A Blockchain based Framework for Secure and Decentralized Energy Trading in a Community

Saurabh Sachdeva
Department of Electrical Engineering
City University of New York, City College of New York, New York, NY, USA, 10031
ssachde000@citymail.cuny.edu

Latif Fatehaj
Department of Electrical Engineering
City University of New York, City College of New York, New York, NY, USA, 10031
lfetaha000@citymail.cuny.edu

Stefan Tan
Department of Electrical Engineering
City University of New York, City College of New York, New York, NY, USA, 10031
stan002@citymail.cuny.edu

Joel James
Department of Electrical Engineering
City University of New York, City College of New York, New York, NY, USA, 10031
jjames003@citymail.cuny.edu

Oluwaseyi Ajayi
Department of Computer Engineering
Vaughn College
Flushing, New York, NY, USA,11369
oluwaseyi.ajayi@vaughn.edu

Tarek Saadawi
Department of Electrical Engineering
City University of New York, City College of New York, New York, NY, USA, 10031
saadawi@ccny.cuny.edu

***Abstract*— Blockchain is a decentralized, digital, and distributed ledger which allows transparent and secure information sharing among the peer-to-peer network. It eliminates the need for a centralized trusted party and, though it was introduced as the backbone technology for cryptocurrencies but has proved to be a promising and revolutionary technology for almost all global industries. The application of blockchain technology in the energy sector proposes a paradigm of solutions to problems of different levels of complexity in the traditional energy ecosystem. Extensive research has been proposed to exploit the inherent benefits of blockchain technology for the integration of distributed energy sources and facilitate peer-to-peer energy trading. This paper proposes a blockchain-based architecture to facilitate secure and decentralized energy trading generated from renewable energy sources. The solution utilizes the Ethereum blockchain and Smart Contracts for energy trading among the members of a small community without any trusted third entity and adopts features to achieve data integrity and confidentiality, and user identity privacy.**

***Keywords*— Blockchain, Energy Trading framework, smart contract, local energy market.**

I. INTRODUCTION

With the world getting more and more connected every day, there is an ever-increasing threat of acts of cyberwarfare, cyberterrorism, and cybercrime which pose a huge security risk. Incidents of cyber-attacks in the past on critical infrastructure have exposed security concerns and have stressed the need to make them more and more resilient to any kind of cyberattacks [1]. Considering the above facts, steps should be taken to accelerate adaptation to reduce the adverse impacts of climate change and any kind of cyber-threats. Moreover, the demand for the reduction of greenhouse gas emissions and for clean energy sources led the proposed energy solutions focused on renewable energy sources like solar, wind and, water. The possibility of low cost, small scale, and decentralized implementation of renewable energy sources such as solar and wind and increased tax and other forms of incentives from the governments on its usage, boosted its adoption throughout the world resulting in individual houses, community buildings or offices being equipped with solar panels or small wind turbines capable of meeting all or some of their energy demand. This led to the appearance of a new class of participants in the energy ecosystem called the prosumer – one who both produces and consumes electricity locally and has the capability to trade excess energy.

The emergence of prosumers provides an opportunity for the setup of a local energy market (LEM) where individual households with distributed energy resources (DERs) can produce, store, and trade energy as compared to the traditional centralized electricity generation and supply ecosystem which only allows for one-way flow of electricity from generation to the utility company to end user. Peer-to-peer(P2P) and decentralized energy trading (ET) can be implemented between the participants within or across microgrids. Several solutions based on the existing technologies have been proposed worldwide for the integration [2] of prosumers in the existing energy setup and to enable and support ET, but these solutions present the issues of centralization, data integrity, and confidentiality, user and anonymity, and transparency. The applications of blockchain technology have recently become fascinating for researchers because of its inherent benefits, such as immutability, enhanced security and traceability which offer solutions to some fundamental problems in smart grids and in the energy sector. This paper aims to exploit these advantages of blockchain technology and propose a blockchain-based framework for secure and P2P ET. The main objective of the proposed model is to enable consumers and prosumers in a small community, to securely trade electricity with each other in a P2P

fashion using blockchain technology without the intervention of a central trusted party to ensure trust. The significant contribution of this paper is the adoption of Ethereum smart contracts (SC) to empower parties to transmit a request for buying energy and float offers for selling energy anonymously throughout the auction process till the agreement is achieved. Moreover, using SC, the auction process is done by implementing multiple filters at different stages to ensure the buyer's energy requirements are met, and the best match is established, and the seller's profitability is maintained, addressing the issue of price imbalance in the local energy market. The management of transactions and verification of identities is done by the network without the involvement of any external trusted mediator. These features, with a detailed description of the auction process, make our proposed approach and study innovative and novel compared to other solutions presented in the research literature.

The remainder of our paper is structured as follows. Section II elaborates on the problem statement and motivation. Section III presents related work and background. The proposed framework is illustrated in section IV, and section V explains the implementation of the proposed architecture. In Section VI, we present the discussion and analysis of the aspects of our proposed framework, and in Section VII, we draw our conclusion.

II. Problem Statement and Motivation

Due to increased energy demand worldwide, traditional energy generation and distribution systems have been facing issues, such as shortage of supply, long-distance transmission losses, and most notably global warming. Increased adoption of power generated from renewable energy sources is being implemented as one of the prominent solutions to save future generations from the havoc of climate change, and governments around the globe are adopting various policies and methods to encourage the production and usage of clean energy [3]. In a smart community, as the number of users who adopt the DERs generators increases, ET becomes essential. Several works of literature have proposed the application of blockchain technology for ET in smart grids and their management. These researchers propose various methods or frameworks to implement ET among the users within or across microgrids, but many important issues have been either partially addressed or left untouched. The issues such as security, privacy, and the absence of proper pricing mechanisms are some of the many vital concerns which have not been fully resolved [4].

ET among the participants connected via a microgrid for energy transfer and distribution within an intelligent community involves several steps. The process begins with consumers requesting energy, and in response different prosumers float the energy selling offers to match the received request and then the most suitable offer is chosen, the system requires to adopt measures to preserve the privacy of identity and confidentiality of data at every step. For the auction to be transparent, competitive, and fair, it is crucial that the anonymity and privacy of the participants are maintained from the beginning through the end of the process. This ensures that the winner is decided strictly per the requirements and rules set before the auction process and that the auction is fair.

Also, during the auction process, upon receipt of the request from the consumers to buy energy, prosumers send their bids, each prosumer quotes a different price independent of the other sellers. Thus, in a scenario where all the sellers decide to quote high prices or when there are not enough sellers in the community, there could be a price imbalance, and consumers may end up paying high electricity prices. Several solutions have been proposed in academic literature to address these concerns. The researchers in [5] proposed a solution to fix the market price for all energy consumers. This method may benefit the buyer but does not encourage the prosumer to join ET, as grid energy prices are 0.7 times more than those in LEM. In [6] authors propose a framework where the double auction closed book technique is applied to decide the trading price. Although the proposed solution reduces the consumer's energy cost, again does not address the concern of energy price imbalance in the LEM as each seller quotes a different electricity price. At the same time, too much regulation of energy prices would not allow prosumers to earn profits and thus may discourage other community members from implementing DERs and joining the ET framework.

Motivated to propose a framework based on blockchain to enable secure ET among the members of a smart community where privacy, data integrity, and confidentiality is preserved, and the energy prices are justified for both buyers and sellers, we decided to propose a blockchain-based framework for decentralized and secure ET in a community connected via a microgrid with users producing energy using renewable energy generators. Our paper makes the following significant contributions:

- A blockchain-based framework is presented for secure and decentralized energy trading among members of a small community or town focusing on distributed energy generation.
- A detailed description of the smart contract-enabled auction process, which allows parties to securely perform energy trading without the intervention of a trusted centralized entity.
- Our proposed framework addresses the issues of data integrity and data confidentiality, user identity management, and privacy and scalability.
- The proposed framework adopts filters at different steps during the auction to address the issue of energy cost imbalance and the prosumer's profitability. We propose the setup of an open and free local energy market with some minor justified regulations.

III. Related Work and Background

With the increasing use of DERs, there has been a lot of research and industrial projects [2] – [3] to integrate the new players in the traditional centralized energy ecosystem and optimize the energy generated from these renewable sources being transferred back into the power grids. In study [7], researchers evaluate the energy and cost savings of the prosumer if he can produce and transfer back his excess energy in the

national grid. The simulation results in the manuscript show that the prosumer benefits in terms of cost, and his usage of the national grid is reduced. However, such a system requires complex management and implementation, leaving many security and privacy concerns. As researchers studied more about emerging blockchain technology, they realized that the inherent benefits of blockchain technology could be used to solve these issues; hence much of research has been done in this area.

In this survey paper [8] authors provide an overview of the application of blockchain technology in smart grid. They outline the primary requirements of a modern smart grid to integrate the decentralized energy resources and different IoT devices, summarize the security, trust, and privacy issues in a smart grid and suggest how blockchain technology can solve some of these challenges. They also presented a detailed discussion about the future opportunities of blockchain in smart grids, its limitations and drawbacks, and how it can address some global challenges our energy systems have been facing. At last, they summarized some blockchain-based practical projects and trials such as SolarCoin, Energy Web Foundation, Power Ledger, etc. [9] – [11], which are being conducted globally to establish the advantages of blockchain technology in the energy sector.

In [12] authors propose an architecture for P2P ET in a microgrid where participants can trade with each other via a smart management system. Using an aggregator for better energy management, they use Ethereum smart contract to perform the real-time ET within the local market. In [13], authors propose SynergyChain - a blockchain-based adaptive model which aims to assist the prosumers in grouping for enhanced scalability and profits. The focus of this paper is to propose a blockchain-assisted model – SynergyChain, which uses SC to create prosumer groups and processing transaction information. The authors also propose using reinforcement machine learning to improve the system performance and increase the prosumer profitability if he chooses to group with other prosumers during ET. In [14], the authors proposed a model to improve the load balance in a smart community by improving the efficiency of the consensus mechanism. The model uses a Proof of Work (PoW) consensus mechanism, which needs enormous computational cost, and so even if the model proposed results in improvement at the same time, it also leads to highcomputational and communicational costs.

Authors in [15], have addressed the issue of data integrity and confidentiality in smart grids. They propose a P2P blockchain-based ET architecture where all the bids are encrypted, and SC, by hiding the inner product encryption performs the matching on the bids. They also verified the feasibility of the proposed system by a prototype implementation that involves smart meters, a distribution system operator (DSO), a server, and a private Ethereum blockchain. The proposed solution involves a DSO, which acts as a trusted entity between the participants and the network, while on the other hand, our solution involves no central authority.

In [16] & [17], researchers propose a secure framework based on private Ethereum blockchain for ET, which allows only authorized participants in the system. In [17], the authors choose to do the negotiation part in the auction off-chain to reduce the computation. Although negotiating off-the-chain results in lesser computational cost, it does not guarantee that the bid satisfies all conditions as evaluated by SC in our proposed solution. In our framework, our SC accepts bids and applies multiple filters at different steps in the auction process to ensure that the bid satisfies all the conditions and security properties.

In study [18], the authors propose an Ethereum-based solution for secure ET, which does not involve any trusted party. The authors describe the auction process and the proposed solution to the issues of privacy, data confidentiality, and integrity. However, the solution does not discuss anything about the possible energy cost imbalance in the market. The solution allows users to float blind bids to prevent any participant from altering the bids but does not check during the bidding and offer stage whether the winning prosumer can supply the requested amount of energy and the selling cost quoted by the prosumers are not too high. The criteria on which the SC decides the best match are unclear keeps repeating the cycle if the awarded prosumer does not have the required energy to find the next prosumer with the available energy. This repetition of the cycle may lead to high computational costs. On the contrary, our solution not only accepts initial hashed offers but also applies multiple filters at different stages to ensure that bids satisfy both the amount of requested energy and the cost as quoted by the buyer and proposes the setup of free LEM with reasonable regulations implemented by the PRA.

IV. PROPOSED FRAMEWORK

In the proposed model, we consider the scenario of a small community inter-connected by a microgrid system. Some households of this community install roof-top Photo Voltaic(solar panels) or small wind-driven generators to meet some or all of their energy needs. Figure 1 illustrates our proposed architecture which uses Ethereum blockchain smart contracts to perform secure ET in a P2P fashion where the participants send the requests and the offers anonymously. The identity of the participants is not revealed until the auction result in terms of the best match has been received. Our proposed architecture consists of the following actors:

- Prosumers - the entity which locally generates electricity for its personal use and stores the excess energy for trading.
- Consumers – an entity that buys electricity for its consumption.
- Power Regulatory Authority (PRA) – The entity which deploys the smart contract and monitors the entire system. Based on various factors such as setup and production costs, inflation etc., it fixes the minimum offer price P_k a seller should get for per unit of energy.

All the participants are equipped with smart meters and batteries to store excess energy for trading or future personal use. The smart meter being an IoT device, becomes a vital link that connects the participant to the smart grid infrastructure. We consider using a smart meter that can connect to and interact with the Ethereum blockchain and has an Ethereum address associated with it. Smart meters are used to keep a record of the amount of energy generated, consumed, and traded by each user.

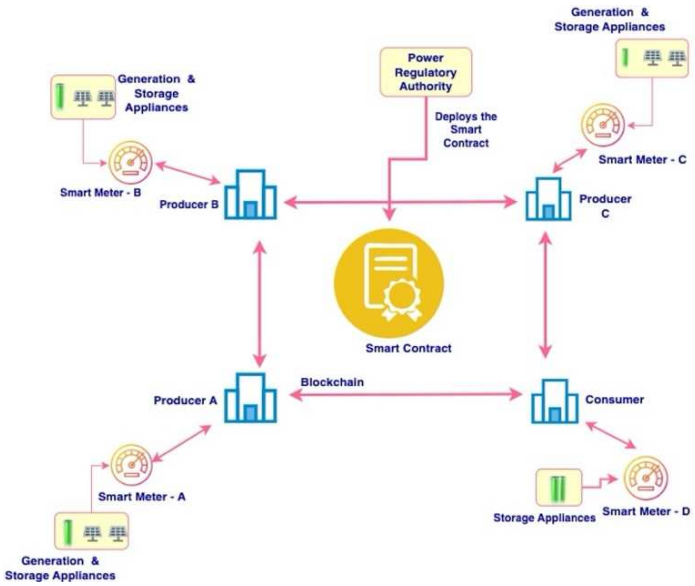

Figure 1. Proposed architecture for Blockchain based secure P2P Energy Trading

Any prosumer can do the following three actions during the ET process: buy energy, sell energy, or do not participate. During an auction and trading process, each prosumer is allowed to act only in one of these three roles as per its energy requirements and status. Here, for this study, we consider a small community where prosumers are small-scale generators. Thus, fixing a minimum offer price P_k by PRA ensures that prosumers at least make decent profits, and this also promotes healthy competition in the market and encourages other households to become prosumers and participate in local ET. Our proposed model applies checks at different stages during the auction so that the buyers do not quote unexplained low buy prices while, at the same time, the sellers do not quote unexplained high selling prices, thereby creating a cost and profitability imbalance in the market. Thus, we propose the setup of a free energy LEM with some justified regulations to safeguard both consumers and prosumers interests.

V. IMPLEMENTATION

In this section, we explain the implementation of our proposed architecture and describe step by step the Ethereum SC that performs ET and provides required functionalities. For our SC development, we used Remix as Integrated Development Environment (IDE) [19] and Meta-Mask as a browser extension for Decentralized Applications(dApps). The SC was written in Solidity [20 language,a prominent language for the development of SC on Ethereum. Table 1 below mentions the nomenclature of the different quantities used during the auction and ET process. Our implementation consists of the following steps:

Table 1- Nomenclature of the different quantities used in the auction.

Name	Description
P_k	Minimum Offer Price per unit of energy which prosumer should receive during energy trading. Fixed by PRA
E_a	Amount of Energy required by the consumer (KWh)
P_m	Maximum price per unit of energy which the buyer is willing to pay.
U_{vb}	Buyer Unique Value
reqID	Unique Id Number generated by SC for all the requests which satisfy the initial criteria.
E_s	Amount of Energy available with seller for trading(kWh)
P_s	Selling Price per unit of energy as quoted by seller
U_{vs}	Seller Unique Value
ofrID	Unique Id number generated by SC for each offer/bid which passes the first filter.

A. *System Initialization, Registration and Authentication*

The PRA deploys the SC on the Ethereum blockchain and all the energy community members (prosumers and consumers) must register with the PRA with their Ethereum address to receive their credentials. In the proposed model, we assume that the microgrid is private and is managed by the local prosumers connected to it. During registration, each member is responsible for initiating the registration and authentication process to join the system. The credentials of each member consist of its unique ID(Uid) and the address ID of its smart meter (SMid). For authentication to join the blockchain and participate in the ET, they must enter the same information provided during PRA registration. If the information matches, the member is added as a verified member. The exact process for authentication is followed when a new member joins the community.

B. *Energy Request and Offers:*

This step is the first step of the ET. When a member of a community, based on his energy needs, decides to buy energy from other participants, it floats the energy request. The auction process starts as soon as a buyer initiates the request by calling the function reqEng() of the SC and gives as input parameters the following quantities – the amount of energy needed E_a, the maximum price per unit of electricity which buyer is willing to pay P_m, deadlines t_1 and t_2 which are used to guide the auction process and cryptographically hashed value H_a (U_{vb}) of a buyer

unique value U_{vb}. U_{vb} is essential and is the buyer's private key and needs to be remembered by the buyer as it shall be used to verify the buyer's identity once the auction is completed. As soon as the request is received, the checks to see that whether the maximum price the buyer is willing to pay should be greater than the minimum price per unit of energy fixed by the PRA ($Pm > P_k$). If this condition is not met, the SC rejects the request. If this condition is met, function reqEng(), uses $H_a(U_{vb})$ to generate a unique number Request Id(reqID) and creates an event to notify all the members about the request being received. By doing so, it associates this unique reqID with the buyer and who initiated the request. Therefore, each member who wants to participate in the auction can now view the attributes (E_a and P_m) associated with a particular reqID. Here, the use of ReqID masks the actual identity of the buyer who initiated the request and called the function of the SC.

Once all the blockchain members have been notified about the incoming energy request, the prosumers who have available excess energy and wish to participate here, referred to as sellers, will have access to the reqID and its attributes (E_a and P_m) and so accordingly can make an offer. The seller initiates the response to the reqID by submitting its initial offer and calling the function sellEng() of the SC and passing the following values as input parameters – amount of energy it has available to sell E_s, cryptographically hashed value $H_a(P_s)$ of desired price per unit of electricity P_s at which it is willing to sell and cryptographically hashed value $H_a(U_{vs})$ of seller unique value U_{vs}. Again, U_{vs} is essential and is the seller's private key who, uses it to compute the $H_a(U_{vs})$ and shall be used to verify the seller's identity. The first filter is applied when all the initial offers are received against a particular reqID. At this point, the function checks all the received offers to verify if the sellers can fulfill the consumer's demand in terms of the amount of energy needed ($E_s \geq E_a$). The sellers whose offers pass the first filters are only allowed to participate further in the auction process, and other sellers' offers are discarded. For all the successful sellers of the first filter, the function uses $H_a(U_{vs})$ to randomly generate a unique number offer ID(ofrID) for each prosumer. Thus, each seller and its offer are linked to a unique ofrID and are further identified by this unique number in the auction process. Figure 2 and Figure 3 illustrate the generation of reqID and OfrID, respectively by the SC.

Any prosumer who wants to submit an initial offer for an active reqID can do so by deadline t_1, and no new initial bids are accepted after this deadline. Once all the initial hashed bids have been received by the deadline t_1 and the first filter has been applied, all the successful prosumers receive a unique offerID and are only allowed to participate further in the auction. Now, since both the buyer and seller and their respective requirements and offers are represented as reqID and ofrId, respectively, thus this prevents them from revealing their actual identity and their requirements or offers. Any malicious actor or node in the system can take undue economic advantage or alter the auction if they are aware of the details of the bids various prosumers are planning to submit. Thus, our model provides privacy protection and data confidentiality by accepting initial offers as hashed

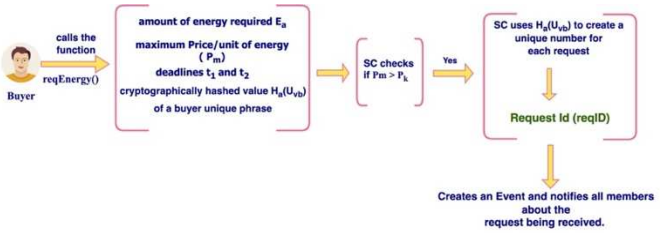

Figure 2- Consumer creates Energy Request.

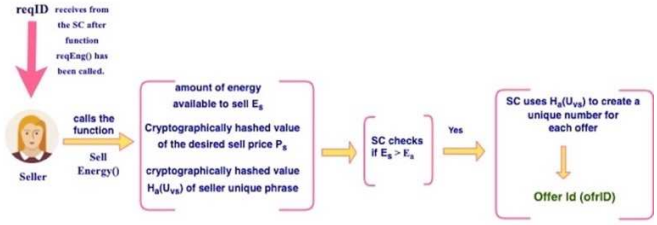

Figure 3- Prosumer responds to the Energy Request and floats the offer.

values without disclosing the identities of the parties submitting it.

C. *Energy Auction and Outcome*

All the sellers with the ofrID number after the deadline t_1, now send their offers in plain text by calling the function sendPlainOffer() of the SC and passing as input parameters the selling price P_s and U_{vs} in plain text to disclose the actual price. Now the 2nd filter is applied once all the actual bids in plain text have been submitted. During the second filter, the SC checks all the bids, each with a unique ofrID received against a particular reqID to verify the following: i) if the offered selling price is equal to or lower than the maximum price buyer is willing to pay ($Ps \leq P_m$) ii) hash value generated by combining the P_s in plain text with the U_{vs} matches the initial hashed offer submitted by the seller $P_{h..}$ The 2nd filter ensures that the sellers whose offers are included in the final auction process quote to sell energy at a price that is lower than or equal to the maximum price the buyer is willing to pay. This check ensures that the buyers do not overpay and encourages healthy competition among the sellers. The 2nd filter also verifies that the price submitted in plain text is the same as the one submitted during the initial offer by comparing the hash values. This verification ensures that no seller modifies the price based on the offer submitted by the other candidates and so cannot obtain any undue economic advantage or act as a malicious node and that the auction is fair, and that the integrity of the auction is maintained. All the candidates for whom both the above conditions are met are regarded as successful candidates of the 2nd filter and their P_s is pushed in a final sellers list L_s. The process of receiving the P_s and passing the offers through the 2nd filter is done till the deadline t_2 as prescribed initially by the buyer.

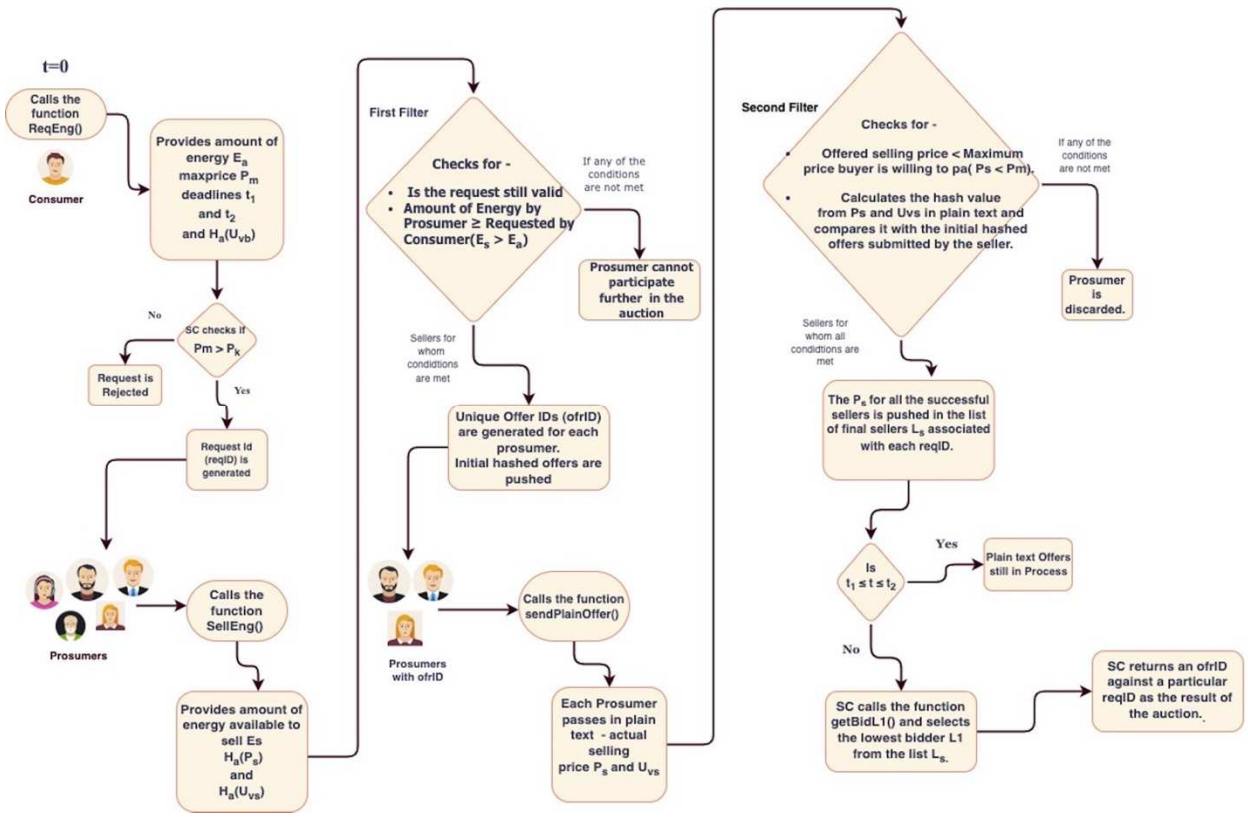

Figure 4-Step by Step Flow Diagram of the Proposed Auction Process

Once the deadline t_2 has passed, the getBidL1() function of the SC accepts a ReqID, and the list Ls associated with it, which contains the sellers' bids that passed both the filters and among whom the winner of the auction must be computed. Out of these offers received against a reqID, the SC now selects the lowest bidder L1 from the list L_s,i.e., the seller who quoted the lowest selling price P_s and the associated ofrID is returned as the winner of the auction. Hence, the SC returns an ofrID against a particular reqID as the result of the auction. This is last step of the auction, where both the buyer and the seller i.e., the consumer and the winning prosumer, must disclose and verify their identity. Algorithm 1 and Algorithm 2 are initiated for consumer identity verification and prosumer identity verification. Throughout the ET process, the buyer has been represented just by a number reqID and the seller by its ofrID, thus providing anonymity. Now, once the auction is complete, in order to disclose and verify its identity the consumer who is the buyer calls the function verifyConsumer() of the SC and passes its reqID and the U_{vb} as its input parameters. The SC generates the cryptographic hash using these inputs, which should match with the hash already liked to the reqID from the function reqEng(). If the match is successful, the function pushes the original Ethereum address (OEA) linked with the reqID that was used to call the function reqEng(). In other words, the identity of the consumer who requested for the energy is revealed. If the match does occur, the consumer's identity is not verified, and the process is repeated. The same procedure is adopted by the winning prosumer, i.e., the seller to disclose and verify its identity. The prosumer calls the function verifyProsumer() and passes the ofrID and the U_{vs} as input parameters. The function verifies the prosumer in the similar manner. Figure 4 demonstrates the step-by-step process of the proposed auction.

Algorithm 1: Consumer Identity Verification

Procedure: Consumer Verification
Inputs: Request Id(reqID), Buyer Unique Value (U_{vb})

```
Calls Verify Consumer (reqID, Uvb)
 Output Hash_Function
  Calls reqEng ()
  Output Initial_hash_Function
If Hash_Function matches Initial_hash_Function
      then
      Validate Consumer
      Return Consumer Verified
else
     Return error
       Consumer not Verified.
    endif
 end Procedure
```

Algorithm 2: Prosumer Identity Verification

Procedure: Prosumer Verification
Inputs: Offer Id(ofrID), Seller Unique Value (U_{vs})

```
Calls Verify Prosumer (ofrID, Uvs)
  Output Hash_Function
Calls sellEng()
 Output Initial_hash_Function
If Hash_Function matches Initial_hash_Function
      then
      Validate Prosumer
      Return Prosumer Verified
else
     Return error
       Prosumer not Verified.
    endif
 end Procedure
```

VI. Discussion and Analysis of the Aspects of the Proposed Framework

A. Integrity of Data

Data integrity is defined as accuracy, completeness, and consistency throughout the entire data life cycle and is a critical feature of any data-centric system. In our proposed framework, data integrity is guaranteed as the initial offers are submitted as hashed values of the unique value private to the participant, and so if any of the actors try to act as an adversary, it is practically impossible for it to change the hash functions. Just for an assumption, if the initial offers are modified, the 2nd filter would be able to detect the change, and the possibility of an attack would be detected. Moreover, blockchain, by its characteristic, is practically immutable and so data submitted to the SC cannot be modified.

B. Data Confidentiality

Confidentiality for data is defined as the protection of data against unauthorized or unlawful access, disclosure, or theft. Our proposed model preserves the confidentiality of data by making the prosumers submit their initial bids as hashed values. Thus, for a malicious actor to violate this confidentiality, it must guess the hash function calculated from the participant's secret value U_{vs}. Moreover, buyer and seller submit the hash functions of their unique value during the auction. Thus, our architecture guarantees the data confidentiality as breaking the 'collision - free' property of cryptographic hash function is unfeasible.

C. Privacy

Privacy, in terms of data and identity means that no personal or sensitive or identifying information is disclosed publicly and is only available on a need-to-know basis. Moreover, privacy is achieved if the user has full control over its data and regulates how different entities can access its information. Our proposed framework ensures privacy and identity protection as consumers and prosumers are represented by their unique reqID and ofrID respectively throughout the auction. Moreover, the identity of the winner prosumer is only disclosed once the auction has ended, and no more changes in bids are possible by a malicious actor. Because of privacy protection, it becomes very difficult for an adversary to predict a participant's behavior and influence the auction in the future.

D. Avoid a Single Point of Failure

Our proposed scheme uses a decentralized Ethereum blockchain and the community microgrid is private and managed by local prosumers. The PRA is a regulatory authority, and we assume that it is impossible for a malicious entity to influence or corrupt its behavior. Also, since the framework involves multiple prosumers, each acting independently, even if some nodes fail or get compromised, the entire system would not be affected. The application of blockchain effectively ensures that there is no single point of failure.

E. Accountability and Reliability

In our proposed framework, we use Ethereum, which is a decentralized, open-source public blockchain with smart contract functionality, and thus all interactions with the SC and the transactions done on this blockchain are available in a public blockchain. With all this information available publicly, it is possible to trace the individual participants interactions and achieve accountability in case of a dispute. The immutability of blockchain and its distributed nature allows verification of any false claims that any malicious node might try to make. Thus, both accountability and reliability are achieved.

F. Socio-Economic Benefits

The implementation of our blockchain based P2P secure ET framework would open a gateway for the end consumers to enter and decide the electricity prices in the LEM who otherwise had no option and say but to buy energy from a utility company at a pre-fixed market price. The significant advantage of local energy production, trading and consumption is the massive reduction in transmission losses and carbon emissions, financial incentives, greater employment opportunities, thereby boosting the local economy, independence from monopoly in electricity generation, transmission, and distribution, and a feeling of involvement and ownership in the local community, and thus would have a huge socio-economic impact.

VII. Conclusion

This paper proposes a secure and decentralized energy trading framework using the Ethereum blockchain and smart contracts. We exploited the opportunity that blockchain

technology provides to propose an innovative smart contract-based framework to set up a local energy market and perform energy trading in a small community without the intervention of a central authority. Our model adopts multiple filters at different steps to ensure that the energy requirements are met and adopts checks to avoid the possibility of any cost imbalance. Our analysis of various aspects of the proposed model suggests that the framework addresses the issues such as privacy, data integrity, and data confidentiality and has a huge socio-economic impact on the local community. A Better energy trading framework with increased profits would encourage more participants in the system, and more such small communities shall also be motivated to implement this technology. In our future work, we plan to perform the performance analysis of our proposed architecture and the auction process, investigate how our system protects against various attack scenarios in real-time settings and extend our framework for energy trading among different communities using blockchain technology.

ACKNOWLEDGMENT

This work was supported by NSF Grant INRC Testbed: COSMOS Interconnecting Continents, and NSF Grant; Japan USA Networking Opportunities JUNO2.

REFERENCES

[1] C. Li, “Securing US Critical Infrastructure against Cyber Attacks”, In Harvard Model Congress, Boston 2022.

[2] M.B.Mollah, J.Zhao,D.Niyato,K.Yan,”Blockchain for Future Snart Grid: A Comprihensive Survey”, IEEE Internet of Things Journal, 2020

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

[4] Bhattacharya, Sweta, Rajeswari Chengoden, Gautam Srivastava, Mamoun Alazab, Abdul Rehman Javed, Nancy Victor, Praveen Kumar Reddy Maddikunta, and Thippa Reddy Gadekallu. 2022. "Incentive Mechanisms for Smart Grid: State of the Art, Challenges, Open Issues, Future Directions" *Big Data and Cognitive Computing* 6, no. 2: 47

[5] L. Park, S. W. Lee, and H. Chang, “A sustainable home energy prosumer-chain methodology with energy tags over the blockchain,” Sustainability, vol. 10, no. 3, 2018, Art. no. 658.

[6] R. Khalid, N. Javaid, A. Almogren, M. U. Javed, S. Javaid, and M. Zuair, “A blockchain-based load balancing in decentralized hybrid P2P energy trading market in smart grid,” IEEE Access, vol. 8, pp. 47047–47062, 2020.

[7] Mhlanga, Jabulani Samuel and Oliver Dzobo. “Standalone hybrid energy system model and control for economic load dispatch.” 2019 Southern African Universities Power Engineering Conference/Robotics and Mechatronics/Pattern Recognition Association of South Africa (SAUPEC/RobMech/PRASA) (2019): 709-713.

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

[9] Solar Coin. Available: https://solarcoin.org/

[10] The Energy Web. Available: http://energyweb.org/

[11] Power Ledger. Available: https://www.powerledger.io/

[12] M. Sabounchi and J. Wei, “Towards resilient networked microgrids: Blockchain-enabled peer-to-peer electricity trading mechanism,” in Proc. IEEE Conf. Energy Internet Energy Syst. Integr., 2017, pp. 1–5

[13] F. S. Ali, O. Bouachir, Ö. Özkasap and M. Aloqaily, "SynergyChain: Blockchain-Assisted Adaptive Cyber-Physical P2P Energy Trading," IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5769-5778, Aug. 2021, doi: 10.1109/TII.2020.3046744.

[14] Z. Zhou, B. Wang, Y. Guo, and Y. Zhang, “Blockchain and computational intelligence inspired incentive-compatible demand response in internet of electric vehicles,” IEEE Trans. Emerg. Topics Comput. Intell., vol. 3, no. 3, pp. 205–216, Jun. 2019

[15] Son, Ye-Byoul, Jong-Hyuk Im, Hee-Yong Kwon, Seong-Yun Jeon, and Mun-Kyu Lee. 2020. "Privacy-Preserving Peer-to-Peer Energy Trading in Blockchain-Enabled Smart Grids Using Functional Encryption" *Energies* 13,no.6: 1321. https://doi.org/10.3390/en13061321

[16] Yahaya, Adamu Sani, Nadeem Javaid, Fahad A. Alzahrani, Amjad Rehman, Ibrar Ullah, Affaf Shahid, and Muhammad Shafiq. 2020. "Blockchain Based Sustainable Local Energy Trading Considering Home Energy Management and Demurrage Mechanism" *Sustainability* 12, no. 8: 3385. https://doi.org/10.3390/su12083385

[17] A. Dorri, F. Luo, S. S. Kanhere, R. Jurdak and Z. Y. Dong, "SPB: A Secure Private Blockchain-Based Solution for Distributed Energy Trading," in IEEE Communications Magazine, vol. 57, no. 7, pp. 120-126, July 2019, doi: 10.1109/MCOM.2019.1800577.

[18] Francesco Buccafurri, Gianluca Lax, Lorenzo Musarella, Antonia Russo, “An Ethereum-based solution for energy trading in smart grids”, Digital Communications and Networks, 2021, ISSN 2352-8648, https://doi.org/10.1016/j.dcan.2021.12.004.

[19] https://remix.ethereum.org/

[20] https://docs.soliditylang.org/en