An Efficient Consensus Protocol for Blockchain Technology in Smart Grid Contracts

[1]Mahamoodkhan Pathan, [2]Rameshkumar J and [3]Chintalapudi V Suresh
[1,2] Department of Electrical Engineering, Annamalai University, Chidambaram, Tamil Nadu, India.
[3]Department of Electrical Engineering, Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India.
[1]pathanmehemudkhan@gmail.com, [2]rameshwin75@gmail.com, [3]venkatasuresh3@vvit.net

Correspondence should be addressed to Mahamoodkhan Pathan : pathanmehemudkhan@gmail.com

Article Info
Journal of Machine and Computing (https://anapub.co.ke/journals/jmc/jmc.html)
Doi : https://doi.org/10.53759/7669/jmc202505003
Received 02 May 2024; Revised from 08 July 2024; Accepted 20 September 2024.
Available online 05 January 2025.

Abstract – The decentralized operation of the power system, which is built entirely on the consensus notion, is one of the most important contemporary subjects in the energy industry. Without the need for a "neutral arbiter, all significant market participants can come to an understanding. Peer-to-peer (P2P) architecture, interface communication, and network security are all discussed in this paper as they pertain to the decentralized nature of the energy market and the paper's proposed solution: a P2P-based platform. For this reason, it is critical to protect the market player's communication interfaces from harmful assaults. In this case, a new blockchain platform coinciding with the P2P energy market ensures that the necessary consensus may be reached safely. An efficient algorithm based on the Relaxed Consensus-Innovation (RCI) protocol controls the energy market, with the goal of facilitating power/price trading between participants in a decentralized, peer-to-peer (P2P) setting. Market participants in the proposed model include a microgrid and a smart grid, both of which are assumed to act in their own self-interest while negotiating with one another in a safe setting. Microgrids use wind turbines, solar panels, tidal turbines, and battery storage units, whereas the smart grid uses distributed generators (DGs) and transmission lines modelled after the IEEE 24-bus test system. In the peer-to-peer energy market, a stochastic framework that is based on unscented transform (UT) has been developed to deal with the uncertainty effects caused by the circumstance. For gauging and validating the fault-tolerant system's resistance to cyber-attack, we model and apply the fault data injection attack (FDIA) on the blockchain-based P2P energy market". Simulation results validate the paper's ideas.

Keywords – Consensus Protocol, Blockchain, Smart Grid, Contracts, Peer to Peer.

I. INTRODUCTION

P2P electricity was developed to reduce reliance on fossil fuels. Few producers will benefit from unregulated energy transfers. Few manufacturers can affect market clearing prices or bids [1]. Because peer-to-peer is decentralized, parties must negotiate rates and energy transactions. The "network graph enables peer-to-peer energy trading on the power grid. Graph theory can help reach a market consensus [2]. In this paper, "neighbour" refers to any pair of agents that share a node in a graph network [3]. A shift in consumer behaviour can be achieved by designing a P2P economy in which all participants take an active role [4]. In this regard, viewpoints from all relevant parties will be taken into consideration. Open data transactions, data privacy, access to big data and local data, and no central supervision are required for P2P energy trading [5]. Using Markowitz portfolio theory, [6]'s P2P market structure optimizes uncertainty risk for sellers and buyers. In [7], researchers built a decentralized energy market where people sold and bought power directly from one another using a gas-energy storage device. Money flows between all agents are modelled and a P2P architecture with a dynamic tariff is proposed in [8]. The findings demonstrate that such a setup would allow prosumers and consumers to both make significant financial gains. In [9], Peer-to-peer energy transactions enhance energy management by coordinating local producers and loads. Hug et al. provide the Relaxed Consensus- Innovation (RCI) approach for peer-to-peer energy transactions. The RCI method's solution is derived from the Lagrange mathematical technique with boundary constraints; the marginal cost serves as the method's objective function [10]. Considering the foregoing, the RCI technique is implemented on a distributed system, and it has been shown in several studies [11] that the RCI method's output response is very near to the answer reached by the centralized approach, albeit with significantly faster convergence time. The literature presents several approaches to dealing with the system's uncertainties, each with its own set of benefits and cons. The approaches could be categorized to deal with uncertainty effects into three broad groups,

Monte Carlo simulation gives the most accurate results, but it's computationally intensive. While analytical approaches may be able to avoid the excessive computing demands of the first group, they often require simplifying the problem to work, which can lead to a loss of precision [12]. The remaining subset can deliver sufficient precision with modest processing cost. Due to its excellent uncertainty modelling capabilities, cheap processing burden, and coupled structure, the unscented transform (UT) approach is used in this research. In addition, a blockchain-based update to the RCI approach has been implemented [13]. It employs a peer-to-peer network to ensure payments without a central authority and can only be exchanged by Bitcoin users. Blockchain technology, which uses a series of blocks to encrypt data transfers, serves as the conceptual backbone of this system. In, it is demonstrated how blockchain technology is utilized to lessen the possibility of operational cost fraud and improve the dependability of the system. In this study, we use blockchain technology and the RCI approach to get a complete consensus [14]. To this purpose, we adapt the RCI approach for usage in distributed computation and introduce it to the blockchain infrastructure as a new type of user. The suggested RCI-blockchain based architecture will be demonstrated to allow the system to establish a consensus while maintaining an adequate level of security. In this work [15], we suggest a blockchain architecture fit for purpose, one that safeguards transactions on the energy market between microgrids and smart grids". The proposed consensus technique is tied to blockchain to ensure the process continues if data is corrupted. Designing an unscented transform-based stochastic framework for the proposed decentralized energy market.

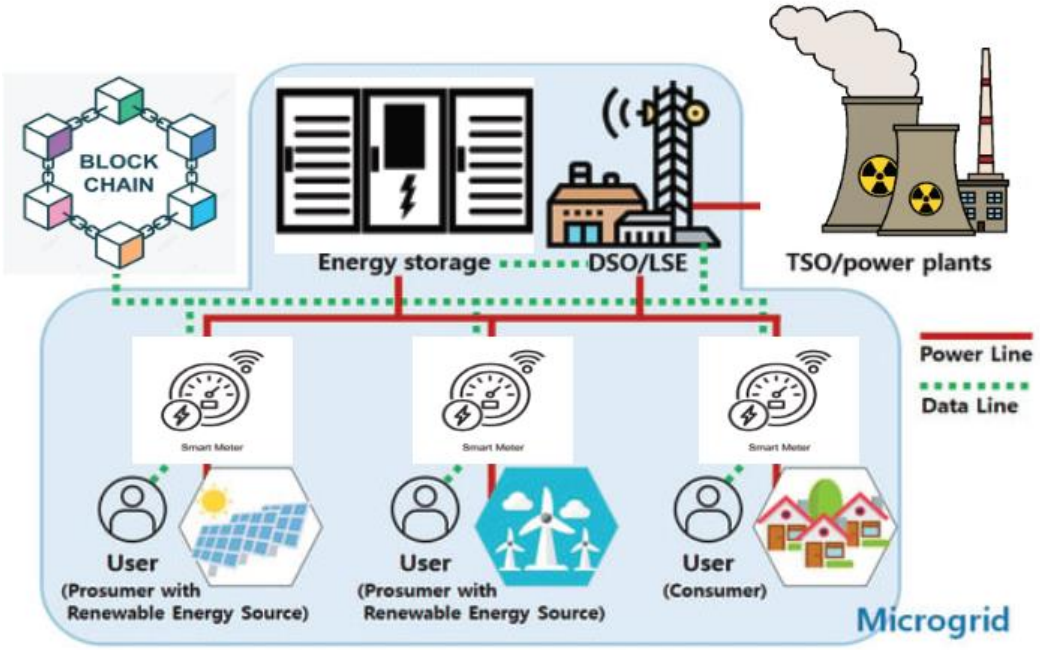

Fig 1. Blockchain Process.

Security Administration Based on A Blockchain Foundation

This "section is dedicated to explaining how the blockchain's design can make modern network administration safer and more efficient. Blockchain technology has captured the interest of many different sectors, from banking and healthcare to manufacturing and the grid. Applications where this security architecture has proven useful include online voting, identity management, and ensuring the integrity of data collected via the internet of things (IoT) [16, 17]. A distributed, publicly accessible, and fault-tolerant database serves as the foundation for blockchain technology. This means that each node in the network can share data while also remaining incapable of exerting centralized control over any other nodes. Using this framework protects your data from hackers. The blockchain system considers undesirable attacker behaviors and tries to disable their adversarial approaches by using honest nodes capable of extensive computational processing. The following provides further detail on the process of validating the protective environment provided by the blockchain system against the actions of harmful adversaries by dissecting two crucial elements of the suggested architecture, namely the blockchain network technique and attack model".

II. BLOCKCHAIN ARCHITECTURE

The "fact that the blockchain does not require a central trustworthy system to function and that it can operate in a decentralized environment for the purpose of transmitting information among nodes is the first and possibly most important characteristic of the blockchain. A trustless system is one that allows an agent to participate in transactions despite the absence of reciprocal trust, and blockchain technology may be able to provide appropriate circumstances for such a system. Conversely, since there is no longer a need for a centralized authority within the blockchain, the trend of

reconciliation, which is normally handled between nodes by a consensus mechanism, can be accelerated. The method also includes crypto graphing the data broadcast by the nodes to increase the security of the secrets being shared. When compared with a centralized database, the blockchain technology offers the following benefits. First, a consensus algorithm is used to verify and authorize transactions in the blockchain process. Two, the distributed ledger technology known as blockchain doesn't rely on a centralized server or network design to coordinate its decentralized network of nodes. The fundamental idea of the blockchain system is depicted in **Fig 1**. Considering the foregoing, the decentralized network, the consensus algorithm, and the cryptographic process are all crucial to the success of the blockchain system".

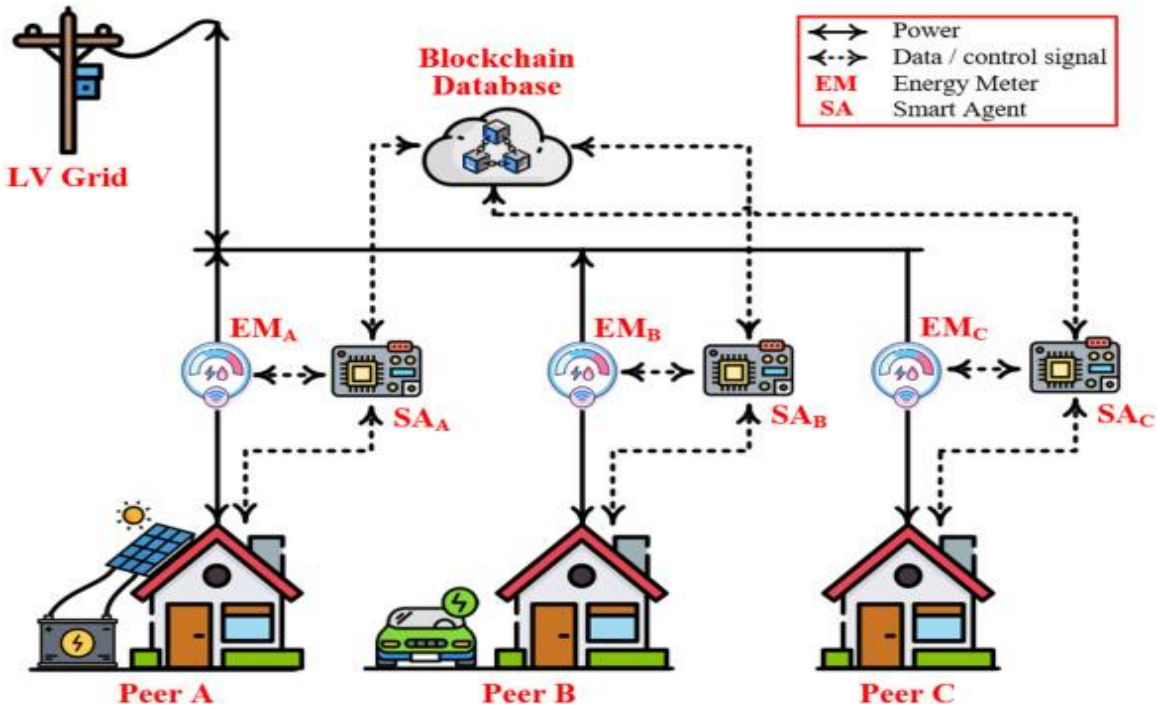

Fig 2. Peer-To-Peer Decentralization.

Decentralized Network

The "main goal of a distributed network is to maintain the dispersed legers specified in each node by optimizing the dispersion of messages delivered between nodes. Messages sent from one node in a blockchain network can be relayed to all other nodes in the network using the network protocol that supports the system. However, no rigorously broadcast system is in place, thus nodes can post messages as evidence of a valid information flow.

The network can be a public or private blockchain based on the graph generated by the nodes for network security. In addition to the public and private blockchains, **Fig 2** illustrates that the decentralized network should be implemented using a peer-to-peer topology in which nodes may freely enter or exit the network. This network design is also extremely robust, which helps to reduce the likelihood of node and link failures. To ensure the reliability and robustness of the blockchain system, its first stage necessitates the establishment of a decentralized network based on the peer-to-peer structure".

The Consensus Algorithm and Protocol

Implementing a consensus protocol over a "peer-to-peer (P2P) structure that is built on a decentralized network is one of the steps involved in the process of constructing a blockchain. Before adding blocks of nodes to the public ledgers, this step is taken to verify the authenticity of transactions that are broadcast across several nodes. At the same time, the ledgers are updated to reflect the transactions that have been completed between the nodes. As a bonus, the consensus protocol may both solicit blocks and give a consensus point for their integration. The number of transactions verified by the protocol is considered.

With the help of the consensus protocol, new transactions are added to the network without affecting the integrity of the already-existing legitimate transactions. New transactions are therefore added to a block and validated by the blockchain system. A fault-tolerant consensus method can ensure that all network nodes agree (on a common value) and produce the appropriate responses for every request that is made. This level of agreement can be reached even with some of the nodes in the network not functioning properly.

The nodes that make up a consensus algorithm collaborate with one another to create an emotional consensus, even though they are in various regions of the world. This means that in iteration r, all nodes communicate with their neighbour, and in iteration r + 1, all nodes receive the responses from their neighbors. The final consideration is node

fault, which indicates that the node has experienced a failure that may have halted its performance. It goes without saying that the presence of a defective node should not prevent the consensus algorithm from reaching a consensus point. To achieve an agreement based on consensus objectives, a network employs a consensus algorithm, which is a set of rules for processing message transactions across all nodes in the network".

An N-node method needs to satisfy four requirements-termination, agreement, validity, and integrity-before it can reach consensus. At the end, all the good nodes will have to agree on one output. To achieve the secondary objective, all healthy nodes will inevitably converge on the same output because of the agreement criterion. To be valid, the validation process must evaluate every node. When the decisions of all nodes are verified by the collective output of the network, then the network may be trusted.

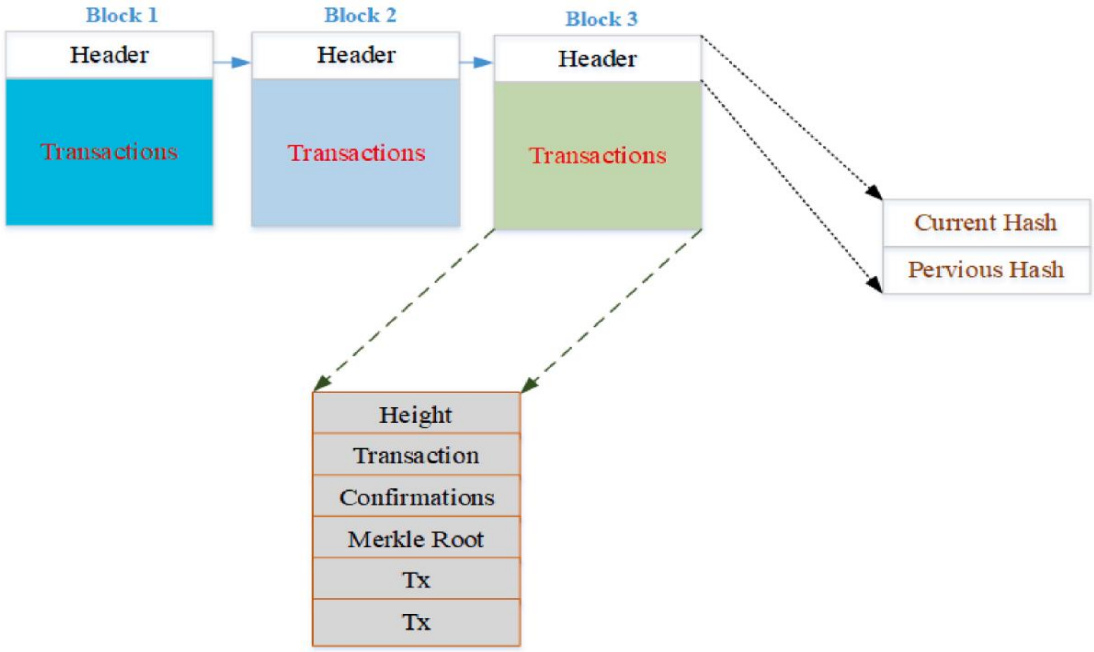

Fig 3. Blockchain Blocks.

Cryptographic Process

Blockchain's decentralized database stores "a growing list of records (each of which is called a block) that are protected from malevolent attackers by means of continuous verification. Each block in a P2P network is a list of transactions that have been accumulated in the ledgers associated with a node in the data structure. A blockchain's block structure is seen in **Fig 3**. This diagram illustrates the basic components of a block, which include a collection of transactions, a timestamp, data from the previous block, and a Merkle root (a transaction tree). In this method, the blocks can be linked to form a chain, and the hash from prior blocks can be used to verify the validity of the entire blockchain. Each node should have entry to the information included within the data blocks they receive. To do this, a block label (often an integer) is added to the block of data to designate a one-of-a-kind hashing algorithm. Each tag represents a predefined hash generator for a node in the previous network. As a result, the data blocks require further processing. With this justification, the nodes will think about encoding the previous/current hash addresses (HAs) with information about the data label of the block to restrict access to the right information. For simplicity, let's pretend the network consists of some nodes, each of which, in iteration r, produces a hash value (current HA) according to its hash function and stores a hash value (previous HA) generated and transmitted by surrounding nodes in iteration r-1. Within a series of nodes, the previous and current HAs been appended to the block label at each node. Two ideas—confirmation and validity of the data block—reflect and present the process's outcome. Nodes in the network will eventually update their data block and label throughout the hashing process, and any malfunctioning nodes will be promptly identified thanks to the encryption technique. The HAs are specified in terms of 32-bit compounded words for a wide range of hash functions, including SHA-512, SHA-384, SHA-256, SHA-224, and SHA-1, and includes the characters 0-9 and A-F". One of the most vital aspects of the blockchain system is the fact that it keeps track of the time it takes for this procedure to complete. Let's say a node's average transaction time is x, and that before sending any data to other nodes, it creates a data block that fully embraces all the transactions. This allows us to derive the following formula for estimating blockchain processing time

$$T_{total\ chain} = x \times T_{signature} + \left(T_{back\ off} + T_{doa}\right) \times 2 + t_{data\ block} + t_{block\ mining} \quad (1)$$

$T_{signature}$ represents the amount of time required to verify the signature. The protocol-specific back-off time, $T_{back\ off}$, the data-exchange latency, T_{doa}, the time required to produce a data block, and the data-block mining latency, $t_{block\ mining}$, are all measured in milliseconds.

Attack Model

Simulating a cyber-attack is a crucial part of validating the proposed concept. Attack graphs, attack trees, and attack networks are the three primary diagram types used in cyberattack modelling research. Using the acyclic directed graph representing relationships between the primary nodes of the network, we can create an attack tree. An "attack graph" can reveal if an invader would be successful in achieving all of their goals by breaking into the network. Modeling network attacks in terms of the attack graph allows researchers to examine the interconnectedness of many aspects of network security, such as the impact and authority of attacks and the effectiveness of security measures taken to counter them. One of the more obvious methods of altering data on a network is the false data injection attack (FDIA). Large data changes in the network can be triggered by FDIA and may be undetected by the typical detection method. It belongs to the category of attack networks and consists of adding fresh information to an existing one. Many hackers may focus their attention on the energy business if they believe they can utilize FDIA to cause unforeseen physical issues and gain financial advantages over other market participants. The first step in solving this conundrum is to model and articulate the FDIA model. So, we'll pretend the attacker has access to the system files. Suppose Q and E represent the information about the system and the goal, respectively, and use equation (2) as the problem function. Clearly, if the attacker replaces Q with Q_{bad}, the value of the objective function will shift from E to E_{λ}. (3). It is crucial to emphasize (4), which states that modifying the system's data should be done in a fashion that leaves the residue norm unaltered to avoid being caught by the corrupt data detection system.

$$E = h(Q) \tag{2}$$

$$E_{\lambda} = h(Q_{bad}) \tag{3}$$

$$\|E_{\lambda} - h(Q_{bad})\| = \|E - h(Q)\| \tag{4}$$

The most crucial step is verifying the attack was successful. Therefore, it is important to specify the following criteria for the FDIA effect:

$$\lambda = h(Q + c) - h(Q) \tag{5}$$

c is the variation associated with the modification of actual data, and λ is the structured attack vector, both defined in the previous equation. Given (5), an effective attack relies on verifying the $h(Q)$ output. Changing the skewed information in the following ways helps narrow the scope of attacks centered on certain targets.

$$Q_{bad,i} = \begin{cases} Q_i + c_i & if\ i \epsilon v \\ Q_i & otherwise \end{cases} \tag{6}$$

Where i is an index describing an attack value (c_i) that will be appended to the system's data (Q_i) in an effort to achieve the desired result (v) number of meters.

Proposed Protected Energy Market Architecture

An autonomous central mechanism is required in the energy market's top-down hierarchical structure to decide the conventional price and the relative strength of the various market participants.

Given the “technological advancements that have been made in today's power system, it is essential that the energy market be pushed toward a P2P design. The protection of the information that is sent between market participants might be considered one of the most crucial challenges”. Microgrids and smart grids are the two separate types of electrical grids that are incorporated into the proposed paradigm. Neither of these grids can function independently of the other.

It is necessary to take a more in-depth look at the objective function of the smart grid as well as the constraints placed on the flow of power. “Each generation unit is responsible for taking into consideration the generation capacity restrictions for both the active and reactive powers. According to the model that has been proposed, it is necessary to compute the overall cost of producing power while considering any operational constraints. These constraints are caused by limitations on the fuel supply and the generators' mechanical conditions. To describe the start-up/shot-down rates of generators, it is necessary to define their power restrictions. The units' ability to generate reserve power makes them attractive participants in the reserve market. at time t, the reserve power limits of the generators. The grid capacity, which is directly tied to the power flow of lines, might inadvertently produce either beneficial or negative effects on the process of selecting the ideal power and, perhaps, reducing the objective function. That's why it's important to model the current in the lines carrying electricity. The bus angles can only go to a maximum or a minimum. Defining the active/reactive

power flow constraints for feeders. In the peer-to-peer energy sector, it is anticipated that the microgrid would play a key role. A microgrid can maintain its operational costs to a low if it buys or sells the additional power at the market rate. Because a centralized microgrid might be necessary for the definition of energy management, the provision of one might be essential. Microgrids consist of a storage facility, distributed generation (DG) sources like a wind farm, solar panels, or a tidal system, and loads that are geographically separated from the grid [18]. A key role of the microgrid system is to allocate power among DGs in a way that satisfies the goal function and all other applicable constraints. The microgrid optimizes the generation price considered for each DG to reduce the associated DG-related and transaction-related operating expenses, as evidenced by (7)". Each DG, such as a wind turbine (WT), tidal turbine (TT), or solar photovoltaic unit (PVU), generates electricity within the bounds of the technologies that enable them. Power storage unit limitations and charging/discharging restrictions are outlined. It goes without saying that at all times, the generated power should be equal to the load. Therefore, the microgrid's power balance is defined by equation (8), where the combined power of generators and loads is equal to the load demand.

$$mincost = min\sum(\mathrm{PWT} + \mathrm{PTT} + \mathrm{PPVU}) \tag{7}$$

$$\mathrm{PWT} + \mathrm{PTT} + \mathrm{PPVU} = \mathrm{PLoad} \tag{8}$$

Proposed Trusted P2P Framework for Energy Management.

The development of a "blockchain-based peer-to-peer (P2P) energy market architecture that ensures the safe flow of data between market participants will be the primary focus of this section. To accomplish this objective, the P2P energy market must develop an acceptable consensus technique that will, among other things, make it easier for market players to engage in power and price transactions that are both effective and efficient. In the peer-to-peer (P2P) energy business, the microgrid is anticipated to play an important role". A microgrid can keep its operational costs to a low by purchasing or selling the additional power at the market rate. Because the concept of energy management can need a centralized microgrid, the deployment of one might be necessary.

It has been suggested that the RCI consensus algorithm might be used as a tool for market participants to come to an agreement on power and price in a way that is compatible with the protocols that are currently in place for blockchain networks. The RCI is analogous to dual increasing techniques, which divide the primary issue into two distinct but interconnected subproblems. These approaches split the problem into two halves. These techniques decompose the primary problem. Finding workable answers to all the subsidiary issues would be beneficial to the overarching objective of fixing the fundamental problem. In the RCI technique, all parties concerned work together toward the goal of finding a solution that satisfies the Karuch-Kuhn-Tucker (KKT) requirements. The RCI technique offers an easy method of addressing the sub-problem, which paves the way for all the participants to exchange as much energy as they can with one another at the best possible price. In comparison to the dual ascent method, the implementation of this method's gradient function contributes to a significant improvement in the solution trend. The Lagrangian Relaxation method takes into consideration not just the restrictions imposed by energy boundaries. **Fig 4** shows the P2P structure connecting the smart grid and the individual microgrids.

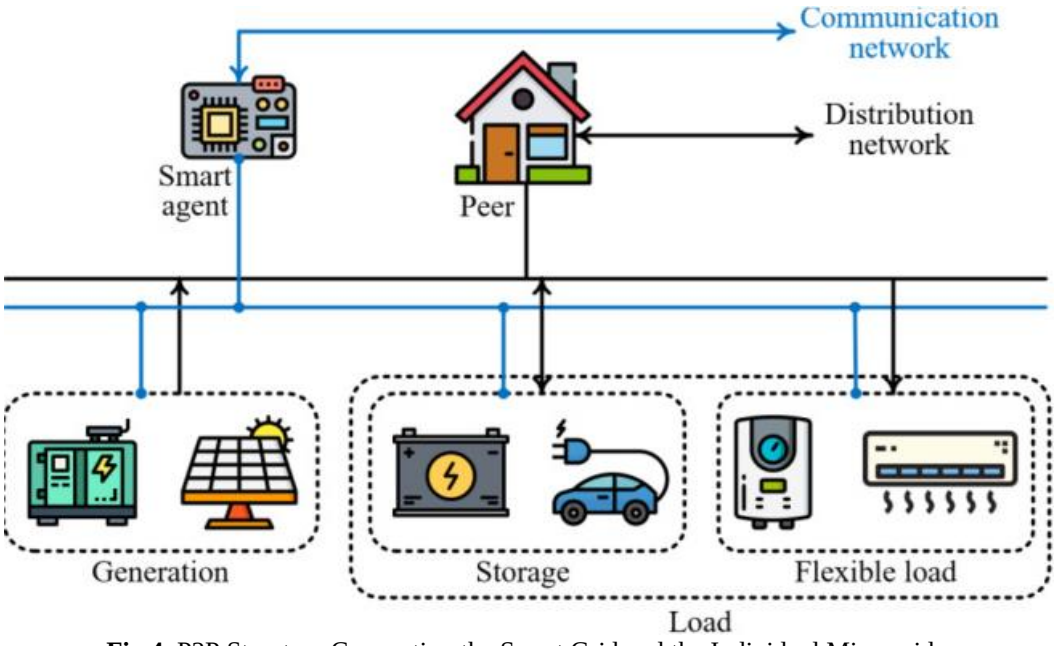

Fig 4. P2P Structure Connecting the Smart Grid and the Individual Microgrids.

Simulation Results

In this part of the article, we test the two primary assumptions that the rest of the research is based on. Testing the blockchain's resistance to hacks and other forms of potentially destructive behaviour is the most pressing concern now. Second, "it is analysed that the efficacy of the proposed consensus algorithm by comparing the traditional centralized energy market with the decentralized peer-to-peer energy market. This helps us determine how well the consensus algorithm works.

Scenario 1: To evaluate how well the proposed consensus approach is in the peer-to-peer energy business

Scenario 2: Evaluating how effective the planned blockchain infrastructure is in comparison to FDIA's

Scenario 3: Consideration of the Impact of Uncertainty on the Peer-to-Peer Energy Market in the paragraphs that follow, we will first describe each scenario, and then go into greater detail about each one.

III. VERIFICATION OF THE SUGGESTED CONSENSUS METHOD IN THE PEER-TO-PEER ENERGY INDUSTRY

Since there are concerns over the safety of the information sent, the first and arguably most pressing problem is the efficiency of the consensus method used in the P2P energy market. This subsection evaluates the suggested algorithm to determine its viability in creating a functional energy market between the microgrid and the smart grid. As was previously said, it is important for the P2P energy market to be able to get trade prices and powers that are optimal for all participants". At first look, considering the full algorithmic process, a P2P-structured energy market appears to be able to efficiently manage power transactions between players, leading to an optimal consensus. "As was previously indicated, the suggested P2P energy market should establish the trading price as an efficient criterion for exchanging power among the participants, in addition to the power transaction. It's clear that the price initially fluctuated widely, but that it has since settled as the number of repetitions has grown. At some point, the market price settled on a stable, time-dependent average. In the energy market, for instance, all players are obligated to either buy or sell at a price of 0.45 per kilowatt-hour ($/kW). It's also worth noting that, from one perspective, the overall cost during the consensus method displays a fluctuating trend comparable to the power/price transaction, as seen in **Fig 5**".

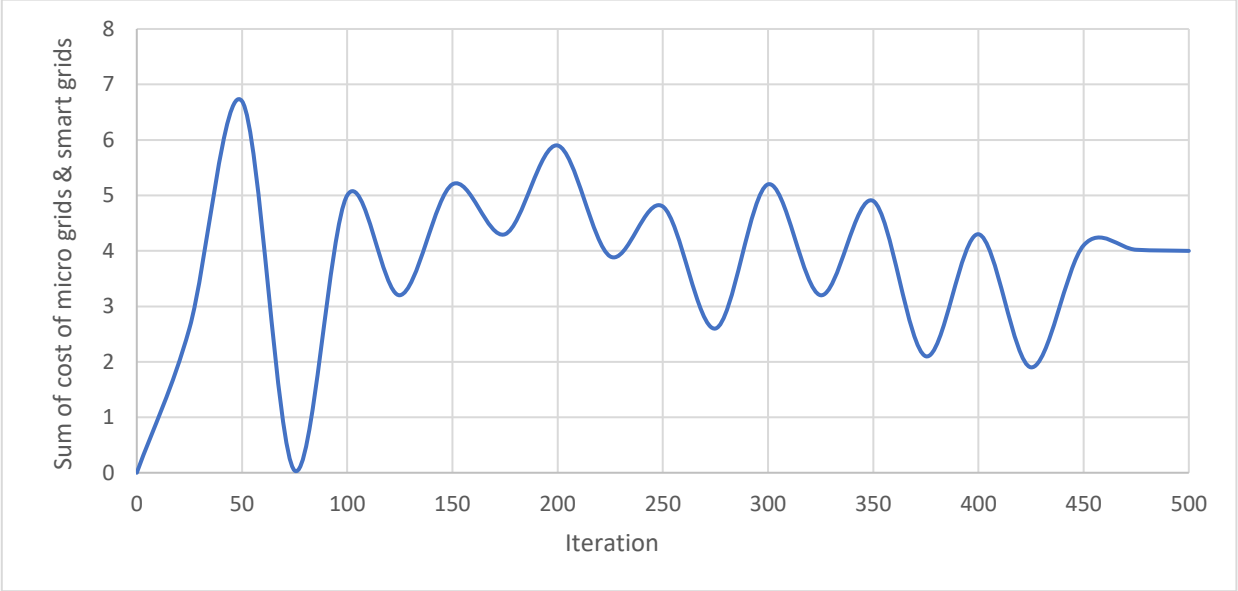

Fig 5. Total Cost.

The combined price tag for the smart grid and the microgrid is close to "4.1107×10^9 ($) dollars. Verifying the outcomes of the proposed peer-to-peer energy market is an important consideration. **Fig 6** and **7** show the comparison between the centralized framework and the suggested P2P structure. Results from the centralized energy market (shown in **Fig 6**) reveal a little discrepancy between the two markets when it comes to power transactions conducted via P2P. The suggested P2P-based energy market displays remarkable accuracy, with a maximum divergence of only 4.16% in power transactions compared to traditional centralized systems. The overall cost is another metric that may be used to evaluate the P2P energy market in addition to the power transaction itself". Total costs for P2P and centralized systems are shown in **Fig 7**. When comparing the centralized and P2P models, you'll notice a small difference (less than 1%) in overall cost: $\$4.11 \times 10^9$. Overall, it appears that the suggested energy market can create an efficient setting in which linked parties can determine and exchange price/power.

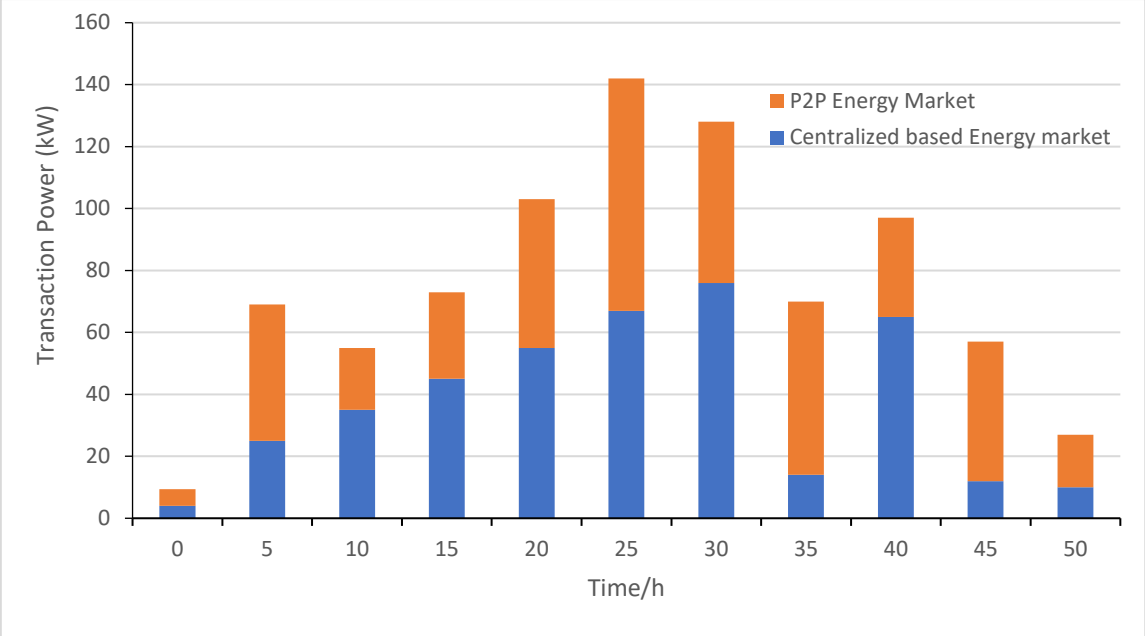

Fig 6. Contrasting The Decentralized and Centralized Models of Power Exchange.

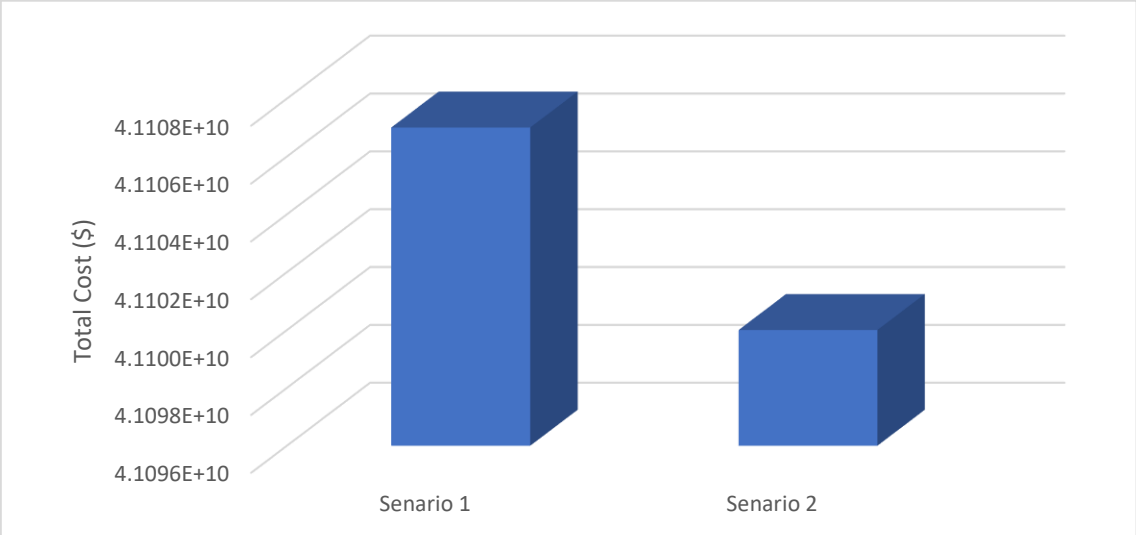

Fig 7. Total Costs in Example Scenario 1 are based on a P2P Structure, whereas those in Scenario 2 are based on a Centralized One.

Comparing Blockchain Framework Performance to FDIA

In this section, we verify that the P2P energy market is safe from malevolent attackers who aim to disrupt the industry standard to further their own political or economic agendas. For an accurate picture of the energy market's safety, it's important to look at how it reacts under attack, without the benefit of the planned blockchain-based protected framework. In "**Fig 8-12**, we simulate an attack of the FDIA kind that is appropriate for use in the P2P energy market with the goal of disrupting the algorithm's consensus process. This attack is suitable for use in the P2P energy market. The power dynamic was thrown off by FDIA, which made it impossible for the parties to reach an agreement through negotiation. Because of the adjustments that FDIA made to the value of the parameter X_k, there are significant fluctuations in the power transactions that take place on both the microgrid and the smart grid. Furthermore, the hacker wants to stay out of a market consensus price. **Fig 12** displays the trade price at time t = 6 that was exposed by the FDIA assault. As can be seen in this study, the trading price exhibits substantial volatility, suggesting that there is no consensus price in the P2P energy market, despite the increasing number of iterations. In conclusion, the results show that the attacker can succeed in destroying the P2P energy market without a robust security infrastructure. Considering this, we want to implement a new blockchain framework in the P2P energy market", the details of which will be laid forth below.

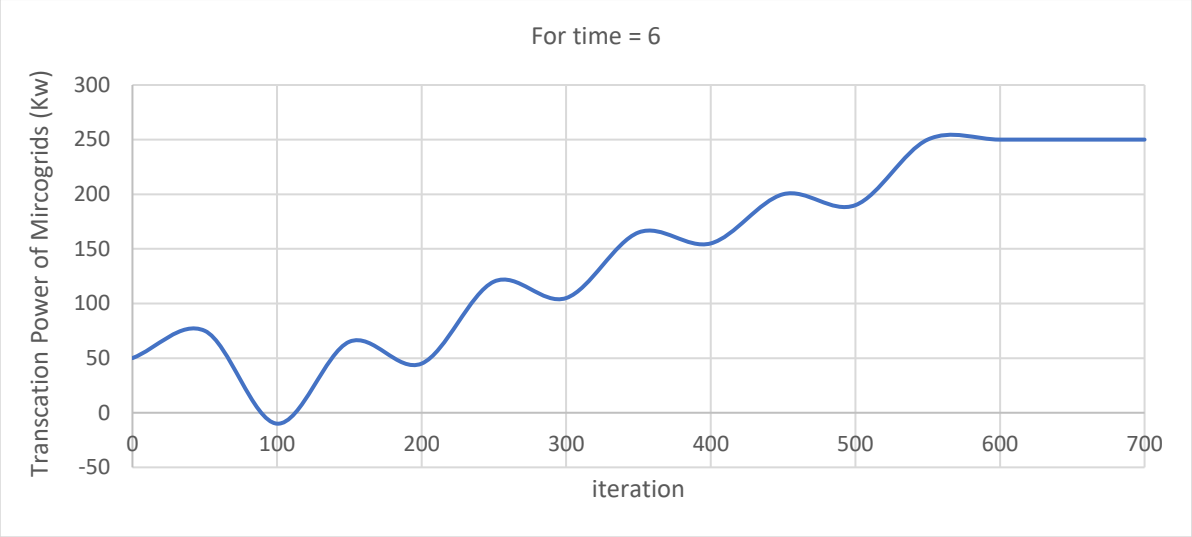

Fig 8. Microgrid Under Attack Power Exchange at time t = 6.

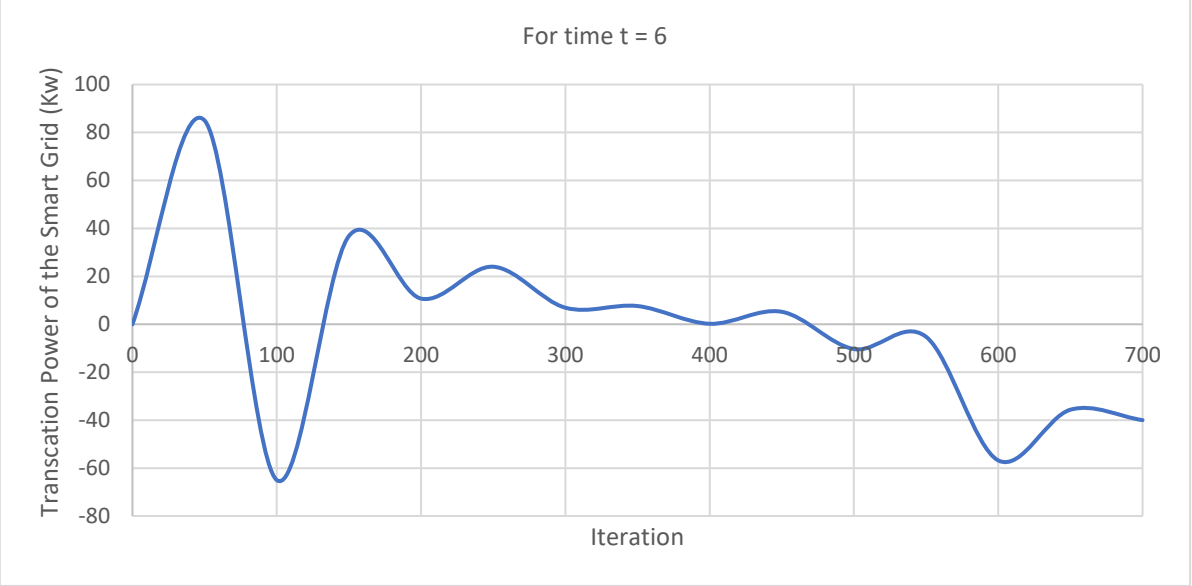

Fig 9. At time t = 6, the Smart Grid's Power Transaction.

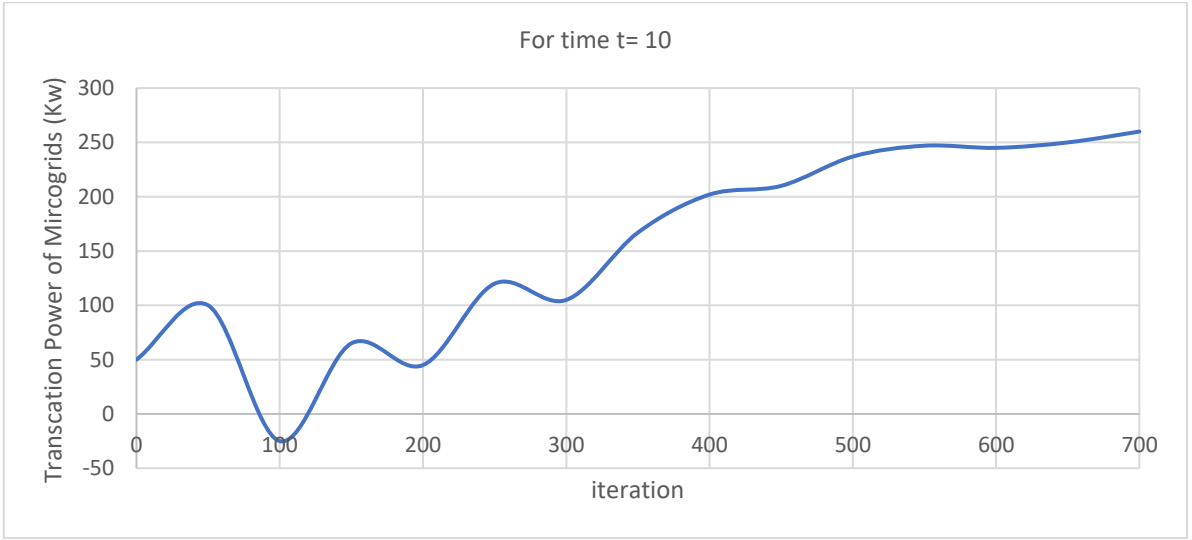

Fig 10. Microgrid Under Attack Power Exchange at time t = 10.

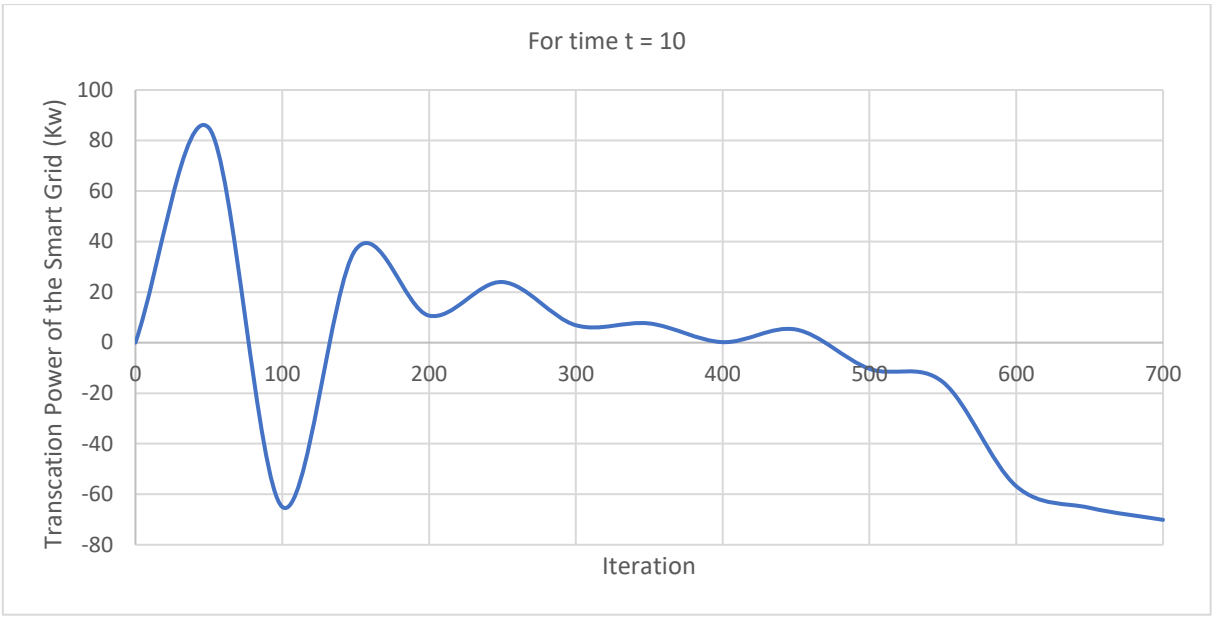

Fig 11. At time t = 10, the Smart Grid's Power Transaction.

Proof-of-Concept for Attack-Resistant Blockchain

In this part, we employ a "probability computing approach to show the likelihood of successful attacks in order to demonstrate the efficacy of the proposed blockchain based architecture against cyber-attacks". When a wrong request is approved, the entire consensus shifts. There are three entry points through which attackers might compromise the information process. Second, disrupt the flow of data during transmission. Third, accounting record manipulation in the database. In this work, we calculate the probabilities of the first two attack modes to assess the blockchain's efficiency. These assaults do not necessarily stop the system from functioning, but they do cause errors in calculations. To prevent data tampering or invalid requests, the blockchain provides a safe and reliable method. "The technological limits of the energy market in power systems should be considered during the transaction planning process". As a result, confirming the wrong request or manipulating the wrong data causes the system to deviate from its optimal operating point. To launch any form of attack, the hacker must first break into the network. Any part of the network is fair game for this type of intrusion. Because there are two distinct forms of sabotage that attackers can employ following a network penetration, the likelihood of each must be determined.

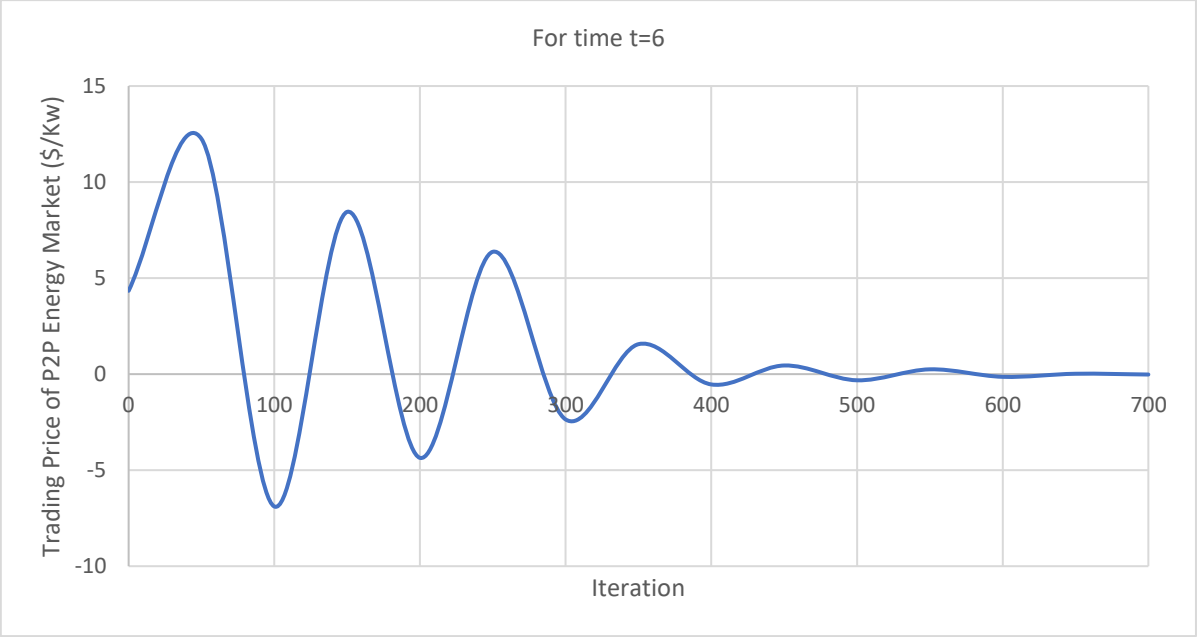

Fig 12. The t = 6 Pricing Transaction that is being Attacked.

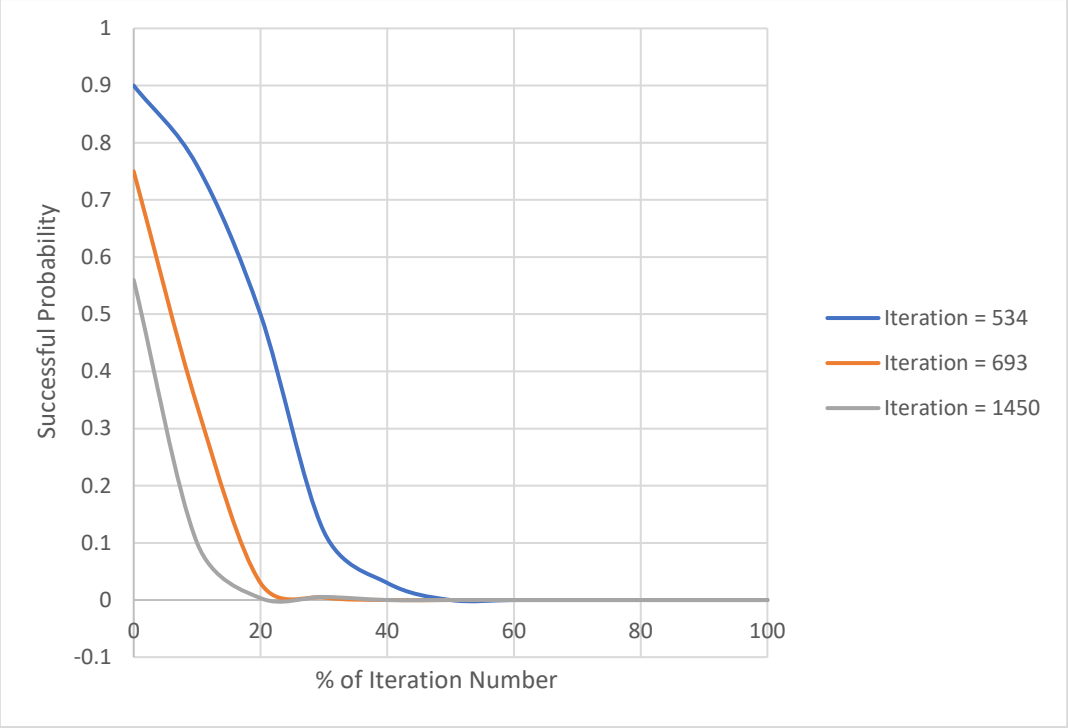

Fig 13. Probability of Success for The Attacker in Their Attack on The Proposed Security Platform.

With the distributed consensus algorithm's inability to arrive at the same result, assaults have zero chance of succeeding because blockchain won't validate them. "Since the data is encrypted using cryptography and the data chain concept, the likelihood of an attack succeeding reduces with each successive round of data transmission". **Fig 13** demonstrates a decreasing trend in the success probability of attacks when stated in terms of the percentage of repetitions. The attack success probability can be thought of as lying in the range [0.9, 1] depending on the processing power available. An experiment comparison graphic is provided for the different iterations in **Fig 13**. **Fig 14** shows uncertainty-based microgrid power transactions.

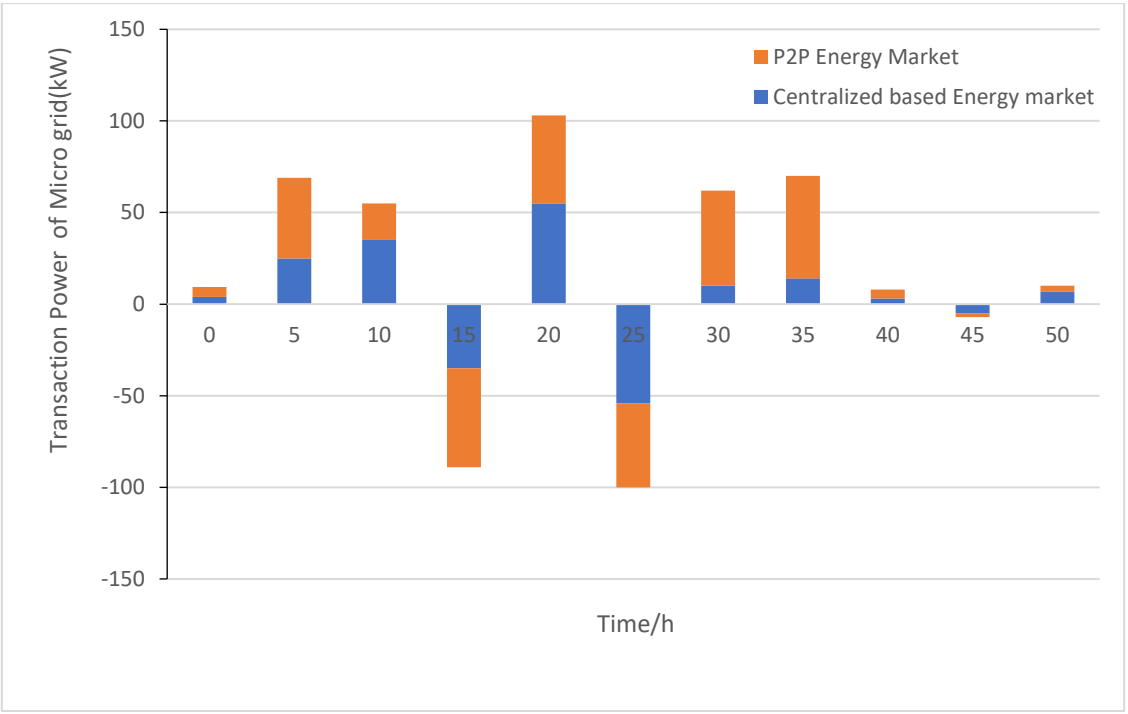

Fig 14. Uncertainty-Based Microgrid Power Transactions.

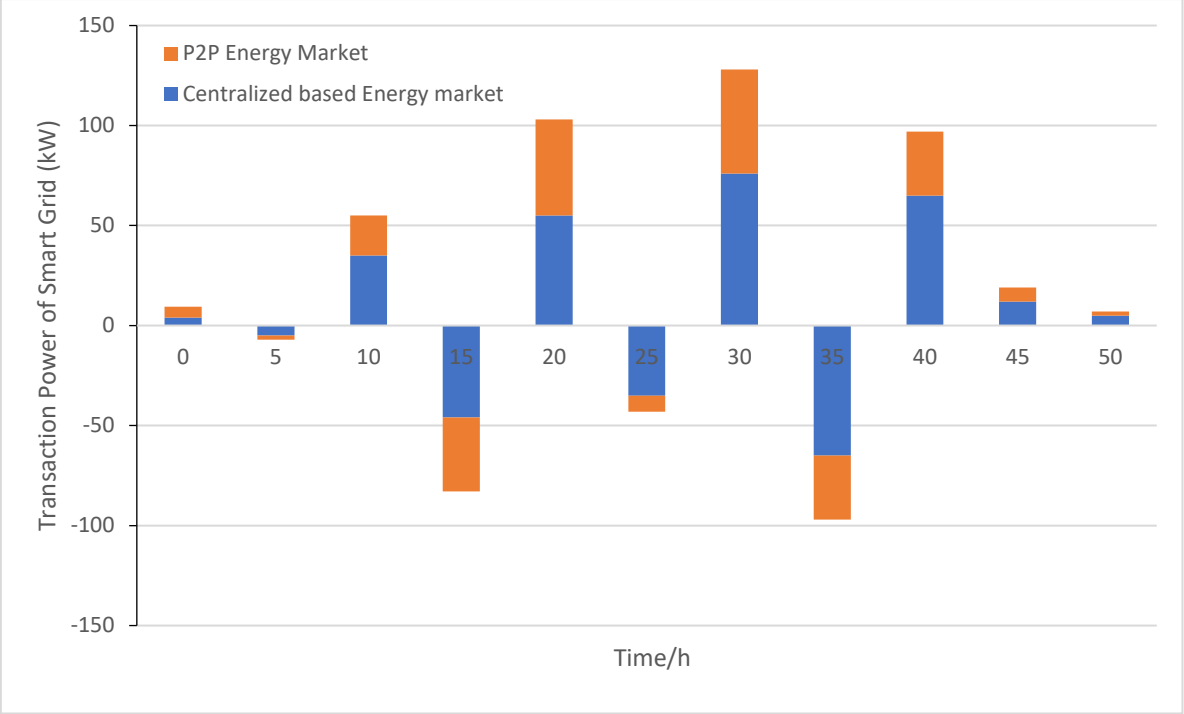

Fig 15. Power Transaction of The Smart Grid Under Uncertainty Condition.

Implications for The P2P Energy Industry at Current Levels of Unpredictability

The stochastic model was able to capture the considerable fluctuations in power/price transaction that were induced by uncertain parameters. These swings, in turn, led to changing behavior on the part of each individual player. **Fig 15** is a representation of the power transition that occurs within the smart grid while it is operating in an unpredictable environment. This transition is comparable to that which occurs within the microgrid system. The changes in the energy market have caused the maximum values of the power transaction to be altered to 25%, 10%, and 10% at 21, 10, 5, and 5, respectively. These new values consider the volatility of the energy market. The quantity of unknowns in a microgrid setup appears to increase the impact of uncertainty on power transactions almost to the level of that in a smart grid setup. For the P2P energy market to reach a consensus on an accurate solution for all participants, it is crucial to take stochastic analysis and uncertainty modelling into account.

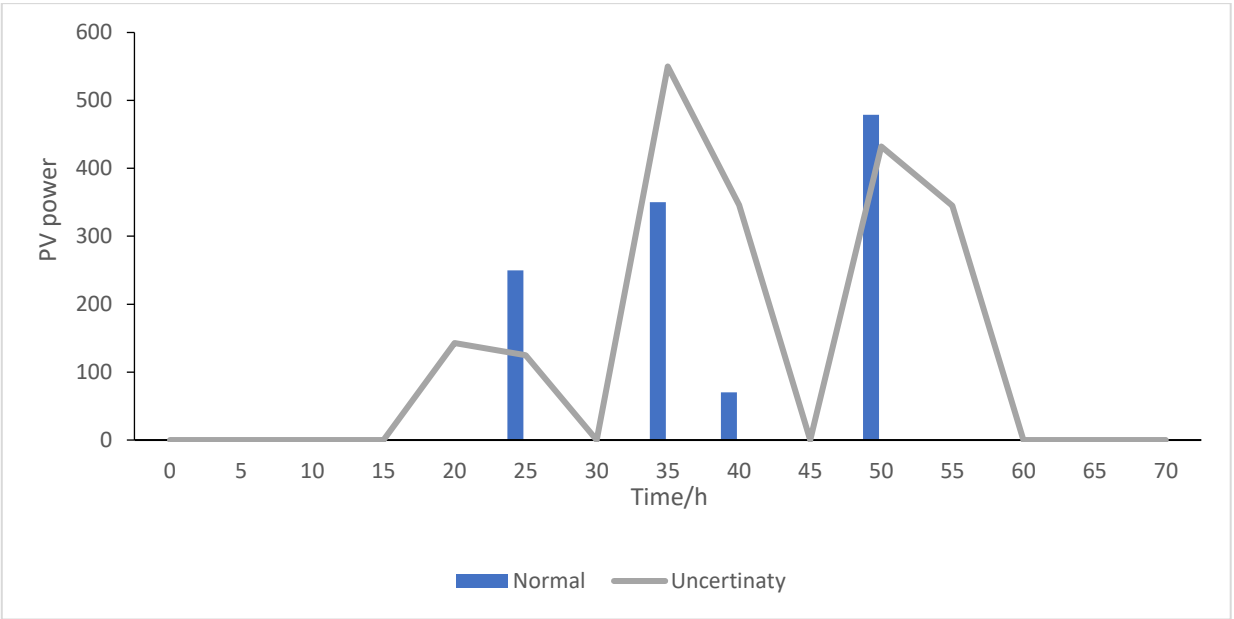

Fig 16. Normal/Uncertain PV Power.

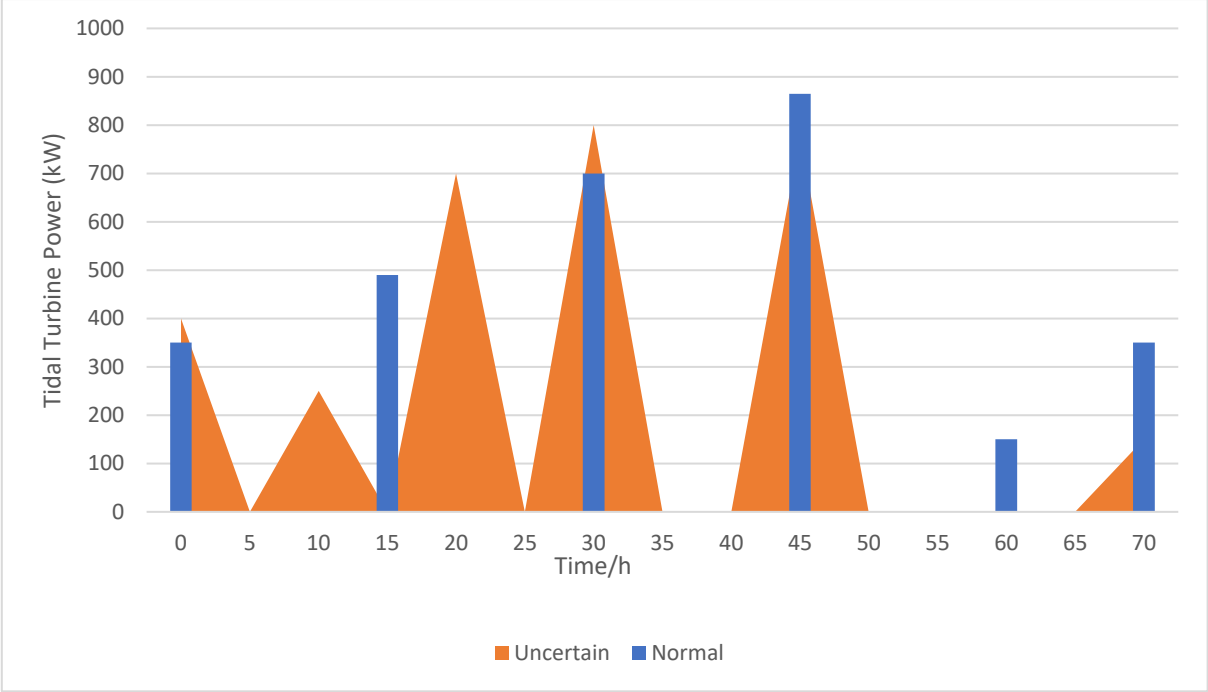

Fig 17. Normal/Uncertain Tidal Turbine Power.

The operation of the microgrid's photovoltaic, wind, tidal turbine, and storage units is depicted in **Fig 16–18** under both normal and uncertain conditions. "As was indicated before, the microgrid is composed of PV, WT, tidal turbine, and storage units. Notably different values when comparing the current circumstance to the typical one indicates that the stochastic model has changed the output power of DGs. According to **Fig 16**, the hours of largest variance (about 78%) in PV power occur during times of uncertainty (such as t = 11). **Fig 17** and **18** present the results of the tidal turbine and the wind turbine, respectively, in a manner comparable to that of PV. In the stochastic framework, the generation-demand balance causes WT's output to drop dramatically, in contrast to the tidal unit, whose uncertainty model led to an increase in generated electricity. As can be observed in **Fig 19**, the total operating cost is higher under the uncertain situation than under the regular one. This increase amounts to \$4.8× 10^9. (see **Fig 5**). To summarize, it is best for each player in the P2P energy market to make advantage of the stochastic framework in order to maximize the benefits of increased bargaining power".

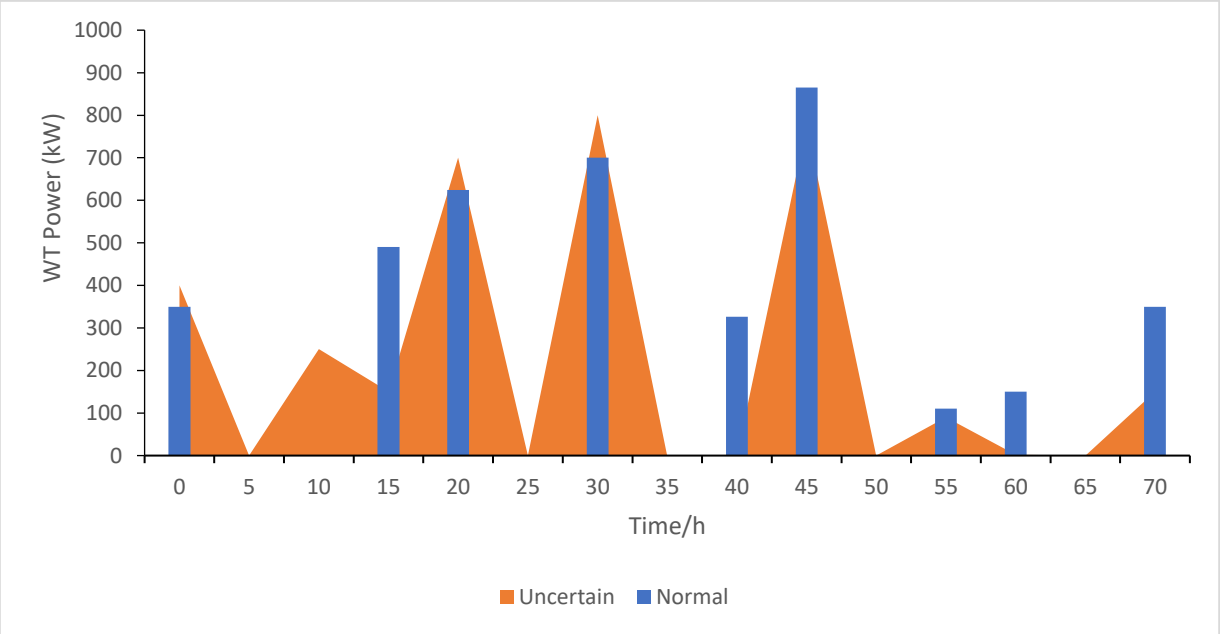

Fig 18. Normal/Uncertain WT Power.

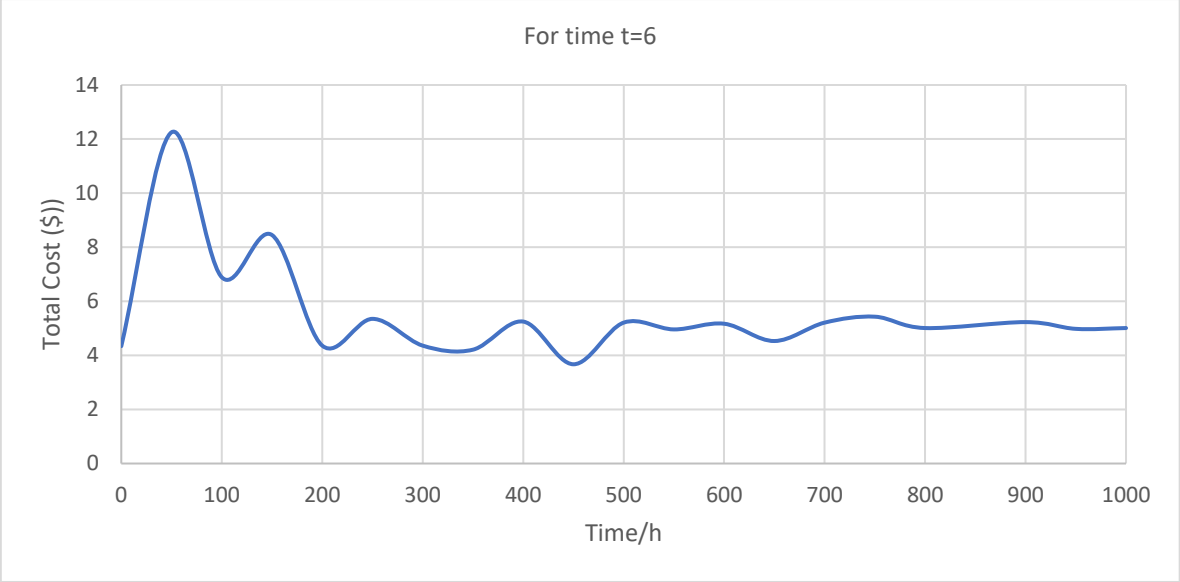

Fig 19. Stochastic Operation Cost.

IV. CONCLUSION

Within the scope of this study, "a peer-to-peer energy market that is capable of functioning in conjunction with both smart grids and microgrids was developed. We evaluated the efficiency of a distributed consensus method that utilizes the blockchain as its underlying infrastructure. All of this was accomplished even though the FDIA was launching an assault. The first is to keep the system secure even when under attack, and the second is to come to an agreement even when cyberspace is under siege. This pattern has developed, and the agents now trade blockchain-based transactions with one another. That the P2P market's output response is so like that of the centralized market is one of the study's most important conclusions. Even when the system is under cyber-attack, the variance is less than 1%. Even though there has been a cyber-attack, the consensus process is still active. The stochastic findings support the proposed uncertain model's claim of high dependability and acceptable performance. In conclusion, the influence of security on the consensus system has been demonstrated, showing that the absence of a blockchain results in unguaranteed convergence of the consensus. This study contributes to the expanding corpus of research on the peer-to-peer (P2P)" energy market that operates on a decentralized model.

CRediT Author Statement

The authors confirm contribution to the paper as follows:
Conceptualization: Mahamoodkhan Pathan and Rameshkumar J; **Methodology:** Chintalapudi V Suresh; **Software:** Chintalapudi V Suresh and Rameshkumar J; **Data Curation:** Chintalapudi V Suresh; **Writing- Original Draft Preparation:** Rameshkumar J; **Validation:** Mahamoodkhan Pathan and Rameshkumar J; **Writing- Reviewing and Editing:** Chintalapudi V Suresh; All authors reviewed the results and approved the final version of the manuscript.

Data Availability

No data was used to support this study.

Conflicts of Interests

The author(s) declare(s) that they have no conflicts of interest.

Funding

No funding agency is associated with this research.

Competing Interests

There are no competing interests

References

[1]. J. Abdella and K. Shuaib, "Peer to Peer Distributed Energy Trading in Smart Grids: A Survey," Energies, vol. 11, no. 6, p. 1560, Jun. 2018, doi: 10.3390/en11061560.
[2]. 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, Aug. 2019, doi: 10.1109/tsmc.2019.2916565.

[3]. M. J. Fell, A. Schneiders, and D. Shipworth, "Consumer Demand for Blockchain-Enabled Peer-to-Peer Electricity Trading in the United Kingdom: An Online Survey Experiment," Energies, vol. 12, no. 20, p. 3913, Oct. 2019, doi: 10.3390/en12203913.
[4]. Shipworth, D. Peer to Peer Distributed Energy Trading Using Blockchains. Available online: http://www.ieadsm.org/wp/files/IEA-DSM-Spotlight-Issue67-December20171.pdf (accessed on 30 January 2020).
[5]. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 30 January 2020).
[6]. Shipworth, D. An Explorative Study on the Implications of Prosumer-Consumer Communities on the Value Creation in the future Electricity Network. Available online: https://doc.rero.ch/record/277573/files/GstreinM.pdf (accessed on 30 January 2020).
[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, Sep. 2018, doi: 10.1109/tdsc.2016.2616861.
[8]. Son, Y.B. Data-Protected Blockchain Using Inner Product Functional Encryption. Master's Thesis, Inha University, Incheon, Korea, 2020.
[9]. Y. Yuan and F.-Y. Wang, "Blockchain and Cryptocurrencies: Model, Techniques, and Applications," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 48, no. 9, pp. 1421–1428, Sep. 2018, doi: 10.1109/tsmc.2018.2854904.
[10]. Ethereum. Available online: https://ethereum.org/ (accessed on 23 January 2020).
[11]. Ethereum White Paper. Available online: https://github.com/ethereum/wiki/wiki/white-paper (accessed on 23 January 2020).
[12]. C. Dannen, Introducing Ethereum and Solidity. Apress, 2017. doi: 10.1007/978-1-4842-2535-6.
[13]. L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making Smart Contracts Smarter," Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, vol. 3, pp. 254–269, Oct. 2016, doi: 10.1145/2976749.2978309.
[14]. Ben-Sasson, E.; Chiesa, A.; Tromer, E.; Virza, M. Succinct non-interactive zero knowledge for a Von Neumann Architecture. In Proceedings of the 23rd USENIX Security Symposium 2014, San Diego, CA, USA, 20–22 August 2014; pp. 781–796.
[15]. E. Ben Sasson et al., "Zerocash: Decentralized Anonymous Payments from Bitcoin," 2014 IEEE Symposium on Security and Privacy, May 2014, doi: 10.1109/sp.2014.36.
[16]. B. Bünz, S. Agrawal, M. Zamani, and D. Boneh, "Zether: Towards Privacy in a Smart Contract World," Financial Cryptography and Data Security, pp. 423–443, 2020, doi: 10.1007/978-3-030-51280-4_23.
[17]. A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," 2016 IEEE Symposium on Security and Privacy (SP), May 2016, doi: 10.1109/sp.2016.55.
[18]. Megha, S.; Lamptey, J.; Salem, H.; Mazzara, M. A Survey of of Blockchain-Based Solutions for Energy Industry. Available online: https://arxiv.org/pdf/1911.10509.pdf