates the request’s source. If any of the information is not correct, then \( S_i \) terminates the process. Otherwise, \( S_i \) checks the validity of the energy request as follows.

a) \( S_i \) computes \( v_1'' = x_i \times v_2' \) and \( v_2'' = \frac{m_1}{v_1} \).

b) \( S_i \) calculates \( c' = H(x_i m_1 H(R_{Bi})) \). It checks that if \( c = c' \), then the submitted information is validated and \( B_i \) is authenticated.

5) After verifying the certificate, \( S_i \) validates the integrity of \( R_{Bi} \), as given below.

a) \( e(x_i m_1 H(R_{Bi}), sig) = e(m_1, m_2) \).

b) If the expression above does not hold, then the information request is rejected by \( S_i \). Otherwise, it is accepted.

2) Energy Seller to Buyer Authentication

The authentication from \( S_i \) to \( B_i \) is explained in this section. To protect the user’s privacy, a one-time secret key is used for each transaction by \( S_i \). Note that when the authentication is not successful, the whole energy trading process is terminated. The authentication process for \( S_i \) to \( B_i \) is similar to that of \( B_i \) to \( S_i \). To preserve the integrity of the energy trading request \( R_s \), \( S_i \) calculates a signature \( \text{sig} = m_2 \frac{m_1 S_{Bi} + q}{m_1 S_{Bi} + q} \) and sends the request =
(Rs|sig|Oi|CRFSi|Ts) to Bi. Ts represents current timestamp of Si and Oi is Si generated public key.

C. TRUSTED ENERGY TRADING

In this section, an incentive-punishment mechanism for energy trading and the proposed pricing scheme are discussed. Furthermore, the proposed blockchain based consensus mechanism is explained.

1) Incentive-Punishment Mechanism

To motivate energy users to contribute more energy and share honest information with other users, we implement an incentive-punishment mechanism. The mechanism is adopted from [8] that is initially used in vehicular social networks. We modified the mechanism and used it in the proposed energy trading model by incorporating energy contribution parameter. In this model, it is assumed that each energy user starts with the same initial rating value and distribution parameter. In this model, it is assumed that each energy user starts with the same initial rating value and distribution parameter. The mechanism is explained.

In the proposed scenario, if a user’s rating is more than the threshold, the user can be used to purchase energy until it is depleted. On the other hand, the reward remains zero until the user completes a non-dubious transaction. In the proposed model, a static threshold point is set by the aggregator. The purpose of the threshold is to select validators that are honest to perform the consensus process and place dubious users into a blacklist. In the proposed scenario, if a user’s rating is more than a threshold, it can take part in the consensus process and block creation. On the other hand, if the rating of a user is less than the threshold, it is blacklisted. The algorithm for the incentive-punishment mechanism is presented in Algorithm 2. The users’ rating and reward values are stored in the blockchain ledger and passed across the users to avoid modification of the values. For every transaction to be efficiently verified and added in the blockchain, an efficient consensus mechanism is required. The details of the consensus mechanism are discussed below.

2) Consensus Mechanism

To further reduce the processing time of PoW consensus mechanism and minimize the number of malicious validators, a selection stage takes place in the energy trading network. The pseudocode of the final stage of validators’ selection model is shown in Algorithm 3 and 4 where the algorithms are used for selecting validators in the proposed model. The proposed selection and consensus processes are slightly modified from [9] to fit into our model. In Algorithms 3, we use \( R_v \in [0, 2] \) to select the final group for the consensus nodes \( N_v \). These nodes are a subset of \( N_v \) that manage the consensus process. The proposed validators’ selection model motivates energy users to compete in a nomination process where each energy user can be selected as a validator according to its \( R_v \) value. The methodology used is based on truthful transactions and energy contribution level.

In the \( R_v \) calculation’s algorithm, we point out three (3) essential factors for \( R_v \) assessment: 1) normalized rating value \( \text{Norm}_{gi} \), 2) success rate \( Sc_j \), and 3) error rate \( er_j \) for node \( j \). The importance of each factor is discussed as follows. After the completion of the consensus process, a new block is created and each validator is rated by Agr either negatively or positively. This rating is based on the behavior that the validators show during the block creation. The validator’s rating is collected by Agr to calculate the normalized rating for all the transactions, which is the metric to measure a node’s truthfulness. The \( er_j \) for node \( j \) is defined as the ratio of number of failures \( er \) that occur for a user to create a valid block to the total number of transactions \( At \) performed by the node to produce blocks, i.e., \( er_j = \frac{er}{At} \in [0, 1] \). The error rate for a user that does not create a block is defined as zero (0). The factor has a negative effect on the \( R_v \) of a user. The \( Sc_j \) for user \( j \) is defined as the ratio of a number of successes \( Sc \) that occur for a user to create a valid block to the total number of transactions \( Bt \) performed by the node to produce blocks, i.e., \( Sc_j = \frac{Sc}{Bt} \in [0, 1] \). The success rate for a user that does not create a block is defined as zero (0). Since we are using blockchain, each validator maintains a copy of the \( R_v \) values for all of the validators. The validators’ group size is created by at least more than two-thirds (2/3) of \( N_v \) nodes selected based on their \( R_v \) as given in Algorithm 4. After the validators’ selection phase, the validators selected for the consensus use PoW to verify and finalize the transactions to be added in the new block and broadcast them in the blockchain. On the other hand,
The copies of blockchain ledger of the remaining nodes are synchronized with the newly added block.

The complexity of the network depends on the node’s selection and validation process. In this study, the validating nodes are selected based on their reputation values. It means that nodes with reputation values greater than the predefined threshold value are selected. Therefore, the complexity of the algorithm is based on the nodes’ selection and validation process. Besides, the cost of maintenance is less as only the selected nodes are required for validating the transactions. Let $CT$ be the cost of selecting a node with a high reputation value, the total cost of selecting $n$ nodes is $n \times CT$. Hence, the time complexity of the proposed algorithm is $O(n)$. Moreover, with the increase in the number of nodes, more rounds are required, which in turn increases the computational complexity and makes the network more complex. However, the proposed system is scalable enough to deal with a large number of nodes without being affected greatly. Besides, in the presence of a large number of nodes, more messages will be generated. It will create resource constraints for the model. However, the proposed scheme efficiently tackles this issue by incorporating the cloud system.

### 3) Proposed Pricing Scheme

In the proposed model, a contract theory [30], [38] is formulated to hide the exact energy consumption patterns of the users. Thus, a prosumer’s type is used to quantify the preference of an energy prosumer that is strictly known by the energy user itself. By considering the energy market with $m$ prosumers, the prosumers are sorted based on their preferences in an ascending order and the prosumers’ types are categorized into $n$ types. Suppose the prosumer’s type is given as $\phi = \{\phi_1, \phi_2, \ldots, \phi_n\}$ where the prosumer’s type having less demand is followed by the one with higher demand, i.e., $\phi_1 < \phi_2 < \phi_3 < \ldots < \phi_n$. Instead of providing the same contract for prosumers with different types, a contract that has $n$ contract items is designed for the users, i.e., one for each type. This means that the contract item designed for type $\phi_n$ prosumer is represented as $(E_n, P_n)$. Where $E_n$ represents the range of energy to be traded and $P_n$ is the price for energy in terms of digital coins. The contract item is defined as $CN = \{(E_n, P_n) \forall n\}$. Since the actual amount of energy demanded by the prosumers is not known, therefore, both S1 and Agr can only get an estimate of the requested energy.

To determine the estimate of the requested energy that is more close to the actual one, robust optimization algorithms or machine learning techniques can be used. However, to simplify the trading process in this research, an average value for the selected energy contract plus a random number, which is not more than the range of energy in the contract item, are used for the computation. The value is calculated concurrently by both Agr and S1. Afterwards, an average of the result is computed by Agr to avoid selfishness of the Ss. The formulation of the energy estimation is given as $E_{approx} = \text{Average}(E_{approxAgr} + E_{approxS1})$. Where $E_{approxAgr} = \text{Average}(E_n) + \text{random}(E_{Agr})$ and $E_{approxS1} = \text{Average}(E_n) + \text{random}(E_{S1})$. random($E_{Agr}$) is a randomly generated amount of energy by Agr, which when it is added to Average($E_n$), the total value must be within the contract energy range. Similarly, random($E_{S1}$) is a randomly generated amount of energy by S1, which when it is added to Average($E_n$), the total value must be within the contract energy range. For each contract item, the price is calculated based on SDR formulation [39]. It is assumed that the price $P_1$ for contract $\phi_1$ is lower than the price $P_2$ for contract $\phi_2$, and so on. In this model, we assume that several buying prosumers TPS select a similar contract item. Similarly, many selling prosumers TPS pick the same contract item.

Since we are using SDR model to determine our price, therefore, an exact number of buying and selling prosumers must be calculated at every time slot $tt$. SDR at time slot $tt$ is given as $SDR(tt) = \frac{TPS(tt)}{TPS}$. The prices for Ss and Bs change with respect to time and number of prosumers. The prices are $P_{buy} \{P_{buy}(1), P_{buy}(2), P_{buy}(3), \ldots, P_{buy}(tt)\}$ and $P_{sell} \{P_{sell}(1), P_{sell}(2), P_{sell}(3), \ldots, P_{sell}(tt)\}$. Cumulatively, $P_n = \{P_{buy}(tt), P_{sell}(tt)\}$ where the buying price is $P_{buy}(tt)$ and the selling price is $P_{sell}(tt)$. Utility grid’s selling and buying prices are denoted as $\mu_{sell}(tt)$ and $\mu_{buy}(tt)$ at each time slot $tt$, respectively. To encourage prosumers to participate in the energy trading, the $\mu_{sell}(tt)$ must not be greater than $P_{sell}(tt)$. Also, $\mu_{buy}(tt)$ must be less than $P_{buy}(tt)$. Therefore, $P_{sell}(tt)$ and $P_{buy}(tt)$ are donated as functions of $SDR$, which are given in Equations (1) and (2). The purpose of Equations (1) and (2) is

---

### Algorithm 1 Algorithm for calculating $R_v$

**Input** $N_{v}$, $er_j$, $Sc_j$, $N$;  
1: $j = 1$;  
2: while ($j \leq N$) do  
3: $R_{vi} = N_{v} - er_j + Sc_j$;  
4: $j = j + 1$;  
5: end while  
6: Broadcast $R_{vi}$ to all the users;  

### Algorithm 2 Algorithm for Grouping the Validators based on $R_v$

**Input** $R_v$ sorted array for $N_v$, nodes, $n$;  
1: Target$R_v = 1 + ((2/3) \times \sum(R_v))$;  
2: Recent$Sum = R_v[n - 1]$;  
3: $j = n - 2$;  
4: while ($j \geq 0$) do  
5: Recent$Sum = Recent$Sum + $R_v[j]$;  
6: Add user $j$ to the $N_v$'s list;  
7: $j = j - 1$;  
8: end if  
9: end while  
10: Return $N_v$'s list;  

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/
to determine the proposed energy selling and buying price, respectively. The relationship between the proposed prices and $SDR(t)$ is shown in Fig. 3a. It is shown from the figure that the $SDR$ value increases when both $P_{buy}(t)$ and $P_{sell}(t)$ increase, i.e., the number of buying prosumers decreases. On the other hand, a decrease in $SDR$ increases both $P_{buy}(t)$ and $P_{sell}(t)$. In order to decrease the proposed selling price, the number of buying prosumers must decrease. On the other extreme, to increase the buying price, the number of buying prosumers must increase.

$$P_{sell}(t) = \begin{cases} 
\left(\mu_{sell}(t)+\mu\right)P_{buy}(t) \\
\left(\mu_{buy}(t)-\mu_{sell}(t)-\mu\right)SDR(t) + \mu_{sell}(t)+\mu 
\end{cases}$$

if $0 \leq SDR(t) \leq 1$, 
$$\alpha_{sell}(t) + \frac{\mu}{SDR(t)}$$
if $SDR(t) > 1$.

(1)

$$P_{buy}(t) = \begin{cases} 
P_{sell}(t).SDR(t)+ \\
\mu_{buy}(t).(1-SDR(t)), 
\end{cases}$$

if $0 \leq SDR(t) \leq 1$,
$$\mu_{sell}(t) + \mu,$$
if $SDR(t) > 1$.

(2)

Where $\mu$ is the compensation price.

VI. SIMULATION RESULTS AND DISCUSSION

This section discusses the simulation results of the proposed model. The experiments are executed on a laptop having a 8.00 GB RAM, an AMD E1-6015 APU @1.4 GHz, and Windows 10 operating system. MATLAB2018a is used to implement the model and perform simulations. For simulations, 100 energy users are considered and it is assumed that the users do not have the same consumption and generation of energy. Moreover, the simulation dataset is taken from [40], which has one hour resolution. The prototype of the proposed blockchain model is implemented and evaluated on JUICE. The platform supports the design of a smart contract using JavaScript based client/web tools, and Solidity for monitoring and management of the codes. Furthermore, it has many inbuilt cryptographic algorithms that can be used to provide security and privacy. After the proposed smart contracts are deployed, Web3J is used to evaluate the smart contract’s functionality. Furthermore, the approximate time of the proposed algorithms is calculated using JavaScript and shell script after 100 iterations. The obtained results are presented in Table 3 that are consistent with the block generation time, i.e., 12 seconds. The results depict that communication cost of invoking the algorithms in the proposed smart contract is in milliseconds provided that the blockchain generation time is reduced. In the proposed model, it is assumed that smart devices are available for both energy consumers and generators. It is also assumed that Agr is a full node in the proposed model, which is among the nodes that are responsible for transaction’s verification. It is also assumed that all of the energy users are equipped with smart meters. In the proposed model, an additional authentication method is introduced to provide more security and increase system’s reliability. However, the computational cost is also increased, which is the proposed system’s tradeoff.

A. PERFORMANCE ANALYSIS OF THE MUTUAL AUTHENTICATION

The method is evaluated based on communication and computational costs.

1) Computational Cost

In this research, the computational cost is defined as the total time required to generate and verify the signature and certificate. We compare the computational cost of the proposed system with some existing schemes in literature. For easy understanding, variables used to compute the computational cost are discussed below.

1) $T_h$: time taken to execute a one-time hash operation.
2) $T_m$: time taken to execute the multiplicative point operation.
3) $T_p$: time taken to execute a pairing operation.
4) $T_{e1}$: time taken to execute exponential operation in $G_1$.
5) $T_{e2}$: time taken to execute exponential operation in $G_2$.

The computational cost in this work is computed in milliseconds (ms). The proposed authentication process consumes $2T_p$, $T_m$, and $T_h$ for one-time verification. In the case of one-time certificate and signature generation, it consumes $T_{e1}$, $4T_p$, and $T_{e2}$. Therefore, the total computational cost is $2(2T_p + T_m + T_h) + 2(T_{e1} + T_{e2})$, which consumes a total of 7.45 ms, where verification cost takes 4.4 ms and generation cost consumes 3.05 ms. The comparison of the proposed method with existing schemes is shown in Table 4. The results show that the proposed model takes less time to complete the authentication process, which signifies better performance.

![Image](image.png)

**Table 3.** Computational Cost of the Proposed Algorithms

| Algorithms          | Average Computational Cost |
|---------------------|----------------------------|
| Deployment          | 17.80 ms                   |
| Energy Trading      | 7.20 ms                    |
| Incentive-Punishment| 6.08 ms                    |
| Validators’ Selection| 9.01 ms                    |

Fig. 2 depicts the experimental results of the existing model [4] and the proposed model in terms of computational cost. From the results, it is observed that the computational cost of the proposed model is lower than the existing model. This depicts that the proposed model is better than the existing model. The reason is that in the proposed model, complex encryption techniques and time consuming signatures are not used. Moreover, multi-signature is not used for the validation of the energy transactions, which makes the model computationally cost efficient.
TABLE 4. Comparison of Computational Cost between the Proposed Scheme and the Existing Schemes for Authentication Process

| Schemes          | Computational Cost |
|------------------|--------------------|
| Scheme 1 [35]    | 2098.112 ms        |
| Scheme 2 [43]    | 13.4 ms            |
| Scheme 3 [4]     | 42.7 ms            |
| Proposed Scheme  | 7.45 ms            |

FIGURE 2. Comparison of the Overall Computational Cost between the Proposed Scheme and the Blockchain based Scheme

2) Communication Cost
The communication cost is computed by assuming the following parameters. \( R_B = R_s = 160 \text{ bits}, CRF_{B_i} = CRF_{S_i} = 160 \text{ bits}, sign = sig = 120 \text{ bits}, O_i = x_i = 120 \text{ bits}, \) and \( T_B = T_S = 16 \text{ bits}. \) The two messages communicated between \( B_i \) and \( S_i \) during the mutual authentication are \((R_s|sign|O_i|CRF_{S_i}|T_S) \) and \((R_B|sign|x_i|CRF_{B_i}|T_B). \) Conclusively, the communication cost of the proposed scheme is \(160+160+120+120+16+160+160+120+120+16 = 1152 \text{ bits}. \) The comparison of computational cost of the proposed and existing schemes is shown in in Fig. 3b. As shown in the figure, the communication cost of the proposed scheme is lower than Schemes 1, 2 and 3, which implies that the proposed scheme is better.

B. RESULT FOR THE INCENTIVE-PUNISHMENT SCHEME
In this section, we discuss the impact of the monetary incentive in the proposed system. From Fig. 3c, it is observed that the incentive or reward for each non-malicious transaction increases for the energy prosumer. The increase is because, for each non-malicious transaction, an energy prosumer is given an incentive. Therefore, as the number of non-malicious transaction increases, the reward increases. On the other hand, for a malicious transaction, it is also shown that the incentive given to the energy user remains zero (0) for all of the time slots. The reason is that for each malicious transaction, an energy prosumer does not receive any incentive. Therefore, the reward will remain zero for all of the time slots provided that a non-malicious transaction is not performed. The reward given in this model is in the form of digital coins, which can also be used to buy energy. The purpose of this approach is to motivate prosumers to participate and contribute more energy in the system without involving in malicious activities. Fig. 3d shows the impact of energy contributed to the proposed reward. The result shows that an increase in energy contribution increases the rewards in the proposed system. This encourages users to contribute more energy to the system. It helps to balance the community energy as well as to get incentives as a validator. It also helps to increase the availability of energy, which leads to energy price reduction in the proposed system.

C. RESULT FOR THE PROPOSED CONSENSUS AND VALIDATORS’ SELECTION MECHANISM
Figs. 4a, 4b, and 4c show the impact of \( Norm_g, Sc, \) and \( er, \) on the validators’ selection factor. From the results shown in Fig. 4a, it is observed that when the \( Norm_g \) increases, the selection factor increases as well. It is because there exists a direct relation between both parameters. Similarly, in Fig. 4b, increase in \( Sc \), increases the selector factor. Furthermore, the results in Fig. 4c show that when the \( er \) increases, the selection factor decreases, which improves the system’s performance by not allowing inefficient and erroneous users (i.e., users with high \( er \)) to be part of the consensus process. The reason is that \( Sc \) is the success rate for a user when performing a valid transaction. Therefore, when the rate of success increases, the reputation value increases, which increases the chances of the user to be selected as a validator. On the other hand, the value of \( er \) increases, which means that the user performs a dubious or erroneous transaction as it is defined as the rate of failure for a user to execute a valid transaction. Therefore, it can lead to a decrease in the users’ reputation value and as a result the chances of the user to be selected as a validator decreases. In conclusion, these parameters allow the system to pick validators that will perform consensus process with no or minimum errors. The fundamental principle behind selecting the validator based on these parameters is to eliminate inefficient users as validators. To verify the effectiveness of the \( R_v \) algorithm in this model, we use the list of the temporarily selected nodes. We trace how these nodes are further selected based on the proposed Algorithm 4. The experiment is conducted for a different number of temporary validators. The comparison between the existing consensus mechanisms and the proposed consensus mechanism in terms of validator nodes’ selection is shown in Fig. 4d. As shown in the figure, it is observed that the proposed \( R_v \) based selection scheme efficiently reduces the number of validators. It also helps the proposed consensus mechanism to be executed in a short time and with less number of malicious validators. In the proposed scheme, 66.67% of the validators are selected to conduct the consensus for every transaction. The consensus process is assumed to have very few malicious users if not
FIGURE 3. (a) Relationship Between the Proposed Prices with Compensation and SDR. (b) Comparison of Communication Cost between the Proposed Scheme and Others for Authentication Process. (c) The Impact of Rewards on Malicious and Non-malicious Activities. (d) The Impact of Energy Contribution in the Proposed Reward

D. RESULTS FOR THE PROPOSED PRICING SCHEME

In this research work, we use the Waterloo North Hydro’s grid prices for Time-of-Use (ToU) pricing scheme [42] as a benchmark scheme. The benchmark scheme is used to formulate the proposed pricing scheme in the trading system. From Fig. 5a, the number of selling and buying prosumers are observed to be the same in the proposed trading scenario when \( SDR(t) = 1 \) (i.e., \( TPB(t) = TPS(t) \)). In this case, the energy is stable in the scenario. It is stable because the proposed \( TPB(t) \) is equal to \( TPS(t) \). Furthermore, the proposed prices are equal to the grid prices along with the compensation price \( P_{selln}(t) = P_{buyn}(t) = \mu_{sell}(t) + \mu \). As shown in Fig. 5b, there is no available selling energy selling in the proposed market when \( SDR(t) = 0 \). Thus, buying prosumers purchase energy using \( \mu_{buy}(t) \) from the power grid. In this case, the selling and buying prices are the same as the grid’s buying price \( P_{selln}(t) = P_{buyn}(t) = \mu_{buy}(t) \). To ensure that the prosumers are better remunerated, \( \mu \) is presented, which ensures that the buying and selling prices are not equal when \( SDR(t) > 1 \) as shown in Fig. 5c and it gives more financial gain to the Ss than the Bs. Based on Equations (1) and (2), the selling and buying prices change, when \( 0 < SDR(t) < 1 \), which are shown in Fig. 5d. To encourage energy prosumers to participate in the system, the selling and buying prices must not be more
than grid’s selling price and must be less than grid’s buying price, respectively. \( SDR(tt) \) determines the prices for energy trading at each time slot based on SDR values, Equations (1), and (2). As shown in Figs. 5a, 5b, 5c, and 5d, it is observed that selling and buying prices in the trading system change when SDR changes. On the other hand, adjusting the energy consumption pattern will enhance SDR value, which will further improve the prices. Using the proposed pricing scheme, energy prices are determined without the involvement of third parties. Moreover, the problem with the usage of fixed pricing scheme, which is both non-beneficial and inefficient for energy users, is solved. The proposed scheme also deals with the issue of energy price determination, which occurs due to negotiation and auction mechanisms. These mechanisms become complex and time consuming when the number of users increases. Moreover, the mechanisms use the arbitrators, which causes trust and privacy issues. In this case, an arbitrator is someone who manages the system.

### E. PRIVACY AND SECURITY ANALYSIS

The privacy and security analysis of the proposed system is explained in this section.

1) Impersonation

Mutual authentication of users is implemented to prevent the proposed system from users’ impersonation attack. The authentication is conducted using anonymous certificate and signature. However, Agr can trace users’ identities if a dubious activity is detected. This process provides information integrity during authentication. In the authentication method, the digital signature and certificate are generated using a one-time private key, which is only known to the user. It becomes inactive after the authentication is completed. Therefore, linkability attacks, privacy leakages, and revealing senders’ sources are not possible in the system.

An attacker cannot leak information or intercept data between the senders’ and the receivers’ nodes within the blockchain to change the content of the message. Information
leakage occurs when information is revealed to other users or unauthorized parties in the system. This is possible if the system is not secured and is monitored for vulnerabilities. This kind of attack is called the passive attack. On the other hand, when the information is modified by unauthorized users, then it is known as an active attack. To protect transactional data from passive and active attacks, an inbuilt blockchain based encryption and decryption technique is applied.

2) Transaction Data Validation and Anonymity

In the proposed consensus mechanism, validator nodes verify and authenticate every transaction that is conducted publicly. It is recalled that the validators’ selection algorithm is used to remove malicious and inefficient nodes before the consensus process takes place. Therefore, it is also assumed that the validators list may consist of minimum number of malicious nodes during the consensus process, which will is not possible for the malicious nodes to control the network by having more than 51% nodes. During the energy trading, a one-time public key is used to prevent malicious nodes from tracing the real identity of the legitimate nodes. Afterwards, the keys become inactive to avoid a linking attack. Furthermore, contract theory and SDR mechanisms are used to prevent energy nodes from knowing the actual energy consumption patterns of other energy nodes.

3) Integrity and Transparency

As the blockchain network is an open system and each user involved can have access to the network. Therefore, users can track every transaction made in the network. Also, the transaction’s information is stored across the network’s nodes in a transparent manner. However, any information modification performed by the adversary is noticeable and traceable.

The hash value of each block is placed in the previous block after adding a new block to the blockchain network. The linkage of the hash value prevents malicious users from tampering the blocks without controlling more than 50% of the network’s nodes. In this case, it is impossible to control system because the network contains very few malicious
users as validators. Also, asymmetric encryption algorithms are used to encrypt the information of the nodes. This operation takes a massive computational cost and a long period to turn an encrypted information into a plain-text without using the private encryption key.

VII. CONCLUSION AND FUTURE WORK

In this study, a two-layered P2P secure energy trading model using the blockchain network and cloud aggregator is proposed. The layers are authentication and secure energy trading. A new consensus process is implemented in the model to minimize the number of malicious users. Afterwards, an incentive-punishment algorithm is presented to motivate energy prosumers to contribute more energy in the system. Furthermore, a contract theory based SDR pricing mechanism is proposed to solve the issues related to auction, fixed, and negotiation pricing schemes. In addition, the proposed pricing mechanism helps to hide the actual energy consumption patterns of the users. The main purpose of implementing the system in real-time environment is to have an efficient and secure energy trading platform. The simulation results for the authentication process show 7.45 ms and 1152 bits in terms of computational and communication cost, respectively. The results obtained are better than existing works [4], [35], [43]. During the consensus process, 66.67% of the validators are chosen to execute the consensus process for each transaction. This selection process efficiently improves the consensus mechanism and reduces the number of malicious validators. Also, the proposed system shows better performance in terms of security, privacy, and trust. Due to the inclusion of an additional authentication mechanism, computational cost increases, which is the tradeoff of the proposed model.

In the future, more complicated models will be explored and powerful techniques will be used to achieve good results for energy trading. Many problems need to be addressed in the near future to provide distributed energy exchange. Even though distributed and decentralized models give a better scalability than centralized schemes, studies and real assessment are required to evaluate systems that are based on blockchain. Another issue that is not fully resolved is the preservation of privacy based on blockchain schemes. Therefore, solutions are urgently needed to ensure privacy of users. Furthermore, blockchain standardization and interoperability issues are to be investigated. In terms of energy trading using blockchain, research is required that will assess the impact of many market schemes and auction mechanisms based on power losses and technical constraints in the distributed platforms.

ACKNOWLEDGEMENT

This work was supported by King Saud University, Riyadh, Saudi Arabia, through Researchers Supporting Project number RSP-2021/184. The work of author Ayman Radwan was supported by FCT / MEC through Programa Operacional Regional do Centro and by the European Union through the European Social Fund (ESF) under Investigator FCT Grant (5G-AHEAD IF/FCT- IF/01393/2015/CP1310/CT0002).

REFERENCES

[1] Okoye, Martin Onyeka, Junyong Yang, Jia Cui, Zhenjiang Lei, Jingwei Yuan, Huixin Wang, Huichao Ji, Jiawei Feng, and Chimenye Ezeb. “A blockchain-enhanced transaction model for microgrid energy trading.” IEEE Access 8 (2020): 143777-143786.
[2] Shahid, Affaf, Ahmad Almogren, Nadeem Javid, Fahad Ahmad Al-Zahrani, Mansour Znait, and Masoum Alam. “Blockchain-based agri-food supply chain: a complete solution.” IEEE Access 8 (2020): 69230-69243.
[3] Li, Jianan, Zhenyu Zhou, Jun Wu, Jianhua Li, Shahid Mumtaz, Xi Lin, Haris Gacanim, and Sattam Alootaibi. “Decentralized on-demand energy supply for blockchain in Internet of Things: A microgrids approach.” IEEE Transactions on Computational Social Systems 6, no. 6 (2019): 1395-1406.
[4] Li, Meng, Donghui Hu, Chhagan Lal, Mauro Conti, and Zijian Zhang. “Blockchain-enabled secure energy trading with verifiable fairness in industrial Internet of Things.” IEEE Transactions on Industrial Informatics 20 (2020): 1-11.
[5] Jindal, Anish, Gagandeep Singh Singh Aujla, Neeraj Kumar, and Mas-simo Villari. “GUARDIAN: Blockchain-based secure demand response management in smart grid system.” in IEEE Transactions on Services Computing, vol. 13, no. 4 (2020): 613-624.
[6] Wang, Wenbo, Dinh Thai Hoang, Peizhao Hu, Zhehui Xiong, Dusit Niyato, Ping Wang, Yonggang Wen, and Dong In Kim. “A survey on consensus mechanisms and mining strategy management in blockchain networks.” IEEE Access 7 (2019): 22328-22370.
[7] Saxena, Neetesh, Santiago Grijalva, Victor Chukwuka, and Athanasios V. Vasilakos. “Network security and privacy challenges in smart vehicle-to-grid.” IEEE Wireless Communications 24, no. 4 (2017): 88-98.
[8] Pu, Yuwen, Tao Xiang, Chunqiang Hu, Arwa Albawai, and Hongyang Yan. “An efficient blockchain-based privacy preserving scheme for vehicular social networks.” Information Sciences (2020): 1-18.
[9] Kudva, Somway, Shahriar Radshah, Shamik Sengupta, Ibrahim Khalil, and Albert Zomaya. “Towards secure and practical consensus for blockchain based VANET.” Information Sciences (2020): 48576-48586.
[10] Park, Sangdon, Jooyoung Lee, Sohee Bae, Ganguk Hwang, and Jun Kyun Choi. “Contribution-based energy-trading mechanism in microgrids for future smart grid: A game theoretic approach.” IEEE Transactions on Industrial Electronics 63, no. 7 (2016): 4255-4265.
[11] Dorri, Ali, Fengji Luo, Saül S. Kanhere, Raja Jurdak, and Zhao Yang Dong. “SPB: A secure private blockchain-based solution for distributed energy trading.” IEEE Communications Magazine 57, no. 7 (2019): 120-126.
[12] Esposito, Christian, Alfredo De Santis, Genny Tortora, Henry Chang, and Kim-Kwang Raymond Choo. “Blockchain: A panacea for healthcare cloud-based data security and privacy?” IEEE Cloud Computing 5, no. 1 (2018): 31-37.
[13] Zhang, Rongqing, Xiang Cheng, and Liqing Yang. “Energy management framework for electric vehicles in the smart grid: A three-party game.” IEEE Communications Magazine 54, no. 12 (2016): 93-101.
[14] Aitzhan, Nurlan Zhumbakuly, 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.
[15] Gao, Jianbin, Kwame Omon Omah, Juma Juma Luo, Emmanuel Boateng Sifah, Abila Smahi, Xia Xia, Xiaosong Zhang, and Guishan Dong. “Gridmonitoring: Secured sovereign blockchain based monitoring on smart grid.” IEEE Access 6 (2018): 9917-9925.
[16] Mikhaelov, Mihail, Sergio Jurado, Narces Avellana, Kristof Van Moffaert, Albert Zomaya. “Towards secure and practical consensus for blockchain enabled V2G network.” IEEE Transactions on Industrial Informatics 15, no. 6 (2019): 3548-3558.
[19] Guan, Zhtiao, Xin Lu, Naiyu Wang, Jun Wu, Xiaojiang Du, and Mohsen Guizani. “Towards secure and efficient energy trading in IoT-enabled energy internet: A blockchain-based approach.” Future Generation Computer Systems 110 (2020): 680-695.

[20] Hayes, Barry P., Subhasis Thakur, and John G. Breslin. “Co-simulation of electricity distribution networks and peer to peer energy trading platforms.” International Journal of Electrical Power & Energy Systems 115 (2020): 1-10.

[21] Han, Dong, Chenguanghao Zhang, Jian Ping, and Zheng Yan. “Smart contract architecture for decentralized energy trading and management on blockchain.” Energy (2020): 1-14.

[22] Unmoren, Ifok Anthony, Syeda SA Jaffary, Muhammad Zeeshan Shakir, Konstantinos Katzis, and Hamed Ahmadi. “Blockchain-based energy trading in electric vehicle enabled microgrids.” IEEE Consumer Electronics Magazine, vol. 9, no. 6 (2020): 66-71.

[23] Yang, Jiawei, Amrit Paudel, and Hoay Beng Gooi. “Compensation for power loss by a Proof-of-Stake consortium blockchain microgrid.” IEEE Transactions on Industrial Informatics (2020): 1-10.

[24] Mengelkamp, Esther, Johannes Gartner, Kerstin Rock, Scott Kessler, Lawrence Orsini, and Christof Weinhardt. “Designing microgrid energy markets: A case study: The Brooklyn Microgrid.” Applied Energy 210 (2018): 880-889.

[25] Kang, Jiawen, Rong Yu, Xumin Huang, Sabita Maharjan, Yan Zhang, and Ekram Hossain. “Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains.” IEEE Transactions on Industrial Informatics 13, no. 6 (2017): 3154-3164.

[26] 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. 1 (2019): 2672-2673.

[27] Yahaya, Adamu Sani, Nadeem Javaid, Muhammad Umar Javed, Muhammad Shahiq, Waiz Zada Khan, and Mohammed Y. Aalsalem. “Blockchain-based energy trading and load balancing using contract theory and reputation in a smart community.” IEEE Access 8 (2020): 222168-222186.

[28] Li, Zhefao, Jiawen Kang, Rong Yu, Dongdong Ye, Qingyong Deng, and Yan Zhang. “Consortium blockchain for secure energy trading in internet of things.” IEEE transactions on industrial informatics 14, no. 8 (2017): 3690-3700.

[29] Jindal, Anish, Gaganjeet Singh Aujla, and Narej 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.

[30] Zhou, Zheyu, 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.

[31] Park, Lee Won, Sanghoon Lee, and Hangbae Chang. “A sustainable home energy prosumer-chain methodology with energy tags over the blockchain.” Sustainability 10, no. 3 (2018): 658.

[32] Samuel, Omaji, and Nadeem Javaid. “A secure blockchain-based demurrage mechanism for energy trading in smart communities.” International Journal of Energy Research 45, no. 1 (2021): 297-315.

[33] Son, Ye-Byoul, Jong-Hyuk Im, Hee-Yong Kwon, Seong-Yun Jeon, and Mun-Kyu Lee. “Privacy-preserving peer-to-peer energy trading in blockchain-enabled smart grids using functional encryption.” Energies 13, no. 6 (2020): 1321.

[34] Jegadesan, Subramani, Maria Azees, N. Ramesh Babu, Unanakshar Subramaniam, and J. Dhaffer Almahkales. “EPAW: efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs).” IEEE Access 8 (2020): 48576-48586.

[35] Umar, Mubarak, Zhenqiang Wu, and Xuening Liao. “Mutual authentication in body area networks using signal propagation characteristics.” IEEE Access 8 (2020): 66411-66422.

[36] Jiang, Zhiping, Kun Zhao, Rui Li, Jizhong Zhao, and Junzhuo Du. “PHYAlert: identity spoofing attack detection and prevention for a wireless edge network.” Journal of Cloud Computing 9, no. 1 (2020): 1-13.

[37] Lin, Chao, Debiao He, Neeraj Kumar, Xinyi Huang, Pandi Vijayakumar, and Kim-Kwang Raymond Choo. “HomeChain: a blockchain-based secure mutual authentication system for smart homes.” IEEE Internet of Things Journal 7, no. 2 (2019): 818-829.

[38] Zhou, Zheyu, Bingchen Wang, Yuefei 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.

[39] Yahaya, Adamu Sani, Nadeem Javaid, Fahad A. Alzahrani, Amjad Rehman, Ibrah Ullah, Affaf Shahid, and Muhammad Shahiq. “Blockchain based sustainable local energy trading considering home energy management and demurrage mechanism.” Sustainability 12, no. 8 (2020): 1-28.

[40] Samuel, Omaji, Sakeena Javaid, Nadeem Javaid, Syed Hassan Ahmed, Muhammad Khalil Afzal, and Farruh Ishmanov. “An efficient power scheduling in smart homes using Jaya based optimization with time-of-use and critical peak pricing schemes.” Energies 11, no. 11 (2018): 3155.

[41] Wang, Yong, Zhe Song, and Tong Cheng. “Improvement research of PBFT consensus algorithm based on credit.” In International Conference on Blockchain and Trustworthy Systems, Springer, Singapore (2020): 47-59.

[42] Waterloo North Hydro’s grid prices 2020. Available online:https://www.wnhydro.com/en/your-home/time-of-use-rates.asp (accessed on 7 September 2020).

[43] Gong, Zheng, Yu Long, Xuan Hong, and Kefei Chen. “Two certificateless aggregate signatures from bilinear maps.” In Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007), vol. 3, (2007): 188-193.
AHMAD ALMOGREN (SM) received the Ph.D. degree in computer science from Southern Methodist University, Dallas, TX, USA, in 2002. He is currently a Professor with the Computer Science Department, College of Computer and Information Sciences (CCIS), King Saud University (KSU), Riyadh, Saudi Arabia, where he is currently the Director of the Cyber Security Chair, CCIS. Previously, he worked as the Vice Dean of the Development and Quality at CCIS. He also served as the Dean for the College of Computer and Information Sciences and the Head of the Academic Accreditation Council, Al Yamamah University. He served as the General Chair for the IEEE Smart World Symposium and a Technical Program Committee member of numerous international conferences/workshops, such as IEEE CCNC, ACM BodyNets, and IEEE HPCC. His research interests include mobile-pervasive computing and cyber security.

ABRAR AHMED received the B.S. degree in computer engineering from COMSATS University Islamabad, (Formerly, COMSATS Institute of Information Technology) Pakistan, in 2006, the M.S. degree from Lancaster University, U.K., in 2008, and the Ph.D. degree in electrical engineering from COMSATS University Islamabad, in 2017. Since 2006, he has been associated with COMSATS University Islamabad, where he currently holds the position of an Assistant Professor. His research interests include wireless channel modelling and characterizing, smart antenna systems, nonorthogonal multiple access techniques, and adaptive signal processing.

SARDAR MUHAMMAD GULFAM received his master’s degree from Tampere University of Technology Finland in 2010. He received his PhD degree in 2017 from COMSATS University Islamabad. Currently, he is working as an Assistant professor in the Department of Electric and Computer Engineering, COMSATS University Islamabad, Islamabad Pakistan.

AYMAN RADWAN received the Ph.D. degree from Queen’s University, Kingston, ON, Canada, in 2009. He is a Senior Research Engineer (Investigador Auxiliar) with the Instituto de Telecomunicações, University of Aveiro, Aveiro, Portugal. He is mainly specialized in coordination and management of EU funded projects. He participated in the coordination of multiple EU projects. He is currently the Project Coordinator of the CELTIC+ Project “MUSCLES,” as well as participating in the coordination of ITN-SECRET. He has also been the Technical Manager of the FP7-C2POWER Project and the Coordinator of the CELTIC+ “GreenT” Project. His current research interests include the Internet of Things, 5G, and green communications.