An effective secured peer-to-peer energy market based on blockchain architecture for the interconnected microgrid and smart grid

An Effective Secured Pee-to-Peer Energy Market Based on Blockchain Architecture for the Interconnected Microgrid and Smart Grid

Abdollah Kavousi-Fard[1], Abdulaziz Almutairi, Ameena Al-Sumaiti[2], Amir Farughian[3], Saeed Alyami

1-University of Michigan, Dearborn, MI, USA.

2-Department of Electrical Engineering, College of Engineering, Majmaah University, Almajmaah 11952, Saudi Arabia.

2-Department of Electrical and Computer Engineering, Khalifa University, Abu Dhabi, UAE. (e-mail: ameena.alsumaiti@ku.ac.ae).

3- School of Technology and Innovations, University of Vaasa, Vaasa, Finland (amir.farughian@uva.fi)

Abstract—One of the most significant current topics in the energy market is the decentralized operation of the power system wherein the entire discipline is constructed based on the consensus concept. In such a framework, an agreement among all effective participants in the market should be brought without the presence of an independent arbitrator. This paper proposes a secured energy market architecture based on peer-to-peer (P2P) idea to provide an appropriate platform based on the decentralized network and key aspects of energy market, including network architecture, interface communication, and network security. It is apparent that communication interfaces connecting the market participants is a fundamental property for achieving this purpose and that must be secured against the malicious attacks. In this regard, reaching the secured consensus is guaranteed by providing a new blockchain platform coincided by P2P energy market. The energy market is conducted by an effective Relaxed Consensus-Innovation (RCI) based algorithm with the aim of bringing the power/price exchanged among connecting participants in the form of P2P structure. In the proposed model, a microgrid and a smart grid are considered as the market participants, who tend to negotiate with each other in a way that follow their own benefits in the secured environment. The microgrid includes the wind turbine (WT), photovoltaic (PV), tidal turbine and storage unit to satisfy its demand and the smart grid is composed of distributed generations (DGs) and lines in the form of the IEEE 24-bus test system. In order to handle the uncertainty effects in the problem, a stochastic framework based on unscented transform (UT) is proposed in the P2P energy market. In order to assess and verify the fault-tolerant system ability against the cyber-attack, the fault data injection attack (FDIA) is modeled and applied to the P2P energy market in a blockchain platform. The simulation results approve the appropriate performance and applicable nature of the proposed concepts in this paper.

Index Terms—Secured P2P energy market, Blockchain architecture, Microgrid, Smart grid, RCI approach, Unscented transform.

NOMENCLATURE

Sets/Indices	
$e\ /\ \Omega^{e}$	Set/index of line
$y\ /\ \Omega^{y}$	Set/index of generator
$t\ /\ \Omega^{T}$	Set/index of time where $\Omega^{T} = \{1\ldots24\}$.
$b, m\ /\ \Omega^{b,m}$	Set/index of number of bus
Constants	
$\mathcal{X}$	Solar radiation
R^{loss}	Power loss related to PV
T_t^V	Wind speed
T_{cutin}^V, T_{rated}^V	The cut-in and rated tidal current speeds
Q	Direct irradiation
γ	Sea water density
λ	Swept area of the turbine blades
S	Wind density
C	Area of rotor blades
$S_{t,y}, D_{t,y}$	Shut up and shut down of the generator.
U_t^{PV}	Capacity of the PVs
$P_{e,t}, Q_{e,t}$	Electrical demands of the smart grid.
$V^{\min}, V^{\max}$	Maximum and minimum value of the storage system energy
P_t^{load}	the demand of the microgrid
P^{min}, P^{max}	Limits of generation active power
Q^{min}, Q^{max}	Limits of generation reactive power
D_G^{+}	Limits of reserve
P	Generation price of the generator.
RW_t, RTI_t, RPV_t, RB_t	Prices of the WT, tidal, PV and storage system, respectively.
$P_e^{max}, P_e^{min}, Q_e^{\max}, Q_e^{min}$	Maximum and minimum of the transaction power of the line
z, w	Value of the average and variance

W^0	weight of the mean value
A_{aa}	covariance matrix
c	Number of uncertain parameters
X	Actual data
X_{bad}	False data
R	vector of stochastic inputs
Variables	
PB_t, PW_t, PTI_t, PPV_t	Power output of the storage, WT, tidal and PV, respectively.
P_{sd_t}	The generations of the smart grid
P_{m_t}	The generations of the microgrid
H_t	Slackness variable
H_t^m, H_t^{sd},	Slackness variables of the microgrid and smart grid, respectively
$Q_{t,y}, Q_{e,t}$	The generation reactive power of the generators and the line reactive power flow.
$P_{t,y}, P_{e,t}$	The generation active power of the generators and the line active power flow.
P_t^{TM}, P_t^{TS}	The exchanged powers between the microgrid and the smart grid.
P_t^{ch}, P_t^{dis}	Ch/Dis powers of storage.
$R_t^{TM(k)}, R_t^{TS(k)}$	Auxiliary coefficients related to microgrid and smart grid
$\kappa_{t,y}$	Binary variables of the generator.
TV_b, η_b	Voltage and angle of the bus.
VB_t	Energy of the storage system.
$\beta_t^{TS(k)}, \beta_t^{TM(k)}$	The trading prices between the microgrid and the smart grid.
mic, C_G	Costs of the microgrid and the smart grid, respectively.

I. INTRODUCTION

In recent years, researchers in the field of energy management and electricity market have paid much attention to the way that energy transactions happen in the market models with the local control [1, 2]. Such research follows two basic approaches: the first one is the participation of all producers and consumers in trading the over plus energy, and the second one is the production of power by the use of the local renewable energy sources [4, 5]. Technically, if the energy transaction does not have to follow any regulation protocol, only few producers will benefit in the energy market, when they can play with the market clearing price or result of tenders [6-7]. In this regard, the peer-to-peer (P2P) electricity market was introduced as a solution [8] in which all agents can participate in the energy trading process, and thus get the opportunity to attend the market plans. Since the peer-to-peer structure does not have any central supervisor, the active players must negotiate with each other on a price and energy transaction platform. To implement the peer-to-peer energy transaction in the power grid, the network graph has a great impact on the energy market. Therefore, graph theory can be used to achieve a fair consensus in the market [9].

In this paper, the expression "neighbor" refers to two agents with a physical relationship together based on the graph network [10]. By creating such a peer-to-peer market that all components try to play actively, the behavior of consumers will be affected and change [11]. In this situation, all agents are allowed to express their suggestions. Therefore, peer-to-peer energy trading must have the following characteristics: transparency in the data transactions, privacy in the data broadcasted, access to big data and local data and avoiding central monitoring [12]. In [13], a P2P market structure is designed that the uncertainty risk is optimized using the Markowitz portfolio theory and such a market structure enhances the welfare of sellers and buyers simultaneously. In [14], a peer-to-peer energy market is developed using the gas-energy storage system to minimize the feeder congestion and enhance the social welfare. In [15], a P2P architecture with dynamic tariff is suggested and the work models the money flow between all agents. The results show that such a structure would provide proper savings for the prosumers and consumers, concurrently. To implement the peer-to-peer energy transaction, a useful method is the Relaxed Consensus- Innovation (RCI) method that is presented by G. Hug et al in [16]. This method is examined on a power grid in which the loads are supplied by the distributed sources and it is suggested that using RCI can be useful for energy management by creating coordination among the local producers and active loads. The solution of the RCI method is based on the Lagrange mathematical method with boundary constraint in which the objective function is the marginal cost [17, 18]. Given all that has been mentioned so far, the RCI method is executed on a decentralized platform and it is demonstrated in several previous studies [19-21] that the output response of the RCI method is so close to the solution attained by the centralized approach but with much higher convergence speed.

With the growing concern over the air pollutions in recent years, the renewable energy sources could attain a brighter and more effective role in the power grids [22-23]. The clean nature, high accessibility at different regions and local power generation too close to the end users are some of the most significant features of these sources which could support their role with higher penetration compared to the conventional fossil fuel based DGs. Unfortunately, all renewable energy sources including the wind turbine and photovoltaic systems have a volatile nature and their output changes depending on the weather condition [24]. Moreover, the electric load estimation/prediction is not a hundred percent correct which makes it an uncertainty source in the power system. In such a situation, it is clear that an appropriate framework is needed to handle and model the uncertain parameters in the power grid for making the realistic analyses. In the literature [25], a variety of methods is developed to handle the uncertainties of the system, showing the specific advantages and drawbacks. In a general classification, there are three main classes for handling the uncertainty effects: 1) Monte Carlo simulation, 2) analytical methods and 3) approximate methods. The Monte Carlo simulation is the most accurate but with the cost of high computational burden. Analytical methods could overcome the high computations of the first group but make use of some simplifications in the problem which can reduce its accuracy. Finally, the last group can provide an appropriate accuracy with a low computational effort.

This paper makes use of the unscented transform (UT) method, which belongs to the approximate class, due to its high uncertainty modeling capability, low computational burden and correlated structure. Moreover, the RCI method has been deployed with a modification based on the blockchain technology. In 2008, a paper was published in [26], called Bitcoin: A Peer-to-Peer Electronic Cash that presented several cryptographic techniques and a peer-to-peer network to guarantee payments without the association of any central authority [26]. The main idea is constructed based on the so-called "blockchain" technology, which makes use of a chain of blocks to secure the data transactions.

Authors in [27] have suggested a blockchain based secure structure to achieve secure demand response problem within the electrical grid. They provided an effective algorithm to opt true nodes to validate the data blocks and to add them to the blockchain structure. Using such structure, the edge calculating and contract concept, the authors in [28] tried to present a secure energy transaction framework for vehicle-to-grid technology with the aim of converging between load and supply. However, in [29] have been proposed the consortium blockchain framework in other to trade energy among electrical vehicles. Also, many other works provided to handle the energy exchanging issue of electrical grids which is secured by blockchain technology

[30]. It is shown in [31] that the blockchain is used to increase the system reliability and avoid fraud in the operating costs. With regard to above literature, this paper aims to concentrate on providing an energy market based on the P2P structure wherein the consensus among all participants is guaranteed by using an appropriate RCI based consensus algorithm. In addition, providing a safety environment based on the blockchain framework to exchange energy among participants is considered as another goals of this paper. Hence, in our research, blockchain technology is deployed to achieve a whole consensus with the RCI method. To this end, the RCI method is modified for distributed calculation and is deployed then as a user for the blockchain system. It will be shown that the proposed RCI-blockchain based architecture will let the system reaches a consensus with an appropriate security. In order to assess the performance of the proposed secured architecture, a cyber attack of type fault data injection attack (FDIA) [32] is modeled, simulated and launched against the system. In order secure the data transactions among the neighboring agents, the proposed consensus algorithm is interconnected to the blockchain system so that the consensus process is not disrupted when there is compromised data.

Given all of the above, the main contributions can be summarized as follows:

- Suggesting an appropriate blockchain structure based on secured peer-to-peer energy market transactions between the microgrid and the smart grid.
- Modeling and implementing FDIA attack to appraise the security of the proposed architecture in the peer-to-peer energy market.
- Developing a stochastic framework based on unscented transform for the proposed peer-to-peer energy market under uncertainty conditions.

The rest of the paper is managed as follows: Section II represents the proposed security management architecture based on the blockchain platform. Section III proposes the secured P2P energy market structure. In section IV, the stochastic framework based on UT is explained to handle the uncertainty effects. The simulation results on the standard test system are discussed in section V. Finally, the main outcomes and merits of the proposed method are described in section VI.

II. BLOCKCHAIN FRAMEWORK BASED SECURITY MANAGEMENT

This section is dedicated to express how the blockchain architecture can provide a secured effective management architecture for the modern networks. The blockchain technology has engrossed a wide range of attention, ranging from the financial markets and healthcare to the industrial processes and the electrical power system. The very successful instances of applications of this security structure can be named as the voting process, identity management and honesty of data brought from the internet of things (IOT) [29]. The blockchain structure is based on a distributed, released and fault-tolerant database in which every component or node can share its information while no node can make a specific control. This framework provides a highly secure environment against attackers who tend to penetrate to the network in order to compromise the data. In other words, the blockchain system considers the existence of malicious behaviors related to attackers and tries to deactivate their adversarial strategies by using the honest nodes, which are able to make high computational processing. In the rest, two vital parts of the proposed architecture including the blockchain network procedure and attack model are explained in order to elaborate on validating the security environment provided by the blockchain system against the malicious attackers.

A. Blockchain Structure

The first and perhaps the most significant feature of the blockchain is that it does not need to a central trusted system and can operate for exchanging information among nodes in a decentralized environment. Blockchain can allege appropriate conditions for trustless systems, wherein an agent participates in the transactions in the lack of reciprocal trust. On the other hand, the reconciliation trend, which should be handled between nodes by a consensus algorithm, can be sped up because of eliminating the central authority in the blockchain structure. In addition, data broadcasted by nodes in this process will be crypto graphed for enhancing the reliability of secrets. All in all, the blockchain system has key advantages in comparison with the centralized database as follows: 1- in the blockchain process, trades are validated and authorized based on a verification procedure managed by a consensus algorithm and 2- blockchain system needs no architecture to connect nodes in the network and organizes them in a peer to peer structure. Fig. 1

demonstrates the basic concept of the blockchain system. As shown in the above argument, the blockchain system' effectiveness depends on three various sections, including the decentralized network, consensus algorithm and cryptographic process.

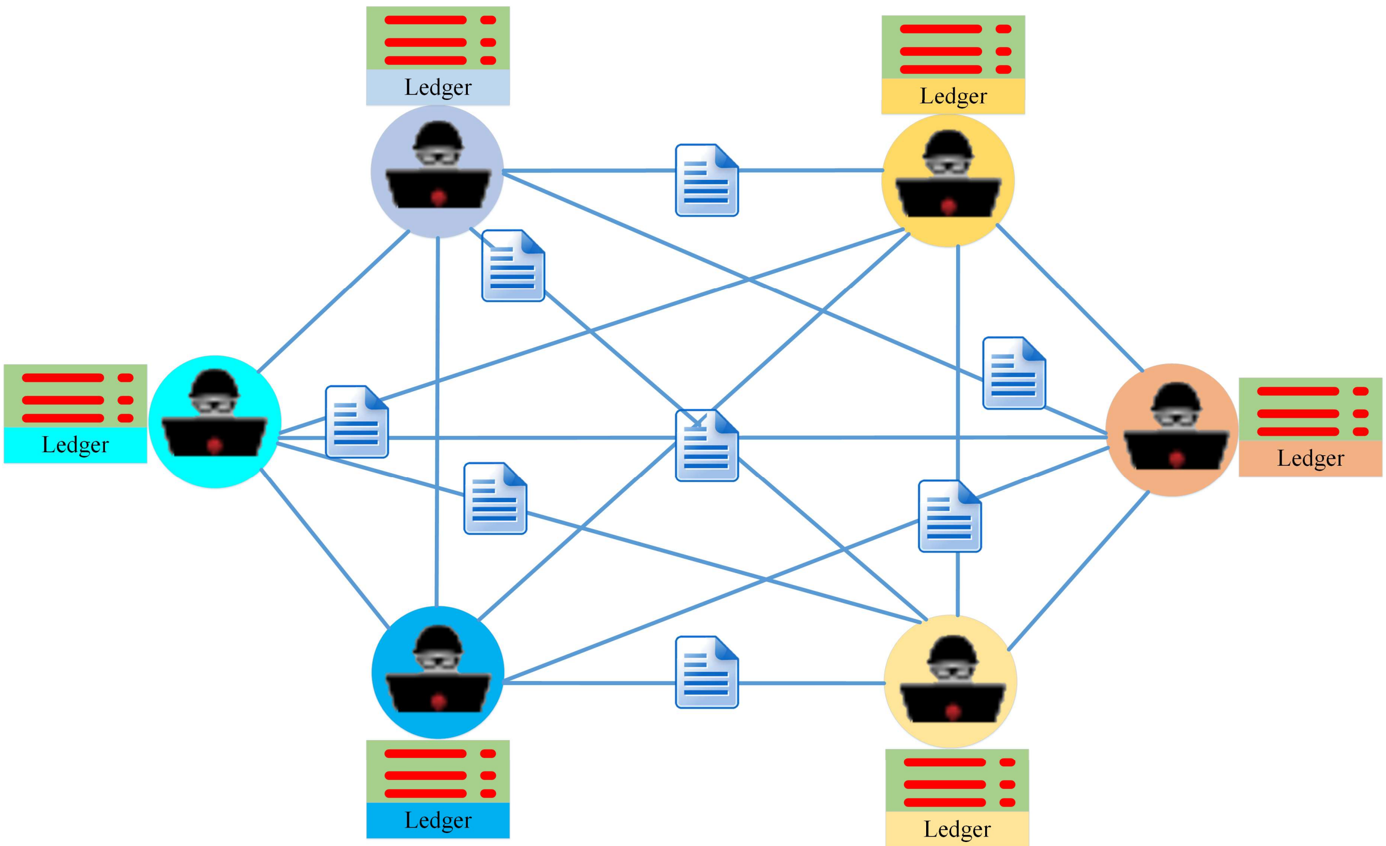

Fig. 1. The blockchain network process

1) *Decentralized network*

The foundation concept of the decentralized network is to enhance the propagating process of messages exchanged among nodes for retaining the distributed legers defined in every node. The network protocol related to the blockchain system permits to broadcast the messages transferred from a node to other nodes in a decentralized structure. Albeit, the network has no pure broadcast process and the nodes of the network are allowed to release their messages to show valid exchange of data. Technically, the network can be either public blockchain or private blockchain with regard to the graph constituted among nodes that will be efficacious on the network security [33]. Apart from being the private and public blockchain, the decentralized network should be performed by concerning on a peer to peer structure in which the nodes can join/leave to/from the network, independently, as shown in Fig. 2. On the other hand, this network architecture is built so robust in order to decline the failures of the nodes and links among them. Overall, in the first stage of the blockchain process, its architecture needs to be designed as a decentralized network based on the peer to peer framework to meet the redundancy and robustness.

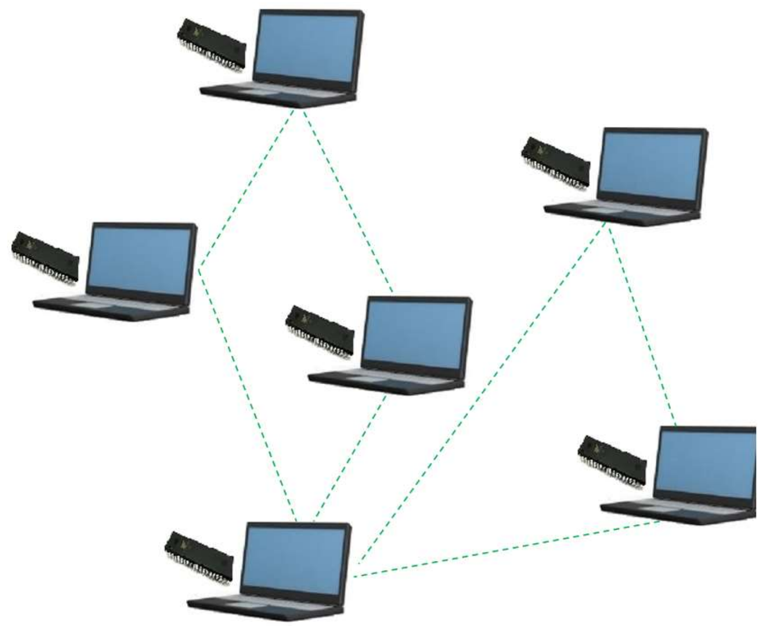

Fig. 2. The decentralized based peer-to peer structure

2) *Consensus protocol and algorithm*

In the blockchain process, consensus protocol is deployed over peer to peer (P2P) structure based on a decentralized network in order to validate transactions propagated among nodes before adding blocks of nodes to the public ledgers. In the consensus procedure based on a defined protocol, the messages are received from the P2P network, and the transactions accomplished among the nodes are registered in the ledgers. Furthermore, the consensus protocol is able to elicit blocks and provide an agreement point concerning the integration of them. This protocol considers the number of transactions made through the verification procedure. By the use of the consensus protocol, it is guarantied that the new transactions can be added to the network without any confliction with the other valid transactions in the system. Hence, the new transactions are inserted in a block and are submitted to the blockchain system for confirmation through the validation process. The consensus algorithms are usually defined based on the fault-tolerant consensus, which is widely studied in the blockchain network. After publishing the information of nodes within the network, a fault-tolerant consensus algorithm can guarantee that all nodes reach an agreement (on a common value) and respond to all requests with appropriate outputs. It should be mentioned that such an agreement among the nodes would be attained even with the occurrence of faulty nodes. In the fault-tolerant consensus algorithm, all nodes strive to get into an affective agreement despite the separated geographically condition of nodes. Concerning the argument mentioned above, there are three key factors in consensus algorithms including the synchrony of the network, consensus protocol and node fault. The synchrony of network is defined based on the degree of coordination among the nodes of a network during the consensus process. It means that for example all nodes send their messages to the adjacent nodes in iteration r, and they (all the nodes) receive the response message related to the other nodes in iteration r+1. As the last factor, node fault means that the node suffers from a failure, which might stop its performance. There is no need to say that it is expected that the consensus algorithm still get into an agreement point even with the existence of a faulty node. As noted before, a consensus protocol represents a set of rules pertaining to the message transactions and processing all nodes to bring an agreement based on the consensus goals.

A consensus algorithm with N nodes should satisfy the following consensus goals: termination, agreement, validity and integrity. For the termination, every non-faulty node should finally settle down on an output. Due to the agreement condition, all non-faulty nodes will eventuality converge to the same output in order to satisfy the second goal. Validity means that all nodes must be appraised by the validation procedure. Finally, the network integrity is provided when every node's decision is confirmed by the output of the other nodes.

3) *Cryptographic process*

The distributed database of the blockchain retains a growing list of records, which is defined as a block and is secured against the malicious attackers through the continues verification. Each block consists of a list of transactions stockpiled in the ledgers related to a node in a data structure, which can be viewed by nodes joined to the P2P network. Fig. 3 represents a block structure in a blockchain system. As it can be seen in this figure, the block structure includes a set of transactions, timestamp, an information pertained to the pervious block and Merkle root, which is a tree chart of transactions. In this way, the blocks are attached together for organizing a chain, where the hash generated by the pervious blocks retains the integrity over the blockchain process.

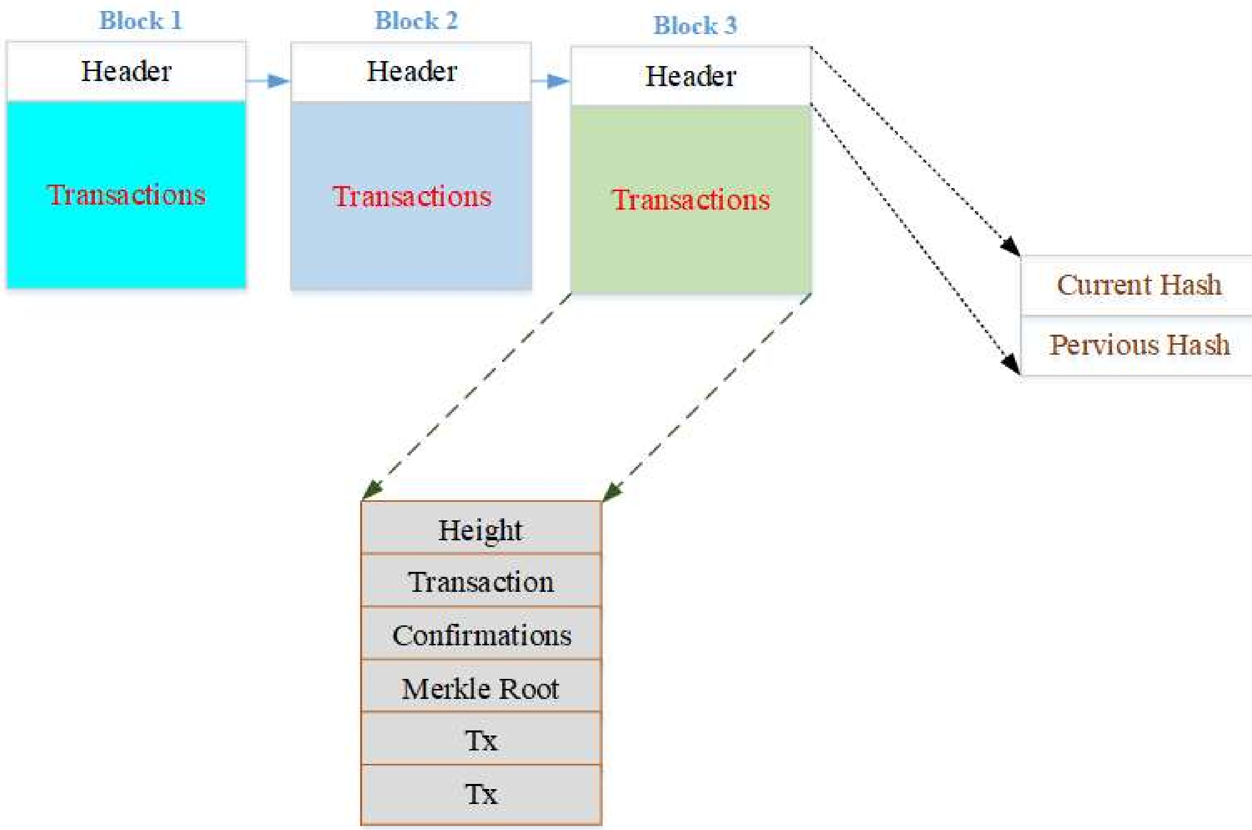

Fig. 3. A block structure in the blockchain system

By receiving the data blocks, each node should make access to the data embedded into the data block. To do so, block label, which can be an integer number, is inserted into the data block for indicating a unique hash function. Each label expresses a hash generator defined for nodes of the previous network. Hence, there is a need for another step that should be conducted on the data blocks. With this argument, the nodes will consider an encryption mechanism pertaining to the data label of the block for making pervious/current hash addresses (HAs) and encode them to limit the access to the correct data. To clarify the pervious/current HAs, assume that the network includes some nodes, each of them generates a HA (current HA) with regards to its hash function in iteration *r* and saves an HA (pervious HA) that is generated and sent by the neighboring nodes in iteration *r-1*. Each node inserts both the pervious and current HAs into its block label and this process is continued within a chain of nodes. Result of this process is reflected and presented in two concepts, i.e. confirmation and validity of the data block. Regarding the encryption algorithm, any faulty node can be recognized quickly and nodes of network will eventuality update their data block and label during the hashing process. The HAs are defined based on the 32-bit compounded words with regards to sundry hash functions [34] such as SHA-512, SHA-384, SHA-256, SHA-224 and SHA-1, including letters and numbers {0-9, A-F}.

The time passing for this process is one of the important features in the blockchain system. Let us assume that the average time for node transactions is q and each node prepares a data block for embracing the transactions and sending to other nodes. Hence, the processing time of the blockchain process can be calculated as follows:

$$T_{tot-chain} = q \times T_{sig} + (T_{back-off} + T_{trm}) \times 2 + t_{prod} + t_{Mining} \tag{1}$$

where T_{sig} shows the time needed to confirm the signature, $T_{back\text{-}off}$ is defined as the back-off time pertained to the used protocol [33], T_{trm} shows the consuming time for data exchange from a node to another, t_{prod} is the time passing in order to provide the data block, and t_{Mining} is the time related to the data block mining.

4) *Attack model*

A significant part of the model is simulating the cyber attack to check the validity of the proposed model. In the literature, methods of modeling the cyber-attack are generally summarized in various ways, consisting of attack graph, attack tree and attack network [38]. The attack tree method is simulated using the acyclic directed graph concerning the main nodes of the network. The method of "attack graph" can indicate whether an attacker could attain all targeting purposes when invading the network. By modeling the network attacks with regards to the attack graph, the different fields of network security, including the influence authority of attacks and security defense can be analyzed. Finally the attack model is considered as a trusty model due to modeling the network attacks from the respective of a malicious hacker. In this way, false data injection attack (FDIA), which is defined in the class of the attack network, can be one of the most obvious attacks for manipulating network information. FDIA can make high variation of data in the network which may not be recognized by an average detection system. In this situation, the energy market can be the attention center of many hackers by the use of FDIA to cause unexpected physical troubles and acquire considerable monetary profits over the other participants in the energy market. To clarify this issue, the first step is to model and express the FDIA model. Let us assume that the attacker can make access to the system data. Equation (2) is considered as the problem function in which X and S are the system data and objective function, respectively. If the attacker alters X to X_{bad}, the objective function value will change from S to S_λ, as shown in (3). By focusing on (4), it is vital to say that manipulating the data of the system should be conducted in such a way that the residue norm is unchanged for escaping the bad data detection system.

$$S = h(X) \tag{2}$$

$$S_\lambda = h(X_{bad}) \tag{3}$$

$$\left\| S_\lambda - h(X_{bad}) \right\| = \left\| S - h(X) \right\| \tag{4}$$

The significant point is to check whether the attack has been successful or not. To this end, it is needed to provide a criterion for the FDIA effect as follows:

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

In the above equation, λ is defined as the structured attack vector, and c represents the variation related to the alteration of real data. Based on (5), the attacker should check the output of $h(X)$ to get into a successful attack. To constrain the attack based on a special target, the manipulated data can be updated as the following:

$$X_{bad,i} = \begin{cases} X_i + c_i & if \quad i \in \upsilon \\ X_i & otherwise \end{cases} \tag{6}$$

where the index i describes the value of attack (c_i) for adding to the data of system (X_i) with the aim of bringing target υ (number of meters).

III. Proposed SECURED ENERGY MARKET ARCHITECTURE

The top-down hierarchical structure based on energy market needs to have an independent central system to determine the conventional price and power among the players participating in the market. Considering the developments of modern power system, it is needed that the market structure be propelled to get a P2P design in the energy market. In this way, the security of data exchanging among the market participates can be one of the most important challenges within the P2P energy market structure. Hence, this section proposes a P2P framework based on secured energy market in order to provide the required formulation to negotiate between the microgrid and the smart grid. In this regard, a blockchain architecture based on RCI consensus algorithm is developed for providing a secured negotiation environment against any malicious behavior of attackers within the energy market. To elaborate on the issue, it is essential to first present the centralized formulation of the proposed problem. As it was mentioned before, the proposed model includes two separately electrical grids, i.e. microgrid and smart grid. Each of these grids tends to participate in the energy market to make the most appropriate balancing price for exchanging power with the other grid.

A. *The Proposed Centralized Formulation*

In the proposed model, the smart grid tries to supply all the electrical demand in such a way that the total cost of generation would be minimized with respect to the operation constraints [35, 36]. On closer examination, the objective function and constraints related to the power flow of the smart grid are literally described in (7) - (19). Based on (7), the objective function consists of the cost function, start-up cost and shot-down cost pertaining to the generation units and transaction costs, which should be minimized. It should be mentioned that the last part of the objective function is assigned the power cost exchanged to another system. Hence, the positive or negative value of power transaction determines the cost/benefit related to the power transaction, respectively. Equations (8) and (9) provide the active/reactive power balance respectively and also the voltage limitation is preserved by (10). Based on (8), variable P_t^{TS} is modeled to determine the power transaction made by the energy market. To clarify about the power balance, some explanations is needed here. As it can be seen, the left-handed part comprises of power of generation units, power crossed through lines and the power transaction. On the contrary, the right-handed part includes summation of load demands, which are satisfied by the smart grid. In addition, each generation unit has to consider the generation capacity constraints for the active/reactive powers due to the fuel limitation and mechanical condition of the generators. To address this problem, equations (11) and (12) delineate the power constraints of generators in which the binary variable $\kappa_{y,t}$ is used to model the start-up/shot-down ($\kappa_{y,t}=1, \kappa_{y,t}=0$) rates of generators. Since the units are able to produce reserve power, they have a tendency to participate in the reserve market for gaining more economic benefits. Equations (13) and (14) meet the generators' limits for the reserve power at time *t*. The grid capacity related to the power flow of lines can indirectly make positive/negative effects in determining the optimal power and eventuality minimizing the objective function. Therefore, the power flow of lines is needed to get modeled as can be seen by (15) and (16). The bus angles are determined by η_b^{max}, which is limited between the max/min values as indicated in (17). The active/reactive power flow limitations for feeders are defined by (18) and (19), respectively.

$$min\,C\_G^{grid} = \sum_t \sum_y \left[P^c\left(P_{t,y}\right) + S_{t,y} + D_{t,y} + CP_t^{TS} \right] \tag{7}$$

$$\sum_y \left(P_{t,y}\right) - \sum_e \left(P_{t,e}\right) + P_t^{TS} = P_{b,t}^L \qquad \forall t \in \Omega^T, \forall b \in \Omega^b \tag{8}$$

$$\sum_y Q_t^G + \sum_e \left(Q_{t,e}\right) = Q_{b,t}^L \qquad \forall t \in \Omega^T, \forall b \in \Omega^b \tag{9}$$

$$TV^{min} \le TV_{b,t} \le TV^{max} \qquad \forall t \in \Omega^T, \forall b \in \Omega^b \tag{10}$$

$$P^{min}\kappa_{y,t} \le P_{t,y} \le P^{max}\kappa_{y,t} \qquad \forall t \in \Omega^T, \forall y \in \Omega^y \tag{11}$$

$$Q^{min}\kappa_{y,t} \le Q_{t,y} \le Q^{max}\kappa_{y,t} \qquad \forall t \in \Omega^T, \forall y \in \Omega^y \tag{12}$$

$$P_{t,y} - P_{t-1,y} \le D_G^{+}\kappa_{y,t-1} \qquad \forall t \in \Omega^T, \forall y \in \Omega^y \tag{13}$$

$$P_{t-1,y} - P_{t,y} \le D_G^{-}\kappa_{y,t} \qquad \forall t \in \Omega^T, \forall y \in \Omega^y \tag{14}$$

$$P_e = \left(TV_b - TV_m\right)R'_e - X'_e\eta_b \qquad \forall b\in\Omega^b, \forall m\in\Omega^m, \forall e\in\Omega^e \tag{15}$$

$$Q_e = -\left(1+2TV_b\right)X'_{e0} - \left(TV_b - TV_m\right)X'_e - R'_e\eta_b \qquad \forall b\in\Omega^b, \forall m\in\Omega^m, \forall e\in\Omega^e \tag{16}$$

$$\eta_b^{min} \le \eta_{b,t} \le \eta_b^{max} \qquad \forall t\in\Omega^T, \forall b\in\Omega^b \tag{17}$$

$$-P_e^{max} \le P_{e,t} \le P_e^{max} \qquad \forall t\in\Omega^T, \forall e\in\Omega^e \tag{18}$$

$$-Q_e^{max} \le Q_{t,e} \le Q_e^{max} \qquad \forall t\in\Omega^T, \forall e\in\Omega^e \tag{19}$$

As mentioned before, the microgrid is assumed as another effective participant in the P2P energy market. Microgrid tends to minimize the operation cost by buying/selling the surplus power based on the energy price determined by the P2P energy market. Therefore, providing the centralized form of the microgrid structure can be vital before the energy management definition in the P2P market structure. The microgrid model is comprised of a storage unit and some distributed generations (DGs), such as wind park, photovoltaic units and tidal system, as well as some loads located far away from the main grid [37]. The microgrid system should be capable of dispatching energy among DGs such that the objective function (20) and the relevant constraints are satisfied. Regarding the generation price considered for each DG, the microgrid tries to minimize the operation costs pertaining to DGs and transaction cost as shown by (20). Each DG generates power according to its technical restrictions, which are represented for wind turbine, tidal turbine and photovoltaic units by (21)-(24), respectively. Limits on storage unit for power balance and constraints of charging/discharging power are given by (25)-(28). It is axiomatic that the equivalence between loads and generated powers should be established at all time. To do so, equation (24) delineates the power balance within the microgrid in which the sum of generation and transaction powers are equal to the load demand. The positive value of power transactions (P_t^{TM}) shows the amount of energy bought from the other grids and visa verse.

$$mic = min\sum_{t\in\Omega^T} CW_t\, PW_t + RTI_t\, PTI_t + RPV_t\, PPV_t + RB_t\, PB_t + CP_t^{TM} \tag{20}$$

$$PW_t = \frac{1}{2} SCK(S_t^V)^3 \qquad \forall t \in \Omega^T \tag{21}$$

$$PTI_t = \begin{cases} 0 & 0 \le T_t^V \le T_{rated}^V \\ 0.5P\gamma\lambda\left(T_t^V\right)^3 & T_{cutin}^V \le T_t^V \le T_{rated}^V \\ PTI_{rated} & T_{rated}^V \le T_t^V \end{cases} \qquad \forall t \in \Omega^T \tag{22}$$

$$PPV_t = \frac{Q \times U_t^{PV}}{Z} \times (1 - R^{loss}) \qquad \forall t \in \Omega^T \tag{23}$$

$$PTI_t + PW_t + PPV_t + PB_t + P_t^{TM} = P_t^{load} \qquad \forall t \in \Omega^T \tag{24}$$

$$VB_t = VB_{t-1} + PB_t \eta^{Bat} \qquad \forall t \in \Omega^T \tag{25}$$

$$PB_t = PB_t^{ch} - PB_t^{dis} \qquad \forall t \in \Omega^T \tag{26}$$

$$P^{\min} \le PB_t \le P^{\max} \qquad \forall t \in \Omega^T \tag{27}$$

$$V^{\min} \le VB_t \le V^{\max} \qquad \forall t \in \Omega^T \tag{28}$$

B. The Secured Energy Management Structure Definition Based on P2P Framework

This part concentrates on providing a P2P energy market structure based on a modified blockchain secured architecture to assure participants to exchange their data in confidently. To do so, the energy market based on P2P structure needs to be handled by an appropriate consensus algorithm with the aim of having effective power/price transaction among participates. Having a secured P2P energy management, the modified blockchain architecture is required to guarantee the security of the P2P energy market. Based on the interrelation of P2P energy management and data security, let us point out another viewpoint. Many disputes have already been expressed over the energy and data exchanges safety in the P2P based energy market. The energy markets are not an exception, since they comprise of different agents, whose participate in the market to trade the energy. In this regard, the necessity of providing a safety environment for data and energy trading is requisite. The proposed blockchain based secure structure will pledge the security and safety of data and energy transactions. To do so, it is essential that different parts of the blockchain, which are the decentralized network, consensus algorithm and cryptographic procedure, should be defined completely and get compatible with the condition of the proposed energy market. Hence, let us assume that the microgrid and the smart grid are spliced in the form of a decentralized network based on a P2P framework as shown in Fig. 4. The cryptographic procedure based on P2P energy market can be constructed as that is discussed in pervious sections. Regarding the blockchain framework, one of the significant main parts is the consensus algorithm, which is considered using the security protocols and condition of P2P energy market. In other words, the consensus algorithm should be capable of working with both the blockchain and P2P energy market.

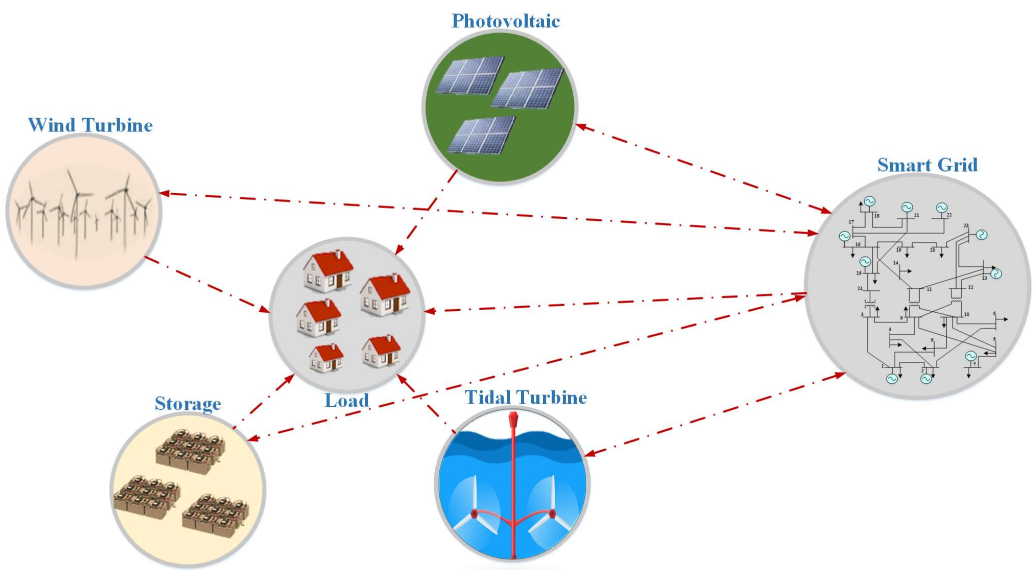

Fig. 4. P2P structure between the microgrid and the smart grid

Getting into an agreement between the microgrid and the smart grid can be assumed as the common point of the blockchain network and P2P market that it can be satisfied by an effective consensus algorithm based on security protocols. To this end, the RCI consensus algorithm is suggested, which is able of bringing consensus power and price among market participants while observing all protocols related to the blockchain network. The RCI is similar to the dual increasing methods in which the main problem contains two sub-problems, separately. Each sub-problem should be optimality solved in such a way that helps the global solution of the main problem. In RCI approach, all participates try to make an agreement with regards to the Karuch-Kuhn-Tucker (KKT) conditions. In this method, the solution trend is improved by adding a gradient function in comparison with the dual ascent method due to the few number of variables. In other words, RCI method provides a direct approach to carry out the sub-problem such that each participant is capable of trading as much as possible energy with others with the best price. Also, constraints of energy boundary are considered by the Lagrangian Relaxation [16]. Based on the structure of the microgrid and smart grid in the pervious section, their objective functions based on RCI algorithm can be updated as follows:

$$min(C\_G + R_t^{TS}(P_t^{TS}) - P_t^{TS^T}\beta_t^{TS}) \tag{26}$$

$$\min(mic + R_t^{TM}(P_t^{TM}) - P_t^{TM^T}\beta_t^{TM})$$

$$min(\overbrace{C\_G + R_t^{TS}(P_t^{TS}) - P_t^{TS^T}\beta_t^{TS(k)} + \overline{H}_t^{sd}\left(P_{sd_t} - \overline{P_{sd}}\right) - \underline{H_t}^{sd}\left(\underline{P_{sd}} - P_{sd_t}\right)}^{smart\ grid} \tag{27}$$

$$+\overbrace{mic + R_t^{TM}(P_t^{TM}) - P_t^{TM^T}\beta_t^{TM(k)}) + \overline{H}_t^{m}\left(P_{m_t} - \overline{P_m}\right) - \underline{H_t}^{m}(\underline{P_m} - P_{m_t})}^{microgrid}$$

(9)-(20) (28)

(22)-(26) (29)

$$P_t^{TS} \geq 0, P_t^{TS} \leq 0, \tag{30}$$

$$P_t^{TM} \geq 0, P_t^{TM} \leq 0, \quad \forall t \in \Omega^T$$

Equation (26) defines the total objective function, consisting of two parts related to the microgrid and smart grid. In the first part, the objective function includes the generation cost (C_G) and cost value pertaining to the power transaction in which $P_t^{TS}$and $\beta_t^{TS(k)}$ indicate the trading power/price from the smart grid to the microgrid, respectively. In a similar manner to the smart grid, the objective function of the microgrid is defined. Regarding the trend of the duals and primal in the RCI method [16], the update of variables is conducted based on KKT conditions and relaxed Lagrangian function of the proposed problem. With doing this, the slackness function as the penalty coefficient is added to the problem function as shown in (27). Equations (28) and (29) illustrate the constraints related to the microgrid and the smart grid as described in the pervious section. The power transaction takes positive/negative values, representing the direction of power between the microgrid and the smart grid as it can be seen in (30). The updated procedure for the trading price is defined for both the microgrid and smart grid based on (31) and (32) in iteration *k+1*, respectively. Also, the dual variables of the boundary constraint (slackness variables) related to the smart grid and microgrid are updated by (33)–(36).

$$\beta_t^{TS(k+1)} = \beta_t^{TS(k)} - \mathcal{X}^k(\beta_t^{TS(k)} - \beta_t^{M-S(k)})\_\kappa^k (P_t^{TS(k)} + P_t^{TM(k)}) \ \forall t \in \Omega^T \tag{31}$$

$$\beta_t^{TM(k+1)} = \beta_t^{TM(k)} - \mathcal{X}^k(\beta_t^{TM(k)} - \beta_t^{TS(k)})\_\kappa^k (P_t^{TM(k)} + P_t^{TS(k)}) \ \forall t \in \Omega^T \tag{32}$$

$$\overline{H}_t^{sd(k+1)} = \max\left(0, \overline{H}_t^{sg(k)} + \xi^k\left(P_{sd_t} - \overline{P_{sd}}\right)\right) \forall t \in \Omega^T \tag{33}$$

$$P_{sd_t} = f(P_{t,y})$$

$$\underline{H_t}^{sd(k+1)} = \max(0, \underline{H_t}^{sg(k)} + \xi^k\left(\underline{P_{sd}} - P_{sd_t}\right)) \forall t \in \Omega^T \tag{34}$$

$$\overline{H}_t^{m(k+1)} = \max(0, \overline{H}_t^{m(k)} + \xi^k(P_{m_t} - \overline{P_m})) \forall t \in \Omega^T \tag{35}$$

$$P_{m_t} = f(PPV_t, PB_t, PW_t, PTI_t)$$

$$\underline{H_t}^{m(k+1)} = \max(0, \underline{H_t}^{m(k)} + \xi^k\left(\underline{P_m} - P_{m_t}\right)) \forall t \in \Omega^T \tag{36}$$

The Lagrangian function has bijective gradient when defined as the function of power set points. Considering KKT conditions, the function of set points related to the smart grid and microgrid can be concluded and updated as follows:

$$PS_{sd_t}^{(m),k+1} = \frac{-b_{sd} + \beta_t^{TS} - \overline{H}_t^{sd} - \underline{H_t}^{sd}}{a_{sd}} \quad \forall t \in \Omega^T \tag{37}$$

$$PS_{m_t}^{(sd),k+1} = \frac{-b_m + \beta_t^{TM} - \overline{H}_t^{m} - \underline{H_t}^{m}}{a_m} \quad \forall t \in \Omega^T \tag{38}$$

where a and b coefficients are defined by the generation cost function. Based on (37) and (38), the power exchange between the microgrid and the smart grid would be updated by (39) and (40) in which $R_t^{TS(k)}$ and $R_t^{TM(k)}$ coefficients are obtained by (41) and (42).

$$P_t^{TS(k+1)} = P_t^{TS(k)} + R_t^{TS(k)}\left(PS_{sd_t}^{(m),k+1} - P_{sd_t}^k\right) \ \forall t \in \Omega^T \tag{39}$$

$$P_t^{TM(k+1)} = P_t^{TM(k)} + R_t^{TM(k)}\left(PS_{m_t}^{(sd),k+1} - P_{m_t}^k\right) \ \forall t \in \Omega^T \tag{40}$$

$$R_t^{S-M(k)} = \frac{|P_t^{TS}| + \gamma^k}{|P_{sdn}| + \gamma^k} \quad \forall t \in \Omega^T \tag{41}$$

$$R_t^{M-S(k)} = \frac{|P_t^{TM}| + \gamma^k}{|P_{mn}| + \gamma^k} \quad \forall t \in \Omega^T \tag{42}$$

It is important to say that the convergence of the consensus algorithm is determined when the iterative procedure is stopped. With doing this, the terminating condition needs to be defined for the RCI consensus algorithm that is provided as below:

$$(\beta_t^{TS(k+1)},\ \beta_t^{TM(k+1)}) - (\beta_t^{TS(k)},\ \beta_t^{TM(k)}) < \varepsilon \tag{43}$$

$$(P_t^{TS(k+1)},\ P_t^{TM(k+1)}) - (P_t^{TS(k)},\ P_t^{TM(k)}) < \gamma \tag{44}$$

$$(H_t^{m(k+1)},\ H_t^{sd(k+1)}) - (H_t^{m(k)},\ H_t^{sd(k)}) < \tau \tag{45}$$

Generality, the RCI method procedure of represented in Fig. 5 can be partitioned three stage in which the first/second stages are considered for updating the dual variable of the power exchanging boundary constraints. After that, the third step provides to update the decision variables in other to apply a gradient stage.

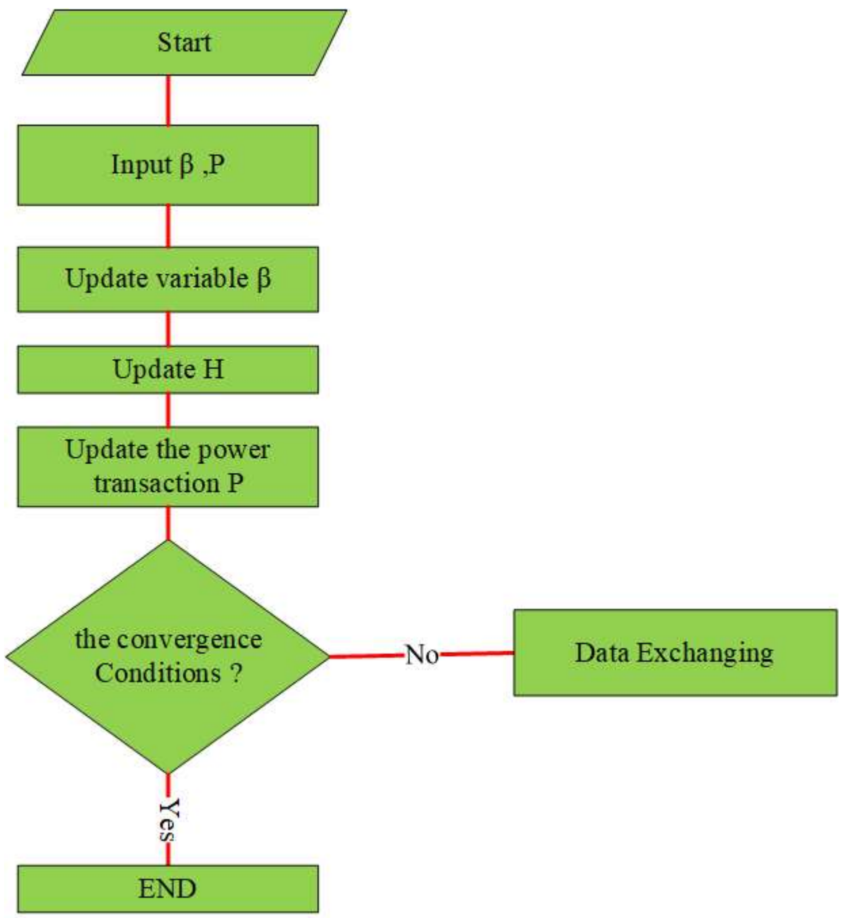

Fig. 5. The proposed algorithm procedure

To sum up, the P2P energy market for microgrid and the smart grid can be conducted based on the proposed RCI consensus algorithm while security protocols related to the blockchain architecture is considered in order to enhance the secured transaction environment against malicious attacks.

IV. UNCERTAINTY QUANTIZATION MODEL

It is important to consider a close look at the significant effects of the uncertain parameters on the energy market. This section tends to model the uncertainty effects pertaining to the renewable resource and loads using UT method. It should be mentioned that the parameters of the wind speed, solar radiation, tidal current and loads can be modeled by the proposed method, which is able to consider the correlation among the parameters. The UT model is represented by $F = \hat{f}(R)$ in which the output of stochastic function (U) is obtained using $2c$+1 different points. The normal distributed function is provided for each variable with regard to the standard deviation and mean value of variables indicated by z and A, respectively. The UT method process can be provided by steps (1) to (3):

Step 1: $2c$+1 variables can be calculated using (45)-(47) as follows:

$$R^0 = z \tag{46}$$

$$R^k = z + \left(\sqrt{\frac{p}{1-W^0} A_{aa}}\right)_k \quad k = 1,2,\ldots,c \tag{47}$$

$$R^{k+c} = z - \left(\sqrt{\frac{p}{1-W^0} A_{aa}}\right)_k \quad k = 1,2,\ldots,c \tag{48}$$

In above equations, A_{aa} illustrates the covariance matrix and $\bar{R} = z$.

Step 2: Weight of points determined by (47) and (48) can be calculated by (49):

$$W^k = \frac{1-W^0}{2c} \quad k = 1,2,\ldots,2c \tag{49}$$

Note that the sum of the weights is equal to 1.

Step 3: The points concluded by step 1 are inserted into the nonlinear function $F^k = \hat{f}(R^k)$ and then, the output values are obtained by:

$$\overline{F}=\sum_{k=0}^{2p}W^{k}F^{k} \tag{51}$$

$$P_{FF}=\sum_{k=1}^{2p}W^{k}\left(F^{k}-\overline{F}\right)\left(F^{k}-\overline{F}\right)^{T} \tag{52}$$

Also, Table I shows the comparison of different uncertainty modeling methods from the point of view of accuracy, complexity and correlation. It indicates that the UT method can provide high accuracy while inflicts medium complexity to the studied system and is able to model the correlation effect among the uncertain parameters.

TABLE I
COMPARISON AMONG DIFFERENT UNCERTAINTY MODELLING METHODS

Methods	**Accuracy**	**Complexity**	**correlation**
Cloud	HIGH	HIGH	×
PEM	MEDIUM	LOW	×
Scenario-based	LOW	MEDIUM	×
The proposed model (UT)	HIGH	MEDIUM	✓

V. SIMULATION RESULTS

In this section, we try to validate the two main concepts proposed in the paper. In the first place, the most significant issue is to check the security of the blockchain structure against malicious attacks in the P2P energy market. In the second place, we check the ability of the proposed consensus algorithm in bringing adaptive power/price among participates by considering P2P energy market compared to the centralized structure. As mentioned before, the market participants are defined based on a self-determining microgrid and smart grid, which include some generation units based on fossil fuel, buses, lines and electrical loads, all of which are connected in IEEE 24-bus test system. Besides that, the microgrid supplies the loads located in the far areas using renewable resources, such as photovoltaic unit, wind turbine, tidal turbine system and storage unit [33-35]. To elaborate on the proposed concepts, we implement and conduct the P2P energy market and the proposed blockchain architecture and then examinate the obtained results based on the different point of views as follows:

Case I: Validating the proposed consensus algorithm in the P2P energy market

Case II: Analyzing the performance of the proposed blockchain framework against FDIA

Case III: Assessing the effect of uncertainty on the P2P energy market

Each case is expressed and discussed in detail in the subsequent sections.

A. Validating the proposed consensus algorithm in the P2P energy market

The first and perhaps the most important issue is the consensus algorithm performance in the P2P energy market considering the data security issues. In this regard, this section assesses the proposed algorithm in order to provide an effective energy market among the participants, i.e. the microgrid and the smart grid. As mentioned before, P2P energy market should be able to obtain the trading price/power with regards to the optimal points for all participates. To this end, we conducted the P2P energy market based on RCI consensus algorithm and provided the results for the microgrid and the smart grid as shown in Figs. (6)- (9). We let the algorithm continue the iterative trends until getting to the consensus point. Figs. (6) and (7) show the transaction power pertaining to the microgrid and the smart grid respectively obtained by the P2P market. Based on Fig. (6), the X/Y and Z axes indicate the time in hour, number of iterations and power transaction value, respectively. Over the iterations 1 to 200, there are high fluctuations in the power transaction all the time. After iteration 200, it is clear that the power transaction gives a slight fluctuation, which is an important indication to reach an optimal agreement point. When increasing the iteration number to 463, the power transaction converges to a steady value, showing very negligible fluctuations. Finally, after iteration 463, the power variation is almost zero and consensus power related to the microgrid has been obtained at all time. The positive/negative values indicate the buying/selling power by the microgrid, respectively. For instance, the power transaction for the microgrid is 20.05 kW at time t=6. It means that microgrid intends to buy 20.05 kW power from the energy market. On the other hand, considering the exchanged power at time t=18, the power of the microgrid is equal to 39.63 kW, and the negative value means that the microgrid wants to sell power to the other participates (here smart grid) of the energy market. Similarly to the microgrid, the iterative procedure pertaining to the power transaction of the smart grid is represented by Fig. (7). after passing the high fluctuations, the power transaction of the smart grid converges to a constant value in iteration 463. On the contrary to the microgrid, the smart grid delivers 39.63 kW from the microgrid at t=18, and 20.05 kW power is exchanged from the smart grid to the microgrid at t=6. It needs to say that all power transferring between the microgrid and the smart grid is obtained with regard to the P2P energy market conditions and objective function of both microgrid and smart grid. At the first glance, considering the whole process of the algorithm, energy market based on P2P structure is capable to manage the power transaction among the participants for reaching an optimal consensus point, appropriately.

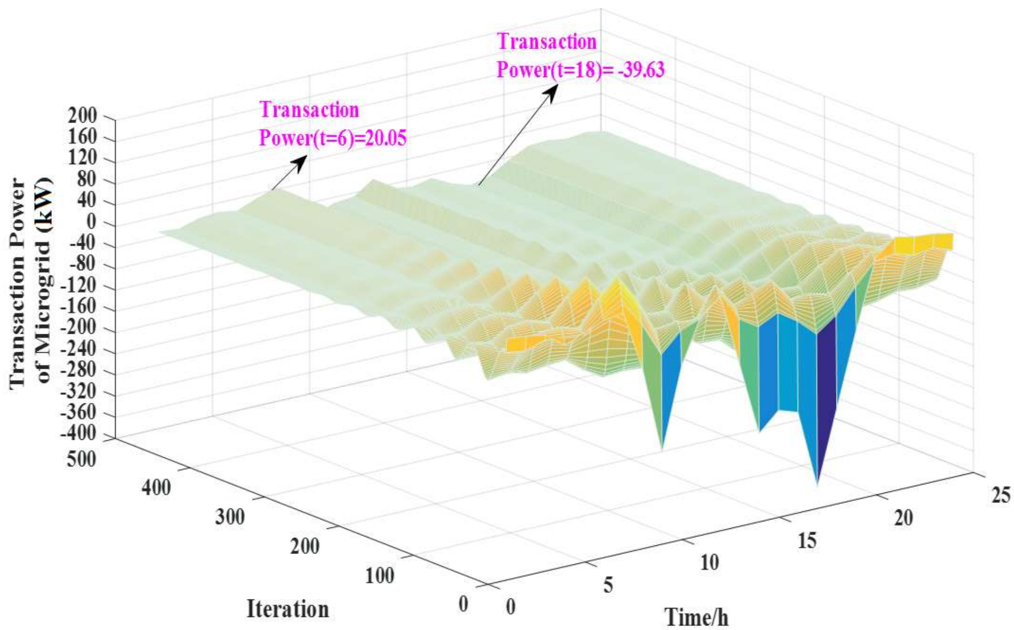

Fig. 6. Power exchanging in the microgrid

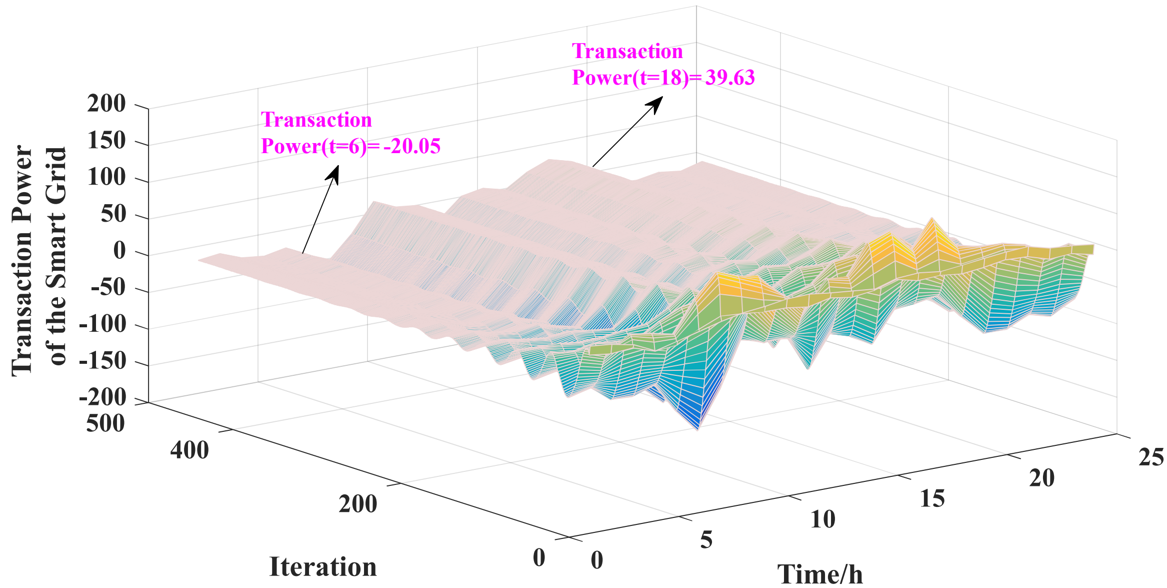

Fig. 7. Power exchanging in the smart grid

As mentioned before, apart from the power transaction, the proposed P2P energy market should determine the trading price as an effective criterion in order to exchange power among the participants. Fig. (8) indicates consensus process of energy price between the microgrid and the smart grid in the P2P energy market. As it can be seen, the price has a marked fluctuation in the first iterations which has converged by increasing the number of iterations. Finally, the trading price obtained a constant value, which is different in each time. For example, results of energy market show that the transaction price is equal to 0.45 ($/kW) and all participants are bound for buying/selling power concerning the calculated price. In addition, it may be an important point of view that the total cost during the consensus procedure represents a fluctuating trend similar to the power/price transaction as shown in Fig. (9). The total cost, which is the sum of the costs of the microgrid and smart grid, is near 4.1107×10^{9}($).

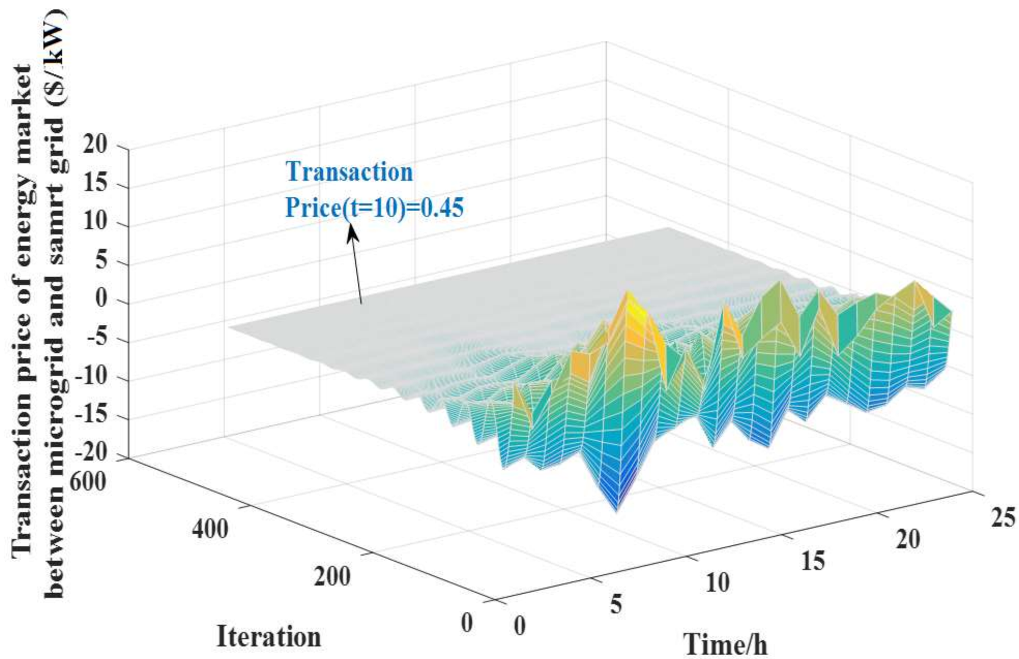

Fig. 8. The power price exchanging in the market

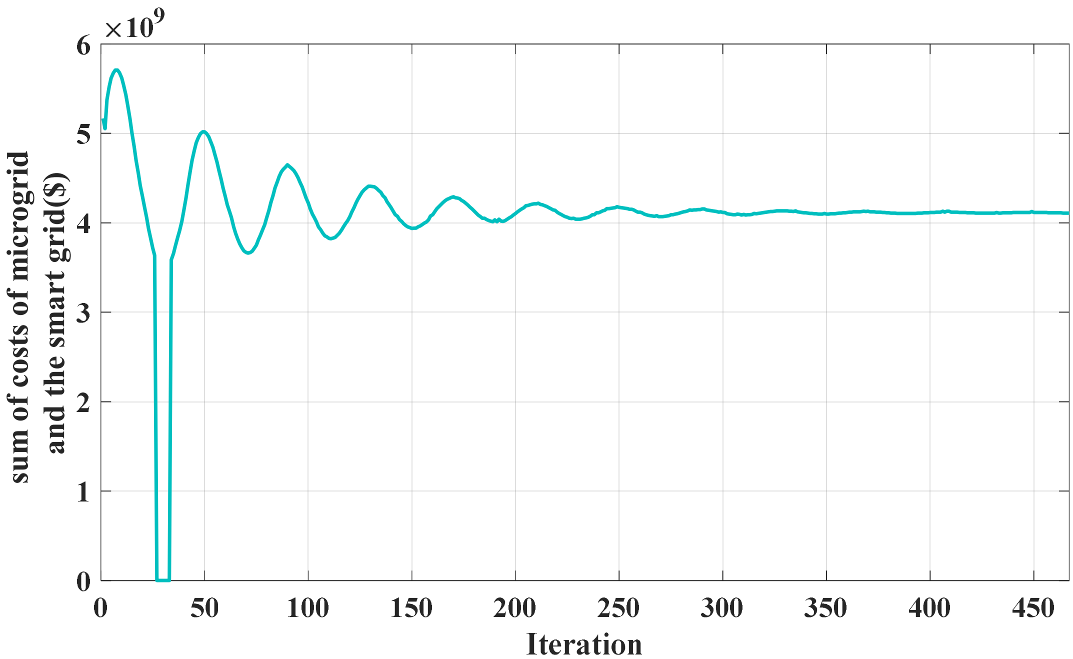

Fig. 9. The total cost

Validating the results of the proposed P2P energy market can be a critical issue. In this regard, we compare the results of the centralized framework with the proposed P2P structure as indicated in Figs. (10) and (11). Based on the results related to the centralized energy market (see Fig. (10)), it is seen that the power transaction based on P2P energy market has a slight deviation compared to the centralized one. The maximum deviation of power transaction between the P2P and centralized structures is 4.16%, which shows the high accuracy of the proposed energy market based on P2P framework. Apart from the power transaction, the total cost can be defined as another criterion for judging the P2P energy market. Fig. (11) represents a comparison of the total cost for P2P and the centralized structures. The total cost in the centralized structure is $4.11×10^9, which has a slight deviation (less than 1%) compared to the P2P structure. All in all, it seems that the proposed energy market is able to provide an effective environment in order to determine and exchange price/power among the participants connected in the form of the P2P structure.

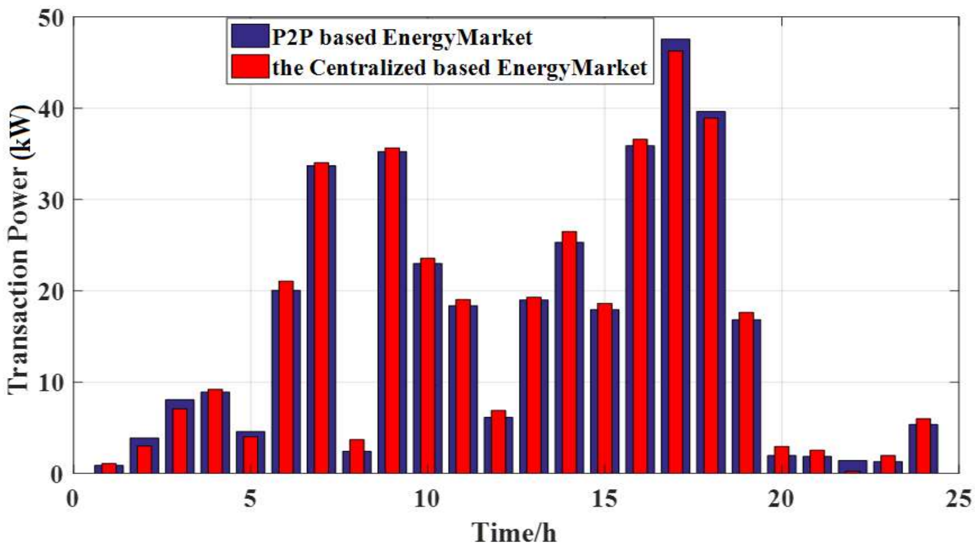

Fig. 10. Comparison of power transaction in the P2P structure and the centralized form

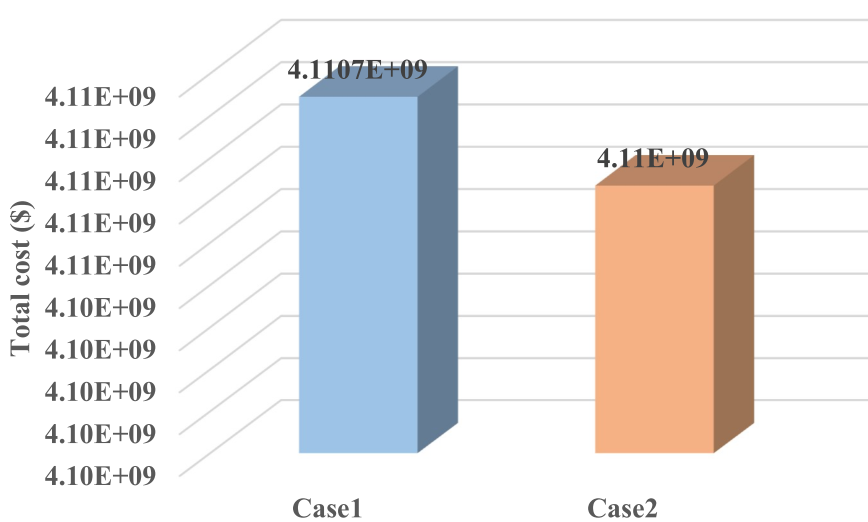

Fig. 11. case1: P2P structure based total cost, case 2: the centralized structure based total cost

B. Analyzing performance of the proposed blockchain framework against FDIA

In this part, we check the security of the P2P energy market against malicious attackers, who intend to destroy the trend of the energy market in order to achieve their social/economic goals. To assess the security of the energy market, the market behavior should be examined in the attack condition ignoring the proposed blockchain based secured framework. Moreover, an appropriate attack of FDIA type is simulated to apply in the P2P energy market with the aim of disrupting the consensus process of the algorithm. Results of the energy market exposed to the cyber attack are represented in Figs. (12) – (16). It should be mentioned that we applied FDIA on RCI algorithm in the energy market at times t=6 and t=10. As it can be seen in Figs. (12) and (13), due to the compromised information made by FDIA in the microgrid and the smart grid system, the algorithm could not converge to the consensus point in spite of increasing the number of iterations at $t=6$. Therefore, the power transaction of the microgrid and the smart grid shows high fluctuations during the consensus process due to changes made on the parameter $\mathcal{X}^k$ by FDIA (refer to (32)). To see the FDIA effect on the P2P energy market, results related to the cyber attack are represented at time t=10 in Figs. (14), (15). Similar to the pervious results (at $t=6$), FDIA disrupted the power exchange among the participants and that it led to not getting an agreement at time t=10. In addition, the hacker aims to avoid getting into an effective consensus price in the market. Fig. (16) shows the trading price exposed by FDIA attack at $t=6$. As that is shown here, there is a high fluctuation in the trading price, which implies no consensus price in the P2P energy market, in spite of rising number of iteration. In summary, results illustrates that the attacker is capable of getting its malicious aims to destroy the P2P energy market if not well equipped by a security platform. Keeping this in mind, we will deploy a new blockchain framework in the P2P energy market as it is explained later.

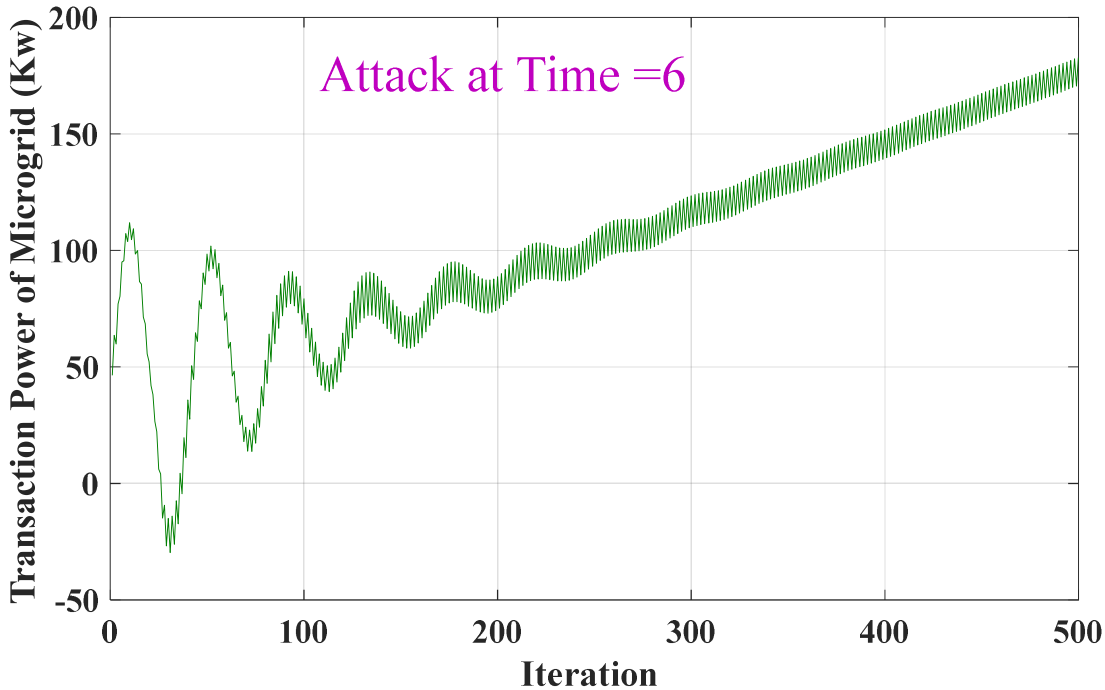

Fig. 12. The power transaction of the microgrid under attack at *t=6*

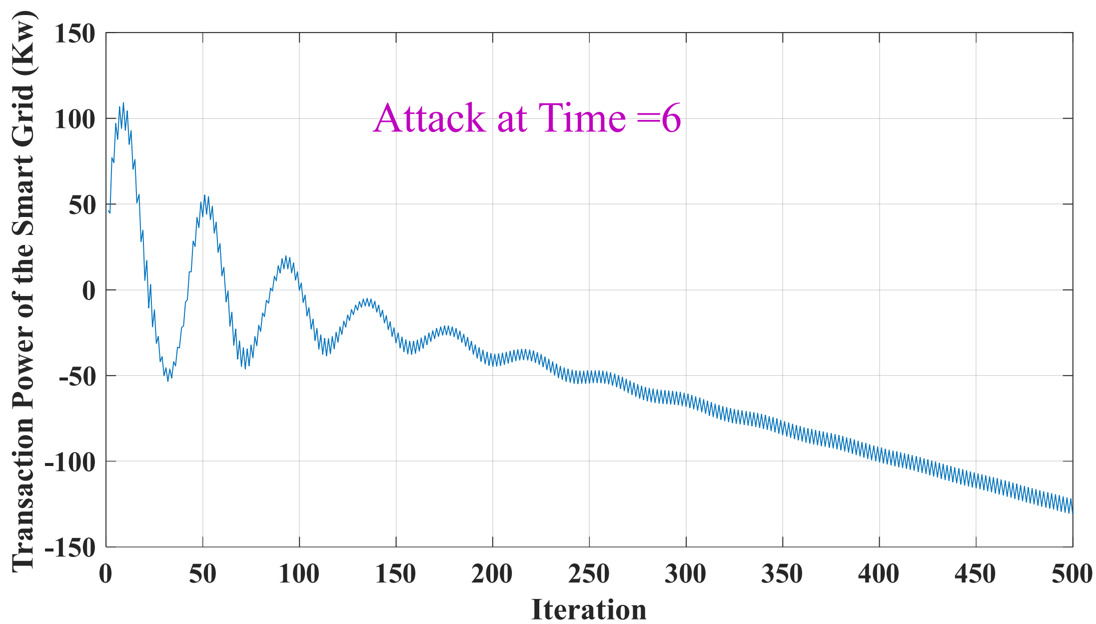

Fig. 13. The power transaction of the smart grid under attack at *t=6*

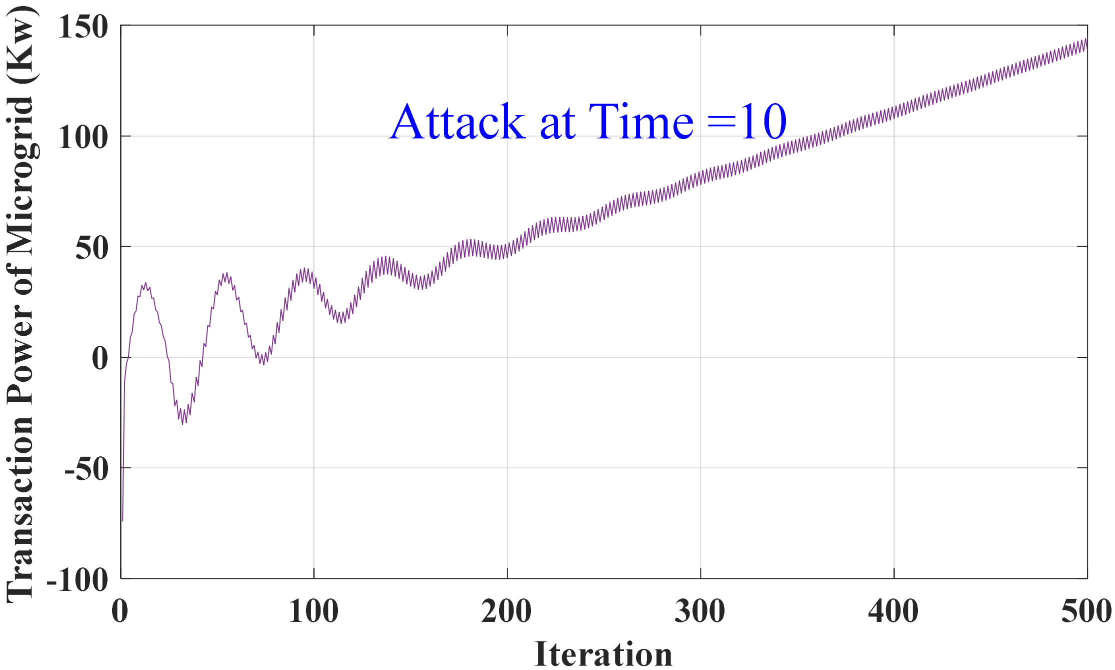

Fig. 14. The power transaction of the microgrid under attack at *t=10*

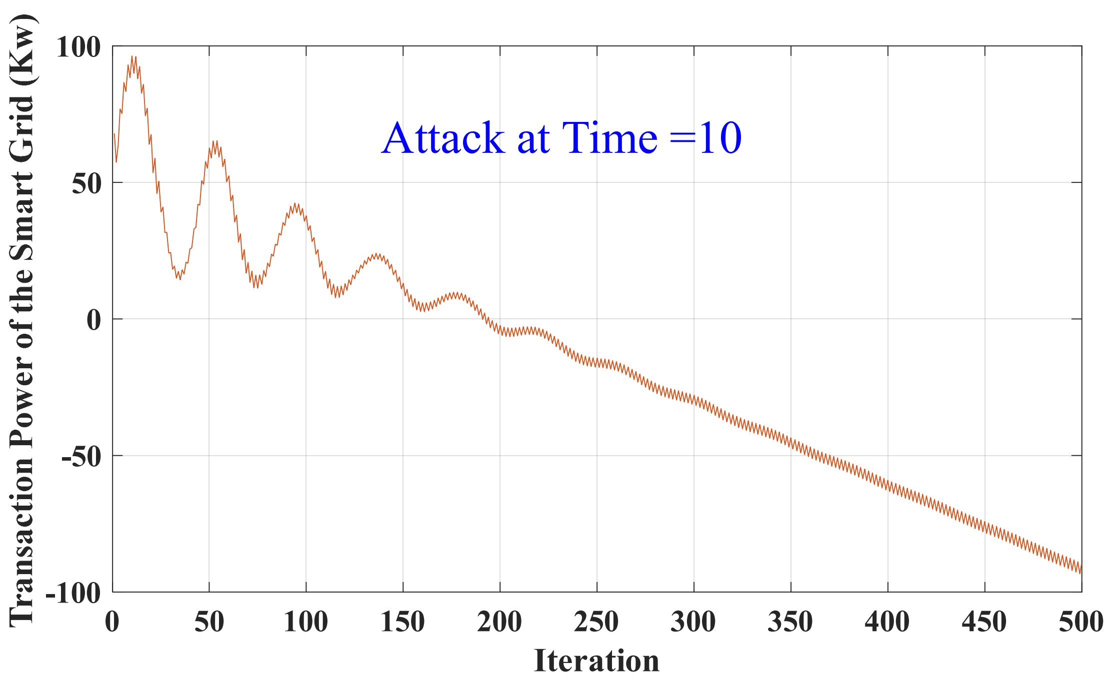

Fig. 15. The power transaction of the smart grid under attack at *t=10*

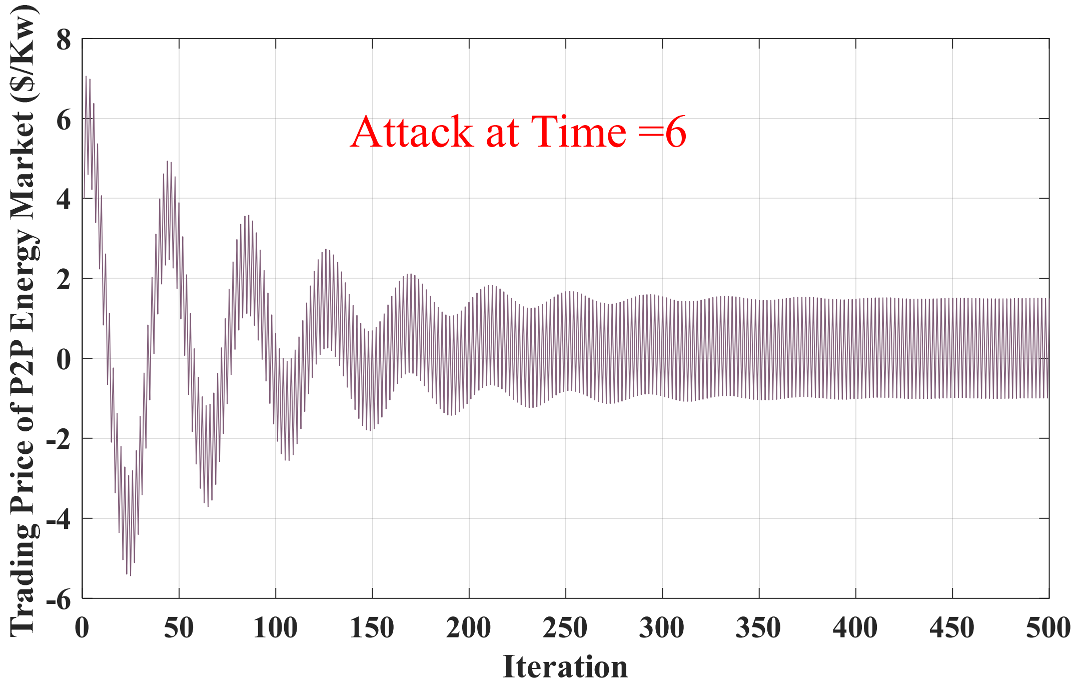

Fig. 16. The price transaction under attack at *t=6*

C- Blockchain efficiency against attacks

In this section, to illustrate the efficiency of the proposed blockchain based architecture against the cyber-attack, the probability computing approach is used to reveal the probability of successful attacks. The whole consensus deviates when an incorrect request is validated. Overall, attackers can penetrate the information process in three-level: first, creating the incorrect request in the validation step. Second, sabotage data when the information is transferring. Third, data manipulation in the database, namely ledgers. In this paper, we focus on the first and second mode of attacks for the calculation of probability to evaluate the functionality of the blockchain. It is important to mention that the above-mentioned attacks do not directly interrupt the system but they will lead to miscalculation. The blockchain provides a secured system against the data manipulation or incorrect requests. According to the nature of the energy market in power systems, the transactions must be considered with technical constraints. Hence, validating the incorrect request or manipulation of data leads to get away from the optimal operating point of the system. Therefore, the attacker tries to penetrate the network for creating both types of attacks. This penetration can be everywhere in the network. When a penetration occurs in the network, the attackers can do two types of sabotages as mentioned above so that the probability of each of them must be calculated. Therefore, the success probability of attacks for generating incorrect request can be express as follows [36]:

$$\frac{1}{3}\prod_{i=1}^{n}\lambda_i \tag{53}$$

wherein:

$0 \leq \lambda_i \leq 1, i = 1, 2, \ldots, n, \ldots, N.$

Here λ_i is the success probability of each attack, and i is the number of iteration data. On the other hand, the success probability of attacks for manipulation of data can also be expressed anywhere as follows:

$$\frac{1}{3}\prod_{i=1}^{n}\eta_i \tag{54}$$

where η_i is the success probability of each attack, and i is the number of iteration data. The η_i is also like λ_i. Therefore, the total success probability of attacks due to the penetration of attackers can be calculated as below:

$$P_a = \frac{1}{3}\left(\prod_{i=1}^{n}\lambda_i + \prod_{i=1}^{n}\eta_i\right) \tag{55}$$

Due to the distributed calculation in the consensus algorithm, the success probability of attacks would be zero because the distributed consensus algorithm does not reach the same answer, and blockchain does not accept it. Furthermore, since the data is encrypted based on cryptography and also according to the data chain principle, the success probability of attack decreases as the exchange of data increases. As shown in Fig. 16, when the success probability of attacks is expressed based on the percentage of iterations, its diagram shows a downtrend in the success probability according to (3). Considering the CPU power, the success probability of attack can be considered in the range of [0.9, 1]. In Fig. (17), a comparative experiments diagram is provided for the various iterations.

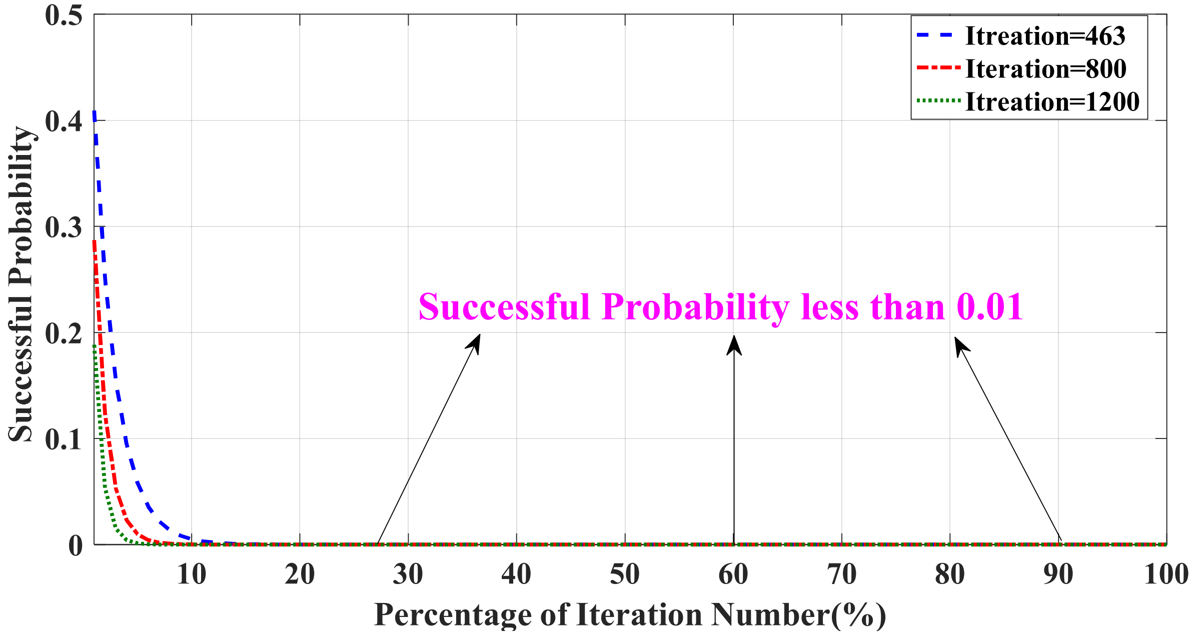

Fig. 17. Success probability of attacker against the proposed security platform

D. The effect of the uncertainty on the P2P energy market

This section investigates the uncertainty effects on the P2P energy market and highlights its effects on the power exchange among the participants. Moreover, it is needed to check how the uncertainty model can alter the performance of the energy market concerning the participants connected in the form of P2P structure. To do so, we deploy UT in the P2P energy market and see the consequence on the power transaction as well as the operation of each participant. Figs. (18)- (24) indicate results of uncertainty modeling using UT method. As mentioned before, the power exchange among participants is determined based on different criteria such as the trading price of energy market and operation condition of each participant. Hence, it seems that stochastic model could model the high fluctuations in power/price transaction due to uncertain parameters, which led to changed operation for each participant. Figs. (18), (19) show power transaction related to the microgrid and the smart grid under both deterministic and stochastic conditions, respectively. According to Fig. (18), the stochastic model causes varied changes in the power transactions of the microgrid compared to the normal condition. With regards to the results, high power variations are mostly seen at hours 21, 22, 24 and 10 with values 25%, 10%, 10% and 15% compared to the centralized form respectively while minimum variation is less than 5% at t=2. Similarly to the microgrid system, the power transition of the smart grid in the uncertain environment is represented in Fig. 19. It is evident that the power transaction is updated based on the market variations, the maximum values of which are changed to 25% ,10% and 10% at hours 21, 10 and 5 , respectively. At the first glance, the uncertainty effects on the power transaction in the microgrid is almost more than the smart grid due to the higher number of uncertain parameters. To sum up, it is important to say that the stochastic analysis and uncertainty modeling are essential to be considered in the P2P energy market in order to bring an accuracy consensus solution for each participant.

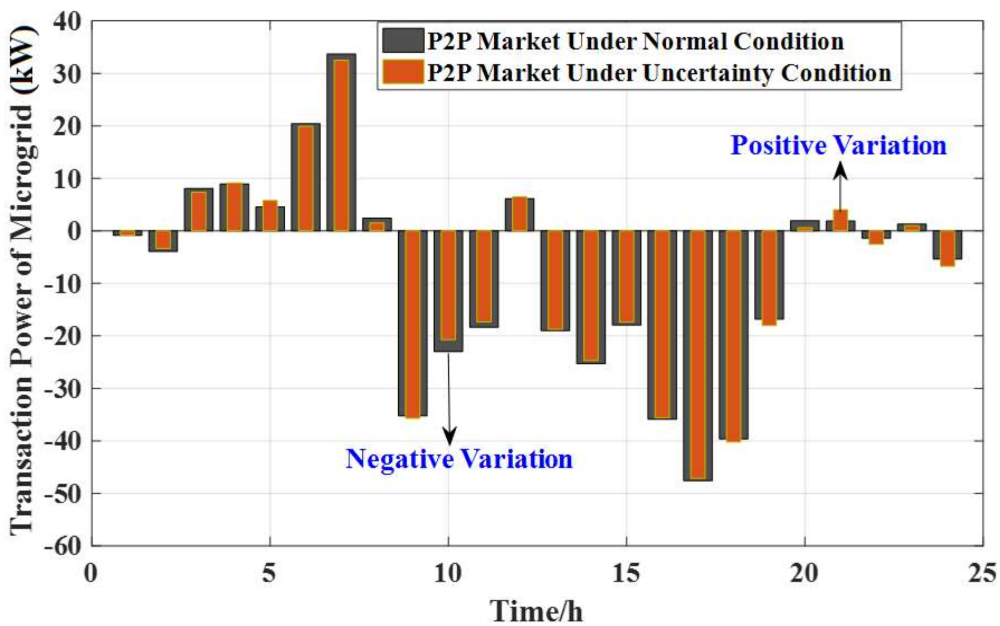

Fig. 18. The power transaction of microgrid under uncertainty condition

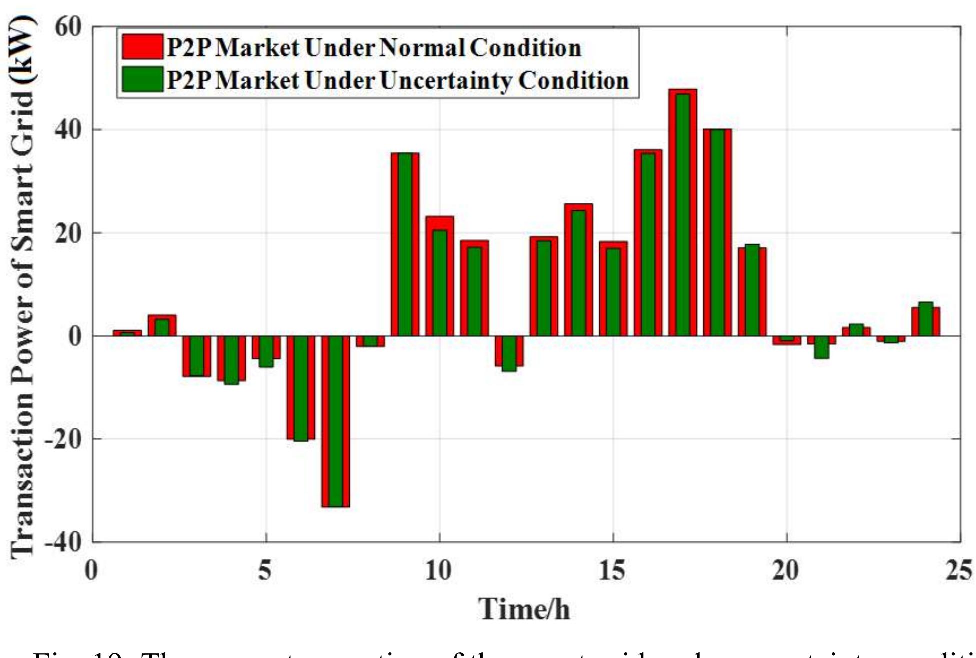

Fig. 19. The power transaction of the smart grid under uncertainty condition

As mentioned before, the microgrid is comprised of PV, WT, tidal turbine and storage units, the operation of which are represented under normal and uncertain conditions in Figs. (20)- (22). It should be mentioned that the stochastic model has altered the output power of DGs, which is shown by marked values compared to the normal condition. Based on Fig. 19, the PV power changes are occurring at the hours when maximum variation is approximately 78% under uncertain condition (such as t=11). Similarly to PV, results of tidal turbine and WT are provided in Figs. (21) and (23), respectively. In contrast to the tidal unit whose uncertainty model led an increased generated power, there is a marked decline in the power generated by WT in the stochastic framework due to the generation-demand balance. The optimal output power of units in the stochastic framework is depicted in Fig. (23). Comparing the total operation cost of the uncertain condition with the normal condition (see Fig. 24), it is seen that the total cost takes a higher value, which is $\$4.8\times10^9$ (see Fig. 9). All in all, each participant in the market is better to make use of the stochastic framework to get more benefits of bargaining power in the P2P energy market.

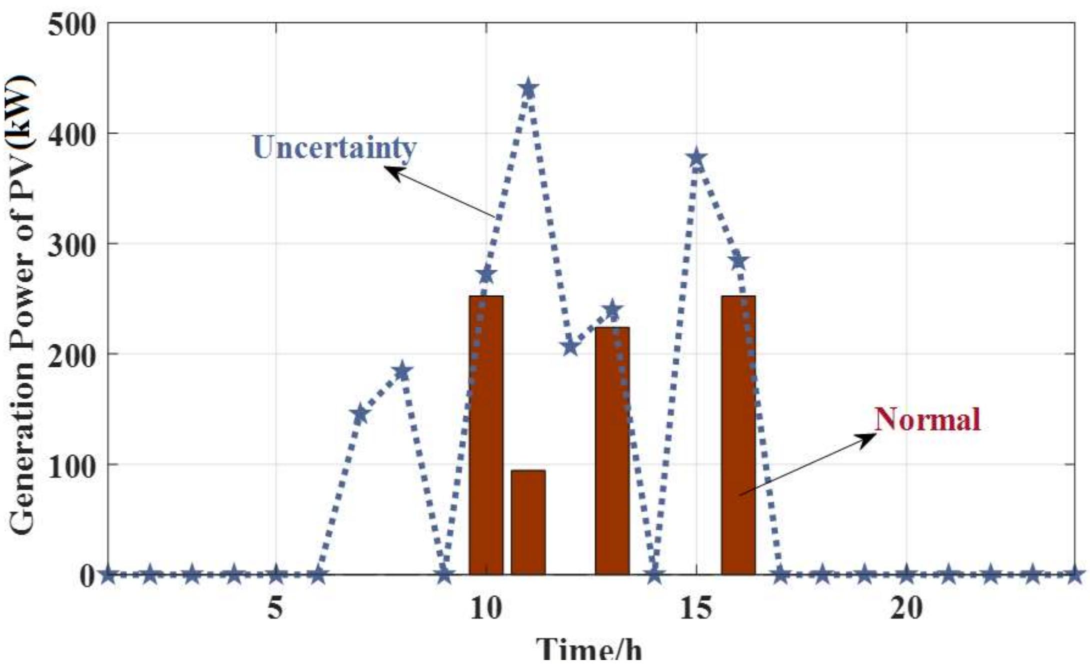

Fig. 20. The power of PV under normal/uncertain conditions

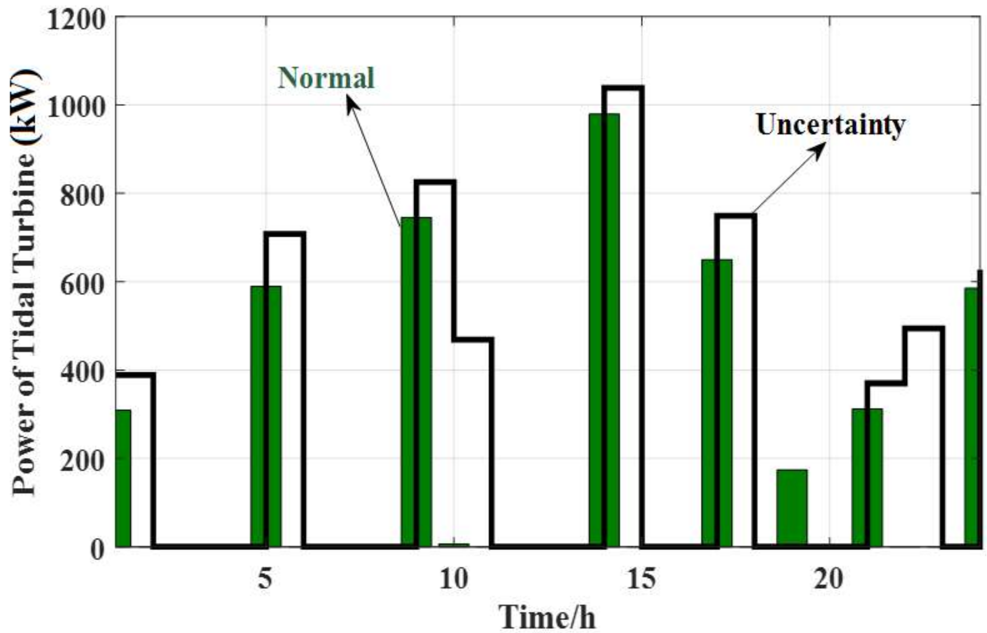

Fig. 21. The power of tidal turbine under normal/uncertain conditions

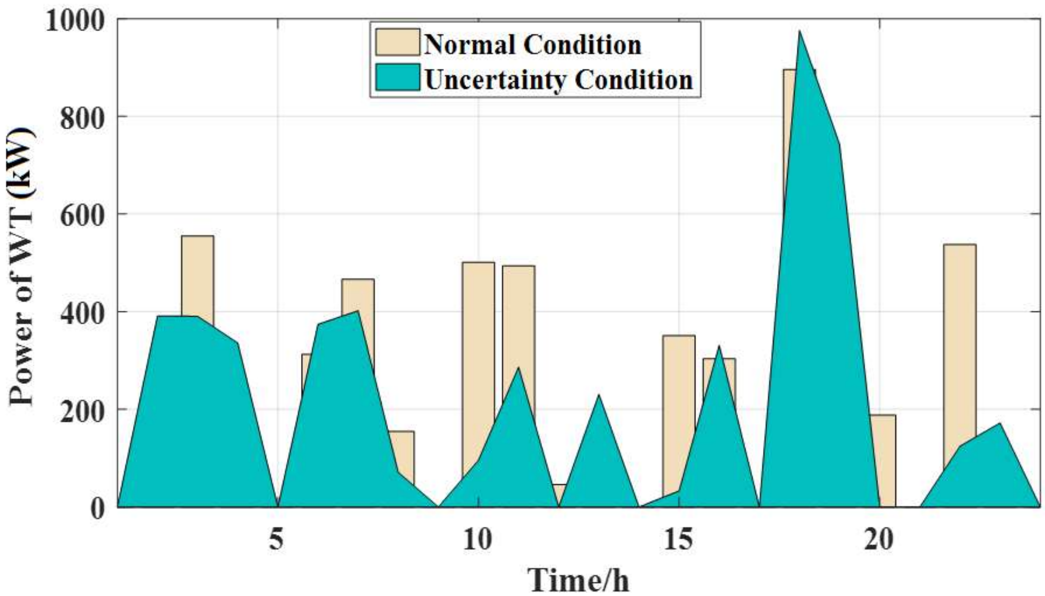

Fig. 22. The power of WT under normal/uncertain conditions

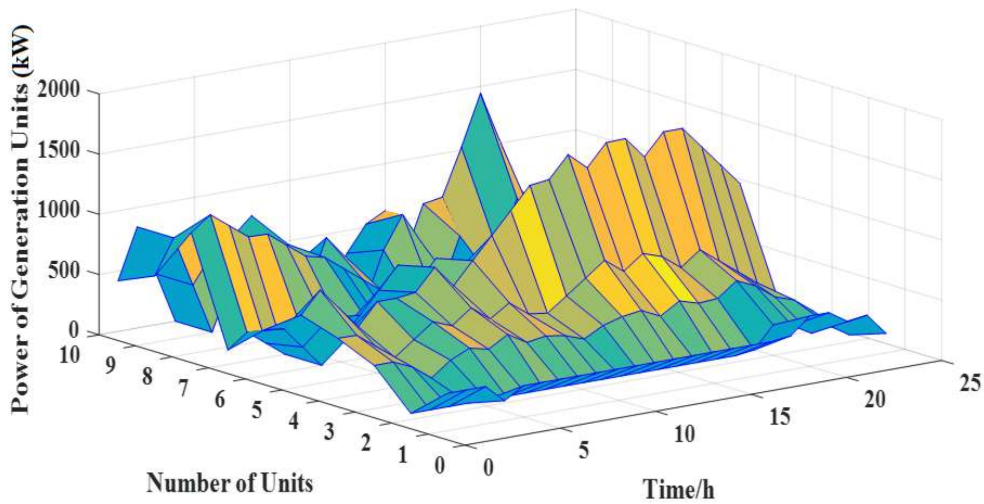

Fig. 23. The power of generation units

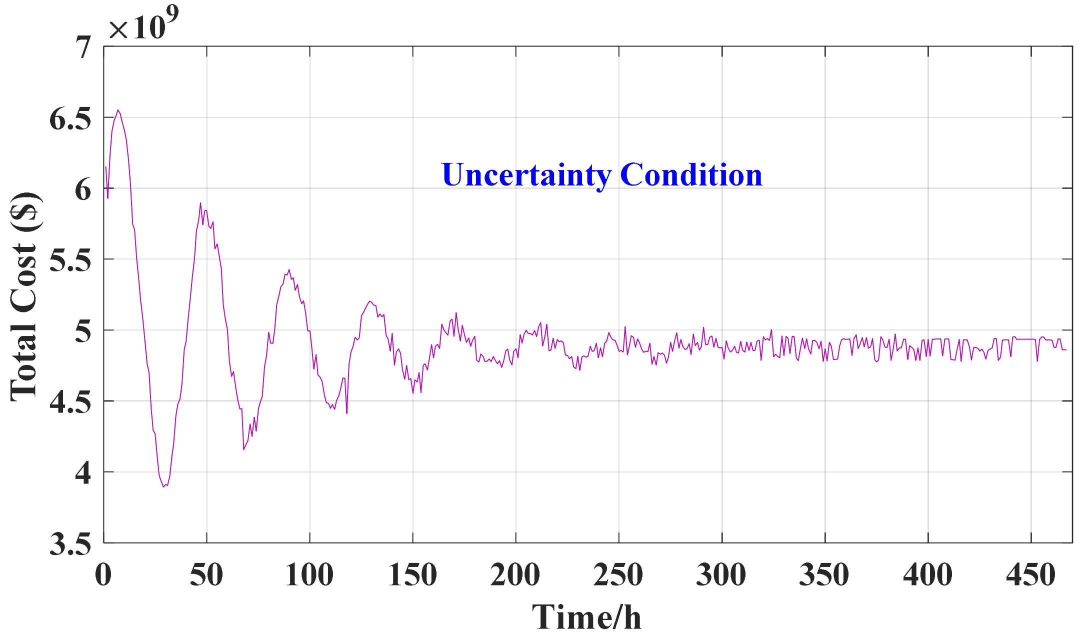

Fig. 24. The total operation cost in the stochastic framework

VI. Conclusion

This paper developed an effective peer-to-peer energy market between the microgrid and the smart grid and evaluated the function of distributed consensus algorithm based on the blockchain platform in the presence of FDIA attack. In order to validate the performance of the proposed method, a smart grid, which is the IEEE 24-bus test system, and a microgrid with a WT, PV, tidal turbine, and storage units are considered as the market participants. In this case, all agents (microgrid and smart grid) participate in the peer-to-peer market, which is secured by the blockchain system. Such a collaboration follows two main goals: the first goal is to ensure the system security in the presence of attacks, and the other is to achieve a consensus even in the case of cyber attack. This trend has been formulated, and the transactions based on the blockchain platform are exchanged among the agents. One of the most significant findings of this study is that the output response of the peer-to-peer market is so close to the centralized market. Hence, the results proved that the RCI based consensus algorithm is able to get into an appropriate agreement in such a way that the deviation of power transaction related to the P2P structure is near 4.16% compared to centralized framework. Such a low difference (less than 1%) is observed even when there is a cyber attack in the system. In other words, the consensus process continues despite of the cyber-attack. The stochastic results advocate the high reliability and appropriate performance of the proposed uncertain model. Based on results, the uncertainty model leads to make a upward rise from 4.11×10^9 to 4.8×10^9 in the total cost of P2P energy market which means that considering the energy market based on stochastic framework is a must. Finally, the effect of security is shown on the consensus system that the lack of blockchain causes to unguaranteed consensus convergence. The current finding adds to a growing body of literature on the decentralized based P2P energy market. For future scope of this work, the smart energy hub system as another agent can be considered in the study or the different attack detection methods in other to provide a safety environment in the energy market can also be investigated in future works.

References

[1] Ming Lei, Mojtaba Mohammadi, “Hybrid machine learning based energy policy and management in the renewable-based microgrids considering hybrid electric vehicle charging demand”, International Journal of Electrical Power & Energy Systems, Volume 128, 10 January 2021.

[2] F. Hasse, “Paving the way for the energy world of tomorrow”, PwC, Berlin - May 11, 2017.

[1] M. Crosa di Vergagni, S. MassuccoE. Ragaini, “A quasi-optimal energy resources management technique for low voltage microgrids”, International Journal of Electrical Power & Energy Systems Volume 121, 20 April 2020.

[2] F. C. Schweppe, M. C. Caramanis, R. D. Tabors and R. E. Bohn, Spot Pricing of Electricity, Kluwer

Academic Publishers, 1988.
[3] Emanuel Bernardi, Marcelo M. Morato, Eduardo J. Adam, “Fault-tolerant energy management for an industrial microgrid: A compact optimization method”, International Journal of Electrical Power & Energy Systems, Volume 124, 17 July 2020.
[4] Sorin, Etienne, Lucien Bobo, and Pierre Pinson. "Consensus-based approach to peer-to-peer electricity markets with product differentiation." IEEE Transactions on Power Systems 34, no. 2 (2018): 994-1004.
[5] Sperstad, Iver Bakken, Espen Hafstad Solvang, and Sigurd Hofsmo Jakobsen. "A graph-based modelling framework for vulnerability analysis of critical sequences of events in power systems." International Journal of Electrical Power & Energy Systems 125 (2020): 106408.
[6] Zhang, Runfan, and Branislav Hredzak. "Nonlinear sliding mode and distributed control of battery energy storage and photovoltaic systems in AC microgrids with communication delays." IEEE Transactions on Industrial Informatics 15, no. 9 (2019): 5149-5160.
[7] C.K. Woo, P. Sreedharan, J. Hargreaves, and F. Kahrl, “A review of electricity product differentiation,” Appl. Energy, vol. 114, pp. 262-272, 2014.
[8] Cui, Shichang, Yan-Wu Wang, and Jiang-Wen Xiao. "Peer-to-peer energy sharing among smart energy buildings by distributed transaction." IEEE Transactions on Smart Grid 10, no. 6 (2019): 6491-6501.
[9] G. Hug, S. Kar, and C. Wu, “Consensus + Innovations approach for distributed multi-agent coordination in a microgrid,” IEEE Trans. Smart Grid, vol. 6, no. 4, pp. 1893-1903, 2015.
[10] Qadir, Saeed, and Yergali Dosmagambet. "CAREC energy corridor: Opportunities, challenges, and IMPACT of regional energy trade integration on carbon emissions and energy access." Energy Policy 147 (2020): 111427.
[11] Vivek Mohan, Siqi BuZhao Xu, “Realistic energy commitments in peer-to-peer transactive market with risk adjusted prosumer welfare maximization”, International Journal of Electrical Power & Energy Systems, Volume 124, 30 July 2020.
[12] Ashim Basnet, Jin Zhong, “Integrating gas energy storage system in a peer-to-peer community energy market for enhanced operation”, International Journal of Electrical Power & Energy Systems, Volume 118, 23 December 2019.
[13] M. YebiyoR. A. MercadoA. Paurine, “Novel economic modelling of a peer-to-peer electricity market with the inclusion of distributed energy storage—The possible case of a more robust and better electricity grid”, The Electricity Journal, Volume 33, Issue 2, 20 February 2020.
[14] Flåm, Sjur Didrik. "Emergence of price-taking behavior." Economic Theory (2019): 1-24.
[15] Moret, Fabio, T. Baroche, E. Sorin, and P. Pinson. "Negotiation algorithms for peer-to-peer electricity markets: Computational properties." In 2018 Power Systems Computation Conference (PSCC), pp. 1-7. IEEE, 2018.
[16] Bilbao-Terol, Amelia, Mar Arenas-Parra, and Vitali Onopko-Onopko. "Measuring regional sustainable competitiveness: a multi-criteria approach." Operational Research (2019): 1-24.
[17] Guerrero, Jaysson, Daniel Gebbran, Sleiman Mhanna, Archie C. Chapman, and Gregor Verbič. "Towards a transactive energy system for integration of distributed energy resources: Home energy management, distributed optimal power flow, and peer-to-peer energy trading." Renewable and Sustainable Energy Reviews 132 (2020): 110000.
[18] Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. Manubot, 2019.
[19] M. J. Ashley and M. S. Johnson, "Establishing a Secure, Transparent, and Autonomous Blockchain of Custody for Renewable Energy Credits and Carbon Credits," IEEE Engineering Management Review,

vol. 46, pp. 100-102, 2018.
[20] A. S. Al-Sumaiti , M.M.A Salama, “Review on issues related to electric energy demand in distribution system for developing countries,” in the 3rd IET conference on Clean Energy and Technology (CEAT), (pp.1-6), Sarawak, Malaysia, November 24-26, 2014
[21] A. K. Banhidarah, A. S. Al-Sumaiti, “Heuristic search algorithms for optimal locations and sizing of distributed generators in the grid: a brief recent review,” the 1st ASET2018 First Multi Conferences on Advances in Science and Engineering Technology: Renewable and Sustainable Energy International Conference, Dubai, UAE, Feb. 2018, pp. 1-5.
[22] A.S. Al-Sumaiti, M.A. Hassan, S. Rivera, M.A.A. Salama, M. El Moursi, T. Alsumaiti, “Stochastic PV Model for Power System Planning Applications”, IET Renewable Power Generation, vol. 13, (16), 2019, p. 3168 – 3179.
[23] Joseph, T., Tyagi, B., & Kumar, V. (2020). Dynamic state estimation of generators using spherical simplex unscented transform-based unbiased minimum variance filter. IET Generation, Transmission & Distribution.
[24] Di Silvestre, M. L., Gallo, P., Guerrero, J. M., Musca, R., Sanseverino, E. R., Sciumè, G., & Zizzo, G. (2020). Blockchain for power systems: Current trends and future applications. Renewable and Sustainable Energy Reviews, 119, 109585.
[25] P. Sarda, M. J. M. Chowdhury, A. Colman, M. A. Kabir, and J. Han, "Blockchain for fraud prevention: a work-history fraud prevention system," in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, pp. 1858-1863.
[26] Liang, G., Zhao, J., Luo, F., Weller, S. R., & Dong, Z. Y. (2016). A review of false data injection attacks against modern power systems. IEEE Transactions on Smart Grid, 8(4), 1630-1638.
[27] A. Jindal, G. Singh Singh Aujla, N. Kumar, and M. Villari. "GUARDIAN: Blockchain-based secure demand response management in smart grid system." IEEE Transactions on Services Computing (2019).
[28] Z. Zhou, B. Wang, M. Dong, and K. Ota. "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing." IEEE Transactions on Systems, Man, and Cybernetics: Systems 50, no. 1 (2019): 43-57.
[29] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain. "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains." IEEE Transactions on Industrial Informatics 13, no. 6 (2017): 3154-3164.
[30] C. Liu, K. Keong Chai, X. Zhang, E. Tseng Lau, and Y. Chen. "Adaptive blockchain-based electric vehicle participation scheme in smart grid platform." IEEE Access 6 (2018): 25657-25665.
[31] Shetty, S. S., Kamhoua, C. A., & Njilla, L. L. (Eds.). (2019). Blockchain for Distributed Systems Security. John Wiley & Sons.
[32] Ding, S., Cao, Y., Vosoogh, M., Sheikh, M., & Almagrabi, A. (2020). A Directed Acyclic Graph Based Architecture for Optimal Operation and Management of Reconfigurable Distribution Systems with PEVs. IEEE Transactions on Industry Applications.
[33] M. Sheikh, J. Aghaei, A. Letafat, M. Rajabdorri, T. Niknam, M. Shafie-Khah and J.P. Catalão, "Security-Constrained Unit Commitment Problem With Transmission Switching Reliability and Dynamic Thermal Line Rating, ". IEEE Systems Journal, 2019.
[34] Sheikh, M., Aghaei, J., Rajabdorri, M., Shafie-khah, M., Lotfi, M., Javadi, M. S., & Catalão, J. P. (2019, June). Multiobjective Congestion Management and Transmission Switching Ensuring System

Reliability. In 2019 IEEE International Conference on Environment and Electrical Engineering and 2019 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe) (pp. 1-5). IEEE.

[35] Roustaei, M., T. Niknam, S. Salari, H. Chabok, M. Sheikh, A. Kavousi-Fard, and J. Aghaei. "A ScenarioBased Approach for the Design of Smart Energy and Water Hub." Energy (2020): 116931.

[36] H. Chabok, M. Roustai, M. Sheikh, and A. Kavousi-Fard, "On the assessment of the impact of a price-maker energy storage unit on the operation of power system: The ISO point of view," Energy (2019): 116224.

[37] Letafat, A., Rafiei, M., Ardeshiri, M., Sheikh, M., Banaei, M., Boudjadar, J., & Khooban, M. H. (2020). An Efficient and Cost-Effective Power Scheduling in Zero-Emission Ferry Ships. Complexity, 2020.

[38] Liang, Gaoqi, et al. "Distributed blockchain-based data protection framework for modern power systems against cyber-attacks." IEEE Transactions on Smart Grid 10.3 (2018): 3162-3173.