Hierarchical Blockchain Design for Distributed Control and Energy Trading within Microgrids

Jiawei Yang, *Student Member*, IEEE, Jiahong Dai, *Student Member*, IEEE, Hoay Beng Gooi, *Life Senior Member*, IEEE, Hung Dinh Nguyen, *Senior Member*, IEEE, Ping Wang, *Senior Member*, IEEE

Abstract—**Blockchain technology is recognized as a suitable tool to secure the energy trading because it could perfectly match the distributed structure of peer-to-peer (P2P) energy market. But its usage is stuck on the transaction level. Control systems are significant to the microgrid as they ensure a stable power delivery system and regulate the performance of parameters such as active power and frequency. This paper proves that the blockchain technology is also effective in securing the distributed control systems against the false data injection attack. A six-prosumer microgrid is tested with the implementation of the hierarchical blockchain system. The security of both the control system and energy trading system of the microgrid is ensured. Smart contracts are created to calculate the feedback measurements for the control system and execute the energy transactions. According to the hierarchical structure, the private blockchain with static nodes is implemented for the distributed control to match the sampling rate. A Proof-of-Authority based blockchain is utilised to support the energy trading. In addition, a double auction based simple iteration (DA-SI) pricing scheme is designed to improve the social welfare of the microgrid. Finally, case studies are presented to verify the proposed hierarchical blockchain system as an effective method to safeguard the control system and maximize the benefits of prosumers. Numerical results show the effectiveness and feasibility of the proposed approach.**

Index Terms—**Distributed control, peer-to-peer energy trading, cyber-security, hierarchical blockchain, smart grid**

I. Introduction

Peer-to-peer (P2P) energy trading has become an increasingly popular research direction since it allows direct energy trading among prosumers without being charged by intermediaries. To ensure the transparency and security of transactions, blockchain technology is widely used to protect the energy trading within microgrids. As blockchain has been already considered as an effective method for supporting P2P energy trading [1], the application potential of blockchain in other aspects of power system such as to safeguard the security of a control system could also be realised. To maintain a robust energy delivery system for energy trading, the requirement for a solid control system for local distributed generators is extremely significant [2]. Nowadays, the software systems for the modern power system, especially for the distributed secondary control, is vulnerable to cyber attacks. False data injection (FDI) is one of the malicious methods to attack the exchange measurement data and control commands via the control network of microgrids [3]. Due to the cryptographic mechanism and distributed ledger features of blockchain, it is valuable to apply blockchain technology to ensure the security of both control systems and energy trading for power systems.

A. Related Work

For the previous research on blockchain based energy trading, the authors in [4] integrate their proposed blockchain framework with a double-auction Vickrey-Clarke-Groves (VCG) mechanism to handle probable market deficiencies. The bilateral contracts and electronic commerce platform are also created to support the trading functionalities with the main grid, which is similarly considered in [5]. Differently, the authors in [5] also take the power loss factor from energy transmission into account and create an internal mining-rewarding mechanism to maintain the consortium blockchain extension, which is also utilised in [6], [7] to provide a quantitative analysis of the blockchain value and disable the dishonesty and malicious behaviours among participants. In [8], the authors design a new slot-ahead electricity market structure based on an end-user marginal price linked with a modified blockchain model. To consider prosumers' behavior deviation in the distributed power dispatch mechanisms, a distributed strategy update algorithm is proposed in [9] to optimize their bids by using the price information. For the implementation of blockchain, the authors in [10] use private blockchain to enhance the stability and efficiency of their proposed energy trading model with the consideration of credit rating. The research work about various pricing schemes for blockchain based energy trading is also investigated. Game theory [11]–[13], demand response [14], [15] and double auction [16], [17] are widely applied in the P2P energy trading. But the mechanisms of game theory and demand response include a complicated iterative computation burden that the smart contract could not afford. Therefore the double auction is considered as the optimal market clearing method to be supported by the blockchain. In addition, while traditional double auctions could only provide a trading price range, determining the optimal price of the market calls for more specific pricing schemes.

As energy trading is operated on the basis of safe energy generation and transmission systems, the cyber-security for the distributed control of power systems becomes a significant task. The centralised control system of the microgrid is vulnerable to the FDI since the microgrid operator could not provide efficient detection and protection. FDI as a major threat to microgrids is studied in the previous work. The authors in [18] introduce an attack vector relaxing error and propose an imperfect false data injection attack model as well as its implementation method. In [19], the authors analyze the FDI attack in the electricity grid that it could compromise either the physical or economic operation of the power system based on the experience from the late 2015 Ukraine Blackout event. The local FDI attack is modelled in [20] with reduced network information to determine the optimal attacking region of modern power grids. In addition to the modelling and simulation, the detection of FDI attack is studied in [14], where a sub-grid oriented micro-service framework which integrates a designed spatial-temporal neural network in AC-model power systems is proposed. Various types of FDI datasets are tested on a public benchmark power grid. The authors in [21] analyse different FDI detection algorithms including the model based and data driven algorithms. The main criteria that should be considered in developing detection algorithms for the FDI attacks is also presented. Other FDI detection methods such as filter-based tracking scheme [22], deep learning [23] and deep neural network [24] are utilised to recognize the behaviour pattern of FDI based on the historical measurement data.

B. Motivation and Contribution

However, the implementation process of blockchain is rarely demonstrated in the previous works and the computation burden of their proposed pricing scheme cannot be afforded by the blockchain system theoretically such as machine learning [25] and game theory [26], [27]. The drawbacks of both public and private blockchains are not addressed since: 1) public chain could cause enormous gas costs and mining consumption; 2) private chain cannot ensure the decentralised trading structure of P2P energy market and it becomes vulnerable when the central agent is attacked or becomes malicious. Additionally, it should be noted that no studies have been considered on expanding blockchain in other aspects of the power system in addition to its usage for P2P energy trading. The bottleneck of blockchain applications in the power system lies essentially in supporting the energy transaction. Current studies on blockchain based control system mainly focus on the access control system with IoT, which ensures the data privacy of networks. The concept of this type of control system is different from that existing in the power system. And for the FDI attack against the distributed control systems, most of the previous studies only focused on modelling and detection without proposing an effective protection approach [28]–[30]. For those studies with respective protection strategies, their designed methods are only effective to few specific FDI attacks or their problem formulation is based on random attacks [31]. Although blockchain is considered as a potential method to address FDI attacks in several works [32], [33], there is no implementation to prove that it could be a comprehensive method to protect the secondary control of the power system.

In this paper, the focus is on designing a hierarchical blockchain based on the Ethereum platform to protect both the control system and energy trading for a microgrid. The first level of blockchain implementation is for the distributed secondary control layer, which requires a secure and efficient communication environment for the neighbouring local distributed generation (DG) controllers. Depending on the cryptographic and consensus protocol feature of the blockchain, any malicious attack is prevented by its adoption [34]. Besides, its data transparency and the decentralization feature could provide an efficient detection of the FDI. Instead of exchanging the money and products (energy) for transactions, the designed smart contracts are responsible for executing the exchange of the input and feedback control commands during each sampling slot. To match each extremely short sampling slot and ensure the control quality, the Ethereum private blockchain with static nodes connection is used for the first level of the proposed hierarchical blockchain system since the public blockchain requires a much longer period for block production and costs enormous gas consumption. It has been proved that a private blockchain is able to mine 20,000 transactions per second [35] which is adequate to match the sampling of the distributed control system (DCS).

The second level of the hierarchical blockchain system is designed for the P2P energy trading within the microgrid. Due to the limited calculation capability of smart contracts, a double-auction with simple iterations (DA-SI) method is proposed to generate the optimal trading price for both consumers and producers to improve the social welfare. In the second blockchain level, an Ethereum based Proof-of-Authority (PoA) private blockchain is adopted to protect each energy transaction. By assigning all of the prosumers as the authority nodes, the PoA consensus protocol regulates the behaviours of prosumers and incentivizes the miners to maintain the blockchain operation [36]. Besides, the mining consumption is controllable since the mining opportunity is competed within the microgrid and the decentralised trading structure is ensured as no central agent could dominate the mining mechanism.

In this context, the contributions of this paper are:

- The breakthrough of the bottleneck of blockchain applications in a power system is achieved by the designed hierarchical blockchain system, which expands its usage to the distributed secondary control layer of the microgrid in addition to the energy trading.
- Both the internal and external FDI attacks against secondary control are analyzed and defended by the proposed blockchain model and the quality of each control process is also ensured as the mining rate is improved to match the sampling rate of control system.
- A smart contract-affordable pricing scheme design is created by using DA-SI method with the PoA consensus protocol, which eliminates the price gap between buying and selling price and improves prosumers' welfare.
- The implementation of the hierarchical blockchain system to protect and support both DCS and P2P energy trading is specifically demonstrated.

The remaining of this paper is organized as follows: Section II presents the system setup of the proposed hierarchical blockchain system for the microgrid. Section III describes the protection mechanism of the first blockchain layer for the secondary control. The second blockchain layer designed for P2P energy trading with the proposed DA-SI scheme is introduced in Section IV and a welfare analysis is presented. A case study as well as the implementation process of the hierarchical blockchain system is shown in Section V. Section VI analyses the performance and security results of the proposed method. Finally, Section VII concludes the study and proposes its related future work.

II. Hierarchical Blockchain System Setup

The proposed hierarchical blockchain system is set up based on Ethereum platform. As one of the biggest blockchain companies, Ethereum provides multiple blockchain services and flexible environment for researchers to build up their own projects. Although Hyperledger Fabric and Hyperledger Besu are also proficient in the private blockchain setup [37], Ethereum private blockchain is facilitated with a simpler and clearer mining mechanism [38] which is more suitable for matching the high-rate sampling frequency of DCS. The blockchain setup for the P2P energy trading within the microgrid is also based on Ethereum but the PoA consensus protocol is adopted to progressively support the DA-SI pricing scheme. Fig. 1 presents the schematic illustration of the proposed blockchain based microgrid system.

According to Fig. 1, the first level of the proposed blockchain system is the private blockchain based DCS for four DG controllers, which safeguards the data transmission and delivers the control commands back to the microgrid. Supported by the first distributed control layer, the second level of the blockchain system is the energy trading layer within the 6-prosumer microgrid, including four producers with respective DG and two consumers. All prosumers are equipped with a battery energy storage system (BESS). Specific explanations of the proposed hierarchical blockchain based microgrid for DCS and energy trading are provided in Sections III and IV respectively.

III. First Level: Private Blockchain Design for DCS

In Fig. 1, the distributed control layer of the DCS simulation setup by RT-LAB is operated in a real-time simulator machine. In this paper, the proposed blockchain system is set up on the four-DG controller microgrid.

A. Working Process

In this section, the working process of the proposed model is specifically explained. The real-time input data sampled from DCS is transferred to a socket interface via the User Datagram Protocol (UDP), which is a communication protocol used to enable low-latency data transmission. The socket interface provides data transmission services between the DCS and the private Ethereum blockchain, including four data transfer channels for the four DG secondary controllers. The data items are packed and categorized for further transmission to the proposed blockchain system by using Remote Procedure Calls (gRPC) which provides services such as authentication and bidirectional streaming. After receiving the input data, the DG controller nodes collect the measurements from each other depending on the communication network provided by the static nodes services shown in Fig. 2.

According to Fig. 2, each controller node could only communicate directly with another two nodes since there is no communication line between the nodes on the diagonal lines. The communication structure of the four DG controllers could be described as a weighted adjacency matrix I as:

$$I = \begin{bmatrix} 0 & in_{12} & 0 & in_{14} \\ in_{21} & 0 & in_{23} & 0 \\ 0 & in_{32} & 0 & in_{34} \\ in_{41} & 0 & in_{43} & 0 \end{bmatrix} \tag{1}$$

where $in_{ij} > 0$ refers to the direct information exchange between controllers DG_i and DG_j. Since there is no communication line between DG_1 and DG_3, DG_2 and DG_4, the corresponding elements are 0.

The static nodes are a set of trusted nodes and the DG controller nodes are connected with each other through $StaticNode.json$, which records their $enode$ [39] addresses of them. $enode$ is the connection port of each blockchain node offered by the Ethereum platform [36]. In addition, static nodes are exempted from maximum peer and remote connection limits and therefore this connection method provides a more flexible communication network and improves the speed of the mining process. Under most ideal conditions, the duration of each block production equals to that of each sampling process ($T_b = T_s$).

The smart contracts are responsible for the controller formulation and feedback calculation. The functions in the smart contracts for data exchange are designed for the four secondary controllers. After being deployed to the blockchain by the $Truffle.js$, the $Web3.py$ calls the functions offered in smart contracts to calculate the control feedback such as frequency U_w sent by the secondary controllers as:

$$U_w = K_w * [(I - D) * F + G * (F^* - F)] \tag{2}$$

$$F = \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{bmatrix} \tag{3}$$

$$D = \begin{bmatrix} in_{12} + in_{14} & 0 & 0 & 0 \\ 0 & in_{21} + in_{23} & 0 & 0 \\ 0 & 0 & in_{32} + in_{34} & 0 \\ 0 & 0 & 0 & in_{41} + in_{43} \end{bmatrix} \tag{4}$$

where G is the weighted matrix and F^* is the reference frequency matrix of the four DG units. K_w refers to the positive control gain. For each controller, the diagonal elements in D refer to the communication lines linked with other controllers according to Matrix I. They are the sum of the elements in every row of Matrix I. The working mechanism of smart contracts is demonstrated by Algorithm I.

It should be noted that the final step of the smart contract execution is to remove the previous data. It is because new measurement data of the next control process will arrive. The removal of the previous data helps to relieve the storage burden of smart contracts and prevent latency caused from the mining process. Then, the new value of the DCS frequency with its objective is calculated as:

$$w_i = w_i^* - k_{wi}P + \delta w_i \tag{5}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2022.3153693, IEEE Transactions on Smart Grid

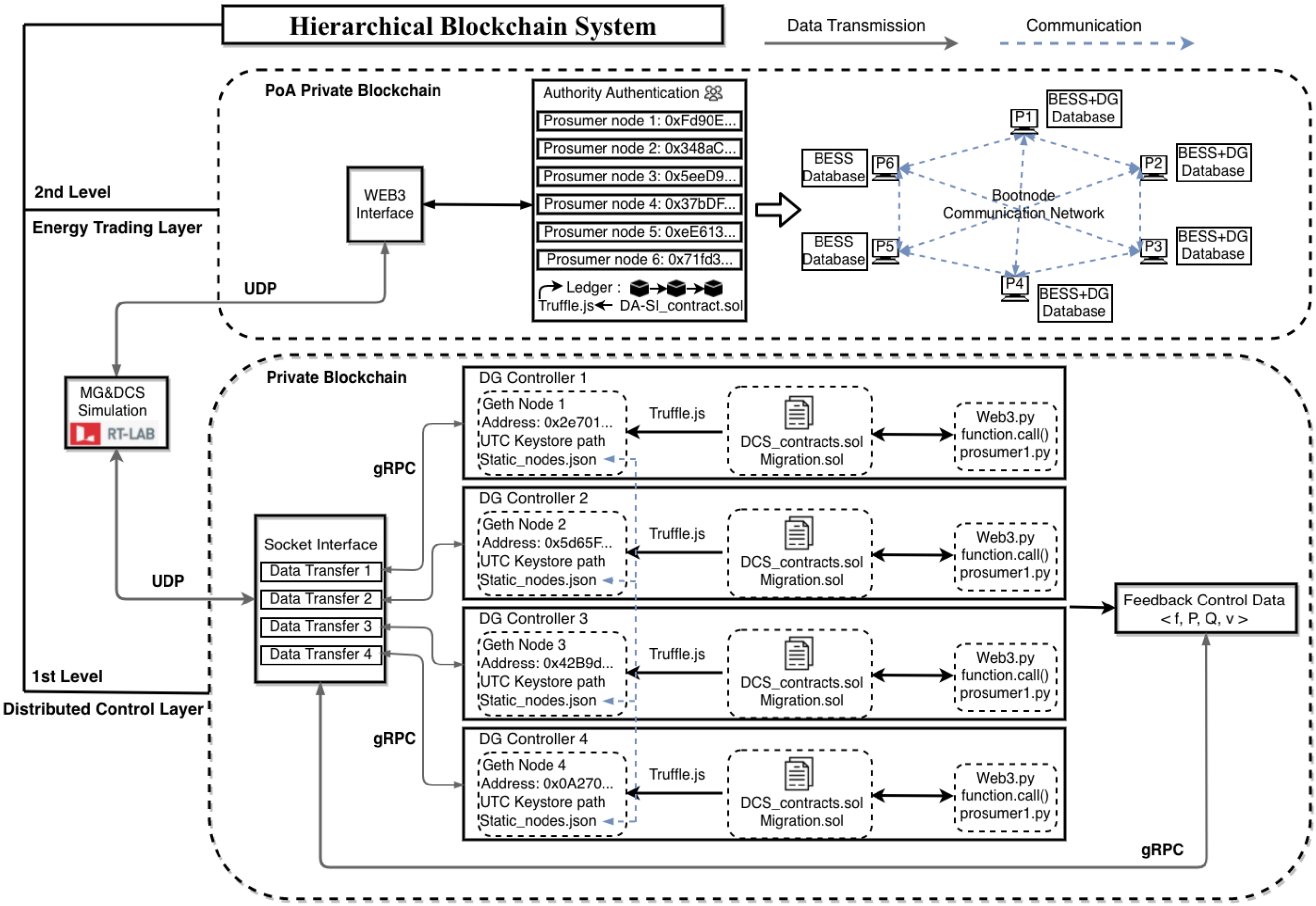


Fig. 1. Schematic diagram for the hierarchical blockchain system based microgrid

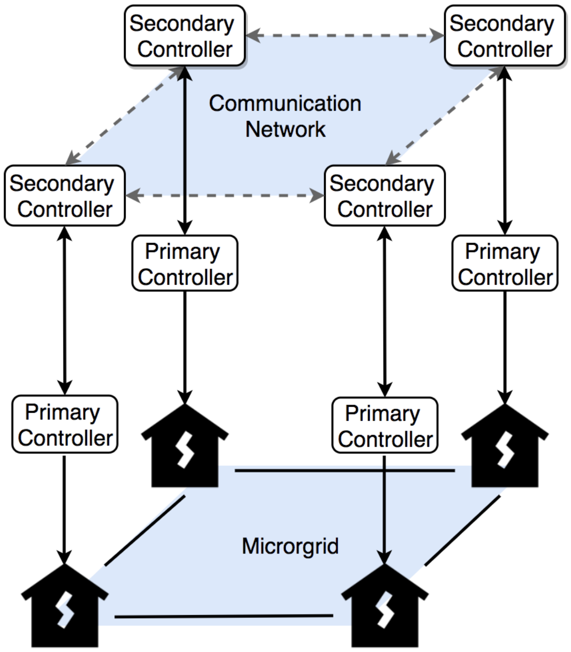


Fig. 2. DCS structure of microgrids

$$\lim_{t \to \infty} w_i(t) = w_i^* \tag{6}$$

Algorithm 1 DCS execution of smart contract

```
for each $smartcontract_i \in [block_i]$ do
    Establish structure of each node:
$< address[account], uint[id], int[f, P, Q, v] >, bool[true]$
    Constructor:
reference value $K_w, w_i^*, owner[msg.sender]$
    Receive data:
Register nodes $< address, id, [f, P, Q, v] >$;
Require $node.engage = true$;
    Input: $int[f, P, Q, v]$
    Calculation:
Function I: feedback calculation for $node1$;
Function II: feedback calculation for $node2$;
Function III: feedback calculation for $node3$;
Function IV: feedback calculation for $node4$;
    Return values to four nodes:
$< address[account], uint[id], int[f, P, Q, v] >, bool[true]$;
    Delete nodes information;
end for;
```

where w_i^* is the reference frequency value for DG_i. k_{wi} is the droop coefficients and δw_i is the compensation item of the secondary control.

Finally, the new measurements are transferred back to the socket interface via the gRPC and further passed to the real-time simulator machine, which is the end of one control process.

B. Protection Rationale

Unlike the traditional private blockchain that only one node is assigned as the miner to pack the data and maintain the operation of a blockchain, all of the four nodes are assigned as miners to share the computation burden of mining. The input and feedback data is protected by a cryptographic packing method called hash function, which encodes the practical measurement data into a set of hash codes. The produced hash codes are extremely difficult to be decoded and traced. Thus, these data items are protected by the blockchain system. The content of each block that will be hashed includes the measurement data, smart contracts, time and previous hash codes of its former block, which is defined as:

$$Block(n) = Hash(DCS < data >, Ctrcs, Time, Block(n{-}1)) \tag{7}$$

where $Ctrcs$ refers to the deployed smart contracts and $DCS < data >$ refers to the measurements of the electrical parameters.

According to (7), the chains of blocks are established because the hash codes of each new block are produced based on those of the previous blocks. This feature protects the DCS system as any malicious attacks on overwriting the content of the blocks would break the chain which could be simply detected and become an invalid attack. Especially for the attacks outside the microgrid such as the FDI attack, the attackers are required to decode the hash code, inject the false data into the DCS data or smart contracts and re-hash the new block content with all of its previous blocks again. Furthermore, since the blockchain only recognizes the longest chain, the mining computation capability of the attackers must overpass those four mining nodes within the microgrid. Such enormous workload is extremely energy consuming which is considered as impossible to accomplish. To enhance the mining rate, the mining difficulty of the blockchain is set at a very low value. With the support from the gRPC, the mining speed is theoretically impossible to be exceeded by any attackers outside the microgrid.

Another type of FDI attack is the attacker inside the microgrid, which means the attacker is one of the assigned miners. In this scenario, DG controller $node1$ is assumed to be the malicious miner. In each control process, the input of the attacker $node1$ is overwritten and injected as false data set:

$$N_1^T = \begin{bmatrix} FD_1 & D_2 & 0 & D_4 \end{bmatrix} \tag{8}$$

where FD is the false input from $node1$ and D_i is the input from the other $nodei$ controllers.

According to (2), a false calculation outcome of the smart contract is generated as:

$$U_{ow1} = K[(D^* - FD_1) + (D_2 - FD_1) + (D_3 - FD_1)] \tag{9}$$

with

$$U_{ow1} = U + \alpha_{ow1} \tag{10}$$

where D^* is the reference value, and α_{ow1} refers to the deviation between the corrected U and the false U_{ow1}.

When it comes to the DG controller $node2$, the input received could be defined as:

$$N_2^T = \begin{bmatrix} FD_1 & D_2 & D_3 & 0 \end{bmatrix} \tag{11}$$

where FD_1 is the input false data from the $node1$.

Its feedback value U_2 is also influenced by the false FD_1 injection which leads to a new false measurement from $node2$ as FD_2 in the next round of control as:

$$U_{ow2} = K[(D^* - D_2) + (FD_1 - D_2) + (D_3 - D_2)] \tag{12}$$

Subsequently, the false feedback provided by the attacker $node1$ then progressively influence the inputs for all the other controller nodes as well as those of the next DCS process until all of the inputs are false data which is shown as:

$$I(x) = \begin{bmatrix} FD_1 & FD_1 & 0 & FD_1 \\ FD_2 & FD_2 & FD_2 & 0 \\ 0 & FD_3 & FD_3 & FD_3 \\ FD_4 & 0 & FD_4 & FD_4 \end{bmatrix} \tag{13}$$

The consequence caused by (13) would lead to frequency concussion and breakdown of the DCS system. In this scenario, the advantage of static nodes based private blockchain could be realised. Within the proposed blockchain system, tracing the data does not require decoding and re-mining for the other miners within the microgrid, and therefore it is convenient and efficient to detect the malicious miner. As mentioned, the list of static nodes is made on the basis of trust among miners of the private blockchain. Since the whole mining process is transparent to the other three miners, once the malicious miner has been detected, it will be defined as an untrustworthy node and its account address will be eliminated in the static nodes list, thereby losing the connection to the whole blockchain based DCS system. The protection rationale of the proposed blockchain system is illustrated in Fig. 3.

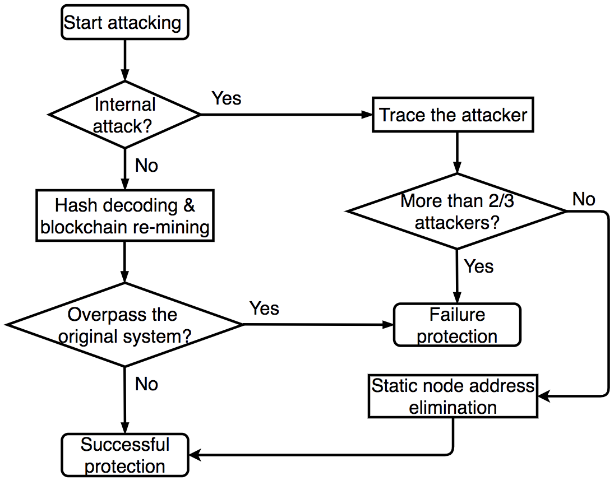


Fig. 3. Protection mechanism against internal and external attacks

Overall, the first level of the hierarchical blockchain system is able to guarantee the integrity and reliability of the DCS system without causing any negative effect as long as 2/3 of the nodes are not compromised according to the Ethereum standards [36].

IV. Second Level: PoA Blockchain Design for Energy Trading

As shown in Fig. 1, the proposed microgrid system includes six prosumers, of which four producers are equipped with DG and the other two are consumers. In the P2P market, producers could also become consumers when their energy generation cannot fulfill their load demands and consumers could become producers when they have surplus energy in their BESS. The energy generated by each producer should firstly fulfill their own demands and the extra energy stored in BESS could be sold in the market. Since private blockchain is applied in the proposed model, the mining consumption is extremely low and thereby being ignored in the welfare calculation.

A. Blockchain Design

Different to the blockchain adopted in the first DCS layer, a PoA based private blockchain is applied for the energy trading layer. According to the PoA consensus protocol, only authority nodes could validate transactions and generate blocks. These authority nodes are also known as trusted nodes. This means that the authority role depends on the reputation of each node. Prosumers earn the right to become authority nodes so they are incentivized to maintain the mining process to attach a positive reputation to their own identity. Malicious operation within the microgrid will be punished by having the node removed from the list of authority nodes. This consensus protocol is more robust and efficient than the others such as Proof-of-Work and Proof-of-Stake due to less energy consumption and latency caused.

In the proposed PoA blockchain system, all six prosumers are initially assigned as authority nodes to share the mining burden. The communication network is supported by a Bootnode service instead of static nodes since the mining process for energy trading is not required to achieve such high-rate block production as that for the DCS system, and the interface of Bootnode enables the supervision of the nodes connection. The information of energy generation and BESS profile is stored in prosumers' respective database. The data of successful energy trading is recorded in the distributed ledger offered by the blockchain system. The proposed DA-SL pricing scheme is coded in the smart contract and deployed to the blockchain by $Truffle.js$. The $WEB3$ interface enables the data transmission of energy transactions between the microgrid and the blockchain system.

The protection rationale for the energy trading layer is similar to that for the DCS layer. As transaction information is hashed and added to the blockchain, it is impossible to be overwritten. In addition, legal behaviours of prosumers are ensured since malicious operation is punished according to the PoA consensus protocol.

B. Pricing Scheme Design

In this paper, a DA-SI pricing scheme is proposed to generate the trading price and clear the market. An effective double auction based pricing scheme should maximize the social welfare and total utilities of prosumers while incentivizing prosumers to bid their price. In the DA-SI pricing scheme, the bid prices of consumers (b_i) are sorted in the descending order with the consideration of the price offered by the utility grid (UG),

$$b_1 > b_2 > ... > b_N > b_{FIT}, \quad N \in [1, 6] \tag{14}$$

where b_{FIT} is the price offered by the feed-in-tariff (FIT) and N is the number of consumers.

The ask prices of the producers (a_i) are sorted in the ascending order with the consideration of the price offered by the utility grid (UG) as:

$$a_1 < a_2 < ... < a_{6-N} < a_{UG}, \quad N \in [1, 6] \tag{15}$$

where a_{UG} refers to the price from the utility grid. With six total prosumers and N conusmers, the number of producers is calculated as $6 - N$.

As illustrated in Fig. 4, the intersection point of the quantity-price curves of the producers and consumers defines the range of the clearing price within $[a_j, b_i]$.

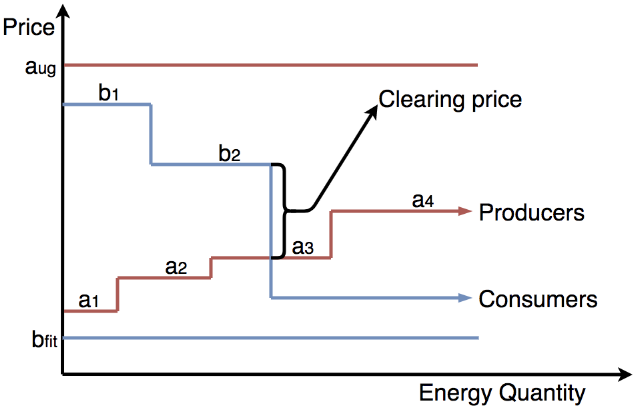


Fig. 4. DA-SI pricing mechanism

To further calculate the clearing price within the range, a simple-iteration (SI) plan is proposed. The final value of the clearing price for each time slot should be related to the supply-demand (SD) ratio according to the rationale of economics [40]. The SD ratio ϵ is calculated as:

$$\epsilon^t = \frac{\sum_{j=1}^{6-N} p_{Gj}^t}{\sum_{i=1}^{N} p_{Di}^t} \tag{16}$$

where p_{Gj}^t refers to the surplus energy generated by producer j and p_{Di}^t is the energy demands of consumer i.

The correlation between the electricity ask prices and the SD ratio should be negatively proportional [41]. With the price range $[a_j, b_i]$ produced from the double auction mechanism, the SI scheme is designed as:

$$A^t(n+1) = \frac{B^t(n)}{\frac{B^t(n)-A^t(n)}{A^t(n)}\epsilon^t + 1}, \begin{cases} A^t(0) = a_j^t \\ B^t(0) = b_i^t \end{cases} \tag{17}$$

$$B^t(n+1) = A^t(n+1)\epsilon^t + B^t(n)(1-\epsilon^t), \begin{cases} A^t(0) = a_j^t \\ B^t(0) = b_i^t \end{cases} \tag{18}$$

where $0 < \epsilon < 1$, and $A(n)$ and $B(n)$ are the ask and bid prices after n iterations.

The iteration will be terminated until the value of the bid price equals the ask price $A(n) = B(n)$. The specific convergence proof of the iterations is introduced in [5]. But unlike the iteration scheme provided in [5], the initial value of $A(0)$ and $B(0)$ are set as a_j and b_i respectively according to the double auction, in which the price range is smaller and thus the iteration calculation burden is progressively relieved and more affordable for smart contracts execution. Finally, the clearing price C for each time slot is defined as:

$$C^t = A^t(n) = B^t(n) \tag{19}$$

The proposed DA-SI pricing scheme is written in the smart contracts. This enables the clearing of energy transactions automatically when the respective value for payments and products is balanced. Then, transactions are validated by the authority prosumers and added to the PoA blockchain. As the price gap between bid prices and ask prices is eliminated, the electricity price is represented by C in the remaining sections.

C. Utility and Welfare Analysis

According to Fig. 1, prosumers within the microgrid are equipped with BESS. If the annual cost of each prosumer's battery system is E_{bs}, then the equivalent daily cost is calculated as $\frac{E_{bs}}{365}$. Another expense of the microgrid is the generation cost E_g from the producers, which is generally defined as a quadratic convex form of each producer's power generation G_j [42],

$$E_{gj} = \alpha_j G_j^2 + \beta_j G_j + \sigma_j \tag{20}$$

where α_j, β_j and σ_j are the cost function parameters related to the types of generation source and the cost of maintenance.

The utility function models the satisfaction level of prosumers related to the amount of energy purchased under various scenarios [43]. A reasonable utility function design should satisfy certain conditions which are:

- If there is no executed energy transaction, the value of customers' satisfaction level is 0.
- Within the scale of the function, the maximum value is supposed to be obtained.

To achieve the above two requirements in the energy trading field and for the purpose of a clear demonstration, a widely adopted piece-wise quadratic utility function is applied for each consumer. This is defined as:

$$U^t(p_i^t) = \begin{cases} 2r_i^t p_i^t - w_i(p_i^t)^2 & p_i^t < \frac{r_i^t}{w_i} \\ \frac{(r_i^t)^2}{w_i} & p_i^t >= \frac{r_i^t}{w_i} \end{cases} \tag{21}$$

where r_i^t and w_i are the private parameters of consumer i, both of which distinguish the consumer from the others. The value of r_i^t may vary in different time slots or with respective behaviours of consumers. w_i is a constant value that relies on specific energy trading conditions.

In this paper, the energy trading is based on the assumption that the energy demands proposed by each consumer are inflexible and necessary. This means the amount of energy demands is the minimum value that achieves the maximum of the utility function.

$$p_i^t = min[\underset{p_i^t = p_{Di}^t = \frac{r_i^t}{w_i}}{\arg\max} \|U^t(p_i^t)\|] \tag{22}$$

where p_i^t is the power demand of prosumer i in t time slot.

Based on (22), the value of r_i^t can be calculated as:

$$r_i^t = w_i \times p_{Di}^t \tag{23}$$

By substituting the result from (23) into (21), the new utility function is formed as:

$$U(p_i^t)^t = \begin{cases} w_i p_i^t \times |2p_{Di}^t - p_i^t)| & p_i^t \neq p_{Di}^t \\ w_i p_{Di}^{2,t} & p_i^t = p_{Di}^t \end{cases} \tag{24}$$

With the consideration of the energy trading, the welfare of consumers within the microgrid for one day is defined as:

$$W_c = \sum_{t=t_1}^{t_h} \sum_{i=1}^{N} \Big(U^t(p_i^t) - C^t p_i^t - \gamma E_{gi}^t \Big) - \sum_{i=1}^{N} \frac{E_{bs}}{365} \tag{25}$$

where $\gamma = 1$ refers to the consumers with DG and $\gamma = 0$ refers to the consumers without DG. t is the time slot.

The welfare of producers within the microgrid for one day is calculated by eliminating the cost of battery and DG maintenance from their incomes via the energy trading as:

$$W_p = \sum_{t=t_1}^{t_h} \Big[C^t \; p_{Di}^t - \sum_{j=1}^{6-N} E_{gi}^t \Big] - \sum_{j=1}^{6-N} \frac{E_{bs}}{365} \tag{26}$$

Finally, the social welfare of the microgrid is defined as the total value of the welfare of all prosumers within the microgrid.

V. Case Studies

In this section, the simulation of the four-DG control system is performed in RT-LAB and MATLAB software. The simulation model of the four-DG islanded microgrid is established and Table I shows the electrical and control parameters for the microgrid.

TABLE I
Parameters of DCS

Parameter	Value
Line Impedance	R =0.4 $\Omega, L = 1.8mH$
Reference frequency	w^* = 50 Hz
Reference voltage	V^* = $230\sqrt{2}V$
DG Impedance	R = 0.1 $\Omega, L = 4.8mH$
$DG_{1,2}$ Capacity	$k_P = 2e^{-4}$, $k_Q = 4e^{-3}$
$DG_{3,4}$ Capacity	$k_P = e^{-4}$, $k_Q = 2e^{-3}$

The information of the software and hardware facilities for the hierarchical blockchain implementation is provided in Table II. For both layers, the blockchain is established by installing $Geth - 1.10.6$ with $Truffle - v5.1.49.js$ and $Web3 - 5.12.0.py$ to deploy and realise the functions written in the Solidity smart contracts.

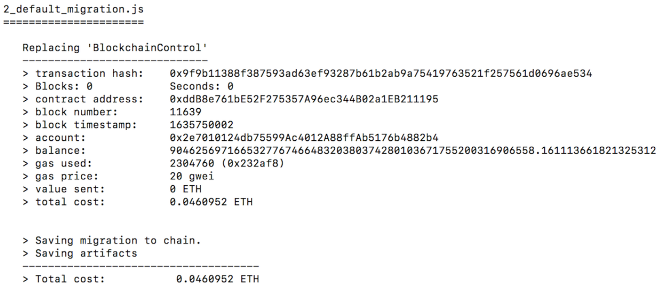
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2022.3153693, IEEE Transactions on Smart Grid

TABLE II
FACILITIES INFORMATION FOR BLOCKCHAIN IMPLEMENTATION

Facility	Version
Geth	1.10.6
Node.js	6.14.6
Truffle.js	5.1.49
Web3.py	5.12.0
Solidity smart contracts	$>= 0.4.22 < 0.7.0$
Raspberry Pi	$10 \times 4 ModelB$
RT-LAB	11.3.1.34
MATLAB	$2014b$
Other Software Scripts	Programming
gRPC	.py
UDP	.py
Static-nodes	.json
Puppeth	Geth-tool
Bootnode	Geth-tool

A. First Level Blockchain Implementation

For the first layer, four of ten Raspberry Pi 4Bs are used for the node installation of the four-DG secondary controllers. $gRPC$ and UDP are set up for the data transmission between different modules illustrated in Fig. 1. Static nodes are set up by storing the enode ports of the DG nodes in $static-nodes.json$ for the communication network. The block production interval is restrained within 200µs. The smart contracts deployment is demonstrated in Fig. 5, which includes the addresses of smart contracts, corresponding authority nodes and hash codes. The control results of the proposed blockchain based DCS and the DCS without blockchain in the normal condition are compared in Fig. 6. The control results under a FDI attack at 6 seconds are compared in Fig. 7 (the data injection is made by $node1$.



```
2_default_migration.js
======================

   Replacing 'BlockchainControl'
   -----------------------------
   > transaction hash:    0x9f9b11388f387593ad63ef93287b61b2ab9a75419763521f257561d0696ae534
   > Blocks: 0            Seconds: 0
   > contract address:    0xddB8e761bE52F275357A96ec344B02a1EB211195
   > block number:        11639
   > block timestamp:     1635750002
   > account:             0x2e7010124db75599Ac4012A88ffAb5176b4882b4
   > balance:             904625697166532776746648320380374280103671755200316906558.161113661821325312
   > gas used:            2304760 (0x232af8)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.0460952 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:           0.0460952 ETH
```

Fig. 5. Smart contracts deployment

According to Fig. 6, the implementation of blockchain does not influence the DCS results negatively as there is no difference in the results between the blockchain based DCS and the DCS without blockchain. According to Fig. 7, without the blockchain protection, the frequency of the microgrid breaks down immediately after the FDI attack, meanwhile the frequency remains near its normal value with the protection of the proposed blockchain system. Therefore, based on the aforementioned results, the proposed blockchain system could ensure the control quality and safeguard the control system simultaneously. For the FDI attacks, Fig. 8 illustrates the gas and energy consumption as well as the mining speed of the attackers compared to the data of the original blockchain maintenance.

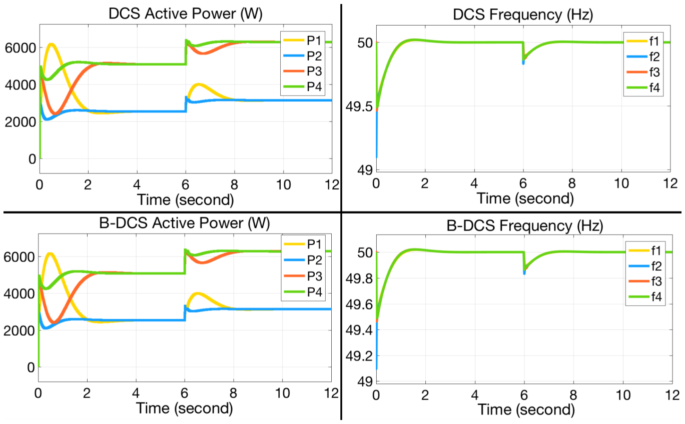


Fig. 6. Comparison of DCS without blockchain (DCS) and with blockchain (B-DCS) in normal condition

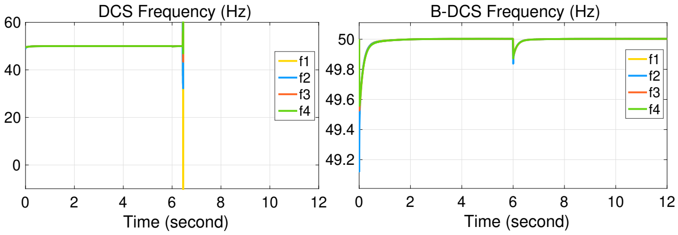


Fig. 7. Comparison of DCS without blockchain (DCS) and with blockchain (B-DCS) under FDI attack

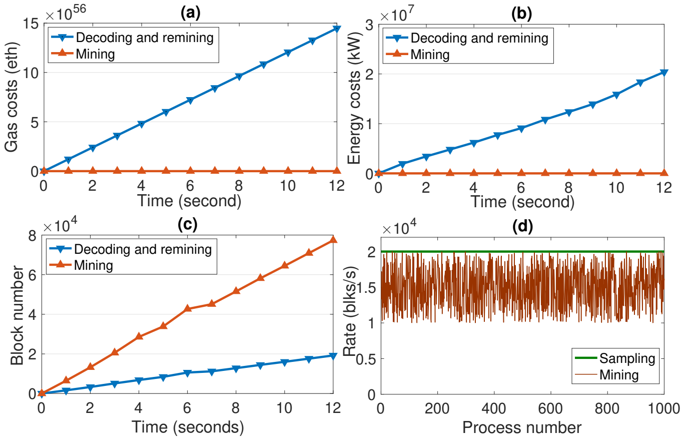


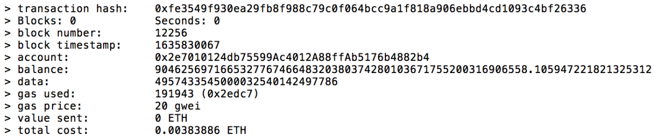
Fig. 8. The comparison of (a) gas costs, (b) energy consumption and (c) mining speed between attackers and authority nodes. (d) The deviation rate between sampling and mining

From the comparison provided in Fig. 8(a), (b) and (c), the gas and energy consumption required for a successful FDI attack is extremely high compared with a normal blockchain maintenance. In addition, the mining speed of the attacker is much slower than that of the authority nodes. Therefore the proposed DCS system is comprehensively protected by the proposed private blockchain system against any possible FDI attack. Although the deviation rate between the DCS sampling and the mining shown in Fig. 8(d) could potentially interfere with the DCS results, this interference could be prevented as long as it is restrained in a controllable scale. The reason for

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2022.3153693, IEEE Transactions on Smart Grid

the cause of the deviation is because the functionality of the Raspberry Pi is not stable, leading to the asynchronisation between the mining rate and sampling rate. But it is convenient to restrain the deviation because of the low mining difficulty offered by private blockchains. In the proposed work, the deviation is restrained in a controllable scale as shown in Fig. 8(d) and the results are shown in Fig. 6.

The specific content of a block is shown in Fig. 9, including the transaction hash, block number and the DCS data. The DCS data is presented as an integer number 49574335450000325540142497786 as smart contracts can only execute integer calculations. The practical meaning of this integer refers to $< 49.5743Hz, 3545w, 325.4014V, 249.7786Val >$ which are the measurement delivered to the DCS.

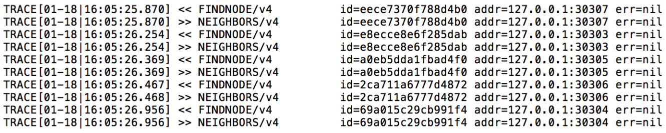


```
> transaction hash:    0xfe3549f930ea29fb8f988c79c0f064bcc9a1f818a906ebbd4cd1093c4bf26336
> Blocks: 0            Seconds: 0
> block number:        12256
> block timestamp:     1635830067
> account:             0x2e7010124db75599Ac4012A88ffAb5176b4882b4
> balance:             904625697166532776746648320380374280103671755200316906558.105947221821325312
> data:                49574335450000325540142497786
> gas used:            191943 (0x2edc7)
> gas price:           20 gwei
> value sent:          0 ETH
> total cost:          0.00383886 ETH
```

Fig. 9. Block information for DCS

B. Second Level Blockchain Implementation

For the second blockchain layer, *Puppeth* is installed for the PoA protocol implementation and the *Bootnode* service is applied for the communication network shown in Fig. 10. 30303 to 30308 are the connection ports for the six prosumers respectively.



```
TRACE[01-18|16:05:25.870] << FINDNODE/v4          id=eece7370f788d4b0 addr=127.0.0.1:30307 err=nil
TRACE[01-18|16:05:25.870] >> NEIGHBORS/v4         id=eece7370f788d4b0 addr=127.0.0.1:30307 err=nil
TRACE[01-18|16:05:26.254] << FINDNODE/v4          id=e8ecce8e6f285dab addr=127.0.0.1:30303 err=nil
TRACE[01-18|16:05:26.254] >> NEIGHBORS/v4         id=e8ecce8e6f285dab addr=127.0.0.1:30303 err=nil
TRACE[01-18|16:05:26.369] << FINDNODE/v4          id=a0eb5dda1fbad4f0 addr=127.0.0.1:30305 err=nil
TRACE[01-18|16:05:26.369] >> NEIGHBORS/v4         id=a0eb5dda1fbad4f0 addr=127.0.0.1:30305 err=nil
TRACE[01-18|16:05:26.467] << FINDNODE/v4          id=2ca711a6777d4872 addr=127.0.0.1:30306 err=nil
TRACE[01-18|16:05:26.468] >> NEIGHBORS/v4         id=2ca711a6777d4872 addr=127.0.0.1:30306 err=nil
TRACE[01-18|16:05:26.956] << FINDNODE/v4          id=69a015c29cb991f4 addr=127.0.0.1:30304 err=nil
TRACE[01-18|16:05:26.956] >> NEIGHBORS/v4         id=69a015c29cb991f4 addr=127.0.0.1:30304 err=nil
```

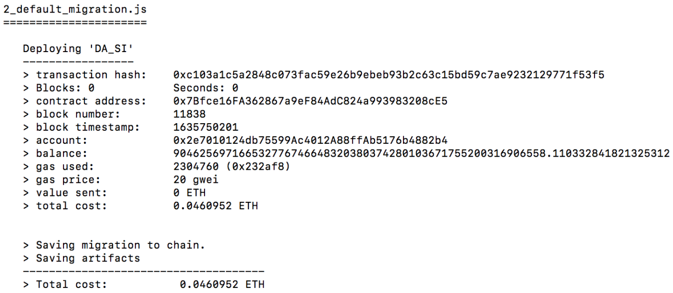
Fig. 10. Bootnode communication services

The RT-lab with MATLAB software is used to simulate the energy trading within the microgrid with consideration of Lithium-ion batteries as the BESS of prosumers. The charging/discharging efficiency is 90% and the annual maintenance cost is 16,000 Singapore cents. The prices offered by the utility grid and FIT are 22.93 cents/kWh and 9.3 cents/kWh respectively. The parameter w_i of the utility function is set as 0.25 and the value of r_i^t is calculated by (23). The other parameters of the producers are listed in Table III.

TABLE III
PARAMETERS OF GENERATORS AND POWER LOSS

Producers	$\alpha(cents/kW^2h)$	$\beta(cents/kWh)$	$\sigma(cents/h)$
1	0.01	4.47	18
2	0.01	3.84	21
3	0.01	4.18	12
4	0.01	2.39	14

The DA-SI pricing scheme is written in smart contracts and deployed to the PoA blockchain which is shown in Fig. 11.



```
2_default_migration.js
======================

   Deploying 'DA_SI'
   -----------------
   > transaction hash:    0xc103a1c5a2848c073fac59e26b9ebeb93b2c63c15bd59c7ae9232129771f53f5
   > Blocks: 0            Seconds: 0
   > contract address:    0x7Bfce16FA362867a9eF84AdC824a993983208cE5
   > block number:        11838
   > block timestamp:     1635750201
   > account:             0x2e7010124db75599Ac4012A88ffAb5176b4882b4
   > balance:             904625697166532776746648320380374280103671755200316906558.110332841821325312
   > gas used:            2304760 (0x232af8)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.0460952 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:           0.0460952 ETH
```

Fig. 11. Smart contracts based DA-SI deployment

To present the advantage of DA-SI, its clearing price and welfare are compared with those of the traditional trading of the prosumer with utility grid (PWG) as well as another widely used double auction scheme which calculates the middle rate of the $[a_j, b_i]$ (DA-MR) [44]. The energy trading information for these three methods is compared in Fig. 12.

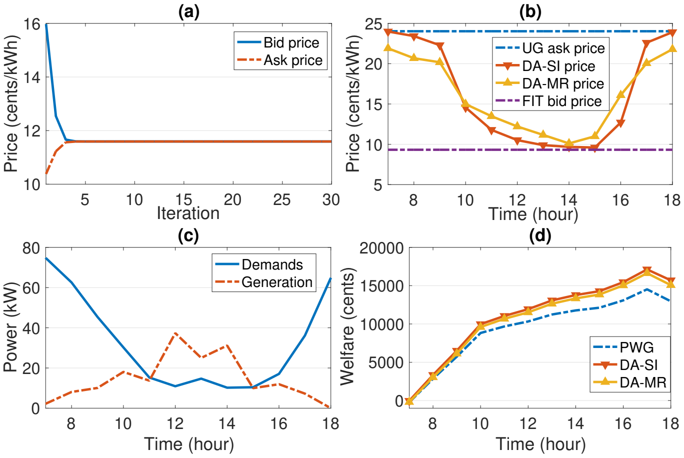


Fig. 12. (a) The iteration calculation process in a time slot of DA-SI. (b) The clearing prices generated by three methods. (c) The total power demands ang generation of the microgrid. (d) the welfare comparison of the three pricing schemes.

The iteration number of DA-SI calculation illustrated in Fig. 12(a) is affordable for smart contracts. After calculating the social welfare for the microgrid with consideration of power demands, generation and the clearing prices, the welfare is improved most by the proposed DA-SI pricing scheme as shown in Fig. 12(d).

The respective welfare generated by different pricing schemes for producers and consumers are presented in Fig. 13, from which the welfare of both producers and consumers is improve most by using the proposed DA-SI pricing scheme, which produces a strong incentive for them to participate in the P2P energy trading market and bid/ask their prices. Overall, the proposed hierarchical blockchain system with DA-SI is able to safeguard the DCS and energy trading while ensuring the quality of the control results and improving the social welfare of the microgrid.

VI. PERFORMANCE AND SECURITY ANALYSIS

In this paper, the proposed hierarchical blockchain system is designed for the microgrid, including the first private

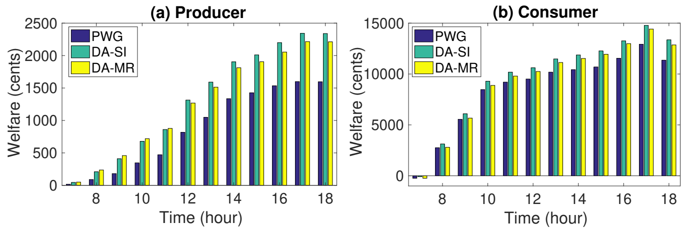


Fig. 13. The respective welfare of (a) producers and (b) consumers provided by different schemes

blockchain level for control system and the second PoA blockchain level for P2P energy trading.

A. Control System Layer

In the first level, the DCS is protected by the private blockchain system against the FDI attack. After the implementation of the blockchain, attackers are required to take tremendous computation burden and energy expense to conduct a successful attack, which is theoretically impossible to achieve. The static nodes service supports the communication network for the four DG controller nodes. By assigning them as the miners, all of the nodes are incentivized to behave legally to avoid the punishment of being eliminated from the static nodes list. In addition, the fast mining rate of the private blockchain enables its execution to match the sampling rate of DCS thereby maintaining a good quality of control results. The performance of the implemented blockchain for the control system is presented in Table IV.

TABLE IV
PERFORMANCE PARAMETERS OF BLOCKCHAIN FOR CONTROL SYSTEM

Time	TPS	Block number	Storage cost (gas)
7	(1-2)$\times 10^4$	0	0
8	(1-2)$\times 10^4$	2.4×10^7	4.6×10^{12}
9	(1-2)$\times 10^4$	6.8×10^7	1.3×10^{13}
10	(1-2)$\times 10^4$	12.2×10^7	2.34×10^{13}
11	(1-2)$\times 10^4$	17.7×10^7	3.39×10^{13}
12	(1-2)$\times 10^4$	23.2×10^7	4.45×10^{13}
13	(1-2)$\times 10^4$	28.7×10^7	5.51×10^{13}
14	(1-2)$\times 10^4$	34.1×10^7	$6.53\ \times 10^{13}$
15	(1-2)$\times 10^4$	38.6×10^7	7.4×10^{13}
16	(1-2)$\times 10^4$	44.1×10^7	8.46×10^{13}
17	(1-2)$\times 10^4$	49.8×10^7	9.56×10^{13}
18	(1-2)$\times 10^4$	55.7×10^7	10.69×10^{13}

According to Table IV, the transaction per second (TPS) of the proposed blockchain is improved to match the sampling rate. The fluctuation of the TPS values is caused by the unstable functionality of the RPI but it is restrained in an acceptable range and would not affect the control results according to Fig. 6. The rapid increasing rate of the block number is extremely difficult for the attacker to surpass, which could effectively solve the external FDI attacks. The detection capability depends on the tracibility and transparency of the blockchain system. The internal FDI attack is addressed by eliminating the address of the malicious node from the static nodes list. In addition, the storage cost is affordable for the controller nodes since each of their gas balance is above 9×10^{56} according to Fig. 11, which proves the feasibility of the proposed method.

B. Energy Trading Layer

In the second level, the energy trading within the microgrid is secured by the PoA consensus protocol based blockchain with the communication service provided by the Bootnode. The trading role of each prosumer is flexible depending on their power generation and demands. With the analysis of the utility function and welfare functions, the proposed DA-SI pricing scheme generates the optimal clearing price for the energy trading and improves the social welfare for the microgrid when it is compared with the DA-MR and PWG methods. The proposed blockchain system is also energy efficient as the mining difficulty is extremely low for private blockchains and thus, the mining consumption could be ignored in the energy trading calculation. The performance of the implemented blockchain for the energy trading is presented in Table V.

TABLE V
PERFORMANCE PARAMETERS OF BLOCKCHAIN FOR ENERGY TRADING

Time	TPS	Block number	Storage cost (gas)
7	0.5-1	0	0
8	0.5-1.0	1.8×10^3	7.2×10^7
9	0.5-1.5	3.6×10^3	3.96×10^8
10	1-2	5.4×10^3	1.2×10^9
11	1.5-2.5	7.2×10^3	3.18×10^9
12	2.5-4.5	9×10^3	6.93×10^9
13	3-4.5	10.8×10^3	11.46×10^9
14	3-4	12.6×10^3	$15.21\ \times 10^9$
15	2.5-4.5	14.4×10^3	17.19×10^9
16	2.5-3.5	16.2×10^3	18×10^9
17	1.5-3	18×10^3	18.33×10^9
18	1-1.5	19.8×10^3	18.4×10^9

Compared to the blockchain performance with that of the control system, the production rate of blocks is more stable and it maintains at two seconds per block as a constant value. This is because the requirement for the mining rate is much slower than that of the control system blockchain and it could be supported adequately by the RPIs. Due to fewer number of mined blocks, the storage cost is also less than that of the control system. The illegal trading behaviours are punished by the PoA consensus protocol by depriving the authority role of the nodes and the opportunity to trade, which ensures the security and data integrity of the prosumers.

At last, the energy consumption caused by the computation and operation of the blockchain for both the control system and energy trading is demonstrated in Fig. 14. The values of the energy consumption of both layers are below $33W$ and thereby being ignored in the welfare calculation. It also proves the energy efficiency of the proposed method as the difficulty of private blockchain is extremely low, leading to less computation cost.

VII. Conclusion

This paper proposes a hierarchical blockchain system for both the control system and energy trading system of a microgrid. Both blockchain levels are set up based on Ethereum

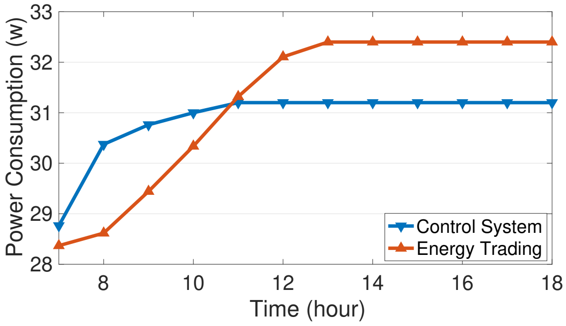


Fig. 14. The total computation and operation consumption of the hierarchical blockchain system

platform and provide a comprehensive protection for the microgrid. The private blockchain with static nodes service is designed to protect the DCS against FDI attacks within and outside the microgrid. It also ensures the control quality without negative impact on the system performance. At this level, the breakthrough of the blockchain application in power systems is achieved by expanding its usage to the control system in addition to secure energy trading. The second level blockchain is set up based on PoA consensus protocol to maintain participants' legal behaviours, and a smart contract based DA-SI pricing scheme is designed to improve the social welfare of the microgrid and maximize the benefit of both producers and consumers. In the case study section, the implementation of the proposed blockchain and the smart contracts deployment are specifically demonstrated. Numerical results verify the effectiveness and feasibility of the proposed method for both distributed control and energy trading system.

The future direction would be scaling up the size of the microgrid and testing the performance of the hierarchical blockchain structure. Since the blockchain system could be damaged if 2/3 of the authority nodes or miners within the microgrid become malicious, a larger microgrid size with more prosumers could provide a more resilient blockchain system against FDI attacks.

VIII. Acknowledgement

This research is supported by the National Research Foudation, Singapore, and EMA-ESG, Singapore under its NRF2019NRF-CG002-002 Award and by the Agency for Science, Technology and Research (A*SATR), Singapore, under its Singapore-Germany Academic-Industry (2+2) International Collaboration under Grant A1990b0060.

References

[1] M. B. Mollah, J. Zhao, D. Niyato, K.-Y. Lam, X. Zhang, A. M. Y. M. Ghias, L. H. Koh, and L. Yang, "Blockchain for future smart grid: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 18–43, 2021.

[2] Q. Shafiee, Stefanović, T. Dragičević, P. Popovski, J. C. Vasquez, and J. M. Guerrero, "Robust networked control scheme for distributed secondary control of islanded microgrids," *IEEE Transactions on Industrial Electronics*, vol. 61, no. 10, pp. 5363–5374, 2014.

[3] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—attacks, impacts, and defense: A survey," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 411–423, 2017.

[4] M. K. AlAshery, Z. Yi, D. Shi, X. Lu, C. Xu, Z. Wang, and W. Qiao, "A blockchain-enabled multi-settlement quasi-ideal peer-to-peer trading framework," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 885–896, 2021.

[5] J. Yang, A. Paudel, H. B. Gooi, and H. D. Nguyen, "A proof-of-stake public blockchain based pricing scheme for peer-to-peer energy trading," *Applied Energy*, vol. 298, p. 117154, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306261921005900

[6] S. Chen, Z. Shen, L. Zhang, Z. Yan, C. Li, N. Zhang, and J. Wu, "A trusted energy trading framework by marrying blockchain and optimization," *Advances in Applied Energy*, vol. 2, p. 100029, 2021.

[7] S. Chen, L. Zhang, Z. Yan, and Z. Shen, "A distributed and robust security-constrained economic dispatch algorithm based on blockchain," *IEEE Transactions on Power Systems*, vol. 37, no. 1, pp. 691–700, 2022.

[8] M. R. Hamouda, M. E. Nassar, and M. M. A. Salama, "A novel energy trading framework using adapted blockchain technology," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 2165–2175, 2021.

[9] S. Chen, C. Xu, Z. Yan, X. Guan, and X. Le, "Accommodating strategic players in distributed algorithms for power dispatch problems," *IEEE Transactions on Cybernetics*, pp. 1–10, 2021.

[10] K. Zhou, J. Chong, X. Lu, Shanlin, and Yang, "Credit-based peer-to-peer electricity trading in energy blockchain environment," *IEEE Transactions on Smart Grid*, pp. 1–1, 2021.

[11] A. Paudel, K. Chaudhari, C. Long, and H. B. Gooi, "Peer-to-peer energy trading in a prosumer-based community microgrid: A game-theoretic model," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 8, pp. 6087–6097, 2019.

[12] M. Pilz and L. Al-Fagih, "Recent advances in local energy trading in the smart grid based on game-theoretic approaches," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 1363–1371, 2019.

[13] K. Anoh, S. Maharjan, A. Ikpehai, Y. Zhang, and B. Adebisi, "Energy peer-to-peer trading in virtual microgrids in smart grids: A game-theoretic approach," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 1264–1275, 2020.

[14] S. Aggarwal and N. Kumar, "A consortium blockchain-based energy trading for demand response management in vehicle-to-grid," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 9480–9494, 2021.

[15] Y. Li, T. Zhao, P. Wang, H. B. Gooi, L. Wu, Y. Liu, and J. Ye, "Optimal operation of multimicrogrids via cooperative energy and reserve scheduling," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3459–3468, 2018.

[16] G. Gao, C. Song, A. Bandara, M. Shen, F. Yang, W. Posdorfer, D. Tao, and Y. Wen, "Fogchain: a blockchain-based peer-to-peer solar power trading system powered by fog ai," *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[17] 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*, vol. 13, no. 6, pp. 3154–3164, 2017.

[18] J. Zhao, G. Zhang, Z. Y. Dong, and K. P. Wong, "Forecasting-aided imperfect false data injection attacks against power system nonlinear state estimation," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 6–8, 2016.

[19] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2017.

[20] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of local false data injection attacks with reduced network information," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1686–1696, 2015.

[21] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2218–2234, 2020.

[22] Z.-H. Pang, G.-P. Liu, D. Zhou, F. Hou, and D. Sun, "Two-channel false data injection attacks against output tracking control of networked systems," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 5, pp. 3242–3251, 2016.

[23] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, 2017.

[24] J. J. Q. Yu, Y. Hou, and V. O. K. Li, "Online false data injection attack detection with wavelet transform and deep neural networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 3271–3280, 2018.

[25] D. Said, "A decentralized electricity trading framework (detf) for connected evs: A blockchain and machine learning for profit margin

optimization," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 10, pp. 6594–6602, 2021.

[26] S. Xia, F. Lin, Z. Chen, C. Tang, Y. Ma, and X. Yu, "A bayesian game based vehicle-to-vehicle electricity trading scheme for blockchain-enabled internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 6856–6868, 2020.

[27] N. Liu, L. Tan, L. Zhou, and Q. Chen, "Multi-party energy management of energy hub: A hybrid approach with stackelberg game and blockchain," *Journal of Modern Power Systems and Clean Energy*, vol. 8, no. 5, pp. 919–928, 2020.

[28] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 612–621, 2014.

[29] C. Liu, H. Liang, and T. Chen, "Network parameter coordinated false data injection attacks against power system ac state estimation," *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1626–1639, 2021.

[30] X. Liu, Y. Song, and Z. Li, "Dummy data attacks in power systems," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 1792–1795, 2020.

[31] S. Lakshminarayana, A. Kammoun, M. Debbah, and H. V. Poor, "Data-driven false data injection attacks against power grids: A random matrix approach," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 635–646, 2021.

[32] M. Ahmed and A.-S. K. Pathan, "False data injection attack (fdia): an overview and new metrics for fair evaluation of its countermeasure," *Complex Adaptive Systems Modeling*, vol. 8, no. 1, pp. 1–14, 2020.

[33] S. Aoufi, A. Derhab, and M. Guerroumi, "Survey of false data injection in smart power grid: Attacks, countermeasures and challenges," *Journal of Information Security and Applications*, vol. 54, p. 102518, 2020.

[34] S. Zhai, Y. Yang, J. Li, C. Qiu, and J. Zhao, "Research on the application of cryptography on the blockchain," in *Journal of Physics: Conference Series*, vol. 1168, no. 3. IOP Publishing, 2019, p. 032077.

[35] C. Gorenflo, S. Lee, L. Golab, and S. Keshav, "Fastfabric: Scaling hyperledger fabric to 20 000 transactions per second," *International Journal of Network Management*, vol. 30, no. 5, p. e2099, 2020.

[36] V. Buterin *et al.*, "Ethereum white paper," *GitHub repository*, vol. 1, pp. 22–23, 2013.

[37] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the thirteenth EuroSys conference*, 2018, pp. 1–15.

[38] M. Valenta and P. Sandner, "Comparison of ethereum, hyperledger fabric and corda," *ebook] Frankfurt School, Blockchain Center*, 2017.

[39] N. Prusty, *Blockchain for Enterprise: Build scalable blockchain applications with privacy, interoperability, and permissioned features*. Packt Publishing Ltd, 2018.

[40] M. J. Miranda and P. L. Fackler, *Applied computational economics and finance*. MIT press, 2004.

[41] N. Liu, X. Yu, C. Wang, C. Li, L. Ma, and J. Lei, "Energy-sharing model with price-based demand response for microgrids of peer-to-peer prosumers," *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 3569–3583, 2017.

[42] X.-F. Wang, Y. Song, and M. Irving, *Modern power systems analysis*. Springer Science & Business Media, 2010.

[43] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Başar, "Demand response management in the smart grid in a large population regime," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 189–199, 2016.

[44] C. Plott, N. Roy, and B. Tong, "Marshall and walras, disequilibrium trades and the dynamics of equilibration in the continuous double auction market," *Journal of Economic Behavior & Organization*, vol. 94, pp. 190–205, 2013.

Jiawei Yang (Member, IEEE) received the B.E. degree in electrical engineering and automation from Wuhan University, China in 2018 and the M.E. degree in electrical and electronic engineering from Nanyang Technological University, Singapore in 2020. He is currently working as a Ph.D. candidate in electrical engineering at Nanyang Technological University, Singapore. His current research interest includes peer-to-peer energy trading and blockchain application in power system control.

Jiahong Dai (Student Member, IEEE) received his B.Eng. degree in Smart Grid Information Engineering from Hefei University of Technology, China, in 2017. He is currently working toward the Ph.D. degree with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. His research interest is cyber-resilience in smart grids, including the application of software-defined network, blockchain technology, and quantum learning in microgrids and versatile validation testbeds for cyber-physical systems and the cybersecurity research.

Hoay Beng Gooi (Life Senior Member, IEEE) received the B.S. degree from National Taiwan University in 1978; the M.S. degree from University of New Brunswick in 1980; and the Ph.D. degree from Ohio State University in 1983, all in electrical engineering. He is an associate professor at School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. His current research interests include microgrid energy management systems dealing with storage, electricity market, and spinning reserve.

Hung Dinh Nguyen (Member, IEEE) received the Ph.D. degree in electric power engineering from the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, in 2017. He is a 2017 Siebel Scholar in energy science. Currently, he is an Assistant Professor in Electrical and Electronic Engineering at Nanyang Technological University, Singapore. His research interests include power system operation and control with machine learning, the nonlinearity, dynamics and stability of large scale power systems; dynamic security assessment (DSA)/energy management system (EMS) and smart grids.

Ping Wang (Fellow, IEEE) received her Bachelor and Master degrees from Huazhong University of Science and Technology, in 1994 and 1997, respectively, and her PhD degree from the University of Waterloo, Canada, in 2008, all in electrical and computer engineering. Currently, she is an Associate Professor at the Department of Electrical Engineering and Computer Science, York University. Prior to that, she worked with Nanyang Technological University, Singapore, from 2008 to 2018. Her research interests are mainly in wireless communication networks, cloud computing and the Internet of Things. Her scholarly works have been widely disseminated through top-ranked IEEE journals/conferences and received the Best Paper Awards from IEEE Wireless Communications and Networking Conference (WCNC) in 2020 and 2012, from IEEE Communication Society: Green Communications Computing Technical Committee in 2018, and from IEEE International Conference on Communications (ICC) in 2007. She is an IEEE Fellow and a Distinguished Lecturer of the IEEE Vehicular Technology Society.