A Multilayered Semi-Permissioned Blockchain Based Platform for Peer to Peer Energy Trading

Ishtiaque Zaman
Dept of Electrical and Computer Engineering
Texas Tech University
Lubbock, USA
Ishtiaque.Zaman@ttu.edu

Miao He
Dept of Electrical and Computer Engineering
Texas Tech University
Lubbock, USA
Miao.He@ttu.edu

2021 IEEE Green Technologies Conference (GreenTech) | 978-1-7281-9139-3/21/$31.00 ©2021 IEEE | DOI: 10.1109/GREENTECH48523.2021.00052

***Abstract*—The recent spike in microgeneration of renewable energy is demanding a smart, reliable, secured and efficient technology to enable Peer to Peer (P2P) energy trading. Due to the inherent characteristics, blockchain has been a preferred technology for realizing P2P energy trading. However, blockchain implementations for P2P energy trading so far are suffering from critical challenges such as security, privacy and scalability. In this paper, we introduce a P2P energy trading platform that leverages the popular blockchain technology and addresses these concerns. In particular, a multilayered semi-permissioned blockchain based platform along with a Quality of Transaction (QoT) module is proposed as a trading platform that can be used for transaction of energy. A two stage blockchain architecture, backed by QoT, ensures proper verification and validation of the participants and transactions. We present two use cases that demonstrate two different attack scenarios to highlight the resiliency of the proposed framework. Finally, a qualitative analysis shows the effectiveness of the system with respect to security, privacy and scalability.**

***Index Terms*—Permissioned Blockchain, Peer-to-Peer Energy Trading, Distributed Energy Resources, Consensus**

I. Introduction

Energy community is experiencing conspicuous changes with the rise of distributed energy resources (DERs). Policies are increasingly being introduced to promote the adoption of DER due to its proven potential in reducing cost and improving reliability [1]. As a result, consumers of utilities are now capable to generate significant amount of energy as commutable assets, therefore transforming themselves into prosumers. However, incentives are required to motivate these prosumers for continuous and increased generation of DER. Prosumers can trade their surplus energy to other prosumers that are lacking energy. This peer to peer (P2P) energy trading capability opens a vast area of research to help penetrate the DERs in the grid as well as to further increase the generation of renewable energy. A comprehensive platform for P2P energy trading can provide a self sustainable energy community by maintaining balance between the production and consumption of DER, thus minimizing the issues caused by the intermittent generation of renewable energy. Hence, this represents an efficient and popular solution for DER integration considering the cost effectiveness of the system [2] and economic benefits of the prosumers.

The dispersed landscape of DER aligns completely with the popular blockchain technology for its underlying features such as decentralization, security and transparency [3]. Blockchain has the infrastructure for a fully decentralized trading platform that maintains information symmetry by shared, immutable and distributed ledgers among the participants [4]. The network is protected by an embedded consensus algorithm that ensures trust-free or trusted cooperation between the participants [5]. Due to the distributed infrastructure, blockchain is increasingly being promoted as an appropriate technology for energy trading in smart grid. The authors in [6] develop a blockchain based platform and used it in the aggregation step of Alternating Direction Method of Multipliers (ADMM) to distribute the utility operator's role across all devices in the network. In [7], the authors develop a blockchain based framework where users can anonymously negotiate energy prices. The payment system of this framework is based on Bitcoin protocol and the security of the system is ensured by proof of work (PoW) consensus algorithm. [8] utilizes ethereum blockchain for transactive energy market by designing a smart contract based auction mechanism. The prototype of this project is tested at Washington State University campus. The authors in [9] proposes a market-based solution for major distribution grid challenges. The solution is based on the blockchain principles and uses proof of stake (POS) as the underlying consensus protocol. [10] presents the concept of digital currency named NRGcoin that can be earned by injecting energy to the grid by the prosumers. The value of the new NRGcoin is determined by the street level low voltage distribute system operator (DSO) who have the smart meter data of each prosumer. Clearly, this method exposes single point of failure (SPoF) as the DSO has the privacy sensitive data from all the participants. [11] introduces a notion of crowdsourced energy system with blockchain in the background that can enable P2P energy trading. To make the system capable for large scale implementation and include a large number of crowdsourcees, the authors employed Redundant Byzantine Fault Tolerant (RBFT) [12] method as the consensus mechanism with the trade off of having a central authority to manage the system.

With the support from the researchers, the power industry is also adopting blockchain to facilitate energy trading among

2166-5478/21/$31.00 ©2021 IEEE
DOI 10.1109/GreenTech48523.2021.00052

their consumers through pilot projects. LO3 Energy [13] developed Brooklyn Microgrid to provide an energy marketplace for locally-generated solar energy. Power Ledger [14] is another company enabling P2P electricity trading among households with solar energy production capabilities.

The state-of-the art solutions prove the applicability of blockchain for P2P energy trading. However, blockchain and its underlying consensus algorithms have their own constraints that can be critical in energy trading scenarios. Implementation of different consensus mechanisms creates different variants of Blockchain architecture and the selection of these algorithms depends on specific use case [15]. Proof of Work (PoW) [16] and Proof of Stake (PoS) [17] are two of the most popular algorithms for blockchain implementation. Despite the promising outcomes in various applications, these algorithms have critical constraints that can potentially limit blockchain implementation in P2P energy trading. In P2P energy trading paradigm, complete anonymity like public blockchains (e.g. Bitcoin, Ethereum etc.) is not suitable since it can compromise the security and scalability of the system as well as the privacy of the prosumers [18]. However, private blockchain can also be exposed to attackers as the system becomes more centralized than that of public blockchain [19]. Therefore, the following aspects should be prioritized for a self sustaining energy trading platform:

- ***Security***: Energy is a crucial commodity and an enticing target for attackers. Moreover, in P2P energy trading, transactions of energy are governed by the end users (prosumers), instead of trained utility operators that can potentially originate operational errors. Therefore, an energy trading platform needs to be immune from external attacks as well as internal errors. However, most implementations of public blockchains now a days employ PoW consensus that can be breached by 51% attack [20]. Some projects use PoS algorithm for achieving consensus [9], however, PoS makes the network more centralized as the participants increase in number which consequently makes the system vulnerable to distributed denial of service attacks (DDoS).
- ***Privacy***: Privacy of the prosumers needs to be ensured in a trading platform. In public blockchain, since the identity of participating prosumers are anonymous and since the smart meter data are broadcast to all the participating prosumers, privacy-sensitive information may be compromised [18]. This may not be the case in private blockchains, however, proper masking is required to protect user's transactions and corresponding communication.
- ***Scalability***: An energy trading platform must be scalable to accommodate the growing number of participating prosumers as well as transactions. However, in the recent implementations, scalability is being overlooked. PoW based blockchain requires resource consuming cryptographic puzzles as part of their validation process that results in high computation and bandwidth allocation cost. High computation cost causes more energy consumption that can amount to large extent. For instance, in May 2018, total energy consumed to mine bitcoin blockchain was more than the entire country of Switzerland [21].

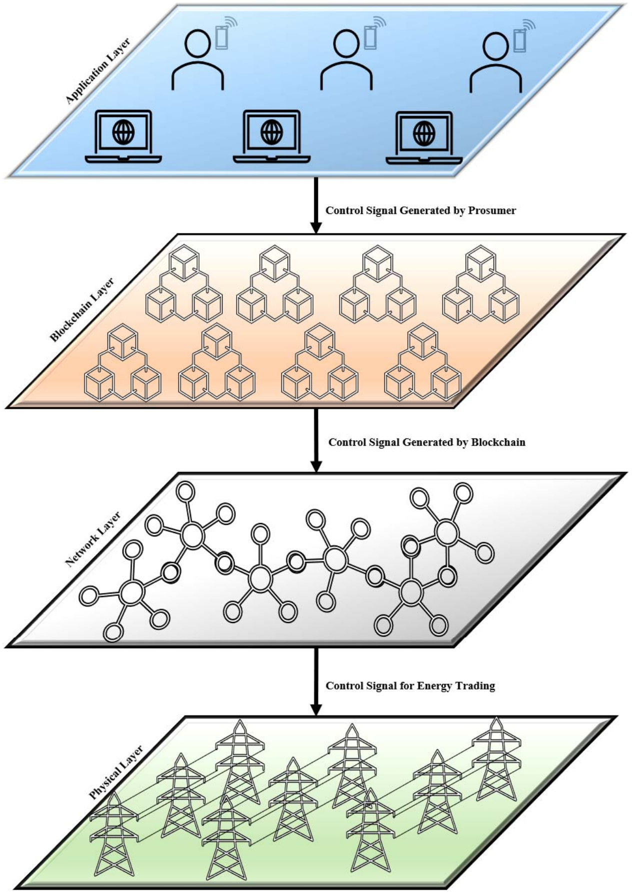
Application Layer
Control Signal Generated by Prosumer
Blockchain Layer
Control Signal Generated by Blockchain
Network Layer
Control Signal for Energy Trading
Physical Layer

Fig. 1. Multilayer Model for Energy Trading

In this paper we present a multilayered semi-permissioned blockchain based P2P energy trading platform that addresses the above mentioned challenges and enables prosumers to seamlessly trade energy in the same network. The term 'semi-permissioned' refers that, a trusted authority is required only for primary enrollment in the network. Transaction validation does not require any trusted authority. Fig. 1 shows the layer-wise architecture of the platform. Prosumers use the application layer to communicate and negotiate on transaction of energy. Transaction is initiated in this layer. The blockchain layer executes the consensus and smart contracts for the transactions. The network layer provides the communication backbone for distributed ledger and electronic fund transfer. Energy is transferred from one point to another in the physical layer. The physical layer is assumed to be bidirectional among the households. This paper proposes a two stage blockchain architecture where the first stage is used to verify the partici-

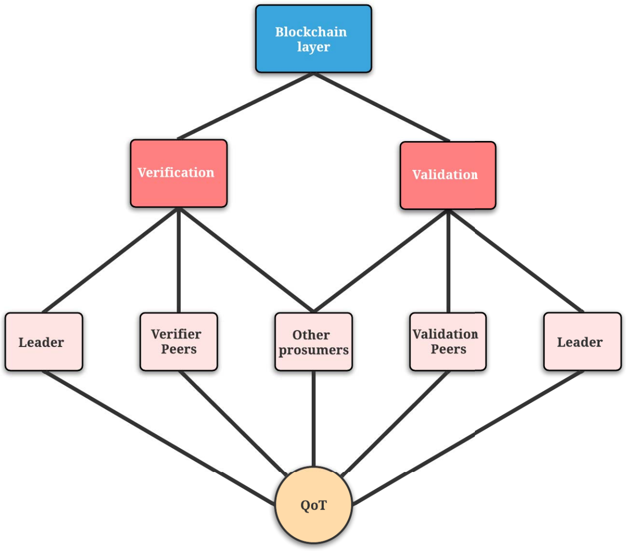

Fig. 2. Framework Components

pants or prosumers and the second stage is used to validate the transactions between the prosumers. Additionally, we measure the quality of a transaction (QoT) and introduce Q-score - a reward system to rate a participant that eventually helps to determine his/her eligibility for future transactions. This two stage blockchain network backed by QoT improves the security, privacy and scalability of the system.

The rest of the paper is structured as follows: Next section discusses the proposed framework and detailed explanation about various components of the framework. In Section III, we present two attack scenarios to demonstrate the resiliency of the framework. Section IV represents a qualitative analysis of security, privacy and scalability of the framework. Finally, we conclude by addressing our research findings and next steps that can help scale the project at an industrial level.

II. Proposed Framework

The proposed framework allows energy trading between prosumers in the same network by providing a blockchain based architecture for verification and validation through a combination of consensus model, smart contract and QoT. The smart meters of each prosumer in the network jointly manage the network to verify new prosumers in the network and validate the transactions for secured and efficient trading. Fig. 2 shows the structure of the framework where the complete workflow is divided into two major segments based on the specific task of the system. Each segment is further divided into several sub-segments depending upon the use cases. In the following subsections each task is described in detail.

A. *Verification of New Prosumers*

When a prosumer wishes to join the network, the network must be able to verify the authenticity of the smart meter representing the new prosumer. In a public blockchain this is achieved by solving cryptographic puzzles, whereas, in private blockchain, a trusted party is responsible for the authentication of the new nodes. The first approach is computationally expensive and the later approach is vulnerable to SPoF attack. [22] uses “Certificate of Existence” to avoid the trusted third party for new prosumer verification. However, this requires the meter manufacturers to populate key pairs which serves as the certification authority. The proposed framework solves this problem using the consensus among the existing prosumers in the network. The idea is to employ the existing participants along with a certified authority to reach in agreement about the authenticity of a new prosumer.

A new smart meter wishing to join the network will be verified by a set of verifier nodes. In the energy trading scenarios each node is considered to be the smart meter of each household. The verifier set is selected by clustered sampling method. These members are the prosumers that voluntarily offer their identities at stake in order to gain the right to validate nodes or create new blocks. This means, the identities, actions and reputation (reward or punishment) of these members are public to the network. The members of verifier set are provided with X509 certificates that will be used for verification purposes. The verifier set is also changeable after each addition of a new smart meter, provided that the new smart meter is also wishing to be selected as the verifier node.

A leader smart meter is selected from the verifier set. A new block is created by the leader smart meter that contains entries about the new smart meter joining request. The selection of the leader node L_i is time dependent and a leader node at ith time instant T_i is determined by:

$$L_i = ((T_i - T_0) \;/\; \tau) \;\%\; n \tag{1}$$

Where, T_0 is time instant of the first block, τ is time interval between the generated blocks and n is total number of smart meters at ith time. After each verification, the leader role is assigned to a different member from the verifier set according to (1). A leader smart meter first verifies the joining requests and then creates a block with all of the requests at T_i. Being a private network, it is assumed that the prosumer's identity is known to the system and the leader just needs to match the joining request with the identity using his certificate. Upon verified by the leader, the block is then signed with leader's private key and sent to other members of the verifier set. After receiving a block from the leader, the verifier peers use their own private key and the leader's public key to verify following conditions:

Condition 1: The block was generated from the leader at T_i
Condition 2: No other blocks have been generated from the same leader at T_i
Once the block passes the verification checks, it is added to the blockchain, the verified new member is issued a X509 certificate. However, if the block fails for verification then the joining request is declined. Fig. 3 shows the workflow of verification step.

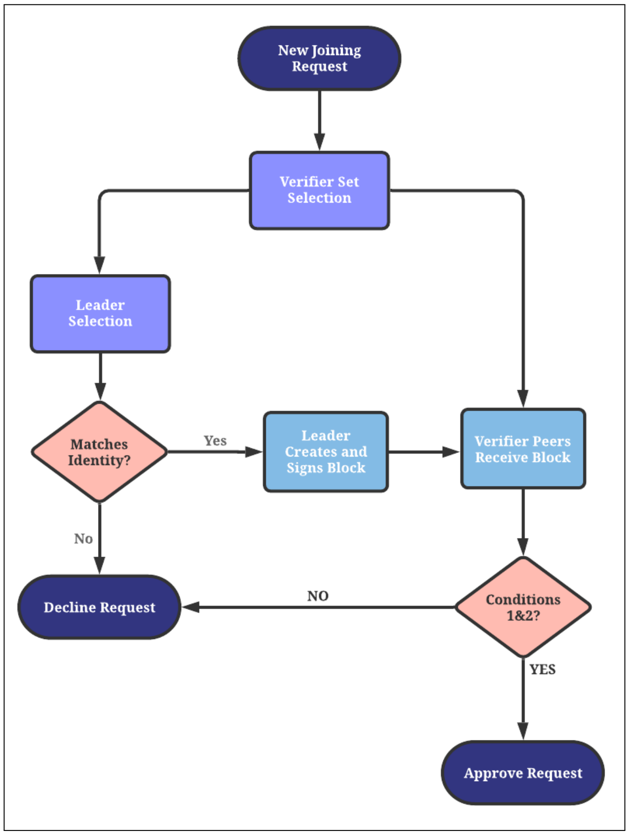

Fig. 3. Verification of New Prosumer

B. Validation of Transactions

The network must be able to validate transactions between prosumers. A prosumer is denoted as a seller or a consumer based on the specific role in a transaction. Moreover, a prosumer is allowed to be both seller and consumer simultaneously in different transactions. Each smart meter has a ledger that contains two types of data: 1) Transaction log and 2) State data. Transaction log is immutable and keeps track of all the transactions. Whereas, state data are key-value pairs that contain information about the state of the energy. Unlike transaction log, state data are versioned and can be updated but not deleted. The key-value pairs in state data include the amount of available energy and information of the corresponding household that owns the energy such as smart meter id. A transaction is executed in three stages-

Preparation Stage: When two prosumers (seller and buyer) agree to trade energy, a transaction is initiated and a set of validating smart meters is selected by clustered sampling method from the participating prosumers of the network. A leader is selected from the cluster and acts as an intermediate node or relay node for the transaction. The cluster is changeable after each transaction and therefore, the leader is also changeable. This makes the process less susceptible to single point of failure. The Leader's smart meter and wallet information are visible to the cluster peers. Transaction initiation invokes a smart contract that includes information related to the transaction such as amount of energy, price of the energy, meter ids of seller, buyer, leader and validation cluster members.

Execution Stage: Transaction is executed at the leader's end. The leader receives the energy amount and his wallet amount changes according to the contract. The members of the cluster check the following conditions:
Condition 1: The energy amounts of seller and leader are updated according to the smart contract.
Condition 2: The wallet amounts of buyers and leader are updated according to the smart contract.
The transaction can be declined at this stage if any one of the conditions 1&2 fails. If both the conditions pass, the ledger is updated temporarily based on the consensus of validation peers and the transaction reaches the final stage. Here, the term 'temporarily' means, only the validation cluster and the leader's ledgers are updated and other members of the network including the seller and buyer still have the previous version of the ledger.

Final Stage: In the final stage, the leader sends the received energy to the buyer and his wallet amount changes back to the previous balance. The members of the cluster now check the following conditions:
Condition 3: The energy amounts of buyer and leader are updated according to the smart contract.
Condition 4: The wallet amounts of seller and leader are updated according to the smart contract.
The transaction can be declined at the final stage if any one of the conditions 3&4 fails. If both the conditions pass, the ledger is permanently updated based on the consensus of validation peers and the transaction is complete. Here, permanently means, all the members of the network now have the updated version of the ledger that include the transaction details. Fig. 4 shows the workflow of validation stage.

C. Quality of Transaction (QoT)

After each transaction, the corresponding smart meters are awarded with a reward point based on the outcome of the transaction. We denote this variable as quality score or Q-score. Q-score is simply a tool for measuring the quality of a transaction and rate the participants on the transaction that potentially protects the system from malicious attackers. When a transaction is successful, positive Q-score is awarded to seller and buyer that are involved in the transaction. Additionally, the corresponding verifier and validation peers including leaders are also awarded with positive Q-scores. Whereas, when a transaction is declined, one of the two cases is more likely to occur. Either the seller have failed to deliver the agreed upon amount of energy or the buyer have failed to pay the price. In the first case, the seller is penalized with negative Q-score while in the later case, the buyer is penalized with negative Q-score. However, in both the cases, the verifier and validation

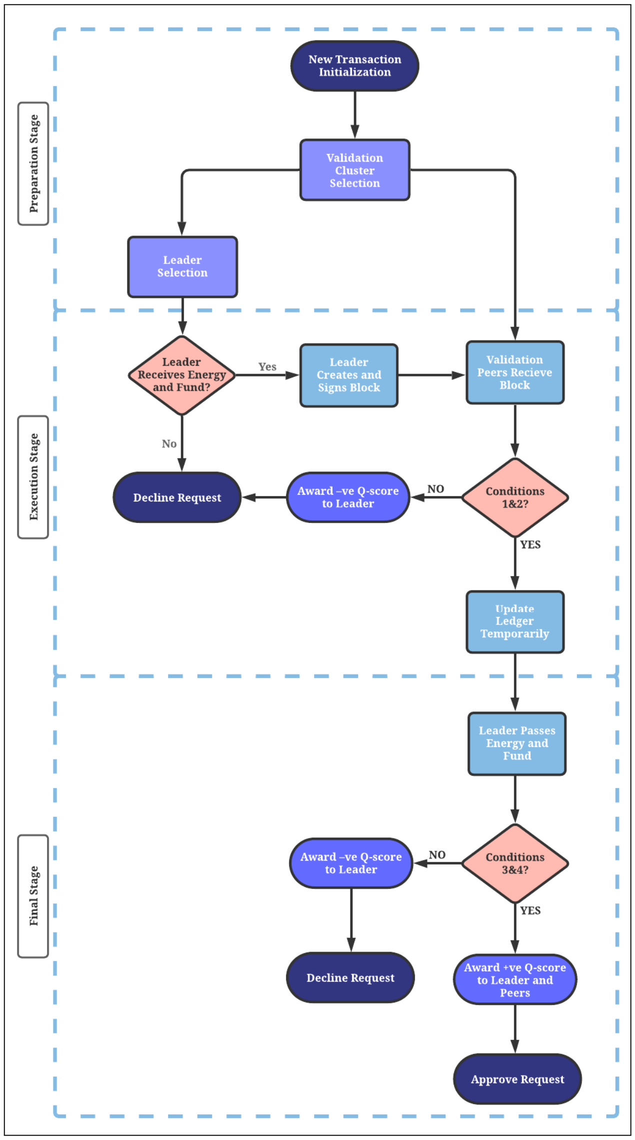
Preparation Stage
Execution Stage
Final Stage
New Transaction Initialization
Validation Cluster Selection
Leader Selection
Leader Receives Energy and Fund?
Yes
No
Leader Creates and Signs Block
Validation Peers Recieve Block
Conditions 1&2?
NO
YES
Award -ve Q-score to Leader
Decline Request
Update Ledger Temporarily
Leader Passes Energy and Fund
Conditions 3&4?
NO
YES
Award -ve Q-score to Leader
Decline Request
Award +ve Q-score to Leader and Peers
Approve Request

Fig. 4. Validation of Transaction

sets are punished with negative Q-scores. The total Q-score in ith transaction is determined by:

$$\begin{aligned}(Q-score)_{(i)} &= v_{(i)} + L_{(i)} + f(x_{(i)},\alpha)\\ where,\ v_{(i)} &= v_{(i-1)} * x_{(i)}\\ L_{(i)} &= L_{(i-1)} * x^3_{(i)}\end{aligned} \tag{2}$$

$$f(x,\alpha) = \begin{cases} (S+B)*x^5 & \text{if } x > 0\\ S*x^5 & \text{if } x < 0 \ \&\ \alpha = +1\\ B*x^5 & \text{if } x < 0 \ \&\ \alpha = -1\end{cases}$$

Here, $x_{(i)}$ is the Q-score of ith transaction and $x_{(i)} \in R$. S and B are the Q-scores of seller and buyer. In case of new prosumer verification, $v_{(i)}$ and $L_{(i)}$ are the Q-scores of verifier peers and leader in ith verification, whereas, in transaction validation case, $v_{(i)}$ and $L_{(i)}$ are the Q-scores of validation peers and leader in ith transaction. α is a signed coefficient associated with the quality of the ith transaction. The value of α is $+1$ when the seller is failed to deliver the energy according to the contract. α is -1 if the buyer fails to pay the price of energy. The total QoT of a transaction is added to the ledger and it is public to all the participating smart meters. The future trading capability of a smart meter is determined by the Q-score. Two prosumers agree to trade energy between themselves based on their Q-score. If a prosumer's Q-score is low and he has been in the network for a substantial amount of time then it is less likely that other prosumers will want to trade with him.

III. Use Cases

In this section, we present two possible use cases where a transaction can be declined. The first use case depicts a scenario when a malicious or faulty seller intentionally or unintentionally fails to deliver the energy amount according to the smart contract while the later one represents the scenario when a malicious or faulty buyer intentionally or unintentionally fails to pay the price of the energy amount according to the smart contract. In both the scenarios, our proposed model appears to be unaffected and is able to detect the flaws in the process. Fig. 5&6 represent the two scenarios where a transaction is eventually declined at the execution stage of transaction validation process.

Malicious Seller Scenario: An attacker may imitate himself as the seller and initiate a transaction with a genuine buyer or a faulty seller may fail to deliver the energy even after the generation of smart contract. In this case, the leader does not receive the required amount of energy after the execution of smart contract and the transaction is declined at the execution stage as condition 1 fails.

Malicious Buyer Scenario: A malicious buyer may also initiate a transaction with a genuine seller and refuse to pay the price of the energy according to the contract. In this case, the leader's wallet information does not change or increase after the execution and the transaction is declined at the execution stage as condition 2 fails.

IV. Security, Privacy and Scalability

The proposed framework addresses security, privacy and scalability issues of an energy trading platform.

A. Security

Inherently, in a blockchain infrastructure, all the transactions, ledgers and smart meters connected to the network are protected by certificates. In a private blockchain, these certificates are administered by a central certification authority. Our proposed framework employs a two stage blockchain to reduce this centralization. When analysing security of a trading platform, the following common attack vectors are considered:

Denial-of-service (DoS) attacks: In DoS attack, a large number of transactions are launched in a network to occupy the

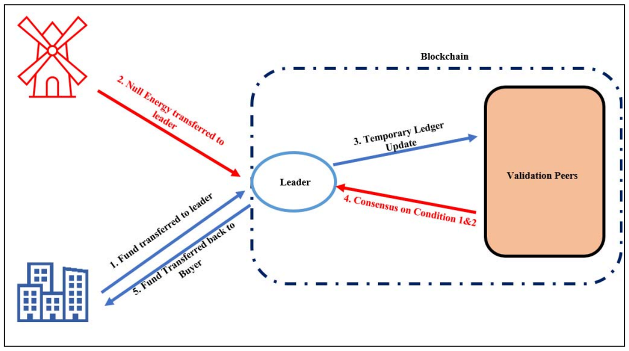
Blockchain
2. Null Energy transferred to leader
3. Temporary Ledger Update
Leader
Validation Peers
4. Consensus on Condition 1&2
1. Fund transferred to leader
5. Fund Transferred back to Buyer

Fig. 5. Malicious Seller Scenario

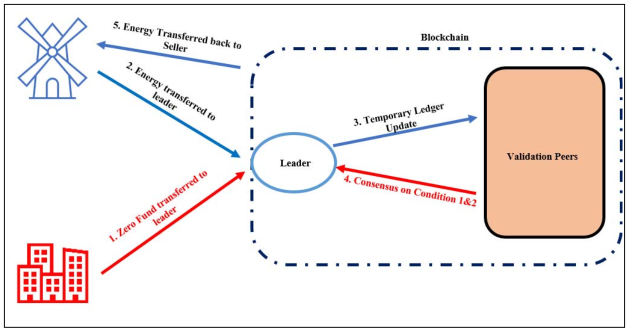
5. Energy Transferred back to Seller
Blockchain
2. Energy transferred to leader
3. Temporary Ledger Update
Leader
Validation Peers
4. Consensus on Condition 1&2
1. Zero Fund transferred to leader

Fig. 6. Malicious Buyer Scenario

bandwidth and disrupt the operation. The proposed framework defends this attack by 1) Changing the verifier set after each prosumer verification, 2) Changing the validation set after each transaction, 3) Managing two different sets for verification and validation tasks and 4) Using Q-score to determines the eligibility of a participant to launch a transaction.

51% attack: In some blockchain where PoW is used, an attacker may increase the computation power to launch a 51% attack. However, in the proposed framework, in order to launch a 51% attack, the attacker needs to obtain control over 51% smart meters of the network. Obtaining control over the nodes in a private blockchain is more challenging than gaining computation power since the later can be achieved from only one node. This makes the system tolerant to internal errors as well since the probability of errors in 51% of the nodes are very low.

B. Privacy

Prosumer's privacy is preserved in this framework by certificates and keys. Only the verifier smart meters have access to the real identity of a new prosumer and that identity is protected by X509 certificates. Since the verifier set changes after each verification, the identity is moved to the new verifier set and erased from previous verifier set. Although the ledgers of all the smart meters are visible to each other, the system is less vulnerable to privacy violation since their identity is managed by their reputation or Q-score.

C. Scalability

In the proposed framework, only a number of smart meters carry out the verification task. Also recall that, in the validation step, only the leader executes a transaction through a smart contract and other validation peers simply check the conditions. This establishes the fact that the network does not require high performance hardware to perform the verification and validation tasks thus, improves the overall scalability of the system.

V. Conclusion and Future Work

A semi-permissioned blockchain enabled quality of transaction based P2P energy trading platform is proposed in this paper. The two stage blockchain infrastructure embedded with Q-score is used to verify the participants and validate their transactions. The optimal use of smart meters for verification and validation purposes improves the scalability. The changeable verifier and validation sets increase the resiliency of the platform against potential attack variants i.e. DoS, 51% attack etc. and enhance the privacy of the system. As our next steps, we aim to implement the proposed framework in an islanded microgrid and benchmark the performance with quantitative analysis using hardware-in-the-loop simulation.

References

[1] D. J. Hess and H. Gentry, "100% renewable energy policies in US cities: strategies, recommendations, and implementation challenges," *Sustainability: Science, Practice and Policy*, vol. 15, no. 1, pp. 45–61, 2019.

[2] T. Morstyn, A. Teytelboym, C. Hepburn, and M. D. McCulloch, "Integrating P2P Energy Trading with Probabilistic Distribution Locational Marginal Pricing," *IEEE Transactions on Smart Grid*, 2019.

[3] C. Burger, A. Kuhlmann, P. Richard, and J. Weinmann, "Blockchain in the energy transition. a survey among decision-makers in the german energy industry," *DENA German Energy Agency*, vol. 60, 2016.

[4] M. Mainelli and M. Smith, "Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)," *Journal of Financial Perspectives*, vol. 3, no. 3, 2015.

[5] R. Beck, J. Stenum Czepluch, N. Lollike, and S. Malone, "Blockchain–the gateway to trust-free cryptographic transactions," 2016.

[6] E. Münsing, J. Mather, and S. Moura, "Blockchains for decentralized optimization of energy resources in microgrid networks," in *2017 IEEE conference on control technology and applications (CCTA)*. IEEE, 2017, pp. 2164–2171.

[7] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2016.

[8] A. Hahn, R. Singh, C.-C. Liu, and S. Chen, "Smart contract-based campus demonstration of decentralized

transactive energy auctions," in *2017 IEEE Power & energy society innovative smart grid technologies conference (ISGT)*. IEEE, 2017, pp. 1–5.

[9] J. Horta, D. Kofman, and D. Menga, "Novel paradigms for advanced distribution grid energy management. arxiv 2017," *arXiv preprint arXiv:1712.05841*.

[10] M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Nowé, "NRGcoin: Virtual currency for trading of renewable energy in smart grids," in *11th International conference on the European energy market (EEM14)*. IEEE, 2014, pp. 1–6.

[11] S. Wang, A. F. Taha, J. Wang, K. Kvaternik, and A. Hahn, "Energy crowdsourcing and peer-to-peer energy trading in blockchain-enabled smart grids," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1612–1623, 2019.

[12] P.-L. Aublin, S. B. Mokhtar, and V. Quéma, "Rbft: Redundant byzantine fault tolerance," in *2013 IEEE 33rd International Conference on Distributed Computing Systems*. IEEE, 2013, pp. 297–306.

[13] The future of energy: LO3 Pando: Blockchain, Transactive Grids, Microgrids, Energy Trading: LO3 Tokens and Information. [Online]. Available: https://lo3energy.com/

[14] Power Ledger: Energy trading platform. [Online]. Available: https://www.powerledger.io/

[15] A. Baliga, "Understanding blockchain consensus models," Tech. Rep., 2017.

[16] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[17] "Proof of stake." [Online]. Available: https://en.bitcoin.it/wiki/Proof_of_Stake

[18] D. Varodayan and A. Khisti, "Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage," in *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2011, pp. 1932–1935.

[19] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in *2017 26th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2017, pp. 1–6.

[20] A. Hertig, "Blockchain's once-feared 51% attack is now becoming regular," *Coindesk. com*, 2018.

[21] "Bitcoin energy consumption index." [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption/

[22] A. Dorri, A. Hill, S. Kanhere, R. Jurdak, F. Luo, and Z. Y. Dong, "Peer-to-peer energytrade: A distributed private energy trading platform," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2019, pp. 61–64.