nature portfolio

Peer Review File

A Blockchain Consensus Mechanism for Real-Time Regulation of Renewable Energy Power Systems

Corresponding Author: Professor Guo-Ping Liu

This file contains all reviewer reports in order by version, followed by all author rebuttals in order by version.

Version 0:

Reviewer comments:

Reviewer #1

(Remarks to the Author)
1. I appreciate the logical structure of the paper, and the experimental validation of Proof of Task (PoT). If data security or cyber-resiliency is the main problem that needs to be addressed in real-time regulation schemes, a solution can be using traditional control in combination with a blockchain network as a secure data transfer mechanism for measurement and control data. A fast and secure consensus algorithm such as Proof of Authority (PoA) can be used. From the perspective of optimizing resources (used for blockchain), how is real-time-control using blockchain a computationally effective solution for secure data transfer?
2. The PoT presented here solves the problem closely related to the control performance of the system. In practical systems, the controller design is an offline problem and control actions are based on the updated active and reactive power setpoints from the offline controller. What are the challenges for the application of PoT in large energy networks or microgrids with numerous distributed energy resources (DERs) to solve the online control problem at lower timescales (milliseconds) at every iteration? Also, does PoT require participation of every peer in solving the optimization problem?
3. Does the raw interaction data refer to predicted future states of the system? If so, what are these states in physical sense?
4. Game-derived strategy proposed for dynamically authorizing blockchain nodes is effective to improve security and provides an added layer of protection against malicious attacks. While executing this strategy, how much added control delay is expected? What are the stages of control delays and what steps are necessary in the predictive control design to accommodate for the total delay in PoT?
5. What are the power flows and data flows in Fig. 5 (Panoramic view of the PoT-based IEEE 9-bus microgrid platform with five distributed generation units)?
6. It was mentioned that the round-trip time delay measured by the timestamping technique ranges from 12-steps to 13-steps. Is there a constraint on the time step of HIL simulation to ensure stability?

Reviewer #2

(Remarks to the Author)
I have reviewed the manuscript entitled 'A Blockchain Consensus Mechanism for Real-Time Regulation of Renewable Energy Power Systems'. In my opinion:
1- The paper introduced Proof of Task as a consensus mechanism, but the specific tasks involved remain unclear. It is crucial to define the tasks used in PoT and demonstrate how they directly relate to real-time control and stability of REPSs. Are these tasks computationally expensive enough to secure the network?
2- While highlighting limitations of existing blockchain protocols, the paper did not compare properly the PoT's performance with established real-time control solutions in REPSs. A clear comparison would strengthen the argument for PoT's necessity and effectiveness.
3- The manuscript mentioned deploying PoT in three REPSs, but the details of these deployments and the specific functionalities PoT provides in each case are missing. More concrete information is needed to assess the generalizability and effectiveness of PoT across various REPS configurations.
4- Also the paper claimed PoT strengthens security, but the mechanism by which it achieves this needs elaboration. Does PoT introduce new vulnerabilities or security considerations compared to traditional consensus mechanisms?
5- While the authors mentioned results showing PoT improves security and computing capability, the data itself is not presented. Including specific performance metrics and how they compare to existing solutions would strengthen the

conclusions.
6- In addition, the manuscript focused on small-scale deployments, but real-world REPSs can be vast. The authors should discuss how PoT would scale to handle a large number of participants and transactions in a complex REPS environment.

Reviewer #3

(Remarks to the Author)
-In Section 1, the authors firstly explained the works relating to the problems and so on. This section is well written, but it did not address the major issue that is imperative to be solved. As a reviewer’s point of view, the literature survey of this section is very weak, unfocused and insufficient. What is the essential problem of this work? The authors should really explain the drawback of approaches in related works especially instead of simply stating what they have done. The authors should discuss the mentioned references in the introduction part.
-What is the major novel/contribution of this paper? In my view, there are many techniques adopted in the recent past for this problem. So, the authors should improve the section with the references. Please explain the main contribution related to previous approaches, and provide a list of paper’s contributions at the end of the introduction.
-I suggest a comparison with the literature, in order to prove the efficiency of the proposed method? It can be seen from the result section that mostly results are not compared with the latest published papers.

Version 1:

Reviewer comments:

Reviewer #1

(Remarks to the Author)
The paper is acceptable in its current form and all the questions and concerns were addressed.

Reviewer #2

(Remarks to the Author)
Thanks for your response and clarifications.

Reviewer #3

(Remarks to the Author)
thank you for putting efforts to revise the paper.

Response Letter

A Blockchain Consensus Mechanism for Real-Time Regulation of Renewable Energy Power Systems

Manuscript ID: NCOMMS-24-12950

Dear Reviewers,

We are grateful to anonymous reviewers for providing insightful and constructive comments. Following the review comments of the reviewers, this paper has been carefully revised. Main modifications on the paper are detailed in the responses to the review comments later.

The changes in the revised manuscript are highlighted and marked in **red** in the highlighted version. A clean version is also provided. Our point-by-point responses to the reviewers' comments are detailed in the following paragraphs. For convenience, in what follows, the reviewers' original comments are included in ***italics***, while our responses are shown in **blue**. Throughout the response letter, the use of citation and notation needs to be clarified to avoid unnecessary confusion. For example, the reference x and equation (y) used in the manuscript itself are cited by the notation [x] and (y), respectively, while those used in the response letter are quoted by the symbol Ref. [x] and Eq. (y), respectively. In particular, Table 1 summarizes the labels of these references and their meanings.

Sincerely yours,

The authors

Table 1: The format of the references in the different documents (i.e., main text, supplementary file, and response letter) as an example of Figure 1, Algorithm 1, etc.

Meaning	**Label**		
	Main text	**Supplementary file**	**Response letter**
Figure	Fig. 1	Supplementary Fig. 1	Figure 1
Algorithm	Algorithm 1	Supplementary Algorithm 1	\
Table	TABLE I	Supplementary Table 1	Table 1
Equation	\	(1)	(Eq. 1)
Citation	[1]	[1]	Ref. [1]

\ means 'Not applicable'.

Contents

Reviewers' Comments and Our Point-by-Point Responses

Response to Reviewer 1

C1.1: *I appreciate the logical structure of the paper, and the experimental validation of Proof of Task (PoT).*

If data security or cyber-resiliency is the main problem that needs to be addressed in real-time regulation schemes, a solution can be using traditional control in combination with a blockchain network as a secure data transfer mechanism for measurement and control data. A fast and secure consensus algorithm such as Proof of Authority (PoA) can be used. From the perspective of optimizing resources (used for blockchain), how is real-time-control using blockchain a computationally effective solution for secure data transfer?

Response:

Thanks so much for your time and efforts in reviewing the manuscript. In addition, many thanks for your acknowledgement of the logical structure of the manuscript and the experimental validation of the proposed Proof of Task consensus mechanism. With regard to the two concerns you raised, we respond to each of them below.

1) Indeed, as you commented, combining a traditional control method with a blockchain network is an effective way to ensure secure data transfer during real-time regulation. For example, the blockchain-based security control proposed in work Refs. [1, 2] makes good use of this idea. In addition, the point you make about PoA being a fast and secure consensus protocol is highly accurate. A large portion of the currently reported work on blockchain-based security control relies on on the PoA-like consensus mechanism. The PoA consensus mechanism can empower security control, but PoA alone does not take advantage of resources other than the multi-party verification of the blockchain. Meanwhile, simply combining PoA and traditional control strategies, without designing blockchain consensus protocols tailored to the dynamical system based on its characteristics, makes the blockchain not well involved in the control process. Therefore, under these approaches, the use of the blockchain and the design of the controller are relatively independent, which may lead to incompatibilities between the blockchain and the system. The differences and relationships between PoT-based control methods and those based on PoA alone are mainly reflected in the following aspects:

1. The problem solved by each peer node in PoT is an online optimization problem for the control system.
2. The verification conditions for each node in PoT to assess the validity of candidate solutions include the stability requirements of the control system.
3. The PoA-like consensus mechanism can be obtained after removing the solving of the optimization problem and the verification of the candidate solutions in PoT.

It can be seen that PoT not only taps into the characteristics of multi-party verification of blockchain, but also the characteristics of multi-party computing, which can better serve the control system. It is worth noting that the additional aspects of PoT compared with PoA do not introduce some drawbacks. In most cases, it is not the use of computational resources that causes a large time delay in a blockchain. This time delay is something that any blockchain goes through, whether it is used for transmission or for control. For tasks that consume computational resources, such as optimization of control performance, optimization in economic dispatch, etc., computing time is required even if external computational resources are used, which is the same as the waiting time required for computation with the blockchain. For very simple control tasks that do not require optimization, the external controller can be executed quickly, and the blockchain can be completed quickly at the same time, at which point the delay is mainly due to communication. Therefore, rather than setting up an additional external computational entity, it is more efficient to utilize the existing multi-node network that is already available in the blockchain, as done in PoT, to solve computational problems. Under PoT, not only is the expected solving time for optimal control not increased, but multiple candidate solutions are also generated within this time frame. This can provide the system with better control commands. In this way, PoT improves the network security of the system while also fully utilizing the computational resources of the blockchain network.

2) From the perspective of optimizing resources, blockchain has the following three main features that can make blockchain-based real-time control a computationally effective solution for secure data transmission and secure control:

- Delegates (authorized peers) on the blockchain network each solve a published meaningful mathematical problem.
- Multiple peer nodes in a blockchain network validate candidate solutions.
- The network decides which candidate solution wins according to the majority rule principle for the validation results.

Firstly, released mathematical problems can facilitate real-time control. In traditional PoW, the problem to be solved in a blockchain network is the hash puzzle. The complexity of the hash puzzle ensures the difficulty of the data to be tampered with. However, solving the problem consumes a lot of computational resources and takes a long time. For some application scenarios, such as the real-time control tasks considered in this manuscript, minute-level wait times are undesirable. Therefore, mathematical problems like the hash puzzle need to be discarded if the blockchain is to be deeply involved in the computational tasks of the controller for REPSs. In PoT, we replace the meaningless hash puzzle with a meaningful optimization problem for the control task. In this way, problem solving in the blockchain no longer needs to take an excessively long time, and does not require that the blockchain nodes must have particularly strong computational power.

Secondly, the feature of multi-node verification can enhance system security. This feature can well enhance the security of data transfer in REPSs. Less computational resources are required for the verification process because it is relatively easy to verify the validity of a solution compared to solving an optimization problem. In particular, resource consumption here is difficult to avoid. This is because it is the core mechanism for securing the blockchain. What distinguishes PoT in this manuscript from existing methods is the proposed new verification mechanism, which doubly verifies the fulfilment of the system stability requirements as well as the relative optimality of the candidate solutions. Under this verification mechanism, we consider the security and stability of the system in a unified manner. This makes the proposed PoT more suitable for control systems. Furthermore, under this relatively optimal verification mechanism, each loyal node with a certain level of computational capability has the opportunity to contribute to the control of REPSs. This could help make the blockchain a computationally effective solution for security control.

Thirdly, the majority rule principle guarantees the security of both measurement data and control commands. As you mentioned, PoA alone can be effective in increasing the security of data transmission, which is essentially due to the use of the majority rule principle. In the proposed PoT, we perform the majority rule principle for both the measurement data and the candidate solutions after local validation. Thus, compared to PoA used in dynamical systems for secure data transmission, PoT adds some less time-consuming operations, i.e., the majority rule principle on the candidate control commands. The reason for performing the majority rule principle on the two types of data, y and u, is that in PoT, the computations of the controller are put into the blockchain network. In this case, the PoT provides protection for the full lifecycle of the control process of REPSs.

To sum up, meaningful mathematical problems as well as exclusive verification mechanisms make real-time control using blockchain a computationally effective solution for secure data transfer. At the same time, the design of these two is also a key step in enabling the blockchain consensus mechanism to facilitate other applications.

Based on the reviewer's comments, the authors have made the following modifications to the content of the manuscript:

> [Section II.B, page 5, highlighted in red]
> " ... The meaningful mathematical problem as well as the exclusive verification mechanism make real-time control using blockchain a computationally effective solution for secure data transfer. ... "
>
> " ... At this stage, the MRP is executed, protecting the source data (measurements) like a practical Byzantine fault tolerance protocol. ... "
>
> [Section II.B, page 6, highlighted in red]
> " ... Furthermore, in step 7, the MRP is performed to protect the target data (control commands) from potential attacks or disloyalty, thereby obtaining a trusted control input. ... "
>
> " ... Finally, in step 9, a smart contract is developed to count the credit score of each delegate participating in the consensus and give corresponding feedback. Recall that in step 3, the system strategically elects delegates that are favorable for output regulation. This strategy relies on the static probability given by the prior knowledge of the vulnerability of different nodes to cyber-attacks. In addition, the smart contract further evaluates these delegate nodes and decides whether to remove a node from the delegation. The election mechanism and the smart contract both complement each other to form a security countermeasure that utilizes both the prior and the posterior knowledge. A priori election strategy resists malicious attacks from the outside, while a posteriori smart contract defends against dishonest behavior occurring inside the blockchain network. "

C1.2: *The PoT presented here solves the problem closely related to the control performance of the system. In practical systems, the controller design is an offline problem and control actions are based on the updated active and reactive power setpoints from the offline controller. What are the challenges for the application of PoT in large energy networks or microgrids with numerous distributed energy resources (DERs) to solve the online control problem at lower timescales (milliseconds) at every iteration? Also, does PoT require participation of every peer in solving the optimization problem?*

Response:

Thank you sincerely for your insightful and helpful comments. For the three points you are concerned, we will respond to each of them below.

1) As you commented, there are many controllers whose design is an offline problem, such as the PI controllers, state feedback controllers, linear–quadratic regulators (LQRs), etc. With these types of controllers, the structure and parameters of the controller are determined in the offline process. Apart from this, there are other controllers whose design is an online problem. They can be broadly classified into two categories: controllers in which the control inputs are obtained directly through solving an optimization problem, such as model predictive control (MPC) and adaptive dynamic programming (ADP) control, and controllers in which the control parameters need to be updated online, such as adaptive control. Therefore, online and offline control problems can be distinguished by whether the process of obtaining control commands involves solving an online mathematical problem (e.g., optimization problem). If it does, then it is an online control problem such as MPC, and if it does not, it is an offline control problem such as PI control. It is worth mentioning that, whether the controller is designed online or offline, it all needs to execute calculation online to obtain the control commands, although the computation is relatively simple and there is no need to solve a mathematical problem sometimes.

In practice, there are two types of configuration of REPSs, each with different characteristics and regulation requirements. One is the REPSs operating in grid-connected mode, and the other is the REPSs operating in islanded mode (i.e., the system is made up of grid-forming converters). For the former, REPSs generally only need to accomplish power regulation, and tasks such as voltage support are performed by the main grid. Therefore, offline control problems are common in the grid-connected operation of REPSs. For the latter, besides the above mentioned power regulation, it also has its own regulation objectives, such as voltage regulation and current sharing. At this point, these tasks can often correspond to an online optimization problem, as considered in this paper. It can be seen that the regulation problem for REPSs considered in this manuscript is also similar to the optimization problem in MPC. Thus, it is an online control problem.

In summary, online computation is unavoidable in real-time control, only the computational effort is not all the same in various applications. Our choice of the online optimization problem resulted from a combined consideration of real-time performance and system security.

2) The challenges of applying PoT in large energy networks or microgrids are mainly communication and time scale issues, one of which you also mentioned in the comments. A specific discussion is given below.

- Challenges in communications. As the scale of energy networks or microgrids increases, the network size of the information layer will also become larger. In a special case where the communication topology is a ring and maintains this configuration during the scale increases, the amount of network neighbors of each generation unit will not increase and the security guarantees provided by the PoT will not be affected, with only the stabilization of the REPSs may become slower. In this context, the scale and complexity of the optimization problem solved by PoT will remain unchanged. Instead, increasing the number of neighbors communicating at the information layer, the regulation will be faster, but more communication brings more potential network risks and more complex optimization problems to be solved, which will increase the pressure on the PoT. It is important to note that the optimization problem to be solved should not be designed in such a way that the generation of control commands is excessively time-consuming. Thus, the choice of communicating neighbors brings about a trade-off between the system security, the regulation speed, and the complexity of the optimization/control problem.

- Challenges in timescales. The timescale selection problem can be attributed to a trade-off between optimality, security and stability. To accommodate the security of the blockchain as well as the optimality of the regulation task, a large time step is required, which can lead to control failures and system destabilization. To accommodate the stability of REPSs, the blockchain would have to perform operations such as problem solving and validation in a short time step, which would undermine some of the benefits of the blockchain and even compromise its security. In the proposed PoT, we have tried to reduce the time consumption of the blockchain while retaining more blockchain features that are meaningful and attractive to the control system. For example, we replace commonly used hash puzzles with optimization problems with constraints, greatly reducing the time consumed by the blockchain in problem solving. The reason for not completely removing the problem solving from the blockchain is that even if it were removed here, the REPSs system would still need other controllers to compute the same problem. However, in order to ensure the security of REPSs, the time consumption induced by the authentication mechanism, for example, is still several times greater than the time step of the system control.

Specifically, control commands for REPSs are often updated and executed on a millisecond time scale. However, when the scale of the energy networks or microgrids is large, the time consumption for solving optimization problems and data communication in PoT is likely to be not on the order of milliseconds but on the order of hundreds of milliseconds. In this way, minimizing the time delays introduced by PoT and trying to compensate for these unavoidable time delays is the key to the successful application of PoT. In PoT, we also propose a distributed networked prediction scheme to compensate for these time delays. Due to information coupling, distributed prediction cannot accurately obtain future system trajectories, and therefore does not fully compensate for the effect of time delay. Excessive delay will still affect the stability of the REPSs.

It should be noted that a waiting time can be fixed after releasing the optimization problem. Then, for a given blockchain network size, increasing the waiting time can increase the likelihood of obtaining the optimum, but the large time delay brought about would affect the stability of the REPSs. For a given waiting time, increasing the size of the blockchain network improves the security of control, but comes with increased costs. Thus, we can find a balance between optimality, security, and stability by adjusting the waiting time. Alternatively, a variant, UPoT, as proposed in the manuscript, can further improve the security of the control by adding additional authentication on the actuator side, but this requires additional time consumption and hardware resources. Thus, PoT provides a security control framework that allows for flexible configuration. The setup of PoT can be accomplished according to the practical application scenarios, in which the factors that need to be considered comprehensively are security, real-time performance, stability, optimality and cost.

3) PoT does not require all peers to participate in solving the optimization problem. As shown in Step 3 in Fig. 1, we have selected a number of peers in the P2P network to participate in the solution of the optimization problem. The reason for selecting a portion of nodes in the P2P network to participate in solving the optimization problem is given as follows.

- Randomly selecting delegations at a time increases the uncertainty of the system and makes it more defensible in scenarios of intelligent attacks;
- Problem solving is the most time-consuming and computationally intensive step in the whole consensus mechanism, so the probability that nodes with poorer computational performance or security are selected as delegations can be reduced first by a priori knowledge in order to reduce the number of candidate solutions in the local validation process and improve the efficiency of PoT;
- Therefore, we designed a random strategy and smart contracts to elect representative nodes with superior computational capabilities and relatively high trustworthiness to participate in problem-solving, local verification, and the distribution of u.

Here, the choice from a P2P network to a delegation network can effectively improve security against malicious attacks on the one hand, and save communication and consensus time on the other. Thus, this step improves the security and real-time performance of the PoT.

Some more detailed explanations of the selection of representative nodes are given below along with Fig. 1. The first validation is for the raw data y and takes place in Step 2, shown in Fig. 1, when each peer participates. It should be noted that the steps indicated by the yellow background in Fig. 1 involve all peers. The steps indicated by the light blue background in Fig. 1 involve only some of the representatives in the peers. It can be seen that solving the optimization problem is Step 4 shown in Fig. 1, which is on a light blue background. At this point only some of the selected peers are involved, i.e. the delegate labeled in the figure.

Based on the reviewer's comments, the authors have made the following modifications to the content of the manuscript:

[Section I, page 2, highlighted in red]
" However, the control of REPSs has its unique characteristics compared with aforementioned energy dispatch and trading, such as many state constraints, complex multi-objective problems, and high real-time requirements with a small time scale [44]. ... "

[Section II.B, page 5, highlighted in red]
" ... It should be mentioned that only peers authorized as delegates are responsible for solving the optimization problem. ... "

[Section IV, page 8, highlighted in red]
" ... The suggested PoT scheme, which allows interconnected distributed generation units to implement online optimal control algorithms and guarantee regulation security, has the potential to address the above challenges. ... "

[Section VIII, page 15, highlighted in red]

“ ... In this case, achieving the same level of security as in small-scale systems requires a larger-scale blockchain, which may lead to a decrease in the real-time performance of PoT. Therefore, a fully distributed communication style would be preferable when deploying PoT in large-scale REPSs, as it facilitates the scalability of PoT. ... ”

“ ... Second, the trade-off between the optimality, security and the real-time nature of blockchain-enabled control needs further consideration. ... ”

“ ... Finally, given the short time cycles required by real-time control systems, a significant challenge in applying PoT to energy networks is the inability to complete the computation of the optimization problem within one or more control cycles. The resulting delay must be carefully managed. Although there is an active compensation mechanism for PoT-induced delays, a more optimal solution may exist. ”

C1.3: *Does the raw interaction data refer to predicted future states of the system? If so, what are these states in physical sense?*

Response:

Thank you sincerely for your insightful and helpful comments. As you commented, “raw interaction data” includes predicted future state values sent by neighboring generation subsystems from the communication network, but also includes other data. In the original manuscript, we mentioned “After the local and neighbors’ raw interaction data y_l, y_j are delivered to all nodes in the local P2P network of the lth subsystem in step 1, ... ”. Specifically, the “local raw interaction data” refers to the data of the subsystem l itself. The “neighbors’ raw interaction data” refers to the predicted future state values sent by the neighbouring generation subsystem over the communication network. Its actual physical meaning is the local measurements and states used for control, such as voltage and current, etc. of the neighbouring generation units in the dc microgrid, and frequency, voltage, active power, reactive power, etc. of the neighbouring generation units in the AC microgrid, and ACE_i, etc. of the LFC in Application 2.

The reason for distinguishing between local and neighboring raw interaction data is that for the controller of the generation subsystem l, the predicted state of the subsystem l is available within its controller, whereas the future states of the neighboring subsystems can not be predicted at the subsystem l, but only at the neighbors themselves.

We refer to the data in Step 1 as raw interaction data because there are two types of data in PoT as follows:

- The predicted value of the measurement data sent by the neighbour’s controller and the local measurement data, denoted as y_j and y_l, respectively;
- The control command derived from complex calculations based on raw interaction data, denoted as u_l.

For PoT, the original data input is the data sent by the neighbors. Nevertheless, a complex computational process such as solution search, feasibility verification, etc. is required from the received raw data to the control commands used by the final actuator. To distinguish between these two data, we refer to the data initially received over the communication network as raw interaction data.

To address your concerns, we have provided a more detailed explanation of raw interaction data in the revised version.

Based on the reviewer's comments, the authors have made the following modifications to the content of the manuscript:

> [Section II.B, page 5, highlighted in red]
> " After the local and neighbors' raw interaction data y_l, y_j are delivered to all nodes in the local P2P network of lth generation subsystem in step 1, the consensus on each $y_j^{[p,i]}$ in step 2 also involves all nodes as it is a very simple operation. It should be noted that the local raw interaction data y_l refers to the measurements of the subsystem l. Meanwhile, neighbors' raw interaction data refers to the predicted future states sent by the neighboring generation subsystem over the communication network. These states contain some physical quantities required for regulation, such as output voltages and currents in REPSs. At this stage, the MRP is executed, protecting the source data (measurements) like a practical Byzantine fault tolerance protocol. ... "

C1.4: *Game-derived strategy proposed for dynamically authorizing blockchain nodes is effective to improve security and provides an added layer of protection against malicious attacks. While executing this strategy, how much added control delay is expected? What are the stages of control delays and what steps are necessary in the predictive control design to accommodate for the total delay in PoT?*

Response:

We sincerely thank you for your insightful and helpful comments. For the three questions you have raised, we would like to respond to each of them in the following.

1) How much added control delay is expected?

Thank you for confirming our game-derived authorization strategy. In our setup, authorization actions under the game-derived strategy are instantaneous and do not incur any additional time delay.

In the proposed PoT consensus mechanism, the game-derived strategy is obtained offline. In the experimental part, we obtained the activation strategy by solving the min-max optimization problem via an offline Nash Q-learning algorithm Ref. [3]. Therefore, although obtaining a Nash equilibrium strategy is somewhat time-consuming, this process would not introduce an additional time delay for online control. As for the execution of this strategy, we treat it as instantaneous because there is no complicated computation involved.

2) What are the stages of control delays?

The stages that bring about the control delay are: Step 1, Step 2, Step 4, Step 5 and Step 7 shown in Fig. 1. In fact, the main processes that cause large delays to online control can be divided into two categories, those that come from the imposed algorithm and those that come from the system itself outside the algorithm. First, during the execution of the algorithm, even if the very time-consuming hash problem is replaced, solving the optimization problem related to the control objective still takes some time. As mentioned earlier, this optimization problem might not be solved in one control cycle, which is a common drawback of MPC-type control methods, and therefore control delays are introduced, mainly in Step 4. The more complex the problem, such as a hash puzzle, the more secure the blockchain can be, but it will also take longer to solve. In addition, verifying the validity of the candidate solution in Step 5 and performing the MRP protocol in Step 2 and 7 may also cause certain processing time, but not as significant as that of problem solving. Second, outside of algorithmic execution, the distributed control architecture allows generation sources to be dispersed over a wide geographical area. At this point, their mutual communication may have some time delay. Depending on various settings such as the complexity of the problem, the topology of the information layer of the whole system, the communication of the actual subsystems, etc., these time delays may also have different expected scales. For example, in Application 1, solving the optimization problem takes about 60 ms and communication takes about 40 ms. With a control period of 20 ms, a 5-step time delay needs to be compensated.

3) What steps are necessary in the predictive control design to accommodate for the total delay in PoT?

The necessary steps for the PoT to accommodate for the total delay include: a) modeling the system more accurately, b) proposing good distributed prediction algorithms, and c) designing the appropriate compensation mechanisms. In our applications, we adopt a distributed networked predictive compensation algorithm based on the first-principles model Ref. [4].

Taking Application 1 as an example, we developed a system model for a multi-bus dc microgrid based on Kirchhoff's voltage and current laws. As can be seen from (9) in the Supplementary File, the microgrid system is an interconnected linear system. The use of traditional prediction algorithms causes problems of requiring fully-connected communication, i.e., it affects the distributed implementation and operation of the controllers. To this end, we propose an estimator-based distributed networked predictive algorithm, which can compensate for the delay encountered by PoTs in a distributed fashion. It is worth mentioning that data-driven predictive approaches can also be explored in addition to the first-principles model-based predictive algorithms used in this manuscript. Namely, a data model of the system can be built based on the observed input and output measurements, and then a data-driven distributed prediction compensation strategy can be designed.

Since this manuscript focuses on the design of the entire consensus algorithm process, Fig. 1 does not provide a detailed depiction of the complete processes of modeling, prediction, and compensation. In fact, the expected control commands need to be given in Step 5 of the problem solving. In this way, the u arriving at the actuator is just what the actuator needs at the current moment to accomplish compensation for the time delay.

To address your concerns, we have added explanations to each of these three questions in the revised manuscript.

Based on the reviewer's comments, the authors have made the following modifications to the content of the manuscript:

[Section II.B, page 5, highlighted in red]
" ... The strategy is obtained offline and its execution introduces no additional delay to the control. ... "

" ... Furthermore, for the inevitable time delays caused by the complex calculation and data communication, especially in some application scenarios sensitive to communication constraints, we also design a prediction technique to actively mitigate these negative factors. ... "

" ... For predictive control to accommodate the total delay in PoT, the following steps are necessary: accurate modelling of the system, an effective distributed prediction algorithm, and an appropriate compensation mechanism. "

C1.5: *What are the power flows and data flows in Fig. 5 (Panoramic view of the PoT-based IEEE 9-bus microgrid platform with five distributed generation units)?*

Response:

Thank you sincerely for your insightful and helpful comments. We apologize for not clearly giving the power flow and data flow of the IEEE 9-bus microgrid platform shown in Fig. 5 in the original manuscript.

Firstly, the caption of Fig. 5 needs to be modified. Specifically, Fig. 5 contains two test platforms, one of which is the hardware microgrid platform and the other is the real-time simulation platform based on OPAL-RT. The real-time simulation platform is used to complete the HIL testing of a three-area power system under PoT-based load frequency control (Application 2), where no actual power flow is involved. Therefore, according to your suggestion, we have given the power flow and data flow of the PoT-based microgrid for Application 1 and 3, as well as the data flow of the PoT-based HIL test system for Application 2. Specifically, the data flow and power flow of the PoT-based microgrid shown in Fig. 5 are presented in Figs. 7 and 9, respectively, where the physical equipment in Fig. 7 and the experimental equipment in Fig. 5 can be matched one-to-one. The data flow of the PoT-based HIL test system shown in Fig. 5 is presented in Fig. 15. Moreover, the data flow of the microgrid with DPoT-based secondary control is presented in Fig. 17. It is worth mentioning that given the same hardware parameters, physical topology, and control objectives, Application 1 and Application 3 have the same steady state, i.e., they have the same power flow. Therefore, the power flow of the microgrid with DPoT-based secondary control is also shown as that in Fig. 9.

Based on the reviewer's comments, the authors have made the following modifications to the content of the manuscript:

[Section V, page 9, highlighted in red]
" ... Now, the PoT-based distributed secondary regulation strategy is tested and deployed on the hardware as shown in Fig. 7, which also show the data flow of the dc microgrid with PoT-based control. ... "

" ... Further, the power flow of the dc microgrid corresponding to the steady state of Fig. 8(d) is presented in Fig. 9. "

[Section VI, page 11, highlighted in red]
“ ... The data flow of the PoT-based interconnected power system is shown in Fig. 15, which also indicates the deployment architecture of the system. ... ”

[Section VII, page 13, highlighted in red]
“ ... The logical structure of the Ethereum platform and the microgrid system is given in Fig. 17. ... ”

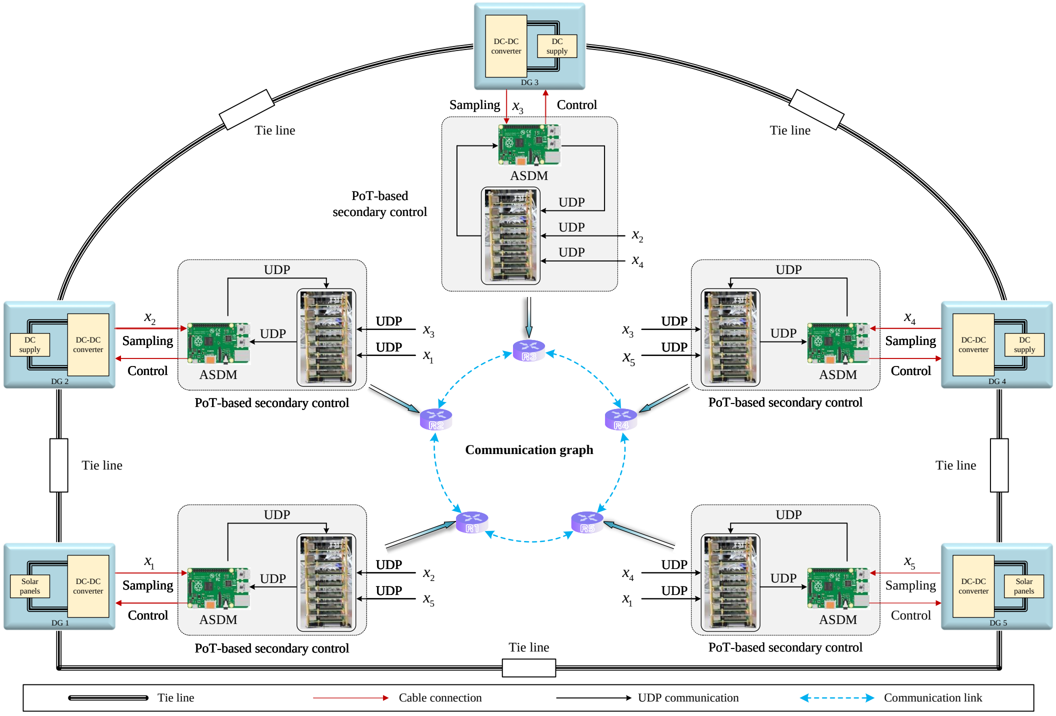


Fig. 7: Data flow of the IEEE 9-bus test bench with PoT-based blockchain, which also presents the deployment architecture of the microgrid under PoT-based secondary control (Application 1). The communication between the generation units at the information layer forms a ring topology. Only part of the tie lines are shown.

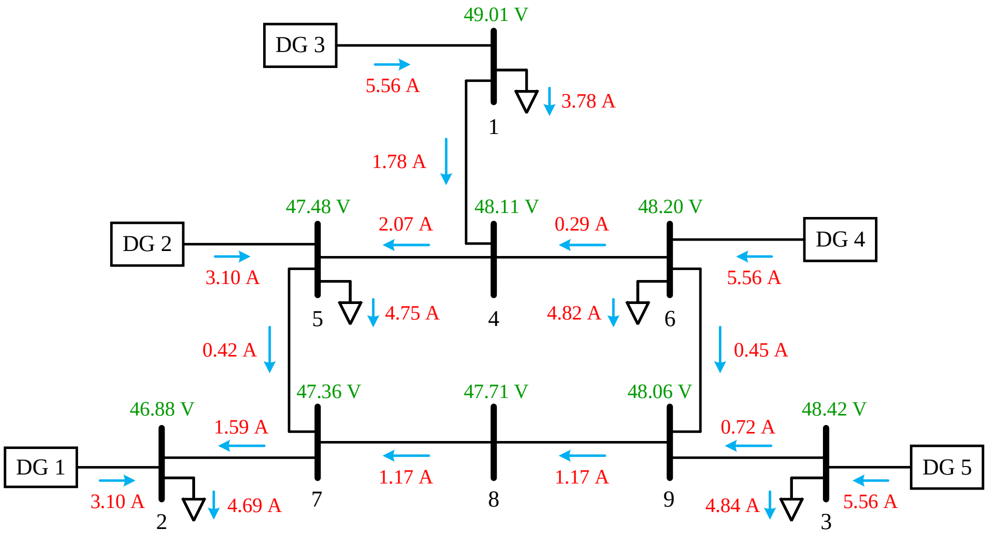


Fig. 9: Power flow of the IEEE 9-bus microgrid system with PoT-based secondary control.

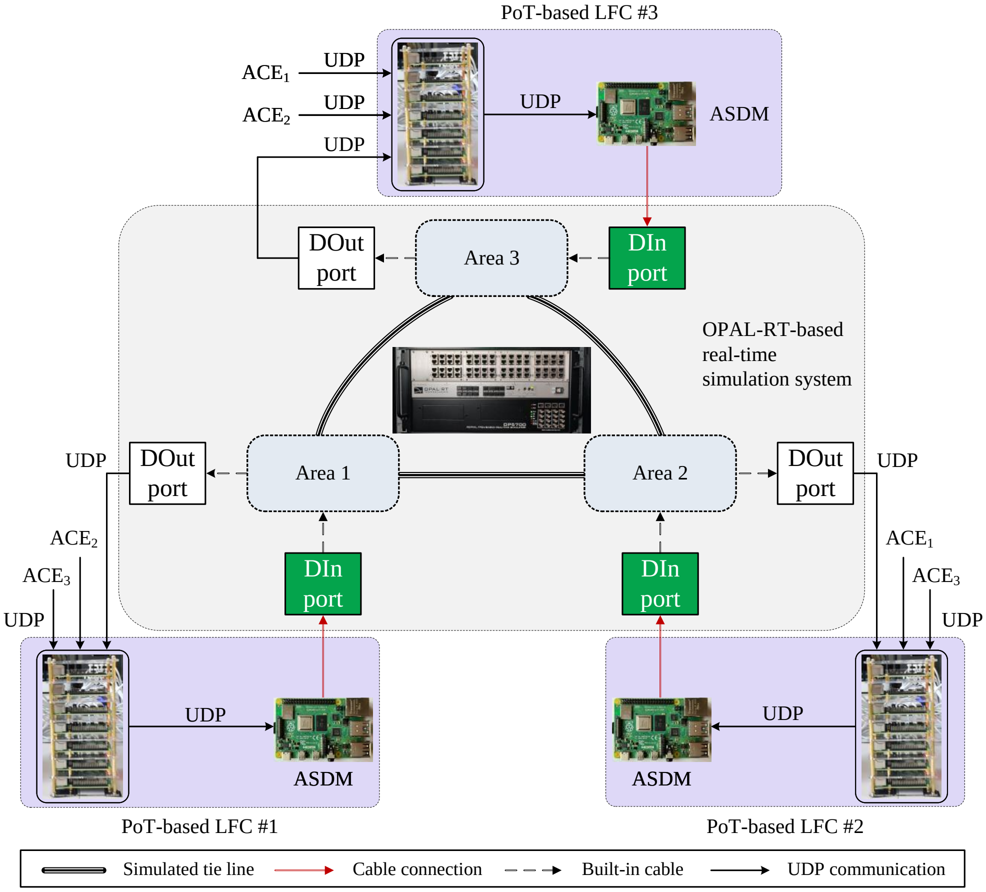


Fig. 15: Data flow of the HIL interconnected power system with the PoT-based LFC scheme (Application 2).

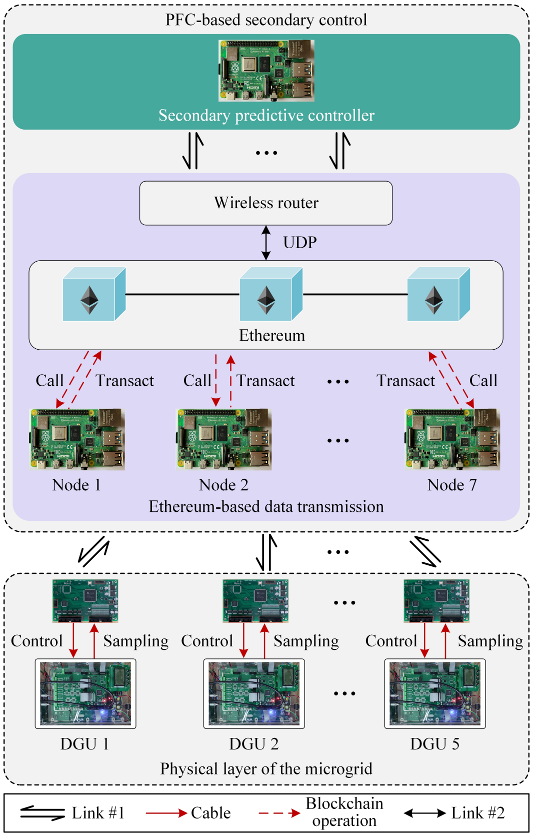


Fig. 17: Data flow of the PFC-assisted microgrid system based on the Ethereum platform (Application 3). Link #1 and Link #2 refer to the communication link between external data and the Ethereum platform, and the communication link between Ethereum nodes, respectively.

C1.6: *It was mentioned that the round-trip time delay measured by the timestamping technique ranges from 12-steps to 13-steps. Is there a constraint on the time step of HIL simulation to ensure stability?*

Response:

Thank you sincerely for your insightful and helpful comments. We apologize for not clearly indicating in the original manuscript the limitations on the time step of the HIL simulation in ensuring stability. Based on your comments, we infer that your concern may be: 1) whether there is a constraint on the number of steps of the time delay in order to ensure the stability of the HIL simulation; or 2) whether there is a constraint on the time step (the time step of solving the model, sampling time step, control time step) of the HIL simulation itself to ensure the stability. We will address each of these two aspects below.

(1) Whether there is a constraint on the number of steps of the time delay in order to ensure the stability of the HIL simulation

For the HIL simulation in Application 2, the number of time delay steps would not affect the stability of the system too much since there is an accurate model of the system and the communication network is fully connected. That is, in HIL simulations, there is no constraint on the number of time delay steps to ensure the stability of a system with a networked prediction algorithm. However, in the case of hardware applications rather than HIL simulations, the number of time delay steps cannot be too large to ensure the stability of real systems with a networked prediction algorithm.

In general, even with networked predictive compensation algorithms, ensuring the stability of the system imposes a constraint on the number of steps of the time delay. Specifically, the limit on the number of steps of the time delay that can be compensated for depends on many factors, such as the accuracy of the system model acquired by the controller, the communication topology, and the prediction algorithm Ref. [4]. The accuracy of the discrete system model greatly affects the effectiveness of the prediction algorithm. The acquisition of discrete models is closely related to the sampling period. For a detailed discussion, please refer to the following point (2). Theoretically, in a centralized control framework or distributed control framework with fully connected communication topology, the networked prediction method can achieve the same control effect at any time delay as that when the system does not encounter a time delay, as long as the system model is sufficiently accurate Ref. [5]. In other words, networked predictive control can compensate for any size of time delay experienced by the system if an accurate system model can be obtained.

For example, in the HIL simulation you mentioned, an ideal system is simulated on an OPAL-RT simulator and the controller can get an accurate system model. At this point, the networked prediction algorithm can compensate for any size of time delay, as memory allows. However, in the case of practical applications rather than real-time simulations, the acquired system models are often not very accurate. For example, models developed from first principles tend to ignore some unmodeled dynamics or noise, etc. In addition, in Application 1, the distributed communication topology, which is not fully connected, makes it impossible for the prediction algorithm unable to perfectly compensate for the time delay. The ability of networked prediction algorithms to compensate for the time delay is limited in these cases. Therefore, in a real hardware system such as those in Application 1 and Application 3, the time consumption of the PoT consensus mechanism should be minimized to ensure that the time delay encountered by the system is within a reasonable range.

(2) Whether there is a constraint on the time step of the HIL simulation itself to ensure the stability

There are three kinds of time steps involved in HIL simulation, one is the time step of solving the model (also known as the run step of the model), the second is the sampling time step, and the third is the control time step.

♣ Firstly, the two basic restrictions on the time step of model solving for HIL simulation are (a) matching the system dynamic characteristics and (b) being smaller than the time step of the switching signal in the model.

The time step of model solving for HIL simulation affects the accuracy of real-time simulation in portraying real physical targets. In general, the smaller the time step allowed by OPAL-RT, the more accurately the real-time simulation reflects the dynamical behavior of the physical target. In addition, the choice of the time step for model solving is often related to the system characteristics. For example, for models with system dynamics characterized by 50 Hz or 100 Hz, a 1 ms solver time step is appropriate. However, when the solver time step is taken as 1 ms, the model may diverge when the system dynamics are characterized above 300 Hz. For the PoT-based REPSs in Application 2, the responses when the solver time step is chosen to be 50 ms and 100 ms are given in Figures 1 and 2, respectively. It can be seen that a solver time period that is too large can lead to instability of the system. This further illustrates that smaller solver time steps can be applied to more application scenarios. However, smaller solving/running time steps imply more times of solving, which is likely to result in the model not being solved in real time. In the HIL simulation of the experimental part, OPAL-RT is used as the target machine to simulate the physical objects. In general, real-time simulators have a minimum allowable solving/running time step that is used to ensure the real-time nature of the simulation program. OPAL-RT gives the minimum allowed solver time step after evaluating the simulation model. This means that OPAL-RT as a hardware device has a computational limit and that it is not possible to achieve an infinitely small solver time step. For the three-area power system considered in the experiments, the minimum solver time step allowed by the equipped OP4512 is 2 μs, which is sufficient to accurately describe the system dynamics.

In addition, for some of the circuit simulations involving containing IGBTs, there is a limitation on the time step of the model solver, i.e., it has to be smaller than the switching period of the PWM signal. For example, if the switching frequency of the PWM signal is set to 10 kHz during simulation, the solver time step will be at least 0.1 ms or less.

♣ Secondly, the limitation of the sampling period and control period in HIL simulation is discussed.

- Regarding the sampling period: According to the Shannon sampling principle, if the sampling frequency is guaranteed to be 5 to 10 times of the highest frequency of the signal in general practical applications, then the digital signal after sampling can completely retain the information of the original signal.
- Regarding the control cycle: a basic restriction is that the update frequency of the control commands should be equal to or several times the sampling frequency.

The sampling and control period of HIL simulation affects the stability and control performance of the system. It can be seen that the sampling period could determine the minimum control period. In general, the smaller the sampling and control period is set, the better control results can be obtained. However, there are two other considerations for setting the control period in practice. On the one hand, if the control period is set too small, the hardware controller is not sufficient to complete the computation of the control commands in one cycle, which can lead to controller failure and is undesirable. On the other hand, a larger control period can significantly reduce computational pressure, but an excessively large control period can lead to control failure, especially for systems that are inherently open-loop unstable. Taking the HIL simulation in Application 2 an example, we present the experimental results for control periods of 1 s. It is noted that the control period for Application 2 in the manuscript is 10 ms. From the results shown in Figure 3, it can be seen that a large control period impairs the dynamic and steady state performance of the system. Therefore, when setting the control period, it is not the smaller the better, but the computational power of the hardware controller and the complexity of the controller should be considered.

Based on the reviewer's comments, the authors have made the following modifications to the content of the manuscript:

> [Section II.B, page 5, highlighted in red]
> " ... For predictive control to accommodate the total delay in PoT, the following steps are necessary:

accurate modelling of the system, an effective distributed prediction algorithm, and an appropriate compensation mechanism. ”

[Section VI, page 12, highlighted in red]
“ ... The time step of the model in HIL needs to be chosen according to the simulation resources of OPAL-RT and the dynamic characteristics of the simulated target system. Here, it is set to 5 μs. In general, the smaller the time step, the more accurate the simulation will be. ”

[Section VII, page 14, highlighted in red]
“ ... As can be seen from Fig. 18(a), the networked prediction mechanism in PoT can compensate for this communication delay. However, the prediction mechanism cannot solve for an arbitrary step of time delay. The number of time steps it can compensate for depends on various factors, including the accuracy of the system model acquired by the controller, the communication topology, and the prediction algorithm. Therefore, when deploying the PFC on the Ethereum platform, one should try to minimize the additional time delay brought by Ethereum. ... ”

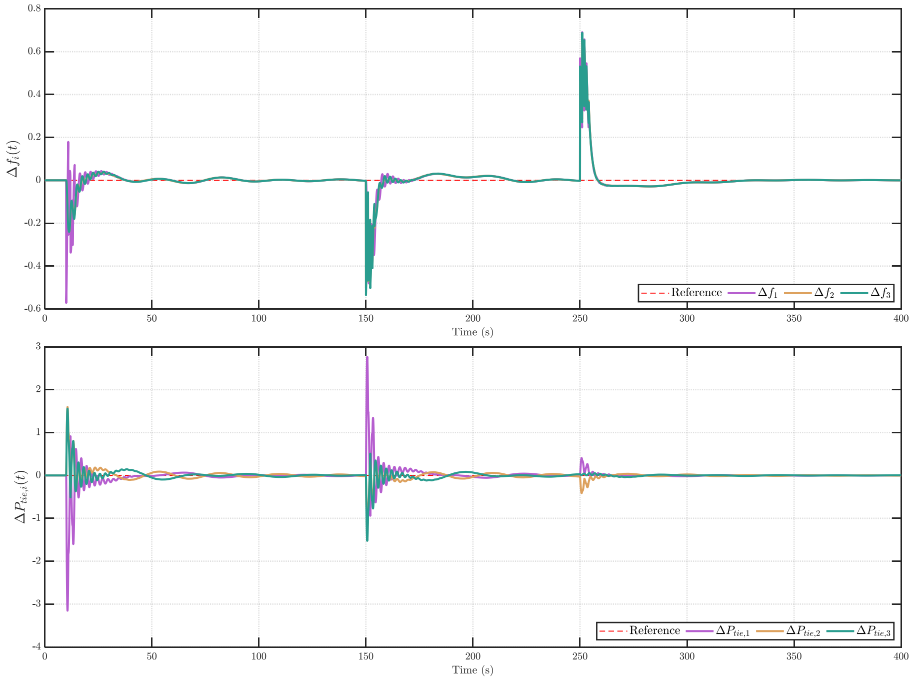


Figure 1: Responses of the three-area power system under the PoT-based LFC scheme with a solver time step of 50 ms.

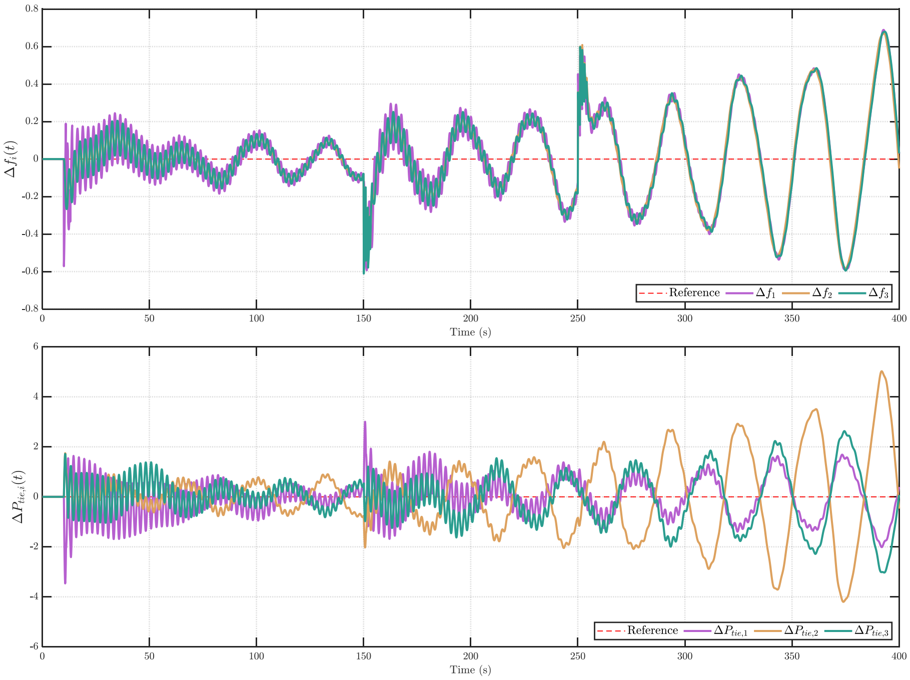


Figure 2: Responses of the three-area power system under the PoT-based LFC scheme with a solver time step of 100 ms.

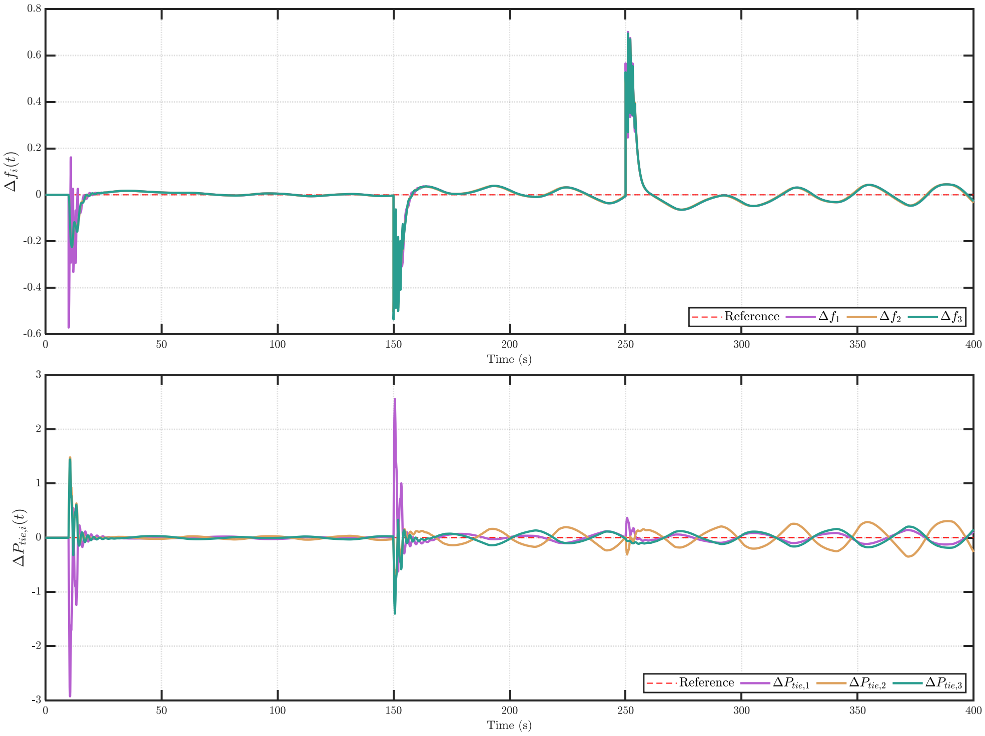


Figure 3: Responses of the three-area power system under the PoT-based LFC scheme with a control period of 1 s.

Reviewer #1 (Remarks on code availability):

C1.7: *The instructions to run the code, and hardware requirements are not mentioned in the README file. Also, the RT-LAB files are not provided. The information provided is not sufficient to reproduce the results of the paper.*

Response:

Thank you sincerely for your insightful and helpful comments. We apologize for not providing enough information in the first manuscript to reproduce the experimental results in the paper. Three types of experiments are covered in this manuscript: a full hardware experiment based on Raspberry Pi and power generation units, a hardware-in-the-loop experiment based on Raspberry Pi and OPAL-RT, and a full hardware experiment based on Raspberry Pi, Ethereum platform and hardware converters. We have added more detailed information to the README files on the Github website, describing the hardware requirements and software running instructions. We are sorry to say that the hardware experiments may be difficult to reproduce because the experimental procedure involves a set of software used to buid and download programs into Raspberry Pi and monitor their operations, which is developed by our research group and is still in the non-open source stage. Therefore, we have provided simulation code that can be completely run in the MATLAB software environment, in order to provide sufficient information to reproduce the results of the paper. The code can be independent of peripheral hardware devices such as the Raspberry Pi.

Specifically, the following three efforts have been made to make it easier and quicker to reproduce the results presented in the experimental section.

- ♣ We have given hardware requirements, software requirements, software code and experimental procedures.

It is important to note that the software code we developed depends on hardware devices (e.g., converters, renewable energy sources-based generators, Raspberry Pi, etc.) and software platforms (NCSLAB, etc.), which means that the code can not run independently on a computer. The running process involves sampling data from the physical object and feeding the calculations back to it, forming a closed-loop system.

- ♣ We have given a semi-physical simulation demo based on the Ethereum platform.

A semi-physical simulation demo is provided for the convenience of readers who do not have the actual power generation device, but have a Raspberry Pi to reproduce the results in the manuscript. In this demo, the actual circuit part is replaced by a mathematical model, while the communication, controller and blockchain are all hardware implementations. The code for the demo and the corresponding instructions for running it are open-sourced on Github, please refer to `https://github.com/blockchainer01/PoTREPSs.git`.

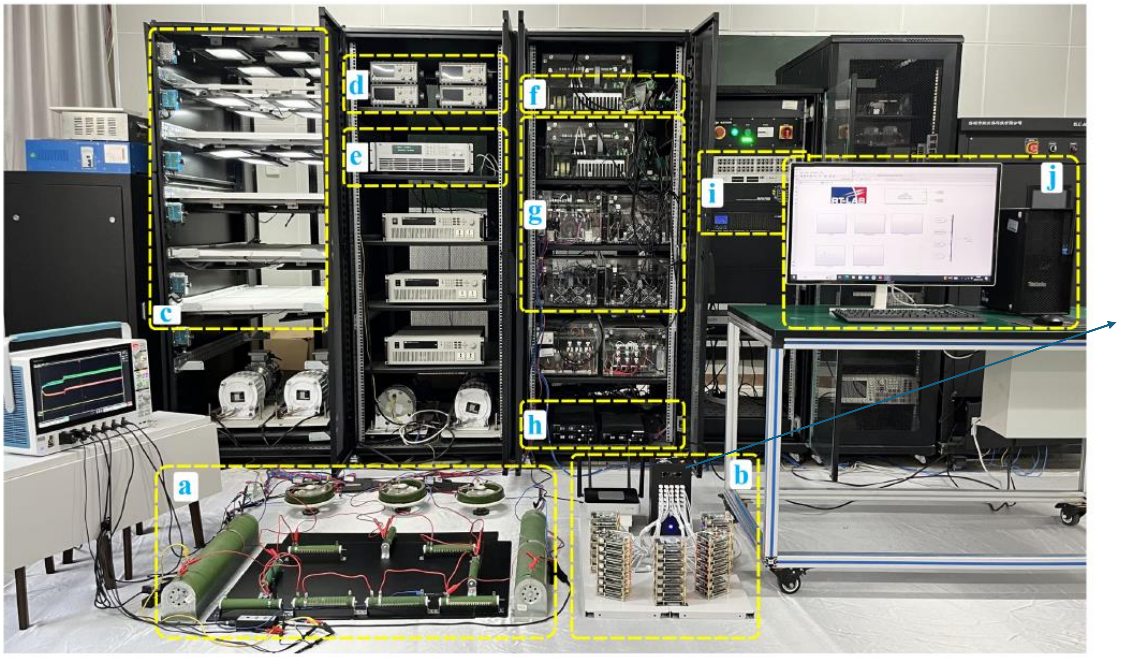
- ♣ We have given a complete simulation demo that can be run on a single computer.

To assist readers to better understand the methodology proposed and to reproduce the experimental results presented in the manuscript, we have released a demo and open-sourced the complete simulation code. The code is available in the ‘simulation’ folder at `https://github.com/blockchainer01/PoTREPSs.git`. The code can be run directly on a computer with MATLAB software. Meanwhile, the detailed instructions to run it are included.

Thus, readers can use the simulation code to reproduce the results presented in the paper and explore their own innovative ideas in line with the methodology of the paper, even though they may not have the relevant hardware to run our excutable code.

In summary, firstly, we have given the hardware requirements, code, etc. for the three applications in the manuscript. Secondly, we have given stand-alone simulation code and running instructions for all three applications. Additionally, for Application 3, we have included semi-physical simulation code and running instructions.

C1.8: *Where can we monitor the blockchain? Please refer to Fig. C1 for the specific comment.*



Where can we monitor the blockchain?

Fig. C1: Panoramic view of IEEE 9-bus microgrid platform with five distributed generation units. The figure from reviewer's comment.

Response:

Thank you very much for your valuable feedback on our manuscript. We use the VNC Viewer software installed on the Raspberry Pi to monitor the entire blockchain experimental platform. In short, the VNC Viewer software is installed on each blockchain node in Fig. C1(b) and connected to a LAN switch. This allows us to monitor the status of the blockchain in the test system on a local computer, as shown in Fig. C1(j). In the following, Application 3 is used as an example to specify the data monitored by the VNC Viewer.

In Application 3, the microgrid system can be divided into three layers: the first layer is the Secondary Controller Layer (SCL), the second layer is the Signal Relay Layer (SRL) and the third layer is the Sampling and Actuator Layer (SAL) of the microgrid. The contents of the monitoring data in the SCL include: the Ethereum platform connection and data on the chain; the status of sending control signal u; the status of receiving signals from the SRL. The contents of the monitoring data in the SRL include: data received from nodes in the controller layer; the status of sending data to the SAL; merged data received from the SAL and merged data forwarded to the SCL. The contents of the monitoring data in the SAL include: control signals received from SRL; the transmission status of control signal u; the transmission status of measurement signal x.

Following your suggestion, we have added the screen for monitoring data on the VNC Viewer, as shown in Supplementary Fig. 13. To be specific, Supplementary Fig. 13**(a)** shows the status of the data sent and received by the node at the SCL. It can be seen that the SCL has sent out u. 'T_out(Transmit out)' indicates that data has been sent out from the SCL. 'V' and 'I' are the received voltage and current signals, respectively, 'Elapse time' is the running time, and 'x' is the received data after the consensus. Supplementary Fig. 13(b) illustrates the status of the data sent and received by the node at the SRL. It can be seen that there are signals u sent out in the Ethereum. 'T_out' indicates that the data has been sent out from the SCL layer, and 'Recv - Send to third layer' indicates that the data has been received from the SCL and sent to five nodes in the SAL, where each node has a corresponding IP and port. 'C_out' is the output prompt after receiving the combined data and completing the consensus. 'Recv - Send' to first layer means to send the consensus data x to the first layer, i.e., SCL. Supplementary Fig. 13(c) shows the status of the data sent and received by the node at the SAL. It can be seen that there are signals u sent out from the SAL. Supplementary Fig. 13(d) shows the status of data uploading to the Ethereum blockchain in the SRL. In the figure, 'Commit new mining work' means that the mining process has been completed. 'Successfully sealed new block' means that a block has been successfully sealed and 'number' is the block number of the operation.

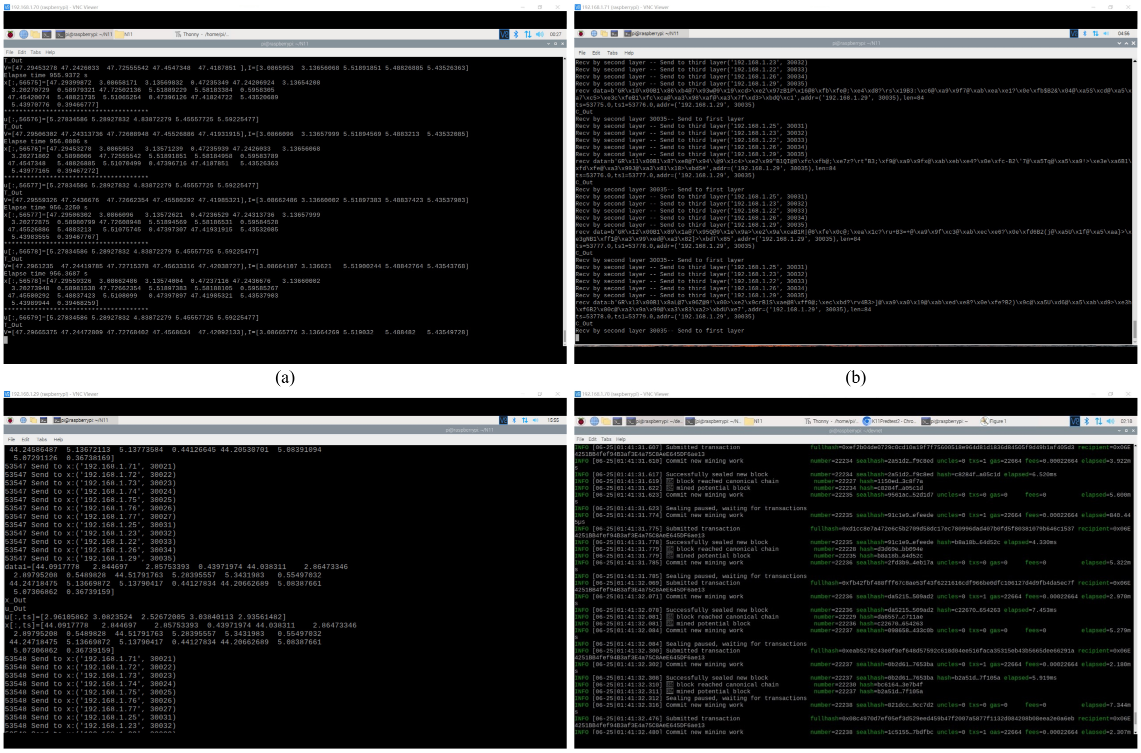
It can be seen that we can monitor the real-time and complete running status of all nodes, by using VNC Viewer and opening multiple windows in the local computer. For example, we can create 7 and 5 windows for the SCL and SRL respectively in VNC Viewer to monitor the node status. We have proven through extensive testing that the program runs normally, and the programs for each node have been uploaded to `https://github.com/blockchainer01/PoTREPSs.git`.

To address your concerns, we have presented some specific monitor screens in the supplementary file. Thank you again for your insightful comments.

Based on the reviewer's comments, the authors have made the following modifications to the content of the manuscript:

[Section VII, page 14, highlighted in red]
" ... The status and performance of the Ethereum is demonstrated in Supplementary Fig. 13. "

[Section IX, page 16, highlighted in red]
" ... The blockchain network consists of Raspberry Pi loaded with Ethereum client, and the details of the softwares involved are available in Supplementary Table 6. ... "



```
T_Out
V=[47.29453278 47.2426033  47.72555542 47.4547348  47.4187851 ],I=[3.0865953  3.13656068 5.51891851 5.48826885 5.43526363]
Elapse time 955.9372 s
x[:,56575]=[47.29399872  3.08658171  3.13569832  0.47235349 47.24206924  3.13654208
  3.20270729  0.58979321 47.72502136  5.51889229  5.58183384  0.5958305
 47.45420074  5.48821735  5.51065254  0.47396126 47.41824722  5.43520689
  5.43970776  0.39466777]
**************************************
u[:,56576]=[5.27834586 5.28927832 4.83872279 5.45557725 5.59225477]
T_Out
V=[47.29506302 47.24313736 47.72608948 47.45526886 47.41931915],I=[3.0866096  3.13657999 5.51894569 5.4883213  5.43532085]
Elapse time 956.0806 s
x[:,56576]=[47.29453278  3.0865953   3.13571239  0.47235939 47.2426033   3.13656068
  3.20271802  0.5898006  47.72555542  5.51891851  5.58184958  0.59583789
 47.4547348   5.48826885  5.51070499  0.47396716 47.4187851   5.43526363
  5.43977165  0.39467272]
**************************************
u[:,56577]=[5.27834586 5.28927832 4.83872279 5.45557725 5.59225477]
T_Out
V=[47.29559326 47.2436676  47.72662354 47.45580292 47.41985321],I=[3.08662486 3.13660002 5.51897383 5.48837423 5.43537903]
Elapse time 956.2250 s
x[:,56577]=[47.29506302  3.0866096   3.13572621  0.47236529 47.24313736  3.13657999
  3.20272875  0.58980799 47.72608948  5.51894569  5.58186531  0.59584528
 47.45526886  5.4883213   5.51075745  0.47397307 47.41931915  5.43532085
  5.43983555  0.39467767]
**************************************
u[:,56578]=[5.27834586 5.28927832 4.83872279 5.45557725 5.59225477]
T_Out
V=[47.2961235  47.24419785 47.72715378 47.45633316 47.42038727],I=[3.08664107 3.136621   5.51900244 5.48842764 5.43543768]
Elapse time 956.3687 s
x[:,56578]=[47.29559326  3.08662486  3.13574004  0.47237116 47.2436676   3.13660002
  3.20273948  0.58981538 47.72662354  5.51897383  5.58188105  0.59585267
 47.45580292  5.48837423  5.5108099   0.47397897 47.41985321  5.43537903
  5.43989944  0.39468259]
**************************************
u[:,56579]=[5.27834586 5.28927832 4.83872279 5.45557725 5.59225477]
T_Out
V=[47.29665375 47.24472809 47.72768402 47.4568634  47.42092133],I=[3.08665776 3.13664269 5.519032   5.488482   5.43549728]
```

(a)

```
Recv by second layer -- Send to third layer('192.168.1.23', 30032)
Recv by second layer -- Send to third layer('192.168.1.22', 30033)
Recv by second layer -- Send to third layer('192.168.1.26', 30034)
Recv by second layer -- Send to third layer('192.168.1.29', 30035)
recv data=b'GR\x10\x00B1\x86\xb4@7\x93w@9\x19\xcd>\xe2\x97zB1P\x16@8\xfb\xfe@;\xe4\xd8?\rs\x19B3:\xc6@\xa9\x9f7@\xab\xea\xe1?\x0e\xfb$B2&\x04@\xa5S\xcd@\xa5\x
a7\xc5>\xe3c\xfeB1\xfc\xca@\xa3\x98\xaf@\xa3\x7f\xd3>\xbdQ\xc1',addr=('192.168.1.29', 30035),len=84
ts=53775.0,ts1=53776.0,addr=('192.168.1.29', 30035)
C_Out
Recv by second layer 30035-- Send to first layer
Recv by second layer -- Send to third layer('192.168.1.25', 30031)
Recv by second layer -- Send to third layer('192.168.1.23', 30032)
Recv by second layer -- Send to third layer('192.168.1.22', 30033)
Recv by second layer -- Send to third layer('192.168.1.26', 30034)
Recv by second layer -- Send to third layer('192.168.1.29', 30035)
recv data=b'GR\x11\x00B1\x87\xe8@7\x94\\@9\x1c4>\xe2\x99"B1QI@8\xfc\xfb@;\xe7z?\rt"B3;\xf9@\xa9\x9fx@\xab\xeb\xe4?\x0e\xfc-B2\'7@\xa5Tq@\xa5\xa9!>\xe3e\xa6B1\
xfd\xfe@\xa3\x99J@\xa3\x81\x18>\xbdS#',addr=('192.168.1.29', 30035),len=84
ts=53776.0,ts1=53777.0,addr=('192.168.1.29', 30035)
C_Out
Recv by second layer 30035-- Send to first layer
Recv by second layer -- Send to third layer('192.168.1.25', 30031)
Recv by second layer -- Send to third layer('192.168.1.23', 30032)
Recv by second layer -- Send to third layer('192.168.1.22', 30033)
Recv by second layer -- Send to third layer('192.168.1.26', 30034)
Recv by second layer -- Send to third layer('192.168.1.29', 30035)
recv data=b'GR\x12\x00B1\x89\x1a@7\x95Q@9\x1e\x9a>\xe2\x9a\xcaB1R|@8\xfe\x0c@;\xea\x1c?\ru+B3=+@\xa9\x9f\xc3@\xab\xec\xe6?\x0e\xfd6B2(j@\xa5U\x1f@\xa5\xaa}>\x
e3gNB1\xff1@\xa3\x99\xed@\xa3\x82]>\xbdT\x85',addr=('192.168.1.29', 30035),len=84
ts=53777.0,ts1=53778.0,addr=('192.168.1.29', 30035)
C_Out
Recv by second layer 30035-- Send to first layer
Recv by second layer -- Send to third layer('192.168.1.25', 30031)
Recv by second layer -- Send to third layer('192.168.1.23', 30032)
Recv by second layer -- Send to third layer('192.168.1.22', 30033)
Recv by second layer -- Send to third layer('192.168.1.26', 30034)
Recv by second layer -- Send to third layer('192.168.1.29', 30035)
recv data=b'GR\x13\x00B1\x8aL@7\x96Z@9!\x00>\xe2\x9crB1S\xae@8\xff0@;\xec\xbd?\rv4B3>]@\xa9\xa0\x19@\xab\xed\xe8?\x0e\xfe?B2)\x9c@\xa5U\xd6@\xa5\xab\xd9>\xe3h
\xf6B2\x00c@\xa3\x9a\x99@\xa3\x83\xa2>\xbdU\xe7',addr=('192.168.1.29', 30035),len=84
ts=53778.0,ts1=53779.0,addr=('192.168.1.29', 30035)
C_Out
Recv by second layer 30035-- Send to first layer
```

(b)

```
 44.24586487  5.13672113  5.13773584  0.44126645 44.20530701  5.08391094
  5.07291126  0.36738169]
53547 Send to x:('192.168.1.71', 30021)
53547 Send to x:('192.168.1.72', 30022)
53547 Send to x:('192.168.1.73', 30023)
53547 Send to x:('192.168.1.74', 30024)
53547 Send to x:('192.168.1.75', 30025)
53547 Send to x:('192.168.1.76', 30026)
53547 Send to x:('192.168.1.77', 30027)
53547 Send to x:('192.168.1.25', 30031)
53547 Send to x:('192.168.1.23', 30032)
53547 Send to x:('192.168.1.22', 30033)
53547 Send to x:('192.168.1.26', 30034)
53547 Send to x:('192.168.1.29', 30035)
data1=[44.0917778   2.844697    2.85753393  0.43971974 44.038311    2.86473346
  2.89795208  0.5489828  44.51791763  5.28395557  5.3431983   0.55497032
 44.24718475  5.13669872  5.13790417  0.44127834 44.20662689  5.08387661
  5.07306862  0.36739159]
x_Out
u_Out
u[:,ts]=[2.96105862 3.0823524  2.52672005 3.03840113 2.93561482]
x[:,ts]=[44.0917778   2.844697    2.85753393  0.43971974 44.038311    2.86473346
  2.89795208  0.5489828  44.51791763  5.28395557  5.3431983   0.55497032
 44.24718475  5.13669872  5.13790417  0.44127834 44.20662689  5.08387661
  5.07306862  0.36739159]
53548 Send to x:('192.168.1.71', 30021)
53548 Send to x:('192.168.1.72', 30022)
53548 Send to x:('192.168.1.73', 30023)
53548 Send to x:('192.168.1.74', 30024)
53548 Send to x:('192.168.1.75', 30025)
53548 Send to x:('192.168.1.76', 30026)
53548 Send to x:('192.168.1.77', 30027)
53548 Send to x:('192.168.1.25', 30031)
53548 Send to x:('192.168.1.23', 30032)
```

(c)

```
INFO [06-25|01:41:31.607] Submitted transaction                    fullhash=0xef2b04de0729c0cd10a19f7f75600518e964d81d1836d84505f9d49b1af405d3 recipient=0x06E
4251BB4fef94B3af3E4a75C8AeE645DF6ae13
INFO [06-25|01:41:31.610] Commit new mining work                   number=22234 sealhash=2a51d2…f9c8ed uncles=0 txs=1 gas=22664 fees=0.00022664 elapsed=3.922m
s
INFO [06-25|01:41:31.617] Successfully sealed new block            number=22234 sealhash=2a51d2…f9c8ed hash=c8284f…a05c1d elapsed=6.520ms
INFO [06-25|01:41:31.619] ▦ block reached canonical chain           number=22227 hash=1150ed…3c8f7a
INFO [06-25|01:41:31.622] ▦ mined potential block                   number=22234 hash=c8284f…a05c1d
INFO [06-25|01:41:31.623] Commit new mining work                   number=22235 sealhash=9561ac…52d1d7 uncles=0 txs=0 gas=0     fees=0          elapsed=5.600m
s
INFO [06-25|01:41:31.623] Sealing paused, waiting for transactions
INFO [06-25|01:41:31.774] Commit new mining work                   number=22235 sealhash=91c1e9…efeede uncles=0 txs=1 gas=22664 fees=0.00022664 elapsed=840.44
5μs
INFO [06-25|01:41:31.775] Submitted transaction                    fullhash=0xd1cc8e7a472e6c5b2709d58dc17ec780996dad407b0fd5f80381079b646c1537 recipient=0x06E
4251BB4fef94B3af3E4a75C8AeE645DF6ae13
INFO [06-25|01:41:31.778] Successfully sealed new block            number=22235 sealhash=91c1e9…efeede hash=b8a18b…64d52c elapsed=4.330ms
INFO [06-25|01:41:31.779] ▦ block reached canonical chain           number=22228 hash=d3d69e…bb094e
INFO [06-25|01:41:31.779] ▦ mined potential block                   number=22235 hash=b8a18b…64d52c
INFO [06-25|01:41:31.785] Commit new mining work                   number=22236 sealhash=2fd3b9…4eb17a uncles=0 txs=0 gas=0     fees=0          elapsed=5.322m
s
INFO [06-25|01:41:31.785] Sealing paused, waiting for transactions
INFO [06-25|01:41:32.069] Submitted transaction                    fullhash=0xfb42fbf488fff67c8ae53f43f6221616cdf966be0dfc106127d4d9fb4da5ec7f recipient=0x06E
4251BB4fef94B3af3E4a75C8AeE645DF6ae13
INFO [06-25|01:41:32.071] Commit new mining work                   number=22236 sealhash=da5215…509ad2 uncles=0 txs=1 gas=22664 fees=0.00022664 elapsed=2.970m
s
INFO [06-25|01:41:32.078] Successfully sealed new block            number=22236 sealhash=da5215…509ad2 hash=c22670…654263 elapsed=7.453ms
INFO [06-25|01:41:32.081] ▦ block reached canonical chain           number=22229 hash=da6557…c711ae
INFO [06-25|01:41:32.081] ▦ mined potential block                   number=22236 hash=c22670…654263
INFO [06-25|01:41:32.084] Commit new mining work                   number=22237 sealhash=098658…433c0b uncles=0 txs=0 gas=0     fees=0          elapsed=5.279m
s
INFO [06-25|01:41:32.084] Sealing paused, waiting for transactions
INFO [06-25|01:41:32.300] Submitted transaction                    fullhash=0xeab5278243e0f8ef648d57592c618d04ee516faca35315eb43b5665dee66291a recipient=0x06E
4251BB4fef94B3af3E4a75C8AeE645DF6ae13
INFO [06-25|01:41:32.302] Commit new mining work                   number=22237 sealhash=0b2d61…7653ba uncles=0 txs=1 gas=22664 fees=0.00022664 elapsed=2.180m
s
INFO [06-25|01:41:32.308] Successfully sealed new block            number=22237 sealhash=0b2d61…7653ba hash=b2a51d…7f105a elapsed=5.919ms
INFO [06-25|01:41:32.310] ▦ block reached canonical chain           number=22230 hash=bc6164…3e7b4f
INFO [06-25|01:41:32.311] ▦ mined potential block                   number=22237 hash=b2a51d…7f105a
INFO [06-25|01:41:32.312] Sealing paused, waiting for transactions
INFO [06-25|01:41:32.316] Commit new mining work                   number=22238 sealhash=821dcc…9cc7d2 uncles=0 txs=0 gas=0     fees=0          elapsed=7.344m
s
INFO [06-25|01:41:32.476] Submitted transaction                    fullhash=0x08c4970d7ef05ef3d529eed459b47f2007a5877f1132d084208b08eea2e0a6eb recipient=0x06E
4251BB4fef94B3af3E4a75C8AeE645DF6ae13
INFO [06-25|01:41:32.480] Commit new mining work                   number=22238 sealhash=1c5155…7bdfbc uncles=0 txs=1 gas=22664 fees=0.00022664 elapsed=2.307m
```

(d)

Supplementary Fig. 13: Data transmission of the dc microgrid system based on the Ethereum platform, where the blockchain is monitored and assessed by VNC Viewer. (a) The status of the data sent and received by the node at the secondary control layer. (b) The status of the data sent and received by the node at the Ethereum-based relay layer. (c) The status of the data sent and received by the node at the physical layer of the microgrid. (d) The status of data uploading to the Ethereum blockchain in the Ethereum-based relay layer.

Supplementary Table 6: Details of the software in the blockchain platform

Software	Version
Geth	1.9.10
Remix	0.91
Solidity	8.10.0
Web3.py	5.12.0
Raspberry Pi	0.91
VNC Viewer	0.91
Python	3.92

Response to the Reviewers: Reviewer 2

C2.0: *I have reviewed the manuscript entitled 'A Blockchain Consensus Mechanism for Real-Time Regulation of Renewable Energy Power Systems'. In my opinion:*

Response: Thanks so much for your time and efforts in reviewing the manuscript. We will carefully respond to your concerns point by point and revise the manuscript. Please find our responses to your inquiries in what follows.

C2.1: *The paper introduced Proof of Task as a consensus mechanism, but the specific tasks involved remain unclear. It is crucial to define the tasks used in PoT and demonstrate how they directly relate to real-time control and stability of REPSs. Are these tasks computationally expensive enough to secure the network?*

Response:

Thank you sincerely for your insightful and helpful comments. For the two points you are concerned, we would like to respond to each of them in the following.

(1) We apologize for not giving a clear description of the 'task' in 'Proof of Task' (PoT) in the original manuscript. The 'task' in PoT refers to the regulation tasks in REPSs. For example, regulation tasks such as voltage restoration and current sharing in dc microgrids and load frequency control in interconnected power systems can be used as 'task' in PoT. The 'task' in PoT is similar to the 'work' in PoW in that they both require peers to solve a mathematical problem. It is well known that under the Proof of Work consensus mechanism, which peer has the right to submit transaction data is determined based on their workload, i.e., computing effort. Most cases of 'work' in PoW refer to solving a hash puzzle. Instead, we have assigned some practical meanings to the actions of the peers. The mathematical problem solved by peers in the PoT consensus mechanism is a constrained optimization problem with constraints corresponding to the control task under consideration, rather than a meaningless hash puzzle. Thus, under the PoT consensus mechanism, the peer that has the right to submit transaction data is the one who is able to find a control command that better accomplishes the control task.

For REPSs, any control task that can be described as a specific mathematical problem can be posted as a 'task' to a P2P network to be solved by peers. In PoT, the problem to be solved is closely related to the control performance of the REPSs, while the verification criterion of the published solution is closely related to the stability of the system. For example, in Application 1 of the manuscript, the 'task' is to implement security voltage restoration and accurate current sharing for a microgrid system, where peers solve a distributed optimization problem. The verification mechanism in PoT verifies not only the optimality of the candidate solution, but also whether the candidate solution satisfies the stability conditions of the system. In this way, the consensus solution is the one that stabilizes the system and makes the performance metric function relatively optimal. Therefore, the tasks in the PoT enable the PoT to simultaneously consider the security of the system, the stability of the system, and the performance of the system.

(2) Together with the verification mechanism, these tasks are capable of securing the network of the control system to a certain extent. Despite the relative simplicity of the task to be solved, the design of the verification mechanism in PoT allows the solution after multi-party authentication to at least stabilize the system, which ensures the security of the control system.

Firstly, such a setup is a compromise between utilizing blockchain computing resources and ensuring real-time computation. Because of the real-time requirements of the control problem, we have to simplify the task to be solved in PoT. High real-time performance is a natural demand for control systems. If the complexity of the problem to be solved is too difficult, then it will result in the corresponding consensus protocol not being applicable to the control system. Therefore, in the field of real-time control, the problem to be solved designed in PoT must not be too difficult, and it is necessary to consider how to facilitate the security of the system from aspects other than computational cost. Secondly, as a further expectation, we want the problem solved by the blockchain nodes to be meaningful for the applications under consideration. Therefore, we replace the original hash puzzle with an optimization problem corresponding to the control task of interest.

Here, the operational mechanisms of blockchain are reviewed here to further analyze the implications of the complexity of the problem to be solved in terms of security. Take a typical PoW consensus mechanism as an example. In PoW, the complexity of the problem to be solved determines how much computational work the miner needs to perform before finding a valid block. The complexity and difficulty of the problem to be solved has several key roles and considerations Refs. [6, 7].

- Control the block generation rate. The complexity of the problem to be solved directly affects the speed of block generation. By adjusting the difficulty of the problem, it can be ensured that the block generation interval remains within a stable and reasonable range to meet constraints such as the throughput of the blockchain network.
- Ensure network security. The higher difficulty means that miners need to do a lot of computational work to find a valid solution and win the right to add a new block to the blockchain, making it necessary for an attacker to invest a lot of resources in order to launch a double-spending attack or other forms of attack. This increases network security and prevents malicious behavior.
- Incentive mechanism. The difficulty of the problem to be solved can be adjusted to ensure that the miners' workload is proportional to the reward they receive. This incentivizes more miners to participate in solving the problem.
- Prevent inflation. By controlling the rate of block generation, the difficulty adjustment mechanism can help control the rate at which reward tokens are issued and prevent inflation.

For the four aspects mentioned above, two of them are closely related to the control system, which are 1) adjusting the block generation speed as needed and 2) ensuring network security, mainly to prevent double-spending attacks.

Regarding the first point, for control systems, we have a completely opposite requirement, which is to achieve consensus as quickly and efficiently as possible. Taking this into account, there is no incentive to increase the complexity of the problem to be solved when the computational power of the miners is increased and the generation of blocks is accelerated, in order to restore the time required to generate a block to a longer target duration.

Regarding the second point, for traditional blockchain consensus protocols, the more complex the hash puzzle, the computational cost is more sufficient to make the network secure against double-spending attacks and similar types of attacks. This practice can prevent the repeated generation of identical valid solutions, protect both parties to a transaction from economic loss, maintain user trust in the blockchain, ensure the stability of the virtual currency market, etc. For the proposed PoT, the reduction in the complexity of the problem to be solved indeed increases the likelihood of the network experiencing double spending attacks. However, in real-time control systems such as REPSs, we need to focus more on the trusted solution itself provided by the blockchain, rather than being overly concerned with whether multiple identical solutions appear simultaneously. As long as correct and usable control commands can be obtained, it indicates that this round of consensus contributes to the cybersecurity and stable operation of the control system. At this point, the occurrence of a double-spending attack is much less harmful to the control system than the occurrence of a data tampering attack. This also highlights the difference between using blockchain to protect the cybersecurity of real-time control systems and using it to protect the cybersecurity of economic dispatch, energy trading, etc.

In summary, complex puzzles to be solved play an important role in the protection of transactions by traditional blockchain. If there is no requirement for real-time performance, such a blockchain consensus mechanism is certainly great. However, in real-time control scenarios, we have to guarantee the basic requirement of real-time and pay more attention to the quality of the solutions submitted by the blockchain. Therefore, the design intent of PoT is to tap into the favorable factors of blockchain technology for control system security and control performance, while discarding the unfavorable factors for real-time control systems. Guided by this idea, PoT has tried its best to exploit the characteristics of multi-party verification and multi-party computation in blockchain. The data results presented in the experimental section validate that the PoT consensus mechanism effectively reduces the probability of successful occurrence of uninterruptedly launched attacks and improves the control performance. This indicates that although PoT sacrifices a small amount of security to achieve real-time performance, it still significantly reduces the likelihood of a successful attack occurring within the REPSs. The solutions in this manuscript are more feasible and effective for real-time control systems, both compared with resilient control methods and with the significantly time-consuming traditional blockchain approaches.

Based on the reviewer's comments, the authors have made the following modifications to the content of the manuscript:

[Section I, page 2, highlighted in red]
" ... In PoT, the term 'task' refers to various control tasks of REPSs corresponding to actual application scenarios. That is, PoT decides whose data will be adopted based on the contributions made by peers in completing control tasks. ... "

[Section II.A, page 4, highlighted in red]
" First, a meaningful optimization problem associated with the control task is issued to be solved by each peer. To be specific, the cost function is a performance metric related to the regulation objective, while the constraints play a critical role in the stable operation of REPSs. ... "

" In summary, the nodes in PoT will solve an optimization problem related to the control task of the REPSs, while the validation of the candidate solutions determines the stability of the system.

Therefore, the completion of PoT will be closely tied to the secure and stable operation of the REPSs. In addition, PoT employs a simpler problem instead of the complex and time-consuming hash puzzle of the traditional blockchain in order to meet the requirements of real-time control. Although PoT is not as secure as PoW, a combination of the problem-solving related to the control task together with a slightly more complex verification mechanism than PoW makes PoT competent for real-time security control of REPSs. "

[Section VIII, page 15, highlighted in red]
" ... In PoT, the control task is formulated as an optimization problem, and the stability requirement of the system is transformed into a validation condition for candidate solutions, providing a new control structure. ... "

C2.2: *While highlighting limitations of existing blockchain protocols, the paper did not compare properly the PoT's performance with established real-time control solutions in REPSs. A clear comparison would strengthen the argument for PoT's necessity and effectiveness.*

Response:

Thank you sincerely for your insightful and helpful comments. We apologize for only emphasizing the limitations of the existing blockchain in the original manuscript, instead of demonstrating the necessity and effectiveness of the proposed PoT through proper and rich comparisons. In the results section corresponding to Application 1 in the original manuscript, we preliminarily compared the PoT with the existing real-time security control of microgrids. Unfortunately, we have only compared it with a method proposed in one paper and have only given waveform results. Based on your suggestions, we have made the following two improvements to the comparison in the results section.

(1) On the one hand, we have updated and added comparative cases.

In the scenario of Application 1, we have updated the existing comparison and added comparison with another existing real-time security control strategy.

Studies addressing security control for REPSs can be categorized into two groups in terms of whether there is the aid of hardware technology (e.g., blockchain technology).

First, the latest method used for comparison in Application 1 belongs to the first category. From the results shown in Fig. 8(a), it can be seen that although the method in [13] can mitigate the effect of the attack to some extent, its results are still not very satisfactory. Besides, it doesn't have any proactive measures in place to deal with the communication-induced time delay and packet loss, which is an additional shortcoming of this type of method in practical applications. Second, to enrich the comparison in Application 1, we have also compared PoT with the second category of security control methods mentioned above. Fig. 8(b) illustrates the experimental results of the existing blockchain-based security control in [56], which is slightly inferior compared to Fig. 8(d). Although this control scheme can reduce the probability of the system being attacked, the computing power that comes with the blockchain is not being utilized. Moreover, in [56], an additional terminal controller needs to be configured for each subsystem, and the time delay introduced by the blockchain is not yet compensated in a distributed form.

Besides, the method only protects against external attacks and is powerless against dishonest blockchain nodes, making the stability of the control system need extra guarantees. At this point, the blockchain only provides a means of data transmission. Instead, as can be seen from Fig. 8(d), the PoT-based control strategy demonstrates unique advantages in solving optimization problems, defending against network attacks, and compensating for communication constraints in the face of the regulation task of REPSs.

Similarly, in the scenario of Application 2 and 3, we have also compared the PoT and DPoT with the approach in the latest published work, respectively. The relevant results are shown in Figs. 16 and 18.

The following conclusions can be drawn from these comparisons. Compared with existing real-time control methods, the PoT-based control scheme can leverage the multi-party verification feature of blockchain to provide REPSs with a proactive defense against cyber-attacks. At the same time, PoT abandons the low real-time inherent in blockchain and takes into account the system stability in the verification mechanism, making it well suited for real-time control of complex dynamical systems such as REPSs. Furthermore, the nature of multi-party computation and the verification mechanism for relative optimality allow PoT to solve complex control problems online. In summary, the PoT-based regulation method can improve the security and control performance of REPSs while ensuring their stable operation and realizing the control objectives. These case studies demonstrate the potential of PoT to become a practical solution for facilitating the security control of REPSs.

(2) On the other hand, we have increased the dimensionality of the experimental comparisons in the results section. In addition to the comparison results, which are presented in the form of oscilloscope waveforms, we have also presented quantitative comparison results including several specified performance metrics. For specific modifications to this part, please refer to the subsequent response to your other comment, i.e., **C2.5**.

It is hoped that the comparisons we have added have strengthened the argument for the necessity and effectiveness of PoT and addressed your concerns. If you have any further suggestions, please let us know and we will be delighted to make improvements.

Based on the reviewer's comments, the authors have made the following modifications to the content of the manuscript:

[Section V, page 8, highlighted in red]

" For comparison, the traditional cooperation-based resilient controller in [13] and the existing blockchain-based security control method in [56] are employed in the testbed first. Fig. 8(a) and Fig. 8(b) give the output responses of the resilient controller and the existing blockchain-based controller subject to attacks and communication delays, respectively. From the waveform results, it can be seen that under the combined influence of attacks and delays, the existing resilient secondary control approach fails to achieve the desired regulation performance, and even leads to system divergence, which is not allowable. Similarly, as shown in the figure, the existing blockchain-based approach is also not competent for distributed security control of dc microgrids. The primary reason for this is that the method in [56] only defends against external attacks, and does not take into account disloyal nodes inside the blockchain network. Moreover, it cannot compensate for communication constraints in a distributed fashion. "

[Section V, page 10, highlighted in red]

“ Based on the data presented in the results above, it can be seen that the defense role imparted by PoT from the physical level greatly reduces the likelihood of REPSs being attacked compared with the existing real-time control method. As shown in TABLE IV, the security of the microgrid system with the proposed method reaches 95%, which are superior to the existing methods. In terms of security, the improvements that PoT brings compared to the existing blockchain-based security control method are not as significant as compared to the traditional resilient method. This demonstrates the effectiveness of blockchain in improving data security. However, in terms of performance metrics shown in Fig. 11, the proposed PoT-based control method still outperforms the existing blockchain-based security control method. ”

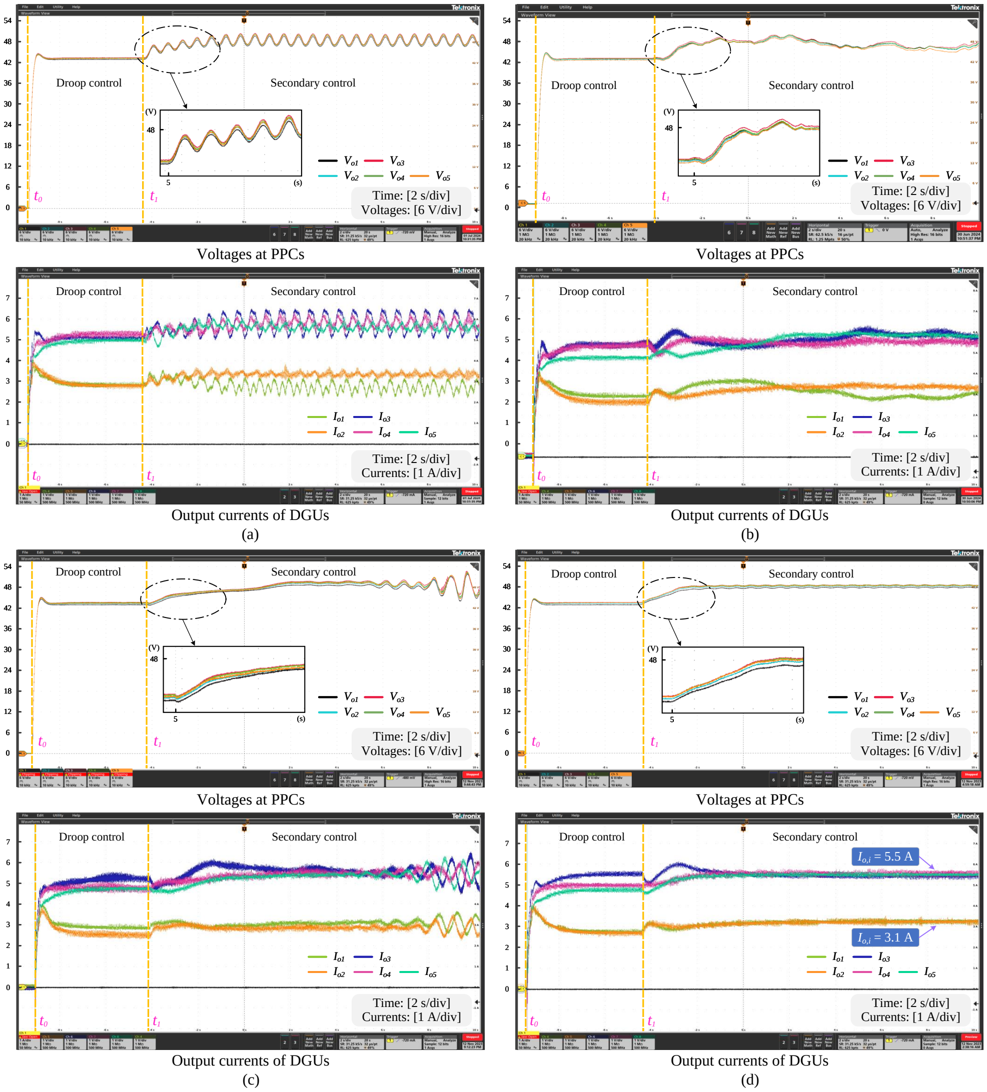
[Section VI, page 12, highlighted in red]
“ For comparison, the PoT-based LFC approach and the normal cooperation-based resilient LFC strategy in [57] are tested in the presence of cyber attacks, and the system responses are shown in Fig. 16. The results indicate that the system subjected to a cyber-attack becomes unstable when utilizing a traditional resilient LFC approach. When using PoT-based LFC, the multi-area power system subjected to the cyber-attack features a smooth response and complies with the generation rate constraints and load reference setpoint constraints. Additionally, the quantitative results, including the performance metrics for both the existing and PoT-based methods, are presented in Supplementary Table 4 and Supplementary Fig. 9. The definitions of these metrics are given in (46) and (47) of Supplementary Note 4. The data in the figure show that $H_{\alpha,lfc}$ and $J_{task,lfc}$ of the proposed method are smaller than those of the existing approach. ... To sum up, the above analysis confirm that the proposed PoT-based distributed LFC algorithm can both guarantee the security of the system and optimise its operation. ”

[Section VII, page 14, highlighted in red]
“ To demonstrate the effectiveness of the proposed method, it is compared with the centralized resilient control method in [58]. As illustrated in Fig. 18(a), the output voltage and current exhibit varying degrees of oscillation under the existing resilient method, and the expected current sharing is not well accomplished. The responses of the dc microgrid system under the PFC-based secondary control method, as depicted in Fig. 18(b), indicate that the average of the output voltages is regulated to the desired level around 48 V and the output currents are accurately shared in the ratio of $1:1:1.8:1.8:1.8$. In addition, some quantitative results are given in Supplementary Table 5, Supplementary Fig. 11 and Supplementary Fig. 12, including comparisons of the security probability as well as performance metrics with the established methods. From these results, it can be seen that PFC-based secondary control is still capable of realizing the desired regulation goals of dc microgrids and actively defending the microgrids against cyber-attacks. ... ”

[References, page 16, highlighted in red]
“ [13] M. Kachhwaha, H. Modi, M. K. Nehra, and D. Fulwani, “Resilient control of dc microgrids against cyber attacks: A functional observer based approach,” *IEEE Transactions on Power Electronics*, vol. 39, no. 1, pp. 459–468, 2024. ”

“ [57] Y. Zhang, C. Peng, C. Cheng, and Y.-L. Wang, “Attack intensity dependent adaptive load frequency control of interconnected power systems under malicious traffic attacks,” *IEEE Transactions on Smart Grid*, vol. 14, no. 2, pp. 1223–1235, 2023. ”

“ [58] P. Lin, C. Deng, Y. Yang, C. H. T. Lee, and W. P. Tay, “Resilience-oriented control for cyber-physical hybrid energy storage systems using a semiconsensus scheme: Design and practice,” *IEEE Transactions on Industrial Electronics*, vol. 70, no. 3, pp. 2508–2519, 2023. ”



Voltages at PPCs

Output currents of DGUs

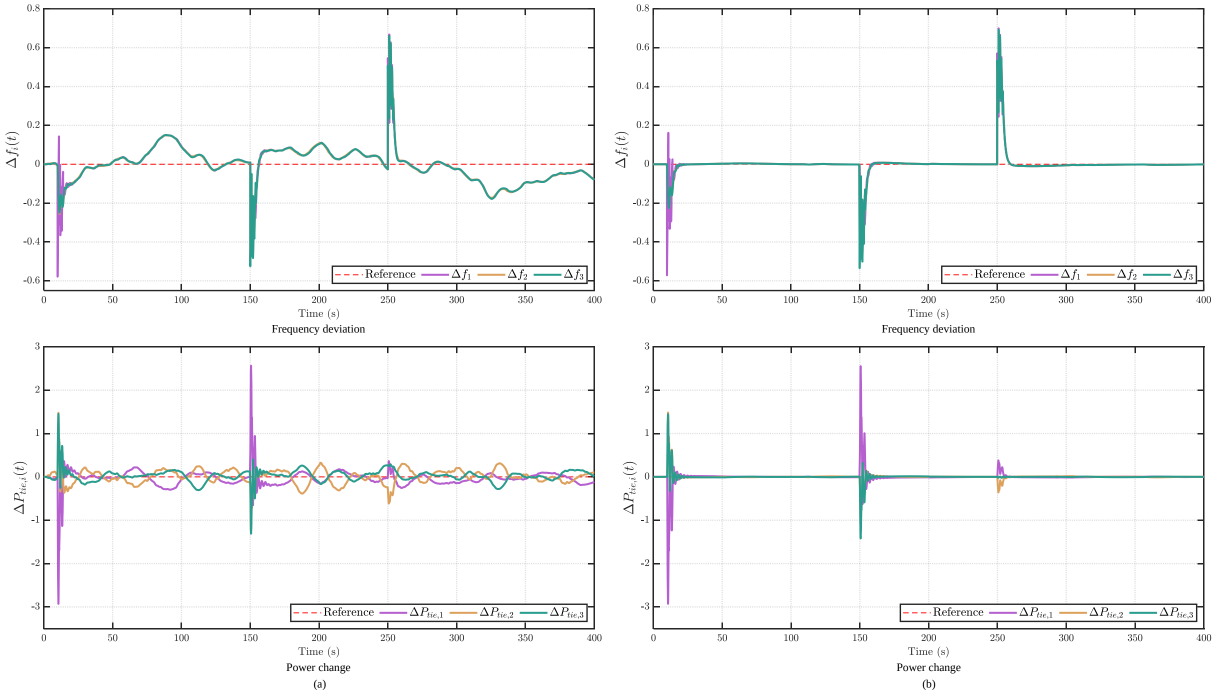
(a)

(b)

(c)

(d)

Fig. 8: Microgrid responses under (a) the resilient method in [13], (b) the blockchain-based method in [56], (c) the PoT-based method without delay compensation, and (d) the PoT-based method.



Frequency deviation

Power change

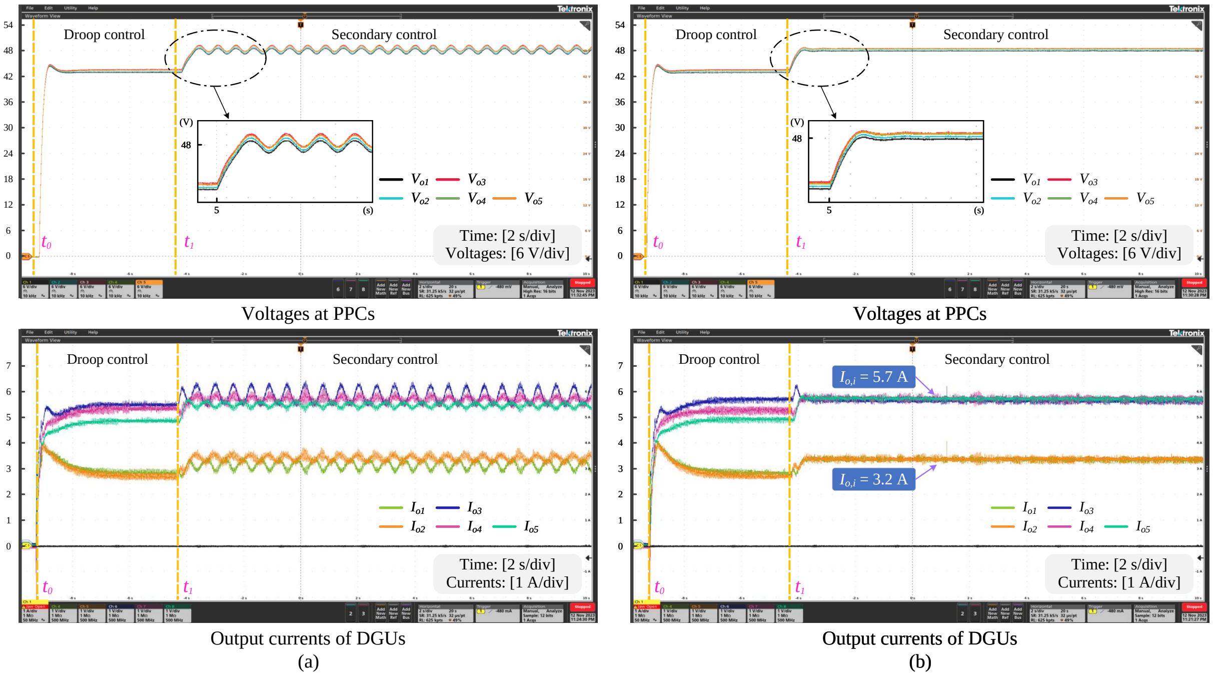
(a)

Frequency deviation

Power change

(b)

Fig. 16: Responses of the three-area power system for (a) the existing resilient method in [57] and (b) PoT-based LFC scheme.



Voltages at PPCs

Output currents of DGUs

(a)

Voltages at PPCs

Output currents of DGUs

(b)

Fig. 18: Microgrid responses under (a) the existing method in [58] and (b) the PFC-based approach.

C2.3: *The manuscript mentioned deploying PoT in three REPSs, but the details of these deployments and the specific functionalities PoT provides in each case are missing. More concrete information is needed to assess the generalizability and effectiveness of PoT across various REPS configurations.*

Response:

Thank you sincerely for your insightful and helpful comments. We apologize for not giving the deployment details and specific functionalities of the PoT under each of the three REPSs in the original manuscript. According to your suggestion, we have added the relevant description in the revised manuscript. Roughly speaking, the Figs. 7, 15 and 17 depict the overall hardware deployment for each of the three applications. In the revised manuscript and supplementary file, we have added more details.

Specifically, we have added code structure diagrams of the proposed method under each of the three applications in the Supplementary File, as shown in Supplementary Figs. 3-6. It is pointed out that the deployment of PoT in practical applications involves two classes of nodes, one class is the local nodes at the device side and the other class is the blockchain nodes at the network side.

The code structures of Application 1 and Application 2 are given in Supplementary Fig. 3 and Supplementary Fig. 4, respectively. Local nodes need to be customized and designed for different application scenarios. For example, underlying dual closed-loop control and droop control, etc. need to be deployed on local nodes for dc microgrids, but these are not required for local nodes in Application 2. For blockchain nodes, comparing Supplementary Fig. 3(b) and Supplementary Fig. 4(b), it can be seen that the code structure regarding the PoT mechanism is the same in these two figures. Therefore, the steps for deploying the PoT are basically the same in different scenarios. In other words, after configuring the components needed for the PoT on the Raspberry Pi, such as the communication module and the verification module, it can be easily used for different application scenarios. Specific deployment details are given on the open source site along with the experimental code.

In order to facilitate the reproduction of the methods presented in this manuscript, we have provided demos of pure software simulations. Specific code and running instructions for these demos are available at `https://github.com/blockchainer01/PoTREPSs.git`.

In addition, the specific functionalities provided by PoT for the three REPSs can be stated as follows:

(1) For Application 1, PoT provides the functionality to derive the **trustworthy control commands** by solving the optimization problem for a dc microgrid suffering from cyber-attacks, to achieve distributed secondary security regulation.

(2) For Application 2, PoT provides the functionality to compute the **trustworthy scheduling decisions** by solving the optimization problem for a three-area power system under cyber attacks, to achieve distributed security LFC.

(3) For Application 3, the functionality of the DPoT is to provide **secure data transmission** for a centralized secondary controller equipped in the dc microgrid system exposed to cyber-attacks.

It is worth noting that most of the added details have been included in the Supplementary File and on an open source website, in order to keep the main body of the paper from becoming too long.

From the methodology, it can be seen that the functions realized by PoT are all related to the control task of the system. The core elements of the PoT consensus protocol are the task-related problem to be solved and the verification mechanism. For different configurations of REPSs, a PoT-based control framework can be used as long as its control task can be transformed into a problem to be solved and a relatively simple verification mechanism can be given. In particular, model predictive control is a typical class of methods for solving problems related to control objectives and with relatively complex computation and relatively simple validation, which are well suited for implementation in PoT. Therefore, in terms of methodology, PoT-based control can be used for a variety of configurations of REPSs. In terms of implementation, the PoT platform we built is mainly a Raspberry Pi based blockchain network as shown in Fig. 5. The network is used to realize general functions as shown in Fig. 1, and the overall process and framework do not depend on specific controlled objects. In practice, once this network is built, it can be used for a variety of systems with some appropriate scaling and adjustment. Specifically, in a new application scenario, it is only necessary to adjust the number of nodes in the network, the solution program carried, and the communication with the hardware according to the configuration, security requirements, and other characteristics of the system. For example, Application 1 and Application 2 are related to microgrid control and load frequency control of multi-domain power systems, respectively, and belong to two types of scenarios. However, they are all based on the same blockchain network and differ only in the configuration of the optimization problems and constraints in the Raspberry Pi nodes, which can be easily implemented through code. In summary, the three specific application scenarios given in the manuscript and the above analysis show that the proposed PoT consensus protocol is effective and generalizable for different configurations of REPSs, and is capable of enabling the security control of communication-based REPSs.

To address your concerns, we have added some deployment details and the introduction of specific functionalities of PoT in the revised manuscript. It is hoped that these modifications and clarifications will address your concerns.

Based on the reviewer's comments, the authors have made the following modifications to the content of the manuscript:

[Section IV, page 8, highlighted in red]
" ... Therefore, the PoT mechanism is embodied in the scenario of large-scale dc microgrid systems as an application. In this case, PoT provides the functionality to derive the trustworthy control commands by solving the optimization problem for a dc microgrid suffering from cyber-attacks, to achieve distributed secondary security regulation. ... "

[Section V, page 9, highlighted in red]
" Fig. 5. Panoramic view of the converter-based IEEE 9-bus microgrid platform with five distributed generation units and the OPAL-RT-based Hardware-In-the-Loop (HIL) platform for the multi-area interconnected power system. ... "

" ... The structure of the code for PoT-based distributed secondary security regulation is depicted in Supplementary Fig. 3. Further, the deployment details of PoT in this application are available at `https://github.com/blockchainer01/PoTREPSs.git`. "

[Section VI, page 11, highlighted in red]
" ... Therefore, it is necessary to design a PoT-based distributed load frequency control method for multi-area power systems. In this case, PoT provides the functionality to compute the trustworthy

scheduling decisions by solving the optimization problem for a three-area power system under cyber-attacks, to achieve distributed security LFC. ... ”

“ ... The structure of the code for PoT-based distributed security LFC and architecture of the HIL test system are given in Supplementary Figs. 4 and 5, respectively. Further, the deployment details of PoT in the three-area power system are available at `https://github.com/blockchainer01/PoTREPSs.git`. ... ”

[Section VII, page 13, highlighted in red]
“ The PFC is a DPoT mechanism presented in Section III.B. Unlike Application 1, a PFC-based secondary control is developed and applied to the dc microgrid here. In this case, the functionality of the PFC is to provide secure data transmission for a centralized secondary controller equipped in the dc microgrid system exposed to cyber-attacks. Since the PFC works in a centralized manner, all DGUs upload measurements or download control commands through the same P2P network shown in Fig. 3. It can be seen that the P2P network in the PFC no longer performs any mathematical problems related to control tasks, but is only used for data transmission. ”

“ ... The structure of the code for the PFC-based secondary control is given in Supplementary Fig. 6. The corresponding deployment details can be found in `https://github.com/blockchainer01/PoTREPSs.git`. ”

[Section VIII, page 14, highlighted in red]
“ ... Furthermore, three different applications suggest that the proposed consensus protocol is effective and generalizable for various configurations of REPSs. ”

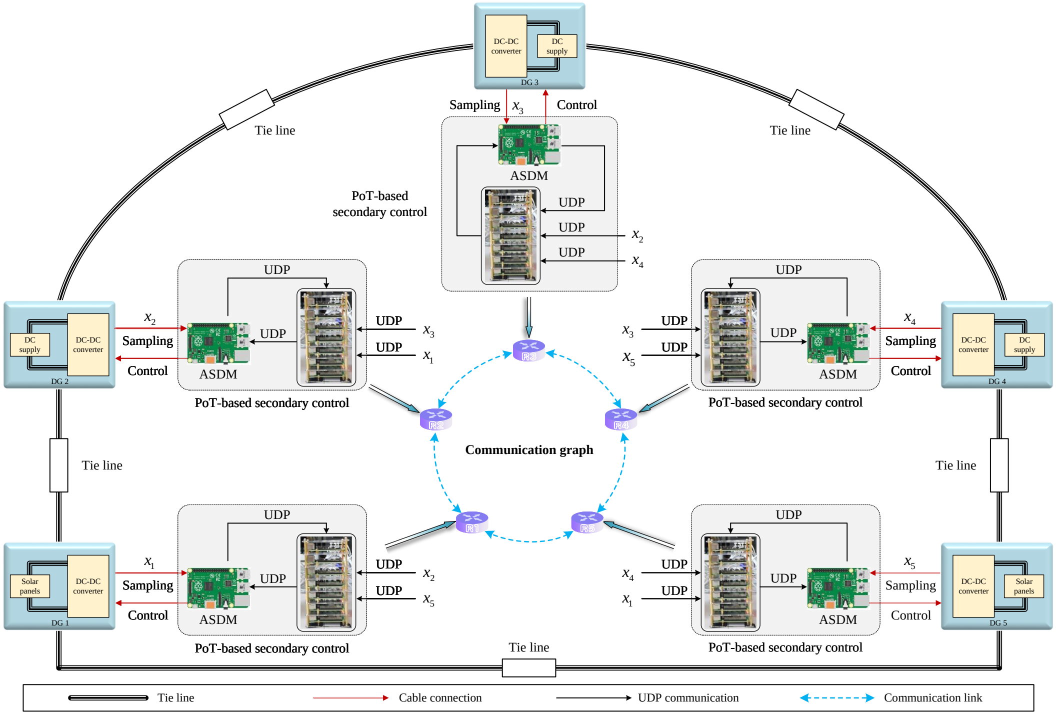


Fig. 7: Data flow of the IEEE 9-bus test bench with PoT-based blockchain, which also presents the deployment architecture of the microgrid under PoT-based secondary control (Application 1). The communication between the generation units at the information layer forms a ring topology. Only part of the tie lines are shown.

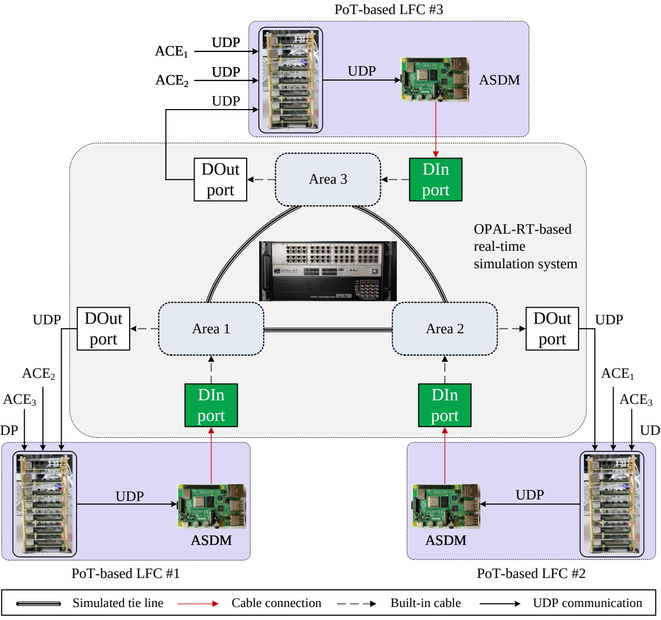


Fig. 15: Data flow of the HIL interconnected power system with the PoT-based LFC scheme (Application 2).

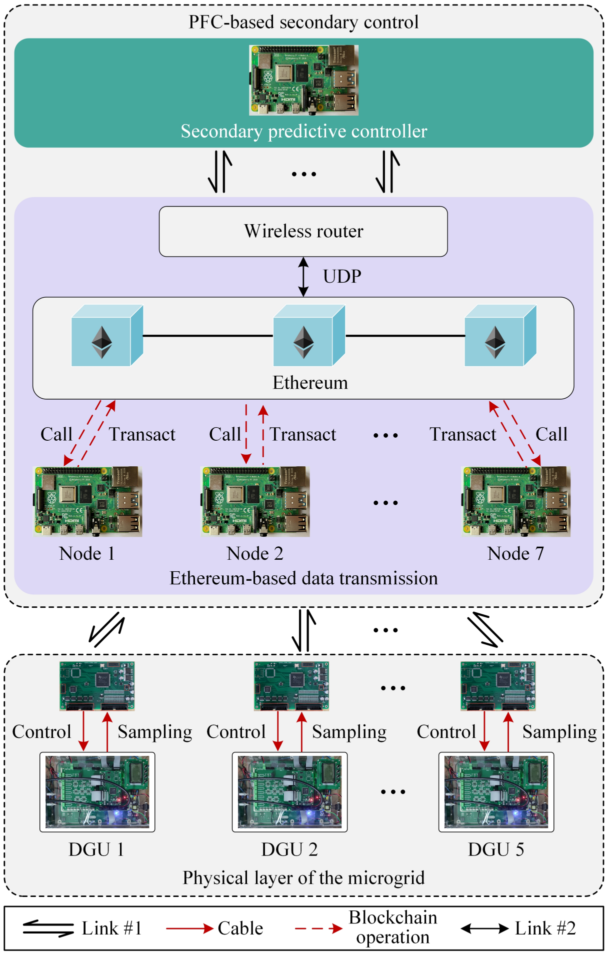
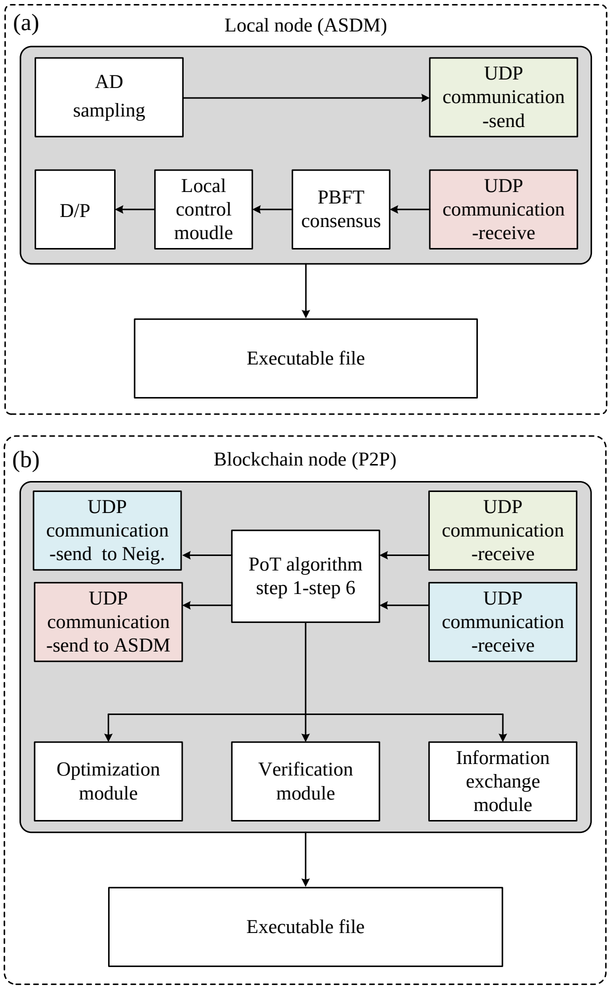
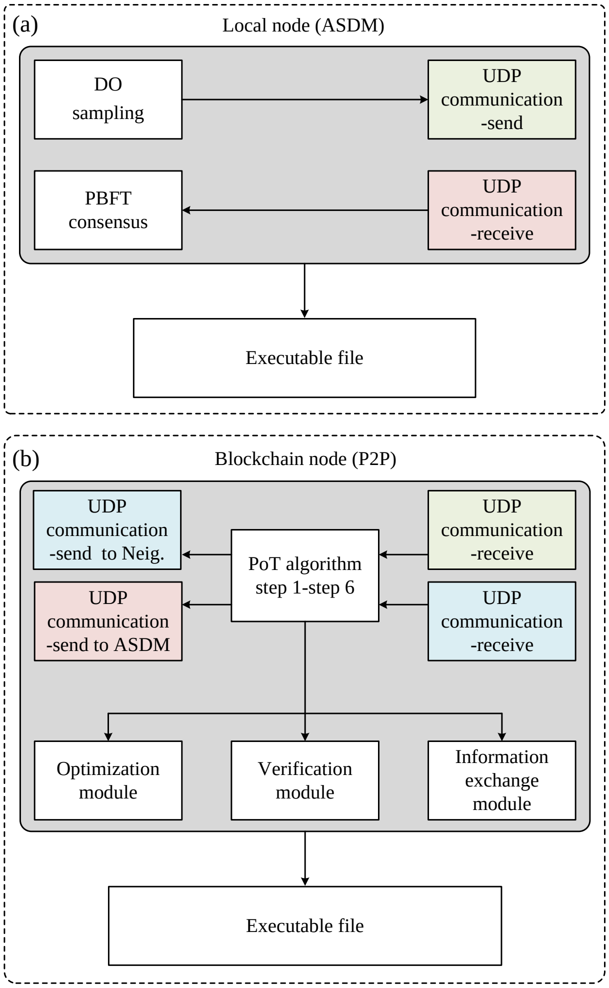


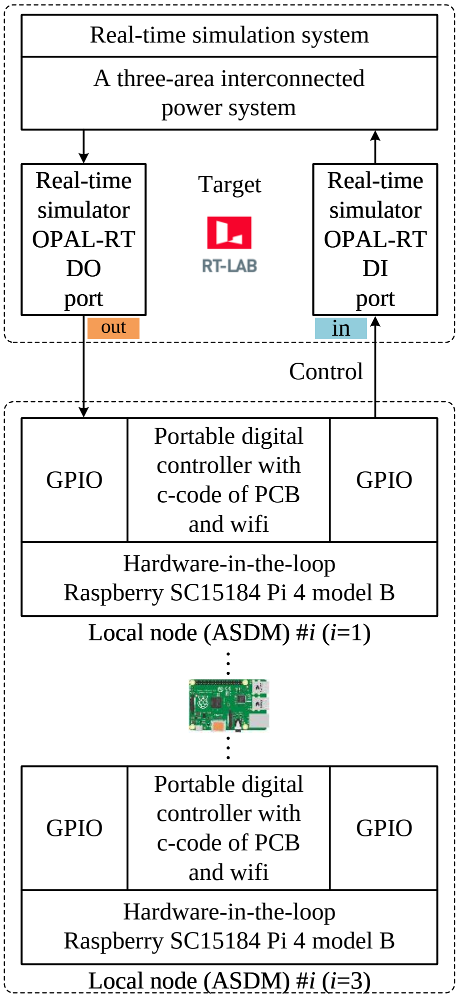
Fig. 17: Data flow of the PFC-assisted microgrid system based on the Ethereum platform (Application 3). Link #1 and Link #2 refer to the communication link between external data and the Ethereum platform, and the communication link between Ethereum nodes, respectively.


(a)
Local node (ASDM)
AD sampling
UDP communication -send
D/P
Local control moudle
PBFT consensus
UDP communication -receive
Executable file
(b)
Blockchain node (P2P)
UDP communication -send to Neig.
PoT algorithm step 1-step 6
UDP communication -receive
UDP communication -send to ASDM
UDP communication -receive
Optimization module
Verification module
Information exchange module
Executable file

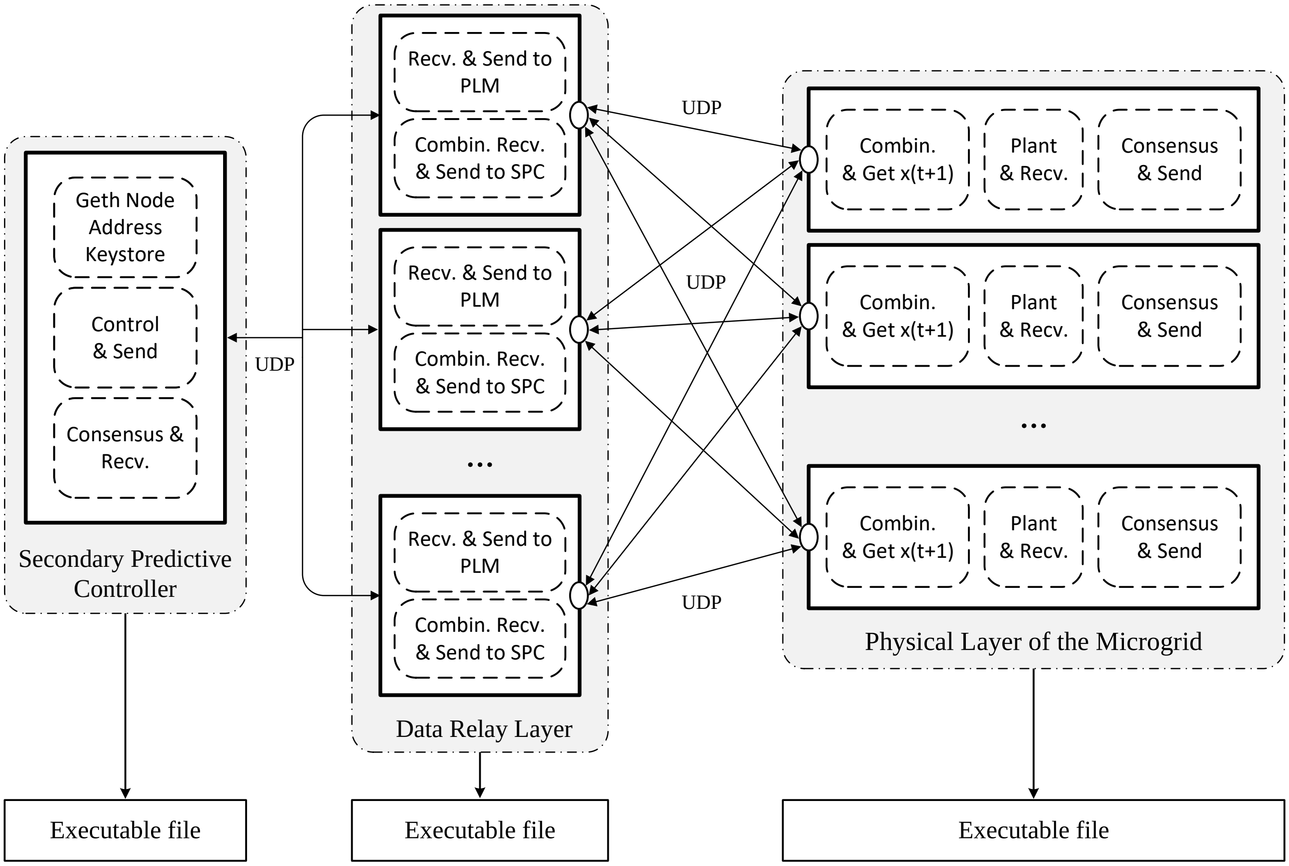
Supplementary Fig. 3: PoT code structure for Application 1.


(a)
Local node (ASDM)
DO sampling
UDP communication -send
PBFT consensus
UDP communication -receive
Executable file
(b)
Blockchain node (P2P)
UDP communication -send to Neig.
PoT algorithm step 1-step 6
UDP communication -receive
UDP communication -send to ASDM
UDP communication -receive
Optimization module
Verification module
Information exchange module
Executable file

Supplementary Fig. 4: PoT code structure for Application 2.


Real-time simulation system
A three-area interconnected power system
Real-time simulator OPAL-RT DO port
Target
RT-LAB
Real-time simulator OPAL-RT DI port
out
in
Control
GPIO
Portable digital controller with c-code of PCB and wifi
GPIO
Hardware-in-the-loop Raspberry SC15184 Pi 4 model B
Local node (ASDM) #i (i=1)
GPIO
Portable digital controller with c-code of PCB and wifi
GPIO
Hardware-in-the-loop Raspberry SC15184 Pi 4 model B
Local node (ASDM) #i (i=3)

Supplementary Fig. 5: Architecture of the HIL test system in Application 2. DO and DI respectively refer to the digital input and output.



Supplementary Fig. 6: PFC code structure for Application 3.

C2.4: *Also the paper claimed PoT strengthens security, but the mechanism by which it achieves this needs elaboration. Does PoT introduce new vulnerabilities or security considerations compared to traditional consensus mechanisms?*

Response:

Thank you sincerely for your constructive comments and valuable suggestions. For the two points you are concerned, we will respond to each of them below.

1) We apologize for not clarifying the mechanism by which PoT strengthens the security of REPSs in the original manuscript. According to your suggestion, we have added some elaborations in the revised manuscript. Specifically, the mechanism to enhance the security of real-time control systems in PoT is mainly reflected in the following four aspects:

- A majority consensus for both raw interaction data y and control commands u. Step 2 and step 7 in Fig. 1 protect each of the two types of data in the control system. Since the raw interaction data is the basis for controller computation, all peers on the P2P network are involved in validating this data, which greatly ensures the security of the original data. There are two reasons for doing so. One reason is that the more peers involved in the validation, the more secure it is. The second reason is that the validation here is a simple value comparison, which does not consume too much time and computing resources. In this way, it allows more nodes to participate.

- A selection or authorization mechanism for peers in PoT obtained based on game theory. After obtaining the trusted raw interaction data, PoT authorizes the nodes in the P2P network based on the game-derived strategy. This algorithm enables the PoT to be intelligent and efficient. Intelligence is reflected in the fact that PoT can give different authorization probabilities to nodes based on their different performances. In this way, PoT introduces new uncertainties into the control system, making it more difficult for malicious adversaries to carry out targeted attacks and improving the security of the system. In other words, PoT increases the information entropy of the data in the control system. The efficiency is reflected in the fact that the authorized nodes form a delegation network of smaller size. In this way, subsequent problem solving occurs only on the delegates, improving the efficiency and real-time performance of PoT.

- The relative optimality verification and system stability verification in PoT. Relative optimality verification somewhat excludes some attack signals, as actual signals could often yield smaller performance metrics than attack signals. In addition, the verification mechanism of relative optimality can make it easier for the PoT to access the available control commands in each consensus round, which improves the real-time performance of the PoT to a certain extent, and also motivates the delegates to solve the problem. The verification of the stability conditions of the system ensures that the PoT ultimately yields a solution that at least stabilizes the system, which provides a minimum level of security for the control system.

- An evaluation mechanism for delegations in PoT. This mechanism works well to exclude dishonest nodes within the delegation. Evaluations can be performed against delegates based on the history of the PoT consensus.

These are the efforts made by PoT to strengthen the security of REPSs. It can be seen that PoT retains some of the basic security elements of blockchain technology, such as majority rule principle, multi-party verification and multi-party solving. However, in order to facilitate real-time control systems such as REPSs, PoT has had to make certain trade-offs in terms of security and real-time performance. This is because if a high level of real-time performance cannot be guaranteed, then the system will definitely be destabilized, at which point the discussion of the security of the controller will be meaningless. To this end, PoT replaces the hash puzzle in traditional blockchain with an optimization problem corresponding to the control task of interest. This optimization problem is much less difficult to solve than the hash problem. At this point, the time consumed by peers in PoT to solve the problem is very small, which can meet the real-time requirements of the control system.

In summary, although a little security is sacrificed to some extent for the essential real-time nature compared to traditional hash-puzzle-based blockchain, the above mechanisms still greatly reduce the likelihood of a successful attack occurring. This makes PoT greatly improve the security of the REPS while ensuring the basic performance requirements of it.

2) Possible vulnerabilities or security considerations introduced by PoT are in the following three areas.

One is that the protection of the raw interaction data y does not involve problem solving, which may introduce security vulnerabilities. In this phase, any P2P network node can submit data with no access conditions. However, adding a problem solving at this stage as well and letting only the node that gets the correct solution submit the data would result in additional time consumption. This in turn leads to the real-time nature of PoT not meeting the requirements of control systems like REPSs. A feasible direction for the above problem is to further design algorithms that are not time-consuming to enhance the protection of the raw interaction data.

The second is that consensus for control commands based on the majority rule principle takes place in delegations, which may raise security concerns. Since the number of delegates is limited and these nodes have the right to solve the optimization problem, the delegation network, indicated by the light blue background in Fig. 1, may be at risk of centralization. The control system will be negatively affected by a successful attack if there are a large number of dishonest delegates, or if a majority of delegates are attacked in this delegation. This means that inappropriate authorization of delegation may result in threats to the security and stability of REPSs. This indicates that PoT places high demands on the authorization algorithm involved in step 3 of Fig. 1. The algorithm needs to try to select delegates with high security and good computational ability. Therefore, the development of algorithms that can efficiently select suitable delegates in real time is a challenging problem worth investigating to further enhance the security of PoT.

Finally, as you commented in C2.1, we have discarded the complex and time-consuming hash puzzle, in favour of an optimization problem that is more conducive to the implementation of the control task and is of moderate difficulty. This approach is an unavoidable choice due to the real-time requirements of the control system, but in some scenarios it does introduce a certain degree of security vulnerability to PoT.

In summary, PoT taps into the security features of the blockchain as much as possible while ensuring real-time performance. In terms of security alone, PoT is really not perfect compared to traditional consensus mechanisms, but it finds a skillful compromise under various considerations such as security and real-time performance of real-time control systems.

To address your concerns, we have included a discussion of the mechanism by which PoT strengthens security, and what still needs to be further improved in terms of security for PoT in the revised manuscript.

It is hoped that the narrative we have added would address your concerns.

Based on the reviewer's comments, the authors have made the following modifications to the content of the manuscript:

[Section II.B, page 5, highlighted in red]
“ ... Taking a large-scale REPS containing N Distributed Generation Units (DGUs) as an example, some necessary elaboration on the mechanism by which PoT strengthens the security of REPSs and clarifications on the deployment and execution of the PoT-based regulation scheme are given below. ”

“ ... At this stage, the MRP is executed, protecting the source data (measurements) like a practical Byzantine fault tolerance protocol. ... ”

“ ... It should be mentioned that only peers authorized as delegates are responsible for solving the optimization problem. This imbues PoT with intelligence and efficiency, allowing it to make the best allocation of computation and consensus tasks based on the likelihood of each node receiving an error message and its past loyalty. It also introduces new uncertainties into the system, making it more difficult for malicious adversaries to launch attacks, thus improving the security of the system. ”

[Section II.B, page 6, highlighted in red]
“ ... Furthermore, in step 7, the MRP is performed to protect the target data (control commands) from potential attacks or disloyalty, thereby obtaining a trusted control input. This control signal is applied to the actuator in step 8 to complete the regulation of the REPSs. Finally, in step 9, a smart contract is developed to count the credit score of each delegate participating in the consensus and give corresponding feedback. Recall that in step 3, the system strategically elects delegates that are favorable for output regulation. This strategy relies on the static probability given by the prior knowledge of the vulnerability of different nodes to cyber-attacks. In addition, the smart contract further evaluates these delegate nodes and decides whether to remove a node from the delegation. The election mechanism and the smart contract both complement each other to form a security countermeasure that utilizes both the prior and the posterior knowledge. A priori election strategy resists malicious attacks from the outside, while a posteriori smart contract defends against dishonest behavior occurring inside the blockchain network. ”

“ On the one hand, using the MRP twice in two steps of PoT makes it possible to protect both measurements and control commands of the REPS. ... ”

[Section VIII, page 15, highlighted in red]
“ ... Moreover, to facilitate real-time control of REPSs, PoT makes certain compromises in security compared with traditional consensus mechanisms. In PoT, for example, the problems that peers solve are relatively simple, and the data transmission does not involve processes such as encryption and decryption. Therefore, it is meaningful and challenging to further enhance the security and privacy of PoT while ensuring its real-time nature. ... ”

C2.5: *While the authors mentioned results showing PoT improves security and computing capability, the data itself is not presented. Including specific performance metrics and how they compare to existing solutions would strengthen the conclusions.*

Response:

We sincerely thank you for your insightful and helpful comments. We apologize for not providing sufficient data in the original manuscript to support the conclusion that PoT improves the security and computing capability of REPSs. Based on your suggestions, we have made the following improvements from a data perspective in the revised manuscript. It is worth mentioning that for a comparison of the results in waveform form, please refer the response to your previous comment, i.e., **C2.2**.

(1) Basic data results in Application 1

In the results section of the revised manuscript, Fig. 10 gives some basic data records of the attacks suffered by REPSs under PoT, including the original attack signals launched by attackers and the actual attack signals encountered by the system under PoT defense, the moments of the original initiated attacks, and the moments of occurrence of these two. This figure directly depicts the raw data and visually demonstrates the effectiveness of PoT in attenuating attacks.

(2) Comparison of security and control performance metrics in Application 1

In the revised manuscript, PoT has been compared with the existing real-time resilient control method [13] and with the existing blockchain-based security control method [56] in Application 1. The quantitative results are presented in TABLE IV, Fig. 11, and Fig. 12.

Specifically, TABLE IV gives the probability of secure data transmission in the microgrid system under the three methods. At this point, the probability that each generation unit in the microgrid under PoT gets a trustworthy control command is about 95%.

Classical metrics including attack probability, deviation between the received value and the sent value, the security performance metric, the control performance metric, etc. are employed for data illustration. Specific expressions for these indicators are given below. In order to reflect the trustworthiness of the data obtained by REPSs under PoT, the security performance metric is set as

$$\begin{aligned} H_\alpha = \sum_{t=t_{\text{sec}}}^{t_{\text{sec}}+T} (\sum_{i=1}^{N} (\sum_{j\in\mathcal{N}_i^c} (\frac{1}{V_{j,\max}^{org}} |\tilde{y}_{ij}^{V}(t) - y_j^{V,org}(t)| + \frac{1}{I_{tj,\max}^{org}} |\tilde{y}_{ij}^{I}(t) - y_j^{I,org}(t)|) \\ + \frac{1}{u_{i,\max}^{org}} |\tilde{u}_i(t) - u_i^{org}(t)|)) \end{aligned} \quad \text{(Eq. 1)}$$

where the meanings of the involved variables are presented in Supplementary Table 8. It should be noted that $V_{j,\max}^{org}$, $I_{tj,\max}^{org}$, and $u_{i,\max}^{org}$ are used for normalization. Similarly, in order to reflect the effectiveness of REPSs under PoT in accomplishing the given control tasks, the control performance metric is defined as

$$J_{task} = \sum_{t=t_{\text{sec}}}^{t_{\text{sec}}+T} \sum_{i=1}^{N} (\frac{1}{\bar{V}_{i,\max}^{org}} |\bar{V}_i(t) - V^{ref}| + \sum_{j\in\mathcal{N}_i^c} (\frac{1}{I_{tj,\max}^{org}} |\frac{I_{tj}^{org}(t)}{\theta_j^s} - \frac{I_{ti}^{org}(t)}{\theta_i^s}|)) \quad \text{(Eq. 2)}$$

where t_{sec}, T and N have the same meaning as given in Supplementary Table 8, $\bar{V}_i(t)$ denotes the estimated value of the voltage, as given in (18) in the Supplementary File, variables V^{ref}, $\mathcal{N}_i^c$ and θ_i have the same meaning as those in the manuscript, and the meanings of the other variables are presented in Supplementary Table 9. As a result of the attack, all of the above metrics are accumulated as the system runs. Therefore, the system responses within 15 s after the secondary control is activated are selected for statistical and illustrative purposes for all subsequent results.

The statistical results of the performance metrics H_α and J_{task} are given for 20 independent trials under different methods, as shown in Fig. 11. Fig. 11(a) shows the results of the security performance metric H_α to demonstrate the effectiveness of different methods for defending against cyber-attacks. Fig. 11(b) presents the curves of the control performance metric J_{task} to show how well the different methods accomplish the control task. The ratio of successful defence w.r.t. the total attack probability for PoT over 20 independent trials is given in Fig. 12 to demonstrate the defensibility of PoT against cyber attacks. The figure illustrates the long-term stable defence performance of the PoT-based approach.

Based on the above results, it can be seen that the defense role imparted by PoT from the physical level greatly reduces the likelihood of REPSs being attacked compared with the existing real-time control method. Compared with the existing blockchain-based security control method, the probability of data being attacked in the system under PoT is smaller, i.e., the security is better. It can be seen that the increase in security here is not as significant as the increase compared to the existing resilient control method, which demonstrates the effectiveness of blockchain in improving data security. However, in terms of performance metrics, the proposed PoT-based control method outperforms the existing blockchain-based security control method. The essential reason for this is that in the existing methods blockchain only provides the system with a mechanism for the secure data transmission, and in the consensus mechanism itself it does not take into account the control tasks, system stability, etc. In particular, the method in [56] only protects the measurement data but not the control commands, and cannot compensate for communication constraints in a distributed fashion. To sum up, from the data-based comparison and discussion above, it can be seen that PoT demonstrates better performance than the existing methods in terms of both security and performance metrics.

(3) Computing performance of PoT in Application 1

The above comparisons indicate that PoT has, to some extent, tapped into the computing power of the entire P2P network to facilitate the accomplishment of control tasks. In addition, we give a more detailed discussion below on the point of PoT improving computing capability.

In order to embody seven blockchain nodes that may be different from each other in practice, we choose several optimization solvers of different types and parameters. The solvers used, with version information, are listed in Supplementary Table 7. The specific settings of each solver are presented in Supplementary Table 2. Figure 4 gives the performance of different solvers in solving the optimization problem of Application 1 for a single time. From the results in Figure 4, it can be seen that different solvers take different times for the same optimization problem. Meanwhile, the optimality of the solutions obtained by different solvers for the same optimization problem varies slightly. For example, there are solvers that consume a little bit more time, but give solutions with a lower cost function. In addition, it can be seen that the same solver performs differently in different settings.

According to the delegation activation and optimality verification mechanisms of PoT, peers with different characteristics can be completely distinguished by three attributes, i.e., (a) being selected in a delegation, (b) solution satisfying the constraints, and (c) solution winning consensus. In order to evaluate the performance of each node in solving the optimization problem, we have designed a scoring rule based on these three attributes, as shown in Supplementary Table 3. It can be seen that each node will get one of the score flags in 0, −1, 1 and 2 during the operation of the system. Based on these score flags, Supplementary Fig. 7 gives the performance of nodes with different solvers in consensus throughout the PoT-based secondary control. In addition, Supplementary Fig. 8 gives a more visual representation of the cumulative number of times each node has won in the PoT consensus mechanism throughout the control process. As can be seen from Supplementary Fig. 7 and 8, different nodes won the PoT consensus at different moments during the operation of the system, and all of them obtain the score flag of 2 more than once. In other words, combining the two factors of solution optimality and solution time, there is not a particular solver that is used all the time during the system operation, but rather different types of solvers alternately win the PoT consensus. From the data shown in the figures, under PoT, the distinct characteristics of blockchain nodes with different types of solvers are explored, which improves the computing power of the controller.

It is worth mentioning that solvers will exhibit different performance for different optimization problems. Therefore, the solver network induced by PoT is more robust throughout the whole regulation process, and also with respect to the variety of optimization problems associated with control tasks. For example, the scale or type of the optimization problem may undergo significantly alterations if the application scenario is changed. At this point, the solver network formed by the PoT mechanism would match the system with the most suitable solution for the control task.

In general, the process of obtaining optimal values for optimization problems with constraints is often time-consuming. It can be seen from Figure 4 that the longer waiting time gives the system a higher probability of obtaining a better solution. However, it instead introduces greater time delays, which can compromise the stability of the system. Therefore, on one hand, for complex optimization problems, waiting for the solver to find the optimal value may result in a lack of real-time performance that does not meet the requirements of the control system. On the other hand, within the waiting time that satisfies real-time requirements of the system, it is very likely that the solver will not be able to find the optimal solution. If the blockchain adopts an absolute verification mechanism similar to the one in Ref. [8] would result in REPSs having no control commands available for the current round of consensus, which would degrade the control performance of the system. Therefore, in contrast to this absolute optimality verification mechanism, the relative optimality verification mechanism in PoT, as shown in Figure 8 of the Supplementary File, allows REPSs to get available control commands at each round of consensus. This taps into the potential active role of each peer for the given control task, increasing the computing power of the entire network and improving the real-time performance of PoT to some extent. To sum up, the approach of letting individual peers solve the optimization problem corresponding to the control task, coupled with a relatively optimal verification mechanism, allows PoT to present benefits in terms of computing power.

(4) Comparative table of basic data, and comparison of security and control performance metrics in Application 2

For Application 2, the quantitative comparison of PoT with the method in the latest published article is provided in the Supplementary File. The corresponding results are presented in Supplementary Table 4, Supplementary Fig. 9, and Supplementary Fig. 10. In order to avoid similarity to the figures in Application 1, the recorded security data and their analysis are given in the Supplementary File and not presented in the main body of the manuscript.

Specifically, Supplementary Table 4 gives the security probabilities of the three-area power system under different LFC methods. Moreover, in order to quantify the trustworthiness of the data after it has been transmitted through the network, the security performance metric for the multi-area power system under load frequency control is set as follows

$$\begin{aligned}H_{\alpha,lfc} = \sum_{t=t_0}^{t_0+T}(\sum_{i=1}^{N}(\sum_{j\in\mathcal{N}_i^c}(\frac{1}{\Delta P_{tie,j,\max}^{org}}|\tilde{x}_{ij}^{P}(t) - x_j^{P,org}(t)| + \frac{1}{\Delta f_{j,\max}^{org}}|\tilde{x}_{ij}^{f}(t) - x_j^{f,org}(t)|) \\ + \frac{1}{u_{i,\max}^{org}}|\tilde{u}_i(t) - u_i^{org}(t)|))\end{aligned} \quad \text{(Eq. 3)}$$

where the meanings of the involved variables are presented in Supplementary Table 10. Variables $\Delta P_{tie,j,\max}^{org}$, $\Delta f_{j,\max}^{org}$, and $u_{i,\max}^{org}$ are used for normalization. Similarly, in order to quantify the effectiveness of different methods for load frequency control, the control performance metric of the system is designed as follows

$$J_{task,lfc} = \sum_{t=t_0}^{t_0+T}\sum_{i=1}^{N}(\frac{1}{ACE_{i,\max}^{org}}|ACE_i^{org}(t)| + \frac{1}{u_{i,\max}^{org}}|u_i^{org}(t)|) \quad \text{(Eq. 4)}$$

where the meanings of t_0, T and N are the same as those given in Supplementary Table 10, the meanings of the remaining variables are explained in Supplementary Table 11. The statistical results of the performance indicators $H_{\alpha,lfc}$ and $J_{task,lfc}$ during the operation of the three-area power system under different methods are given in Supplementary Fig. 9(a) and Supplementary Fig. 9(b), respectively. It can be seen that the performance metrics $H_{\alpha,lfc}$ and $J_{task,lfc}$ of the power system with the PoT-based LFC strategy are better than that of the power system with the established approach. Further, Supplementary Fig. 10 shows the security performance of PoT in distributed regulation of the power system under 20 independent repeated trials. Consistent with the results in Application 1, PoT enhances the security of load frequency control in the face of cyber threats due to characteristics such as the fact that PoT protects both the raw interaction data and the target data.

(5) Comparative table of basic data, and comparison of security performance metrics in Application 3

In the revised manuscript, DPoT is compared with the state-of-the-art approach for Application 3. The corresponding results are shown in Fig. 18 of the revised manuscript. It can be seen that even the simplest PoT variants still contribute to the security control of REPSs. Similar to Application 1 and Application 2, the quantitative comparison of PFC with the existing method is presented. The corresponding results are shown in Supplementary Table 5, Supplementary Fig. 11 and Supplementary Fig. 12.

Specifically, the security probability of PFC-based secondary control for the dc microgrid system under different methods is given in Supplementary Table 5. Moreover, the security performance metric of the dc microgrid in the centralized secondary control paradigm is given as

$$\begin{aligned}H_{\alpha,pfc} = \sum_{t=t_{\sec}}^{t_{\sec}+T}(\sum_{i=1}^{N}(\frac{1}{V_{i,\max}^{org}}|\tilde{y}_i^V(t) - y_i^{V,org}(t)| + \frac{1}{I_{ti,\max}^{org}}|\tilde{y}_i^I(t) - y_i^{I,org}(t)| \\ + \frac{1}{u_{i,\max}^{org}}|\tilde{u}_i(t) - u_i^{org}(t)|))\end{aligned} \quad \text{(Eq. 5)}$$

where $\tilde{y}_i^I(t)$ and $\tilde{y}_i^V(t)$ represent voltage and current values of DGU i actually used by the centralized controller, respectively, the meanings of the other variables are the same as those in Supplementary Table 8. To reflect the effectiveness of PFC-based secondary control in accomplishing the regulation tasks given by (12) and (13) of the Supplementary File, the control performance metric is defined as

$$J_{task,pfc} = \sum_{t=t_{\mathrm{sec}}}^{t_{\mathrm{sec}}+T} \Big(\sum_{i=1}^{N} \Big(\frac{1}{V_{i,\max}^{org}} \Big| \frac{1}{N} \sum_{i=1}^{N} V_i(t) - V^{ref} \Big| + \sum_{j \in \mathcal{N}_i^c} \Big(\frac{1}{I_{tj,\max}^{org}} \Big| \frac{I_{tj}^{org}(t)}{\theta_j^s} - \frac{I_{ti}^{org}(t)}{\theta_i^s} \Big| \Big) \Big) \Big) \qquad \text{(Eq. 6)}$$

where the meanings of the variables are shown in Supplementary Table 8 and Supplementary Table 9. The security and control performance metrics of the microgrid under the existing control method as well as the PFC-based secondary control method are available in Supplementary Fig. 11(a) and (b). It can be seen that the PFC-based secondary control exhibits better security and control performance compared with the existing security secondary control strategy. Further, Supplementary Fig. 12 shows the security performance of PFC in centralized regulation of dc microgrids under 20 independent repeated trials. As can be seen from the figure, the PFC-based secondary control has shown satisfactory safety performance in a number of tests. In addition, PFC, as a simplified version of PoT, brings slightly less security to the REPSs system than PoT, which is supported by comparing the results shown in Fig. 12 and Supplementary Fig. 12.

To address your concerns, we have added data analysis as well as specific performance metric comparisons to the revised manuscript, to strengthen the conclusions that PoT improves the security and computing capability of REPSs. In order to avoid an overly lengthy body of the manuscript, the comparative results and analytical discussion of some of the data are included in the supplementary file.

Based on the reviewer's comments, the authors have made the following modifications to the content of the manuscript:

[Section V, page 9, highlighted in red]

" In addition to the waveform results and associated discussion above, quantitative comparisons and analysis are given. Specifically, TABLE IV gives the probability of secure data transmission in the microgrid system under the three methods. The moments of the original attack and the moments of the effective attack after PoT on all 15 signals in the microgrid system are given in Fig. 10(a). Taking the control signal u_1 of the 1st DGU as an example, the original attacked signal and the attacked signal under PoT are given in Fig. 10(b). To better illustrate the effectiveness of the proposed method from a data perspective, the security performance metric H_α and the control performance metric J_{task} are defined as (30) and (31) in Supplementary Note 3, respectively. Fig. 11(a) shows the results of H_α for the REPSs in 20 independent trials under three different methods to demonstrate the effectiveness of different approaches for defending against cyber-attacks. Fig. 11(b) presents the results of J_{task} in the same scenario to show how well the different methods accomplish the control task. The ratio of probability of successful defense w.r.t. probability of unsuccessful defense for PoT over 20 independent trials is given in Fig. 12 to intuitively demonstrate the defensibility of PoT against cyber attacks. The figure illustrates the long-term stable defense performance of the PoT-based approach. "

[Section V, page 10, highlighted in red]

" Based on the data presented in the results above, it can be seen that the defense role imparted by

PoT from the physical level greatly reduces the likelihood of REPSs being attacked compared with the existing real-time control method. As shown in TABLE IV, the security of the microgrid system with the proposed method reaches 95%, which are superior to the existing methods. In terms of security, the improvements that PoT brings compared to the existing blockchain-based security control method are not as significant as compared to the traditional resilient method. This demonstrates the effectiveness of blockchain in improving data security. However, in terms of performance metrics shown in Fig. 11, the proposed PoT-based control method still outperforms the existing blockchain-based security control method. ”

[Section VI, page 12, highlighted in red]
“ For comparison, the PoT-based LFC approach and the normal cooperation-based resilient LFC strategy in [57] are tested in the presence of cyber attacks, and the system responses are shown in Fig. 16. The results indicate that the system subjected to a cyber-attack becomes unstable when utilizing a traditional resilient LFC approach. When using PoT-based LFC, the multi-area power system subjected to the cyber-attack features a smooth response and complies with the generation rate constraints and load reference setpoint constraints. Additionally, the quantitative results, including the performance metrics for both the existing and PoT-based methods, are presented in Supplementary Table 4 and Supplementary Fig. 9. The definitions of these metrics are given in (46) and (47) of Supplementary Note 4. The data in the figure show that $H_{\alpha,lfc}$ and $J_{task,lfc}$ of the proposed method are smaller than those of the existing approach. Supplementary Fig. 10 shows the consistent performance of the PoT method over multiple trials. To sum up, the above analysis confirm that the proposed PoT-based distributed LFC algorithm can both guarantee the security of the system and optimise its operation. ”

[Section VII, page 14, highlighted in red]
“ To demonstrate the effectiveness of the proposed method, it is compared with the centralized resilient control method in [58]. As illustrated in Fig. 18(a), the output voltage and current exhibit varying degrees of oscillation under the existing resilient method, and the expected current sharing is not well accomplished. The responses of the dc microgrid system under the PFC-based secondary control method, as depicted in Fig. 18(b), indicate that the average of the output voltages is regulated to the desired level around 48 V and the output currents are accurately shared in the ratio of $1:1:1.8:1.8:1.8$. In addition, some quantitative results are given in Supplementary Table 5, Supplementary Fig. 11 and Supplementary Fig. 12, including comparisons of the security probability as well as performance metrics with the established methods. From these results, it can be seen that PFC-based secondary control is still capable of realizing the desired regulation goals of dc microgrids and actively defending the microgrids against cyber-attacks. ... ”

Based on the reviewer’s comments, the authors have made the following modifications to the content of the supplementary file:

[Section VI.F, page 31, highlighted in red]
“ To reflect the trustworthiness of the data obtained by REPSs under PoT, the security performance

metric is set as

$$H_{\alpha} = \sum_{t=t_{\text{sec}}}^{t_{\text{sec}}+T} (\sum_{i=1}^{N} (\sum_{j\in\mathcal{N}_i^c} (\frac{1}{V_{j,\max}^{org}} |\tilde{y}_{ij}^{V}(t) - y_j^{V,org}(t)| + \frac{1}{I_{tj,\max}^{org}} |\tilde{y}_{ij}^{I}(t) - y_j^{I,org}(t)|) \\ + \frac{1}{u_{i,\max}^{org}} |\tilde{u}_i(t) - u_i^{org}(t)|)) \tag{30}$$

where the meanings of the involved variables are presented in Supplementary Table 8. It should be noted that $V_{j,\max}^{org}$, $I_{tj,\max}^{org}$, and $u_{i,\max}^{org}$ are used for normalization. Similarly, in order to reflect the performance of the control strategy in accomplishing a given control task of the REPSs, the control performance metric is defined as

$$J_{task} = \sum_{t=t_{\text{sec}}}^{t_{\text{sec}}+T} \sum_{i=1}^{N} (\frac{1}{\bar{V}_{i,\max}^{org}} |\bar{V}_i(t) - V^{ref}| + \sum_{j\in\mathcal{N}_i^c} (\frac{1}{I_{tj,\max}^{org}} | \frac{I_{tj}^{org}(t)}{\theta_j^s} - \frac{I_{ti}^{org}(t)}{\theta_i^s} |)) \tag{31}$$

where t_{sec}, T and N have the same meaning as given in Supplementary Table 8, $\bar{V}_i(t)$ is presented in (18), variables V^{ref}, $\mathcal{N}_i^c$ and θ_i have the same meaning as those in the manuscript, and the meanings of the other variables are available in Supplementary Table 9. "

[Section VII.D, page 35, highlighted in red]

" In order to quantify the trustworthiness of the data after it has been transmitted through the network, the security performance metric for the multi-area power system under load frequency control is set as follows

$$H_{\alpha,lfc} = \sum_{t=t_0}^{t_0+T} (\sum_{i=1}^{N} (\sum_{j\in\mathcal{N}_i^c} (\frac{1}{\Delta P_{tie,j,\max}^{org}} |\tilde{x}_{ij}^{P}(t) - x_j^{P,org}(t)| + \frac{1}{\Delta f_{j,\max}^{org}} |\tilde{x}_{ij}^{f}(t) - x_j^{f,org}(t)|) \\ + \frac{1}{u_{i,\max}^{org}} |\tilde{u}_i(t) - u_i^{org}(t)|)) \tag{46}$$

where the meanings of the involved variables are presented in Supplementary Table 10. Variables $\Delta P_{tie,j,\max}^{org}$, $\Delta f_{j,\max}^{org}$, and $u_{i,\max}^{org}$ are used for normalization. Similarly, in order to quantify the performance of different load frequency control methods, the control performance metric of the system is designed as follows

$$J_{task,lfc} = \sum_{t=t_0}^{t_0+T} \sum_{i=1}^{N} (\frac{1}{ACE_{i,\max}^{org}} |ACE_i^{org}(t)| + \frac{1}{u_{i,\max}^{org}} |u_i^{org}(t)|) \tag{47}$$

where the meanings of t_0, T and N are the same as those given in Supplementary Table 10, and the meanings of the remaining variables are explained in Supplementary Table 11. "

[Section VIII, page 37, highlighted in red]

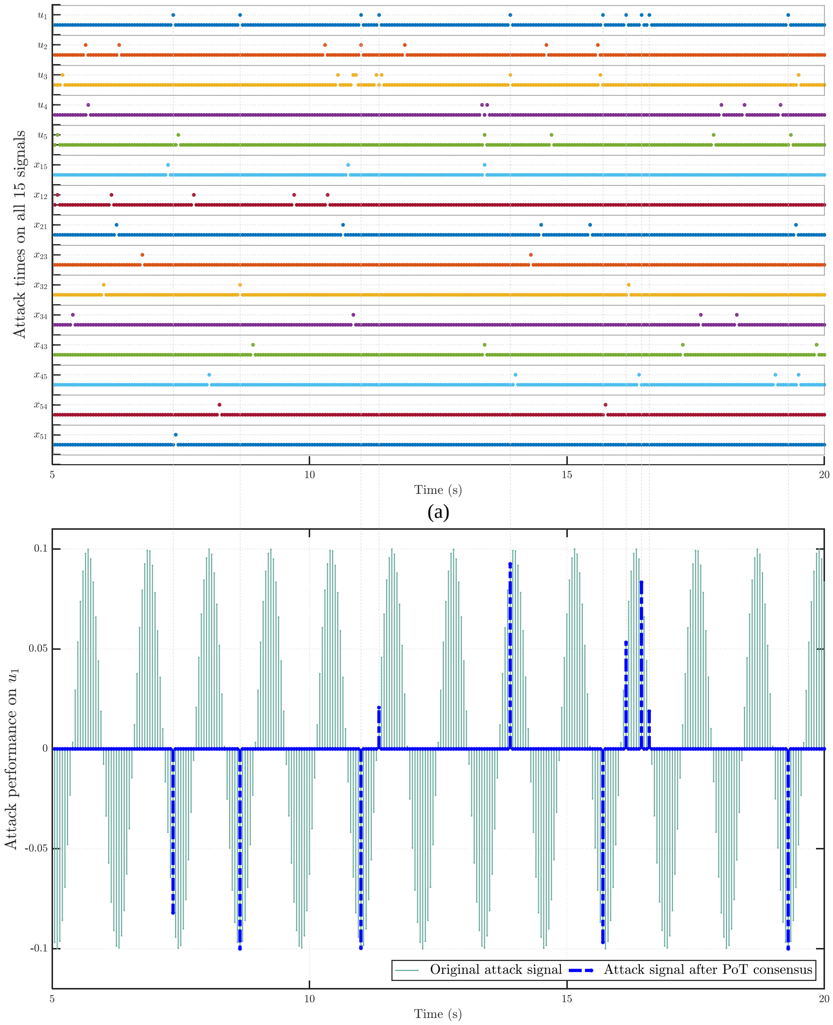
“ Similar to Application 1 and Application 2, the security performance metric of the dc microgrid in the centralised secondary control paradigm is given as

$$H_{\alpha,pfc} = \sum_{t=t_{\mathrm{sec}}}^{t_{\mathrm{sec}}+T} \Big(\sum_{i=1}^{N} \Big(\Big(\frac{1}{V_{i,\max}^{org}} |\tilde{y}_i^V(t) - y_i^{V,org}(t)| + \frac{1}{I_{ti,\max}^{org}} |\tilde{y}_i^I(t) - y_i^{I,org}(t)| + \frac{1}{u_{i,\max}^{org}} |\tilde{u}_i(t) - u_i^{org}(t)|\Big)\Big) \tag{49}$$

where $\tilde{y}_i^I(t)$ and $\tilde{y}_i^V(t)$ represent voltage and current values of DGU i actually used by the centralized controller, respectively, the meanings of the other variables are the same as those in Supplementary Table 8. In order to evaluate the performance of various secondary control methods for accomplishing the regulation tasks given by (12) and (13), the control performance metric is defined as

$$J_{task,pfc} = \sum_{t=t_{\mathrm{sec}}}^{t_{\mathrm{sec}}+T} \Big(\sum_{i=1}^{N} \Big(\frac{1}{V_{i,\max}^{org}} \Big|\frac{1}{N} \sum_{i=1}^{N} V_i(t) - V^{ref}\Big| + \sum_{j \in \mathcal{N}_i^c} \Big(\frac{1}{I_{tj,\max}^{org}} \Big|\frac{I_{tj}^{org}(t)}{\theta_j^s} - \frac{I_{ti}^{org}(t)}{\theta_i^s}\Big|\Big)\Big)\Big) \tag{50}$$

where the meanings of the variables are shown in Supplementary Table 8 and Supplementary Table 9. ”



(a)

(b)

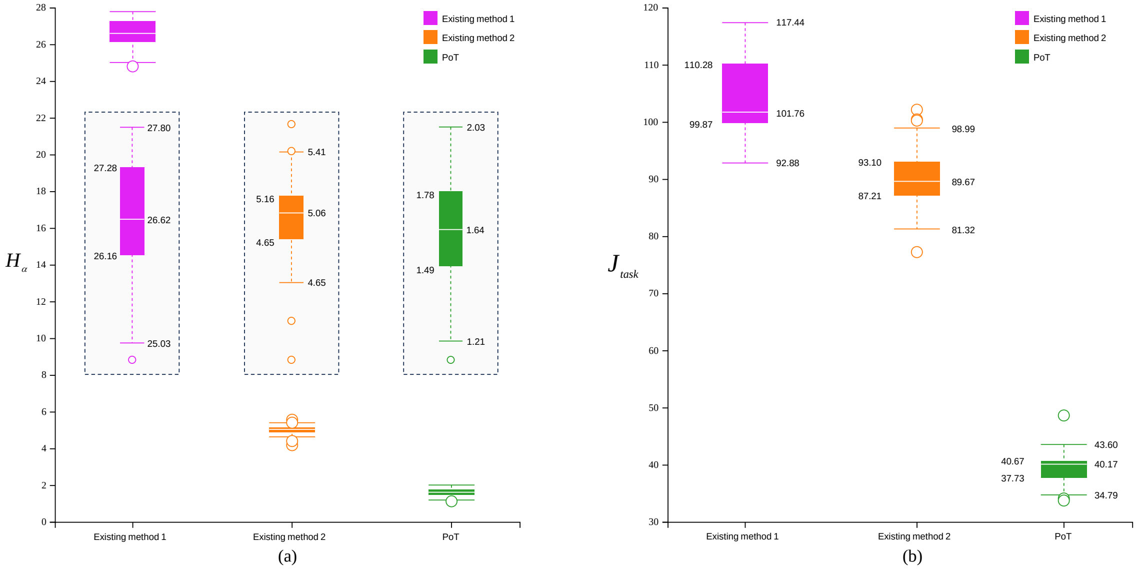
Fig. 10: (a) Moment of occurrence of cyber-attacks on all 15 signals of the dc microgrid, and (b) defend performance against attacks on the control signal u_1 of the dc microgrid with PoT-based secondary control. Near dense and sparse points in (a) constitute 1 set of data, and there are 15 sets of data in total. In each set of data, the dense and sparse dots represent the original attack and the effective attack imposed on the PoT, respectively. The meanings of the variables in the figure are available in Supplementary Table 1.

Supplementary Table 1: Meaning of 15 variables given in Fig. 10

Affiliated	**Legend**	**Meaning**
DGU 1	u_1	Control command
	x_{12}	State sent by DGU 2
	x_{15}	State sent by DGU 5
DGU 2	u_2	Control command
	x_{23}	State sent by DGU 3
	x_{21}	State sent by DGU 1
DGU 3	u_3	Control command
	x_{34}	State sent by DGU 4
	x_{32}	State sent by DGU 2
DGU 4	u_4	Control command
	x_{43}	State sent by DGU 3
	x_{45}	State sent by DGU 5
DGU 5	u_5	Control command
	x_{51}	State sent by DGU 1
	x_{54}	State sent by DGU 4

TABLE IV: Probability of secure data transmission in the microgrid system with different approaches

Methods\ DGUs	DGU 1	DGU 2	DGU 3	DGU 4	DGU 5
Method 1*	0.53	0.54	0.63	0.55	0.58
Method 2*	0.81	0.77	0.75	0.80	0.79
Method 3*	**0.94**	**0.96**	**0.95**	**0.95**	**0.97**
Method 1*, Method 2* and Method 3* refer to the approach proposed in [13], [56] and this paper, respectively.					



(a)

(b)

Fig. 11: Comparison of the performance metrics of the tested microgrid system under different approaches: (a) the security performance metric H_α, (b) the control performance metric J_{task}. The middle part of (a) shows three enlarged subplots. The methods labeled as 'Existing method 1' and 'Existing method 2' correspond to the approaches in [13] and [56], respectively.

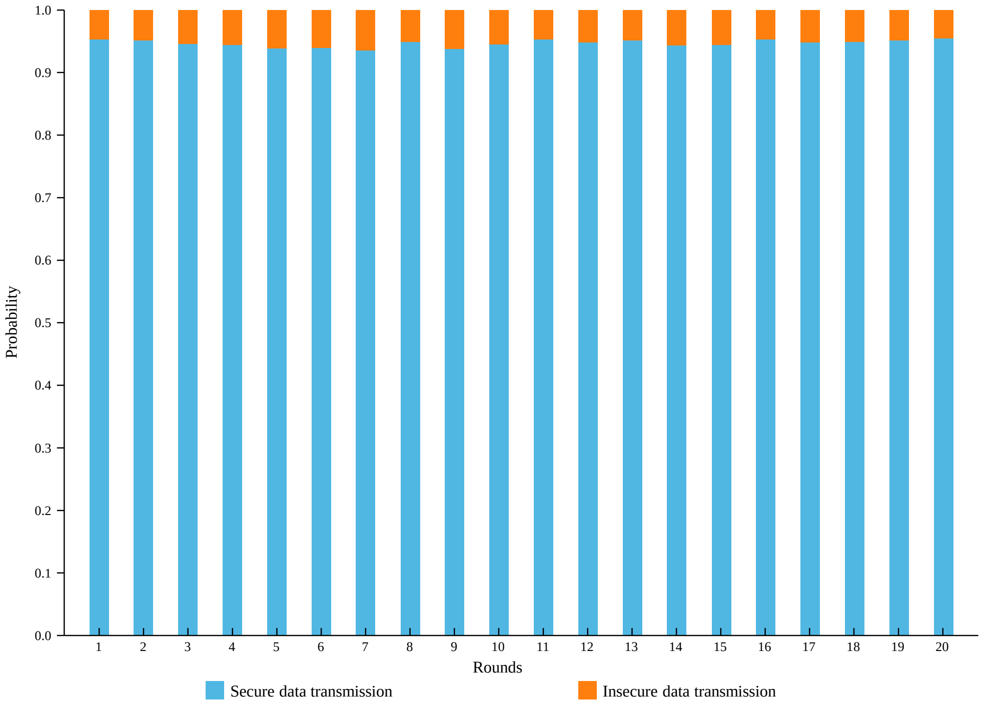


Fig. 12: Ratio of probability of successful defense w.r.t. probability of unsuccessful defense for dc microgrids under PoT-based secondary control over 20 independent repeated trials.

Supplementary Table 8: Meanings of the variables in equation (30)

Variable	Meaning
t_{sec}	Moment activating the secondary control strategy
T	Action time of the secondary control strategy
N	Number of DGUs contained in the microgrid
$y_j^{V,org}(t)$	Ideal voltage value of DGU j in the microgrid
$y_j^{I,org}(t)$	Ideal current value of DGU j in the microgrid
$u_i^{org}(t)$	Ideal control command of DGU i in the microgrid
$\tilde{y}_{ij}^{I}(t)$	Voltage value actually used by the controller in the microgrid, which received by DGU i from DGU j
$\tilde{y}_{ij}^{V}(t)$	Current value actually used by the controller in the microgrid, which is received by DGU i from DGU j
$\tilde{u}_i(t)$	Control command actually used by the actuator of DGU i in the microgrid
$V_{j,\max}^{org}$	Maximum ideal voltage value of DGU j during secondary control period
$I_{tj,\max}^{org}$	Maximum ideal current value of DGU j during secondary control period
$u_{i,\max}^{org}$	Maximum ideal control command of DGU i during secondary control period

Supplementary Table 9: Meanings of the variables in equation (31)

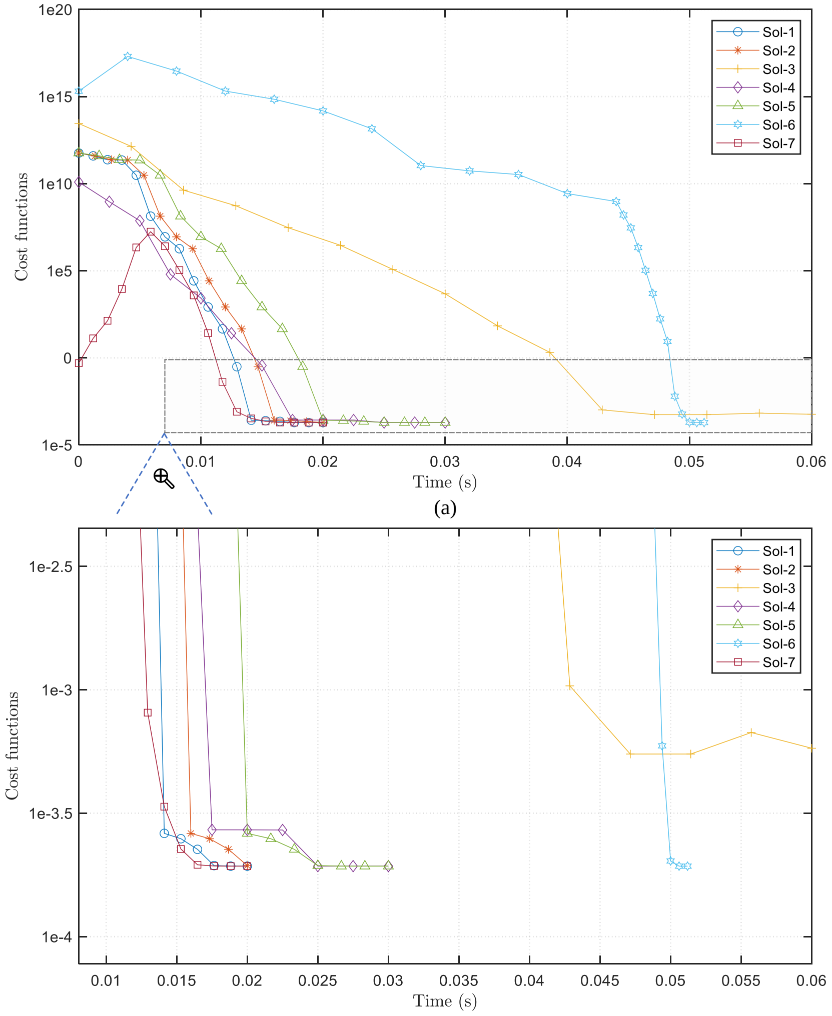
Variable	Meaning
$\bar{V}_{i,\max}^{org}$	Maximum ideal estimated voltage value of DGU i during secondary control period
$I_{tj,\max}^{org}$	Maximum ideal current value of DGU j during secondary control period
$I_{tj}^{org}(t)$	Ideal/measured current value of DGU j in the microgrid

Supplementary Table 7: Details of solvers used in the experiments

Solver	**Version**
CPLEX	12.10.0
GUROBI	10.0.3
XPRESS	9.4.0
COPT	7.1.3
MOSEK	10.2.0

Supplementary Table 2: Meaning of seven legends shown in Supplementary Fig. 7

Legend	**Meaning**	
	Solver name	**Solver setting**
Sol-1	CPLEX	Default
Sol-2	CPLEX	Barrier.convergetol = $1e-3$
Sol-3	GUROBI	Default
Sol-4	XPRESS	Default
Sol-5	CPLEX	Barrier.convergetol = $1e-9$
Sol-6	COPT	Default
Sol-7	MOSEK	Default



(a)

(b)

Figure 4: Performance of different solvers in solving a single optimization problem under Application 1. The horizontal and vertical coordinates of the position where the curve ends indicate the time for the solver to complete the solution and the final cost function, respectively.

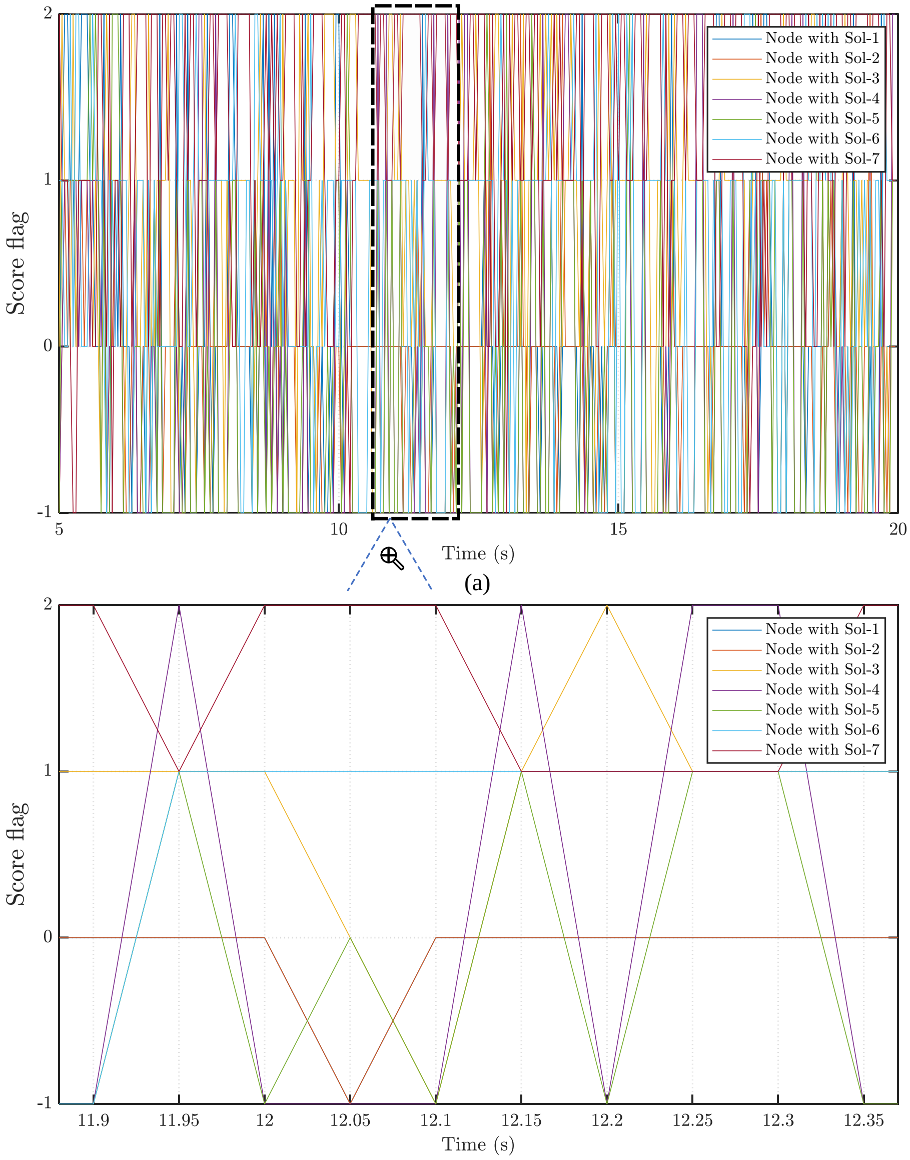
Supplementary Table 3: Score flags and their meanings for peers with a solver

Score flag of a peer with a specific solver	**Meaning**		
	Being selected in a delegation	**Solution satisfying the constraints**	**Solution winning consensus**
0	×	\	\
−1	√	×	\
1	√	√	×
2	√	√	√

√ means ‘Yes’.

× means ‘No’.

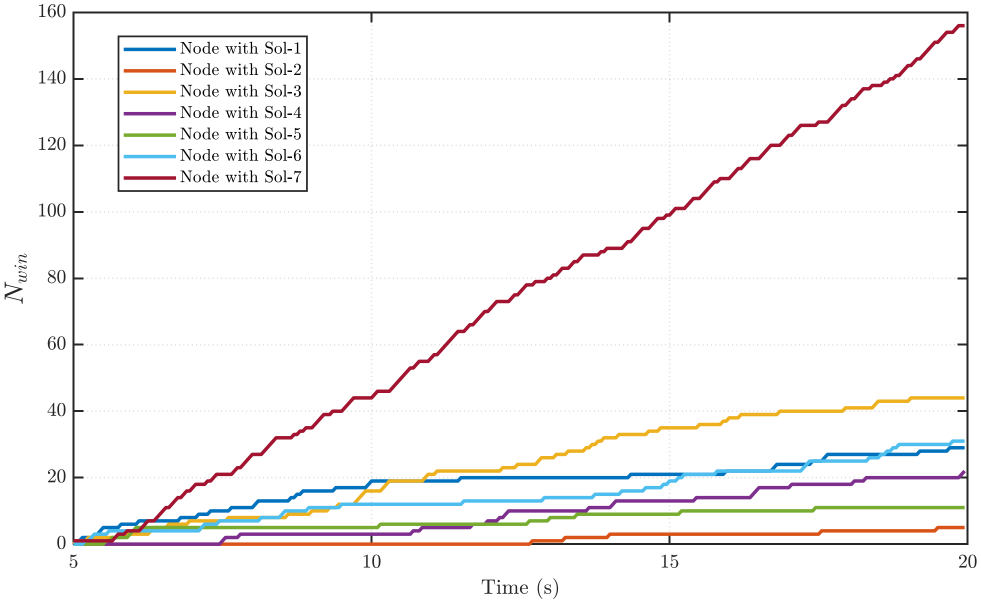
\ means ‘Not applicable’.



(a)

(b)

Supplementary Fig. 7: The performance of the solver at each node throughout the PoT-based secondary control process. The meanings of ‘Sol-1~Sol-7’ in the legends are given in the Supplementary Table 2. The values of ‘Score flag’ are -1, 0, 1 and 2. The meanings of these four values are shown in the Supplementary Table 3.

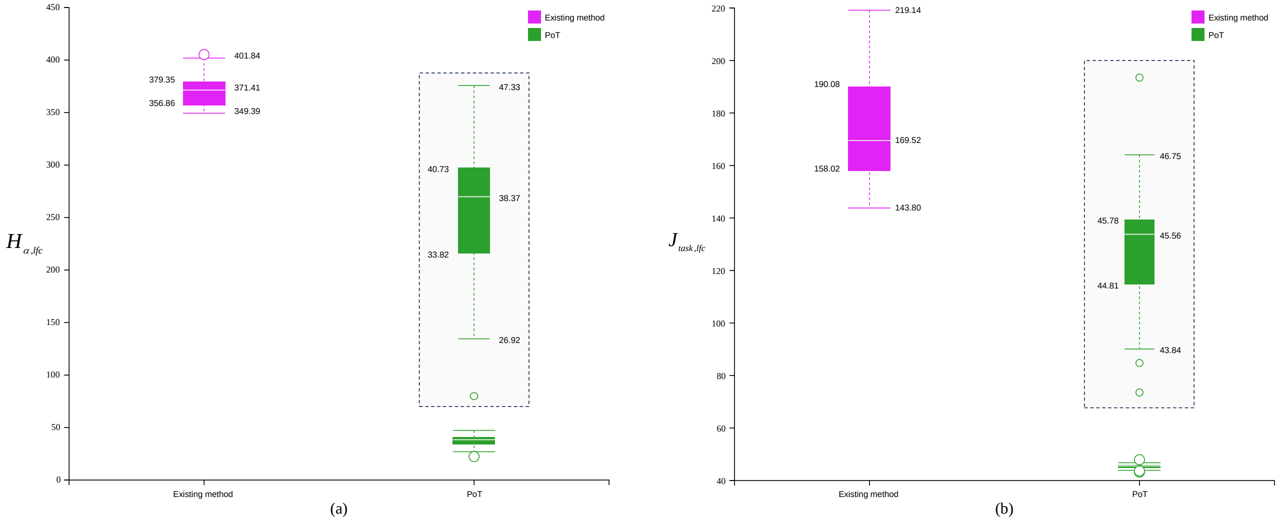


Supplementary Fig. 8: The cumulative number N_{win} of times each node wins PoT consensus throughout the control process, i.e., the number of times 'Score flag' takes the value of 2.

Supplementary Table 4: Probability of secure data transmission in the multi-area power system with different approaches

Methods\Areas	**Area 1**	**Area 2**	**Area 3**
Method 1*	0.54	0.57	0.61
Method 2*	**0.96**	**0.93**	**0.97**

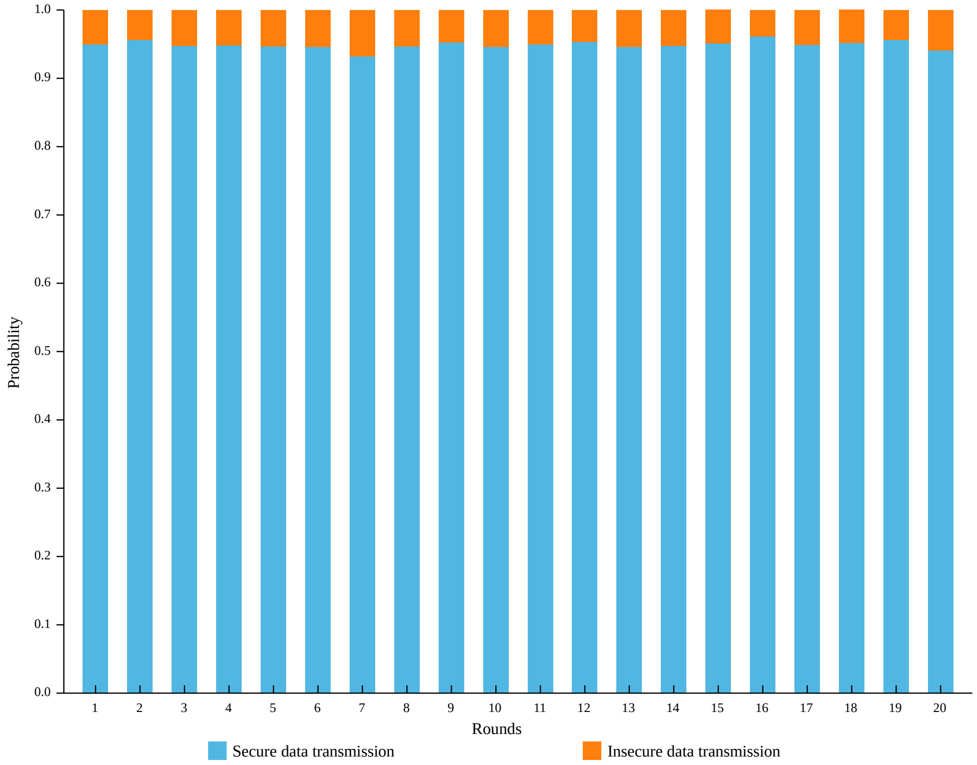
Method 1* and Method 2* refer to the approach proposed in [57] and the PoT-based LFC method in this paper, respectively.



(a)

(b)

Supplementary Fig. 9: Comparison of the performance metrics of the tested three-area power system under different approaches: (a) the security performance index $H_{\alpha,lfc}$, (b) the control performance index $J_{task,lfc}$. The middle part of the figure shows two enlarged subplots. The method labeled as ‘Existing method’ corresponds to the approach in [57] of the paper.



Supplementary Fig. 10: Ratio of probability of successful defense w.r.t. probability of unsuccessful defense for the tested three-area power system under PoT-based LFC over 20 independent repeated trials.

Supplementary Table 10: Meanings of the variables in equation (46)

Variable	**Meaning**
t_0	Moment activating the specific load frequency control
T	Action time of the load frequency control strategy
N	Number of subsystems contained in the three-area power system
$x_j^{P,org}(t)$	Ideal power deviation value (i.e., ideal $\Delta P_{tie,j}(t)$) of subsystem j in the three-area power system
$x_j^{f,org}(t)$	Ideal frequency deviation value (i.e., ideal $\Delta f_j(t)$) of subsystem j in the three-area power system
$\tilde{x}_{ij}^P(t)$	Power deviation value actually used by the controller in the power system, which received by subsystem i from subsystem j
$\tilde{x}_{ij}^f(t)$	Frequency deviation value actually used by the controller in the power system, which received by subsystem i from subsystem j
$\tilde{u}_i(t)$	Control command actually used by the actuator of subsystem i in the power system
$u_i^{org}(t)$	Ideal control command of subsystem i in the power system
$\Delta P_{tie,j,\max}^{org}$	Maximum ideal power deviation value of subsystem j during power system operation
$\Delta f_{j,\max}^{org}$	Maximum ideal frequency deviation value of subsystem j during power system operation
$u_{i,\max}^{org}$	Maximum ideal control command of subsystem i during power system operation

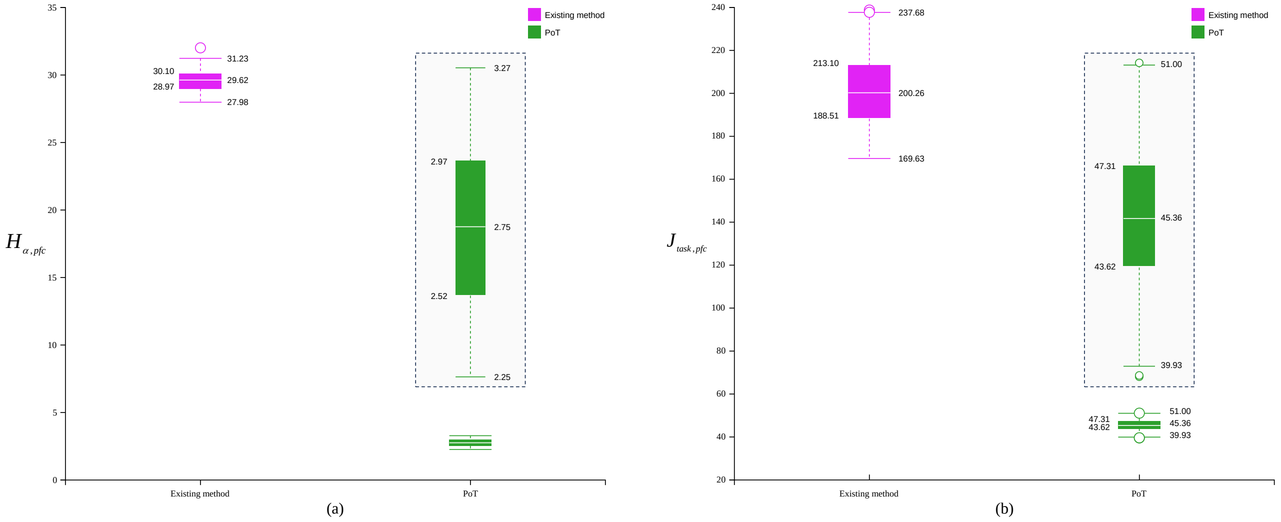
Supplementary Table 11: Meanings of the variables in equation (47)

Variable	**Meaning**
$ACE_{i,\max}^{org}$	Maximum ideal area control error of subsystem i during power system operation
$ACE_i^{org}(t)$	Ideal area control error of subsystem i in the three-area power system, which is calculated from the measured power deviation and frequency deviation values

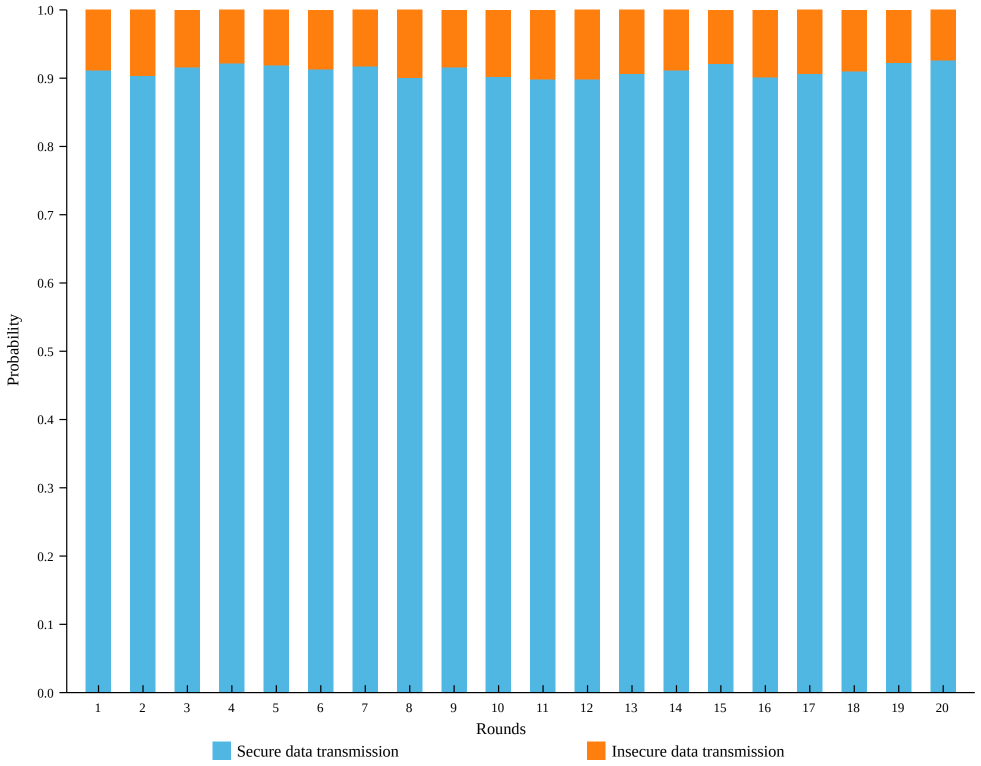
Supplementary Table 5: Probability of secure data transmission in the dc microgrid system with different approaches

Methods\DGUs	DGU 1	DGU 2	DGU 3	DGU 4	DGU 5
Method 1*	0.48	0.47	0.47	0.48	0.51
Method 2*	**0.90**	**0.91**	**0.91**	**0.92**	**0.92**

Method 1* and Method 2* refer to the approach proposed in [58] of the paper and the PFC-based secondary control in this paper, respectively.



Supplementary Fig. 11: Comparison of the performance metrics of the microgrid system under different centralized approaches: (a) the security performance index $H_{\alpha,pfc}$, (b) the control performance index $J_{task,pfc}$. The middle part of the figure shows two enlarged subplots. The method labeled as 'Existing method' corresponds to the approach in [58] of the paper.



Supplementary Fig. 12: Ratio of probability of successful defense w.r.t. probability of unsuccessful defense for dc microgrids under PFC-based secondary control over 20 independent repeated trials.

C2.6: *In addition, the manuscript focused on small-scale deployments, but real-world REPSs can be vast. The authors should discuss how PoT would scale to handle a large number of participants and transactions in a complex REPS environment.*

Response:

Thank you sincerely for your constructive comments and valuable suggestions.

In fact, for both large-scale and small-scale REPSs, each DG unit deploys its own controller based on the overall needs of the system. In the following, we discuss how PoT would scale to address the security regulation of large-scale complex REPSs, both at the physical/electrical level and at the information level.

♣ From the physical/electrical layer perspective. Whether on a large or small scale, REPSs will first determine their physical topology, such as the common star, ring, and mesh structures. It can be seen that the number of neighbors of each generation unit may increase in case of mesh topology. However, these changes that occur on the physical/electrical layer do not affect the optimization problem in PoT, since the communication and physical/electrical layers are not required to be consistent during the design phase of the controller. Therefore, the transition from small-scale REPSs to large-scale REPSs does not pose additional challenges for PoT-based security regulation.

♣ From the information layer perspective. In the transition from small-scale to large-scale REPSs, the systems need to focus on how the data is transferred in the information layer, as this will directly determine how the controllers in the system are deployed and the control performance. For large-scale complex

REPSs, the number of generation units becomes larger, leading to more communication options and more total communication transactions. As can be seen from the narrative in Section II of the manuscript, distributed security regulation for REPSs can be realized based on PoT. Therefore, the scalability of PoT is discussed below from the perspective of distributed communication.

1) The deployment and application of PoT-based security regulation will not be affected if fully distributed communication is used for large-scale REPSs. In other words, under this communication method, PoT used in the experimental results section for small-scale REPSs can be directly scaled up to large-scale REPSs, with at most the need to adjust the control parameters. It is worth mentioning that 'fully distributed communication' here refers to the case where each generation unit has only two communicating neighbors and the communication network has a spanning tree. In this case, for each generation unit, the data interacted through PoT does not change, nor does the optimization problem to be solved. Although the overall number of optimization problems becomes larger, the extra optimization problems will be solved by the extra generation units. At this point, for each generation unit, the steps for applying PoT on large-scale REPSs and small-scale REPSs are the same.

When it comes to regulation performance, things are a bit different. Although the communication of each generation unit does not change in this case, the communication scale of the whole system becomes larger. At this point, the path for the system to achieve full information sharing will become longer. This leads to faster regulation of PoT under small-scale REPSs compared with large-scale REPSs for the same control parameters. Three dc microgrids containing 6, 10 and 15 DGUs are used as case studies to illustrate the effect of fully distributed communication on the speed of PoT-based regulation. It is assumed that the task of the dc microgrid is to achieve voltage restoration and current sharing. The results under these three cases are given in Figures 5, 6 and 7, respectively. It can be seen that for the same control parameters, the dc microgrid containing 15 DGUs is regulated slower than the one containing 6 and 10 DGUs. The reason for this is that in order to achieve accurate power sharing, it is required that ultimately, on the entire large-scale microgrid system, information can be propagated throughout the network by communicating only with its neighbors. When the size of the information layer is large, it takes longer to reach global consistency of the information, which reduces the speed of the PoT-based regulation strategy. Therefore, scaling the PoT-based regulation strategy from small-scale REPSs to large-scale REPSs under fully distributed communication will not face challenging problems.

2) If non-fully distributed communication is used, some DGUs will have more than two neighbors, the extreme scenario of which is fully connected communication. In this case, when there is an additional generation unit in the REPS, certain generation units may have an additional communicating neighbor. As there are more neighbouring units and more data interacting across the network, more data needs to be protected. These transactions are more likely to be attacked, thus requiring a larger scale blockchain, which may bring about a decrease in real-time performance. The increase in the number of neighbours simultaneously leads to an increase in the size of the optimization problem, which reduces the real-time performance. In summary, in order to solve the problem of security regulation on large-scale REPSs under this communication style, the PoT needs to be carefully designed to achieve a good trade-off between security and real-time performance. Therefore, in practice, we can try to adopt a fully distributed communication approach, which can better allow PoT to scale to large-scale REPSs.

To address your concerns, we have added a discussion of how to scale PoT to large-scale and complex REPSs in the conclusion section of the revised manuscript.

Based on the reviewer's comments, the authors have made the following modifications to the content of the manuscript:

[Section VIII, page 14, highlighted in red]

" Regardless of the size, REPSs would first determine their physical topology, such as the common star, ring, and mesh structures. In some topologies, the number of neighbors that are electrically connected to the generation unit increases as the system size increases. However, these changes in the electrical layer faced when scaling up to large-scale REPSs will not pose additional challenges for PoT applications, as there is no requirement for the information layer and the electrical layer to be connected in the same way in PoT. At this point, the REPSs need to focus on the mode of data communication within the information layer, as this will directly determine the deployment and the control performance of PoT. If a fully distributed communication is adopted, the PoT deployment and application will not be affected when scaling up to large-scale REPSs, because the number of communicating neighbors will remain unchanged. With a non-fully distributed communication, the amount of data that neighbors interact with each other over the network becomes more, and the possibility of these data being attacked becomes greater. In this case, achieving the same level of security as in small-scale systems requires a larger-scale blockchain, which may lead to a decrease in the real-time performance of PoT. Therefore, a fully distributed communication style would be preferable when deploying PoT in large-scale REPSs, as it facilitates the scalability of PoT. "

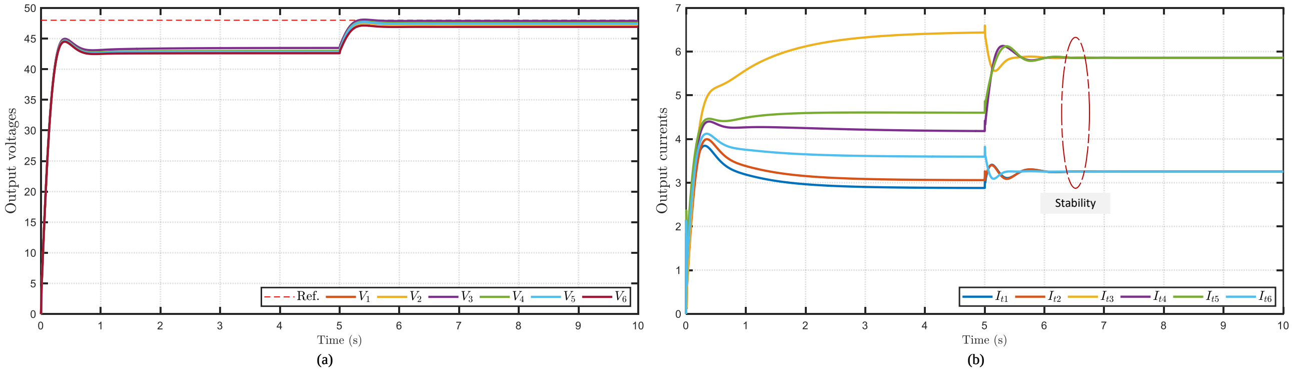
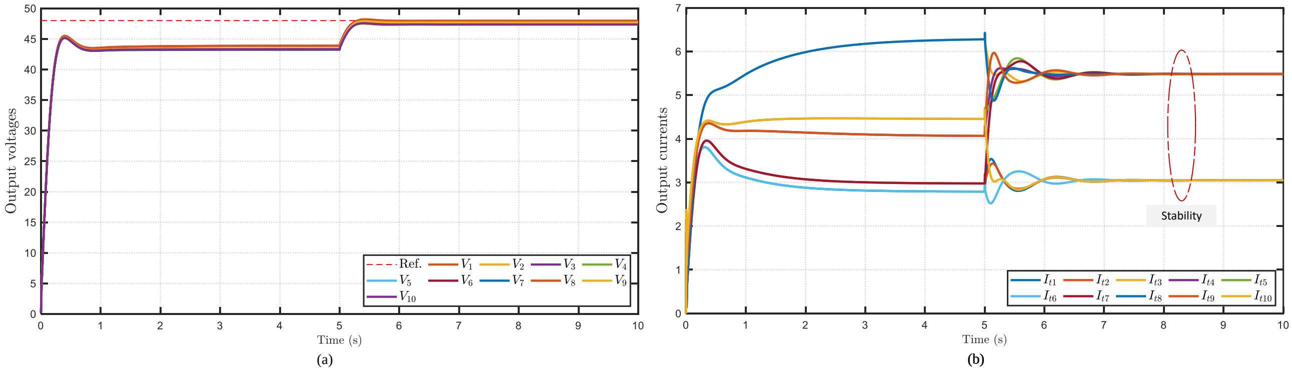


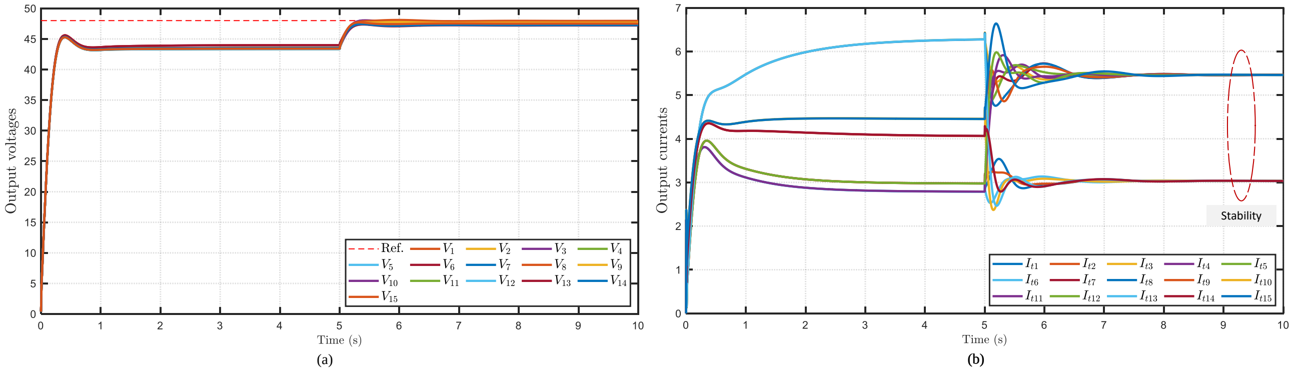
Figure 5: Responses of the microgrid system with 6 DGUs. (a) Output voltages. (b) Output currents.



(a)

(b)

Figure 6: Responses of the microgrid system with 10 DGUs. (a) Output voltages. (b) Output currents.



(a)

(b)

Figure 7: Responses of the microgrid system with 15 DGUs. (a) Output voltages. (b) Output currents.

Response to the Reviewers: Reviewer 3

C3.1: *In Section 1, the authors firstly explained the works relating to the problems and so on. This section is well written, but it did not address the major issue that is imperative to be solved. As a reviewer's point of view, the literature survey of this section is very weak, unfocused and insufficient. What is the essential problem of this work? The authors should really explain the drawback of approaches in related works especially instead of simply stating what they have done. The authors should discuss the mentioned references in the introduction part.*

Response:

We sincerely appreciate the time and effort you dedicated to reviewing our manuscript. Your recognition of our written fills us with gratitude, and your valuable comments and suggestions have helped us greatly improve the manuscript. We have taken into account all your comments in the revised manuscript, where the modifications have been highlighted in red.

We apologize for not clearly articulating the main problem to be addressed and for not adequately explaining the drawbacks of approaches in related work in the original manuscript. Regarding the two concerns you have mentioned, we will respond to each of them below.

1) About the main issues addressed in this manuscript

The major issue that is imperative to be solved is the data security problem encountered in the real-time regulation of renewable energy power systems in the presence of frequent data interactions. The main characteristic of renewable energy power systems is that small-capacity but large-numbered generation units are dispersed across different geographical areas. For such small-capacity medium- and low-voltage power systems, operators are more likely to consume new energy generation locally, for example by utilizing the surrounding parks, etc., than to transmit it over long distances. This leads to the fact that this system will operate in an open network environment and its data interactions will often be exposed to cyber threats, as it may not be possible to resort to the dedicated communication networks of the large power grids. At this point, it is crucial to realize real-time security regulation of REPSs in the face of potential cyber risks.

While many efforts have achieved excellent results against specific attacks Ref. [9], they rely on an understanding of the dynamic properties of the attack and may not allow the captured data of the system as trustworthy as possible. The reason is that most of them take countermeasures that passively tolerate negative impacts after attack happens or execute detection-based packet discard to protect against specific types of attacks Ref. [10]. In this way, existing resilient methods are insufficient and limited in the degree of defense motivation. The emerging blockchain technology holds the promise of addressing the security issues at the root Refs. [11,12]. However, existing work simply introduces traditional consensus protocols such as PoA into the communication channel for secure data transmission, without mining the properties of the blockchain itself and the control needs of REPSs thereby merging the two Ref. [2]. Therefore, the aim of this manuscript is to fully exploit the multi-party computation and multi-party verification features of the blockchain, and to propose a blockchain consensus protocol dedicated to real-time control, which provides a secure real-time regulation scheme for REPSs in the presence of cyber threats. In PoT, it is not only expected that the probability of the system being attacked becomes smaller, but also that the system uses as much real data as possible to achieve better control.

2) About explaining the drawbacks of related work and discussing the mentioned references in the introduction

Following your suggestions, we have carefully discussed the mentioned references in the introduction of the revised manuscript and carefully analyzed the strengths and drawbacks of the existing work. At the same time, the necessity of the presented work is further elaborated on the basis of these analysis. Specifically, for the data security problems encountered in the real-time regulation of REPSs, the strategies proposed in the existing work can be categorized into the following two main aspects. One is to passively tolerate the negative effects of cyber-attacks through the design of resilient control strategies. The second is to proactively detect and mitigate the effects of cyber-attacks through algorithm design. The main problem is that defenses based on purely software algorithms are limited in the improvements they can bring to system security. In particular, the first type of approach designs tolerant strategies after the attack has occurred and does not fundamentally reduce the likelihood of a system being attacked. The second type of approach reduces the likelihood of an attack on the system and thus improves the security of the system. However, once an attack has been detected, most of these methods do not provide adequate compensation for missing data and there is no guarantee of control performance. On the contrary, the defense scheme proposed in this manuscript incorporates the advantages of both hardware and software, which enhances the regulation security of REPSs at the physical level. In addition, these purely software algorithmic approaches proposed in existing work can actually be deployed in the framework proposed in this manuscript. A more detailed account of the literature comparison can also be found in the response to your next comment.

To address your concerns, we have carefully revised the introduction part to highlight the major issue addressed in this manuscript while strengthening the literature survey. If you have any further suggestions, please let us know and we will be delighted to make improvements.

Based on the reviewer's comments, the authors have made the following modifications to the content of the manuscript:

[Abstract, page 1, highlighted in red]
" With the ongoing development of renewable energy sources, information technologies and physical energy systems are further integrated, which leads to challenges in guaranteeing the secure and stable operation of renewable energy power systems (REPSs) in the face of potential cyber threats. ... "

[Section I, page 1, highlighted in red]
" ... Motivated by these challenges, a growing body of impressive research has been devoted to the development of security control for REPSs to defend against potential cyber threats [13-18]. To be specific, control strategies for attack prevention [15], attack detection [16], and attack mitigation [17] have been proposed and applied to REPSs, including learning-based, game-theoretic, set-theoretic, and cryptography-based approaches. While these efforts have achieved excellent results against specific attacks, they rely on an understanding of the dynamic properties of the attack and may not allow the captured data of the system as trustworthy as possible [15]. The reason is that most of them take countermeasures that passively tolerate negative impacts after attack happens or execute

detection-based packet discard to protect systems against specific types of attacks [18]. In this way, existing resilient methods are insufficient and limited in the degree of defense motivation. ”

[Section I, page 2, highlighted in red]
“ ... For example, Shibata proposed a blockchain mechanism for solving complex optimization problems [36], combining with the original hash puzzle of PoW. This work offers blockchain the potential to fuel the training of deep learning algorithms and solve other computational tasks, but it inherits the limitations of PoW in terms of consuming large amounts of resources to solve hash puzzles and waiting a long time for a usable solution. Subsequently, AlAshery et al. suggested a mechanism, Proof of Clearance (PoC) [37], which replaced the hash puzzle in PoW with a winner determination problem in the energy trading market. PoC has been successfully applied in dispatch of energy power systems and trading of energy markets, but the condition to verify whether the candidate solution is optimal or not is not explicitly given in this consensus mechanism, which is an aspect worth further improvement. Apart from the above work, a consensus mechanism, Proof of Solution (PoSo), which substitutes the meaningless mathematical puzzle in PoW with a meaningful optimization problem, was innovatively proposed [38]. PoSo has achieved impressive results in the field of energy dispatch and trading due to the skillfully designed verification mechanism. However, the limitation of PoSo is that it is only applicable to optimization problems whose optimal solutions can be verified using the Karush–Kuhn–Tucker condition and the second-order sufficient condition, which may not be suitable for some applications. Beyond these, there is a lot of meaningful work being reported on the use of blockchain to improve the efficiency, security, and reliability of energy dispatch and trading in power systems [39-43]. ”

“ ... However, the control of REPSs has its unique characteristics compared with aforementioned energy dispatch and trading, such as many state constraints, complex multi-objective problems, and high real-time requirements with a small time scale [44]. ... ”

“ ... To this end, there are efforts to tap the potential of blockchain in the area of control for dynamical systems [45-49]. Specifically, the authors of [45] introduced the blockchain consensus mechanism to a networked control system and analyzed the relationship among blockchain-induced communication delay, the size of the P2P network, and system stability. Although the authors have further investigated predictive control to make blockchain more suitable for security control of networked systems [46], their work remains at the level of simply combining blockchain with control systems and mitigating the drawbacks that blockchain brings to the system, rather than proposing a new consensus mechanism from the perspective of integrating the characteristics of real-time control itself and the multi-party nature of blockchain. Yang et al. successfully applied blockchain to the secondary control of microgrids, in which attack nodes are excluded from the distributed control system through the PoA mechanism [47]. However, similar to [46], this work applied existing consensus mechanisms to the security control framework, without considering the characteristics of real-time control itself and the multi-party nature of blockchain to design a consensus protocol exclusively for the control of REPSs. Abdullah et al. proposed a blockchain-based data-driven fault-tolerant control framework that can effectively mitigate the response of Industry 4.0 smart factories in the event of anomalies such as a cyber attack [48]. However, for systems with small sampling periods such as REPSs, the proposed method may fail because the paper assumes minute-level sampling for industrial control systems. ”

[References, page 16, highlighted in red]
“ [13] M. Kachhwaha, H. Modi, M. K. Nehra, and D. Fulwani, “Resilient control of dc microgrids against cyber attacks: A functional observer based approach,” *IEEE Transactions on Power Electronics*, vol. 39, no. 1, pp. 459–468, 2024. ”

“ [14] A. Presekal, A. S¸tefanov, V. S. Rajkumar, and P. Palensky, “Attack graph model for cyber-physical power systems using hybrid deep learning,” *IEEE Transactions on Smart Grid*, vol. 14, no. 5, pp. 4007–4020, 2023. ”

“ [15] H. M. Khalid et al., “Wams operations in power grids: A track fusion-based mixture density estimation-driven grid resilient approach toward cyberattacks,” *IEEE Systems Journal*, 2023. ”

“ [16] T. Tabassum, S. Lim, and M. R. Khalghani, “Artificial intelligence-based detection and mitigation of cyber disruptions in microgrid control,” *Electric Power Systems Research*, vol. 226, p. 109925, 2024. ”

“ [17] A. Rahiminejad et al., “A resilience-based recovery scheme for smart grid restoration following cyberattacks to substations,” *International Journal of Electrical Power & Energy Systems*, vol. 145, p. 108610, 2023. ”

“ [18] Q. Tang, C. Deng, Y. Wang, F. Guo, and S. Fan, “Iterative observer-based resilient control for energy storage systems in microgrids under fdi attacks,” IEEE Transactions on Smart Grid, 2024. ”

“ [34] S. M. Danish, K. Zhang, F. Amara, J. C. O. Cepeda, L. F. R. Vasquez, and T. Marynowski, “Blockchain for energy credits and certificates: A comprehensive review,” *IEEE Transactions on Sustainable Computing*, no. 01, pp. 1–13, 2024. ”

“ [41] Y. Wu, Y. Wu, H. Cimen, J. C. Vasquez, and J. M. Guerrero, “Towards collective energy community: Potential roles of microgrid and blockchain to go beyond p2p energy trading,” *Applied Energy*, vol. 314, p. 119003, 2022. ”

“ [42] L. Ali et al., “Integrating forecasting service and gen2 blockchain into a local energy trading platform to promote sustainability goals,” *IEEE Access*, 2023. ”

“ [43] C.-T. Huang and I. J. Scott, “Peer-to-peer multi-period energy market with flexible scheduling on a scalable and cost-effective blockchain,” *Applied Energy*, vol. 367, p. 123331, 2024. ”

“ [48] A. B. Masood, A. Hasan, V. Vassiliou, and M. Lestas, “A blockchain-based data-driven fault-tolerant control system for smart factories in industry 4.0,” *Computer Communications*, vol. 204, pp. 158–171, 2023. ”

“ [49] V. Veerasamy, Z. Hu, H. Qiu, S. Murshid, H. B. Gooi, and H. D. Nguyen, “Blockchain-enabled peer-to-peer energy trading and resilient control of microgrids,” *Applied Energy*, vol. 353, p. 122107, 2024. ”

" [57] Y. Zhang, C. Peng, C. Cheng, and Y.-L. Wang, "Attack intensity dependent adaptive load frequency control of interconnected power systems under malicious traffic attacks," *IEEE Transactions on Smart Grid*, vol. 14, no. 2, pp. 1223–1235, 2023. "

" [58] P. Lin, C. Deng, Y. Yang, C. H. T. Lee, and W. P. Tay, "Resilience-oriented control for cyber-physical hybrid energy storage systems using a semiconsensus scheme: Design and practice," *IEEE Transactions on Industrial Electronics*, vol. 70, no. 3, pp. 2508–2519, 2023. "

C3.2: *What is the major novel/contribution of this paper? In my view, there are many techniques adopted in the recent past for this problem. So, the authors should improve the section with the references. Please explain the main contribution related to previous approaches, and provide a list of paper's contributions at the end of the introduction.*

Response:

Thank you for your valuable comment and helpful suggestions.

We apologize for not explaining the major innovations or contributions of this manuscript through a thorough literature comparison in the original manuscript. As you commented, there are various types of security control schemes for REPSs in the available literature. They can also achieve favorable output regulation in the event that REPSs suffer from network anomalies or cyber-attacks. However, the methods proposed in this manuscript have advantages that they do not offer.

Studies addressing security control for REPSs can be categorized into two groups in terms of whether there is the aid of blockchain technology. As mentioned in the previous reply, methods without the aid of blockchain can also be divided into two categories. The other class is resilient control methods that passively tolerate network anomalies. One class is security control methods based on detection and compensation. Specifically, the contributions of this manuscript can be discussed in the following aspects compared to the methods reported in the existing literature.

♣ Firstly, we will explain the contribution of this manuscript by comparing it with each of the two types of approaches that do not use blockchain.

1) Comparison with existing resilient control methods that passively tolerate network anomalies

For example, the authors in Ref. [13] proposed a resilience-based frequency regulation scheme for microgrids, which gives the system robustness against external cyber attacks. The method assumed a specific type of attack before the corresponding controller design. That is, the method relies too much on modeling the attack signal when designing resilient control. In fact, the attack signal may not be a single deterministic or probabilistic model, but a complex combination of multiple attack signals. These attack signals may not be accurately modeled by some mathematical expressions. In this case, the resilient control proposed in Ref. [13] may not perform well in defense. The authors in Ref. [14] proposed a distributed robust recovery resource allocation method based on the tri-level defender-attacker-defender model. The proposed method is expected to accelerate the recovery process of the power system after a successful attack occurs. However, this approach focuses mainly on the recovery of the power system after an attack, which does not proactively reduce the likelihood of the power system being affected by a cyberattack in the early stage.

Moreover, the limitation of this type of approach is that tolerating the negative effects of an attack has a very limited improvement on the control performance of the system. The proposed PoT-based security control approach, on the other hand, is striving to make the system as immune as possible from attacks and aims to obtain the required control commands based on trustworthy data for the system at every control cycle. First, we have designed a series of proactive defense mechanisms, which are committed to minimizing the likelihood of a signal being attacked before an attack occurs. As a result, this approach can be more active and effective in protecting the stability and security of the REPSs. Second, multi-party verification with multiple nodes is the most crucial step for us to obtain secure data, which is a universal rule that does not depend on a specific attack model, making our approach more practical and flexible in practical applications. In addition to securing the control commands, the PoT will also be responsible for solving the control problems in REPSs. As a result, it also leverages the advantages of blockchain in multi-party computation to fuel the improved control performance of REPSs. In contrast to these passive means of tolerating cyber threats, PoT not only allows blockchain to serve the secure transmission of data for REPSs in a proactive manner, but also involves it in the computation of the controller.

2) Comparison with existing security control methods based on detection, prevention and compensation

There is a lot of work on defending power systems against encountered attacks by means of detection, prevention and compensation Refs. [15–18]. For example, the authors in Ref. [19] proposed a robust data-driven attack detection algorithm for power systems experiencing cyber-attacks. The authors in Ref. [20] proposed an integrated security control approach for islanded microgrids using model-free and model-based techniques. The approach proposed in Ref. [20] not only detects cyber-attacks like the one in Ref. [19], but also mitigates the negative impact of cyber-attacks on power systems. However, such deep learning-based methods presented in Ref. [19] and Ref. [20] still have some limitations. Firstly, these methods methods often require a large amount of training data to accurately detect attacks, while there are not so many attack samples in real power systems. Secondly, the methods in Ref. [19] and Ref. [20] mainly consider network attacks in a centralized framework and cannot be executed in a distributed manner, while many REPSs operate based on a distributed control architecture. Furthermore, these methods are only capable of detecting a particular type of cyber attack, i.e., only FDI attacks are considered.

It can be seen that the most significant difference between this type of approach and the one proposed in this paper is that they still compensate and mitigate the attack only after it has occurred. This practice is somewhat conservative, as the likelihood of the system acquiring authentic data is not essentially increased Ref. [10]. PoT-based defenses can provide security for REPSs in real time without the aid of additional detection and mitigation, enabling proactive and effective security regulation of REPSs from the data source.

In summary, it can be seen that compared to the existing non-blockchain-assisted secure real-time control strategies, the PoT security regulation mechanism proposed in this manuscript provides a new perspective for solving the data security problems encountered in the real-time regulation process of REPSs. In particular, it preserves the unattacked real data to the maximum extent with the multi-node feature, and recovers it through physical and algorithmic level efforts. Compared with existing approaches based on pure software algorithms, the PoT security regulation mechanism acts at the source of data generation and attack occurrence to make the system proactively defend against external attacks, thus improving the reliability and security of system operation. Moreover, PoT also aims to achieve satisfactory control performance. It can be seen that PoT-based security control both reduces the occurrence of effective attacks in the system and maintains the control performance of the system.

♣ Secondly, PoT also has its distinctive features compared to the existing blockchain-based security control methods. In order to make blockchain consensus protocols serve the real-time control of dynamic systems like REPSs, we have taken the following two innovative initiatives:

1. Replaces the problem solved by the blockchain nodes in traditional consensus protocols. We have replaced the hash puzzle in typical consensus protocols (e.g., PoW) with an optimization problem corresponding to the control task under consideration.

2. Modifies the authentication mechanism in traditional consensus protocols. We have replaced the verification of the absolute correctness of the solution to puzzles in traditional consensus protocols (e.g., PoW, PoC, PoSo) with the verification of the relative optimality of multiple solutions according to a specified performance metric as well as the verification of the stability conditions of the REPSs.

In this way, the PoT consensus protocol proposed in this manuscript not only realizes the data protection of REPSs, but also devotes itself to the realization of the control tasks of REPSs.

Compared with PoC proposed in Ref. [21] and PoSo proposed in Ref. [8], the verification mechanism of relative optimality in PoT can make it easier to obtain a usable data for each round of consensus. This initiative improves the real-time nature of PoT, making it more suitable for fast response control systems such as REPSs. In Refs. [8, 21], the scheduling problem in an energy network is considered, which has relatively relaxed requirements on the time scale for the consensus protocol to obtain a feasible solution, e.g. the time scale of minutes or even days. However, the control problems for the REPSs considered in this manuscript impose high requirements on the time scale of updating the feasible solutions, which is typically on the millisecond level. Therefore, the existing consensus protocols are not very suitable for the control of REPSs, and there is imperative to propose blockchain consensus protocols with higher real-time performance, which explains the necessity of PoT.

In order to further elaborate the contribution of this manuscript, the proposed PoT-based approach is compared with the latest blockchain-based security control approach for REPSs in the following. The work in Ref. [2] merely introduced the blockchain into the control system, allowing it to take on the task of data transmission, and does not link the consensus protocol to the system dynamics. Furthermore, the verification in Ref. [2] simply compares multiple data and employs a traditional PoA consensus mechanism. Although the authors analyzed the relationship between blockchain network size, system stability, and time delay, and illustrated the possibility and feasibility of blockchain empowering the security of dynamical control systems from a theoretical point of view, it did not in turn design a blockchain consensus protocol that is more suitable for dynamical systems based on its characteristics. This will result in a greater waste of resources. Although the approaches proposed in Refs. [1, 22–24] have achieved some success, they have similar limitations as the one in Ref. [2]. That is, they only make blockchain transfer data and do not utilize any other more features than the multi-party verification. Under these approaches, the relationship between blockchain and dynamical systems is relatively independent and they are not strongly coupled at the design stage, which may lead to incompatibility between blockchain and systems.

In contrast to these approaches, the two major initiatives of PoT mentioned above further tap into the resources of blockchain that have positive implications for control systems while improving system security.

Therefore, PoT brings many new features to the control system, such as online controller solving. At the same time, PoT allows both of the two main features of the blockchain, multi-party computation and multi-party verification, to serve the control tasks of REPSs, truly interacting the blockchain with the control system. In addition, the modular design of PoT results in a variety of variants that make it suitable for many scenarios. For example, a simplified PoT, called DPoT, can be used in situations where only secure data transmission is required.

Following your suggestion, at the end of the Introduction we have provided a list summarizing the contributions of this manuscript. In particular, we have added some literature to each entry in the list to further highlight the features that distinguish this manuscript from existing work. In addition, TABLE I and TABLE II of the manuscript compare the PoT consensus mechanism with the existing consensus mechanisms, and the PoT-based security control method with the existing security control approaches, respectively. To avoid an overly lengthy introduction section of the manuscript, we have tried to be concise and give rich narratives and comparisons in the manuscript. It is hoped that these modifications will clearly demonstrate the contribution of this work.

Based on the reviewer's comments, the authors have made the following modifications to the content of the manuscript:

[Section I, page 2, highlighted in red]
" To sum up, most of them only involved blockchain as a way of data interaction in power energy systems, without actually engaging blockchain in the achievement of control tasks. Furthermore, existing research has only leveraged the multi-party verification nature of blockchain technology, while its other inherent capabilities remain underutilized. As a result, research on blockchain for control of power energy systems is still at an embryonic stage. In this work, we suggest a blockchain consensus mechanism named Proof of Task (PoT) for real-time control of REPSs. In PoT, the term 'task' refers to various control tasks of REPSs corresponding to actual application scenarios. That is, PoT decides whose data will be adopted based on the contributions made by peers in completing control tasks. This blockchain consensus mechanism possesses several distinctive features as follows. "

" (1) Similar to the mathematical puzzles in PoW, the problems to be solved by the peers under PoT are also computationally intensive. The difference is that we have assigned some practical meanings to the actions of these peers. In PoT, the problem to be solved is *closely related to the control performance* of the system, while the verification criterion of the published solution is *closely related to the stability* of the system. This could enable better integration of blockchain into the REPSs, which has not been attempted in previous work on blockchain-based security control [46]–[48]. "

" (2) Other blockchains evaluate the posted solution into absolute right or wrong, and the solution judged as wrong will be directly discarded [37], [38]. Instead, PoT employs a practical validation mechanism that evaluates the accomplishment degree of the submitted solution in achieving control objectives. Such a feature allows the system to get usable data in each round of consensus, which greatly improves the efficiency of consensus, while effectively ensuring the real-time performance of regulation. "

" (3) Unlike existing consensus mechanisms [37], [38], PoT protects both source data (measurements) and target data (control commands), which not only defends against malicious nodes inside the network, but also improves system resilience against external cyber-attacks. Combining the practical verification mechanisms mentioned above, it can be seen that PoT imparts attractive attributes to REPSs, i.e., higher security and more computational resources, while ensuring the system stability and accomplishing regulation objectives. "

" (4) In comparison to existing consensus mechanisms used for dynamical systems [45], [47], PoT leverages the two main features of blockchain, multi-party computation and multi-party verification, to serve the regulation task of REPSs. Moreover, distinct from existing security control methods based on purely software algorithms [14], [16], PoT endows the system with the capability to proactively defend against attacks through efforts at both physical and algorithmic levels, without the assumption of a specific model of the attack signals. "

C3.3: *I suggest a comparison with the literature, in order to prove the efficiency of the proposed method? It can be seen from the result section that mostly results are not compared with the latest published papers.*

Response:

Thank you for your valuable comment and helpful suggestions. We apologize for not comparing the proposed method with the methods in the latest published papers. As per your suggestion, we have compared all the presented results in each of the three applications with the latest published papers, including waveform and quantitative comparisons.

1) Waveform comparison results

- **In Application 1**, in the revised manuscript, PoT has been compared with the latest real-time resilient control method [13] and with the existing blockchain-based security control method [56]. The corresponding results are presented in Fig. 8. It can be seen that compared with the existing real-time resilient control and the blockchain-based approach, the PoT-based scheme not only reduces the probability of attacks on various types of data in microgrids, but also significantly improves the dynamic performance of microgrids during the regulation process by means of optimization.
- **In Application 2**, in the revised manuscript, PoT is compared with the method in the latest published article [57]. The corresponding results are presented in Fig. 16. Consistent with the results in Application 1, PoT enhances the security of load frequency control in the face of cyber threats due to characteristics such as the fact that PoT protects both the raw interaction data and the target data.
- **In Application 3**, in the revised manuscript, DPoT is compared with the state-of-the-art approach [58]. The corresponding results are shown in Fig. 18. It can be seen that even the simplest PoT variants still contribute to the security control of REPSs.

The above waveform comparison results vividly illustrate the advantages of the proposed method over the existing methods in maintaining the stability, enhancing the security, and ensuring the successful completion of control tasks for REPSs subject to cyber threats.

2) Quantitative comparison results

Application 1:

In the revised manuscript, PoT has been compared with the existing real-time resilient control method [13] and with the existing blockchain-based security control method [56] in Application 1. The quantitative comparison results are presented in TABLE IV and Fig. 11. Specifically, TABLE IV gives the probability of secure data transmission in the microgrid system under the three methods. At this point, the probability that each generation unit in the microgrid under PoT gets a trustworthy control command is about 95%.

Classical metrics including attack probability, deviation between the received value and the sent value, the security performance metric, the control performance metric, etc. are employed for data illustration. Specific expressions for these indicators are given below. In order to reflect the trustworthiness of the data obtained by REPSs under PoT, the security performance metric is set as

$$\begin{aligned} H_\alpha = \sum_{t=t_{\text{sec}}}^{t_{\text{sec}}+T} \Big(\sum_{i=1}^{N} \Big(\sum_{j\in\mathcal{N}_i^c} \Big(\frac{1}{V_{j,\max}^{org}} |\tilde{y}_{ij}^{V}(t) - y_j^{V,org}(t)| + \frac{1}{I_{tj,\max}^{org}} |\tilde{y}_{ij}^{I}(t) - y_j^{I,org}(t)| \Big) \\ + \frac{1}{u_{i,\max}^{org}} |\tilde{u}_i(t) - u_i^{org}(t)| \Big) \Big) \end{aligned} \qquad \text{(Eq. 7)}$$

where the meanings of the involved variables are presented in Supplementary Table 8. It should be noted that $V_{j,\max}^{org}$, $I_{tj,\max}^{org}$, and $u_{i,\max}^{org}$ are used for normalization. Similarly, in order to reflect the effectiveness of REPSs under PoT in accomplishing the given control tasks, the control performance metric is defined as

$$J_{task} = \sum_{t=t_{\text{sec}}}^{t_{\text{sec}}+T} \sum_{i=1}^{N} \Big(\frac{1}{\bar{V}_{i,\max}^{org}} |\bar{V}_i(t) - V^{ref}| + \sum_{j\in\mathcal{N}_i^c} \Big(\frac{1}{I_{tj,\max}^{org}} \Big| \frac{I_{tj}^{org}(t)}{\theta_j^s} - \frac{I_{ti}^{org}(t)}{\theta_i^s} \Big| \Big) \Big) \qquad \text{(Eq. 8)}$$

where t_{sec}, T and N have the same meaning as given in Supplementary Table 8, $\bar{V}_i(t)$ denotes the estimated value of the voltage, as given in (18) in the Supplementary File, variables V^{ref}, $\mathcal{N}_i^c$ and θ_i have the same meaning as those in the manuscript, and the meanings of the other variables are presented in Supplementary Table 9. As a result of the attack, all of the above metrics are accumulated as the system runs. Therefore, the system responses within 15 s after the secondary control is activated are selected for statistical and illustrative purposes for all subsequent results.

The statistical results of the performance metrics H_α and J_{task} are given for 20 independent trials under different methods, as shown in Fig. 11. Fig. 11(a) shows the results of the security performance metric H_α to demonstrate the effectiveness of different methods for defending against cyber-attacks. Fig. 11(b) presents the curves of the control performance metric J_{task} to show how well the different methods accomplish the control task.

Based on the above results, it can be seen that the defense role imparted by PoT from the physical level greatly reduces the likelihood of REPSs being attacked compared with the existing real-time control method. Compared with the existing blockchain-based security control method, the probability of data being attacked in the system under PoT is smaller, i.e., the security is better. It can be seen that the increase in security here is not as significant as the increase compared to the existing resilient control method, which demonstrates the effectiveness of blockchain in improving data security. However, in terms of performance metrics, the proposed PoT-based control method outperforms the existing blockchain-based security control method. The essential reason for this is that in the existing methods blockchain only provides the system with a mechanism for the secure data transmission, and in the consensus mechanism itself it does not take into account the control tasks, system stability, etc. In particular, the method in [56] only protects the measurement data but not the control commands, and cannot compensate for the communication constraints in a distributed fashion. To sum up, from the data-based comparison and discussion above, it can be seen that PoT demonstrates better performance than the existing methods in terms of both security and performance metrics.

Application 2:

For Application 2, the quantitative comparison of PoT with the method in the latest published article is provided in the Supplementary File. The corresponding results are presented in Supplementary Table 4 and Supplementary Fig. 9. In order to avoid similarity to the figures in Application 1, the recorded security data and their analysis are given in the Supplementary File and not presented in the main body of the manuscript.

Specifically, Supplementary Table 4 gives the security probabilities of the three-area power system under different LFC methods. Moreover, in order to quantify the trustworthiness of the data after it has been transmitted through the network, the security performance metric for the multi-area power system under load frequency control is set as follows

$$\begin{aligned} H_{\alpha,lfc} = \sum_{t=t_0}^{t_0+T} (\sum_{i=1}^{N} (\sum_{j\in\mathcal{N}_i^c} (\frac{1}{\Delta P_{tie,j,\max}^{org}} |\tilde{x}_{ij}^{P}(t) - x_j^{P,org}(t)| + \frac{1}{\Delta f_{j,\max}^{org}} |\tilde{x}_{ij}^{f}(t) - x_j^{f,org}(t)|) \\ + \frac{1}{u_{i,\max}^{org}} |\tilde{u}_i(t) - u_i^{org}(t)|)) \end{aligned} \qquad \text{(Eq. 9)}$$

where the meanings of the involved variables are presented in Supplementary Table 10. Variables $\Delta P_{tie,j,\max}^{org}$, $\Delta f_{j,\max}^{org}$, and $u_{i,\max}^{org}$ are used for normalization. Similarly, in order to quantify the effectiveness of different methods for load frequency control, the control performance metric of the system is designed as follows

$$J_{task,lfc} = \sum_{t=t_0}^{t_0+T} \sum_{i=1}^{N} (\frac{1}{ACE_{i,\max}^{org}} |ACE_i^{org}(t)| + \frac{1}{u_{i,\max}^{org}} |u_i^{org}(t)|) \qquad \text{(Eq. 10)}$$

where the meanings of t_0, T and N are the same as those given in Supplementary Table 10, the meanings of the remaining variables are explained in Supplementary Table 11. The statistical results of the performance indicators $H_{\alpha,lfc}$ and $J_{task,lfc}$ during the operation of the three-area power system under different methods are given in Supplementary Fig. 9(a) and Supplementary Fig. 9(b), respectively. It can be seen that the performance metrics $H_{\alpha,lfc}$ and $J_{task,lfc}$ of the power system with the PoT-based LFC strategy are better than that of the power system with the established approach. Consistent with the results in Application 1, PoT enhances the security of load frequency control in the face of cyber threats due to characteristics such as the fact that PoT protects both the raw interaction data and the target data.

Application 3:

To fully illustrate the effectiveness of the proposed method in Application 3, the quantitative comparison with the existing methods is also given. The corresponding results are shown in Supplementary Table 5 and Supplementary Fig. 11.

Specifically, similar to Application 1 and Application 2, Supplementary Table 5 gives the security probability of PFC-based secondary control for the dc microgrid system under different methods. Moreover, the security performance metric of the dc microgrid in the centralized secondary control paradigm is given as

$$H_{\alpha,pfc} = \sum_{t=t_{\sec}}^{t_{\sec}+T} \Big(\sum_{i=1}^{N} \Big(\frac{1}{V_{i,\max}^{org}} |\tilde{y}_i^{V}(t) - y_i^{V,org}(t)| + \frac{1}{I_{ti,\max}^{org}} |\tilde{y}_i^{I}(t) - y_i^{I,org}(t)| + \frac{1}{u_{i,\max}^{org}} |\tilde{u}_i(t) - u_i^{org}(t)|\Big)\Big) \qquad \text{(Eq. 11)}$$

where $\tilde{y}_i^I(t)$ and $\tilde{y}_i^V(t)$ represent voltage and current values of DGU i actually used by the centralized controller, respectively, the meanings of the other variables are the same as those in Supplementary Table 8. To reflect the effectiveness of PFC-based secondary control in accomplishing the regulation tasks given by (12) and (13) of the Supplementary File, the control performance metric is defined as

$$J_{task,pfc} = \sum_{t=t_{\sec}}^{t_{\sec}+T} \Big(\sum_{i=1}^{N} \Big(\frac{1}{V_{i,\max}^{org}} \Big|\frac{1}{N} \sum_{i=1}^{N} V_i(t) - V^{ref}\Big| + \sum_{j \in \mathcal{N}_i^c} \Big(\frac{1}{I_{tj,\max}^{org}} \Big|\frac{I_{tj}^{org}(t)}{\theta_j^s} - \frac{I_{ti}^{org}(t)}{\theta_i^s}\Big|\Big)\Big)\Big) \qquad \text{(Eq. 12)}$$

where the meanings of the variables are shown in Supplementary Table 8 and Supplementary Table 9. The security and control performance metrics of the microgrid under the existing control method as well as the PFC-based secondary control method are available in Supplementary Fig. 11(a) and (b). It can be seen that the PFC-based secondary control exhibits better security and control performance compared with the existing security secondary control strategy. As can be seen from the figure, the PFC-based secondary control has shown satisfactory safety performance in a number of tests.

To address your concerns, we have added experimental comparisons of the proposed method with those in the latest published papers in the revised manuscript. We have also given some quantitative results and the corresponding comparisons.

Based on the reviewer's comments, the authors have made the following modifications to the content of the manuscript:

[Section V, page 8, highlighted in red]

" For comparison, the traditional cooperation-based resilient controller in [13] and the existing blockchain-based security control method in [56] are employed in the testbed first. Fig. 8(a) and Fig. 8(b) give the output responses of the resilient controller and the existing blockchain-based controller subject to attacks and communication delays, respectively. From the waveform results, it can be seen that under the combined influence of attacks and delays, the existing resilient secondary control approach fails to achieve the desired regulation performance, and even leads to system divergence, which is not allowable. Similarly, as shown in the figure, the existing blockchain-based approach is also not competent for distributed security control of dc microgrids. The primary reason for this is that the method in [56] only defends against external attacks, and does not take into account disloyal nodes inside the blockchain network. Moreover, it cannot compensate for communication constraints in a distributed fashion. "

[Section V, page 9, highlighted in red]

" In addition to the waveform results and associated discussion above, quantitative comparisons and analysis are given. Specifically, TABLE IV gives the probability of secure data transmission in the microgrid system under the three methods. The moments of the original attack and the moments of the effective attack after PoT on all 15 signals in the microgrid system are given in Fig. 10(a). Taking the control signal u_1 of the 1st DGU as an example, the original attacked signal and the attacked signal under PoT are given in Fig. 10(b). To better illustrate the effectiveness of the proposed method from a data perspective, the security performance metric H_α and the control performance metric J_{task} are defined as (30) and (31) in Supplementary Note 3, respectively. Fig. 11(a) shows the results of H_α for the REPSs in 20 independent trials under three different methods to demonstrate the effectiveness of different approaches for defending against cyber-attacks. Fig. 11(b) presents the results of J_{task} in the same scenario to show how well the different methods accomplish the control task. ... ”

[Section V, page 10, highlighted in red]

“ Based on the data presented in the results above, it can be seen that the defense role imparted by PoT from the physical level greatly reduces the likelihood of REPSs being attacked compared with the existing real-time control method. As shown in TABLE IV, the security of the microgrid system with the proposed method reaches 95%, which are superior to the existing methods. In terms of security, the improvements that PoT brings compared to the existing blockchain-based security control method are not as significant as compared to the traditional resilient method. This demonstrates the effectiveness of blockchain in improving data security. However, in terms of performance metrics shown in Fig. 11, the proposed PoT-based control method still outperforms the existing blockchain-based security control method. ”

[Section VI, page 12, highlighted in red]

“ For comparison, the PoT-based LFC approach and the normal cooperation-based resilient LFC strategy in [57] are tested in the presence of cyber attacks, and the system responses are shown in Fig. 16. The results indicate that the system subjected to a cyber-attack becomes unstable when utilizing a traditional resilient LFC approach. When using PoT-based LFC, the multi-area power system subjected to the cyber-attack features a smooth response and complies with the generation rate constraints and load reference setpoint constraints. Additionally, the quantitative results, including the performance metrics for both the existing and PoT-based methods, are presented in Supplementary Table 4 and Supplementary Fig. 9. The definitions of these metrics are given in (46) and (47) of Supplementary Note 4. The data in the figure show that $H_{\alpha,lfc}$ and $J_{task,lfc}$ of the proposed method are smaller than those of the existing approach. ... To sum up, the above analysis confirm that the proposed PoT-based distributed LFC algorithm can both guarantee the security of the system and optimise its operation. ”

[Section VII, page 14, highlighted in red]

“ To demonstrate the effectiveness of the proposed method, it is compared with the centralized resilient control method in [58]. As illustrated in Fig. 18(a), the output voltage and current exhibit varying degrees of oscillation under the existing resilient method, and the expected current sharing is not well accomplished. The responses of the dc microgrid system under the PFC-based secondary control method, as depicted in Fig. 18(b), indicate that the average of the output voltages is regulated to the desired level around 48 V and the output currents are accurately shared in the ratio of $1 : 1 : 1.8 : 1.8 :$

1.8. In addition, some quantitative results are given in Supplementary Table 5, Supplementary Fig. 11 and Supplementary Fig. 12, including comparisons of the security probability as well as performance metrics with the established methods. From these results, it can be seen that PFC-based secondary control is still capable of realizing the desired regulation goals of dc microgrids and actively defending the microgrids against cyber-attacks. ... ”

Based on the reviewer's comments, the authors have made the following modifications to the content of the supplementary file:

[Section VI.F, page 31, highlighted in red]

“ To reflect the trustworthiness of the data obtained by REPSs under PoT, the security performance metric is set as

$$\begin{aligned} H_\alpha = \sum_{t=t_{\mathrm{sec}}}^{t_{\mathrm{sec}}+T} \Big(\sum_{i=1}^{N} \Big(\sum_{j \in \mathcal{N}_i^c} \Big(\frac{1}{V_{j,\max}^{org}} |\tilde{y}_{ij}^{V}(t) - y_j^{V,org}(t)| + \frac{1}{I_{tj,\max}^{org}} |\tilde{y}_{ij}^{I}(t) - y_j^{I,org}(t)| \Big) \\ + \frac{1}{u_{i,\max}^{org}} |\tilde{u}_i(t) - u_i^{org}(t)| \Big) \Big) \end{aligned} \tag{30}$$

where the meanings of the involved variables are presented in Supplementary Table 8. It should be noted that $V_{j,\max}^{org}$, $I_{tj,\max}^{org}$, and $u_{i,\max}^{org}$ are used for normalization. Similarly, in order to reflect the performance of the control strategy in accomplishing a given control task of the REPSs, the control performance metric is defined as

$$J_{task} = \sum_{t=t_{\mathrm{sec}}}^{t_{\mathrm{sec}}+T} \sum_{i=1}^{N} \Big(\frac{1}{\bar{V}_{i,\max}^{org}} |\bar{V}_i(t) - V^{ref}| + \sum_{j \in \mathcal{N}_i^c} \Big(\frac{1}{I_{tj,\max}^{org}} \Big| \frac{I_{tj}^{org}(t)}{\theta_j^s} - \frac{I_{ti}^{org}(t)}{\theta_i^s} \Big| \Big) \Big) \tag{31}$$

where t_{sec}, T and N have the same meaning as given in Supplementary Table 8, $\bar{V}_i(t)$ is presented in (18), variables V^{ref}, $\mathcal{N}_i^c$ and θ_i have the same meaning as those in the manuscript, and the meanings of the other variables are available in Supplementary Table 9. ”

[Section VII.D, page 35, highlighted in red]

“ In order to quantify the trustworthiness of the data after it has been transmitted through the network, the security performance metric for the multi-area power system under load frequency control is set as follows

$$\begin{aligned} H_{\alpha,lfc} = \sum_{t=t_0}^{t_0+T} \Big(\sum_{i=1}^{N} \Big(\sum_{j \in \mathcal{N}_i^c} \Big(\frac{1}{\Delta P_{tie,j,\max}^{org}} |\tilde{x}_{ij}^{P}(t) - x_j^{P,org}(t)| + \frac{1}{\Delta f_{j,\max}^{org}} |\tilde{x}_{ij}^{f}(t) - x_j^{f,org}(t)| \Big) \\ + \frac{1}{u_{i,\max}^{org}} |\tilde{u}_i(t) - u_i^{org}(t)| \Big) \Big) \end{aligned} \tag{46}$$

where the meanings of the involved variables are presented in Supplementary Table 10. Variables $\Delta P_{tie,j,\max}^{org}$, $\Delta f_{j,\max}^{org}$, and $u_{i,\max}^{org}$ are used for normalization. Similarly, in order to quantify the performance of different load frequency control methods, the control performance metric of the system is designed as follows

$$J_{task,lfc} = \sum_{t=t_0}^{t_0+T} \sum_{i=1}^{N} (\frac{1}{ACE_{i,\max}^{org}} |ACE_i^{org}(t)| + \frac{1}{u_{i,\max}^{org}} |u_i^{org}(t)|) \tag{47}$$

where the meanings of t_0, T and N are the same as those given in Supplementary Table 10, and the meanings of the remaining variables are explained in Supplementary Table 11. ”

[Section VIII, page 37, highlighted in red]

“ Similar to Application 1 and Application 2, the security performance metric of the dc microgrid in the centralised secondary control paradigm is given as

$$\begin{aligned} H_{\alpha,pfc} = \sum_{t=t_{\text{sec}}}^{t_{\text{sec}}+T} (\sum_{i=1}^{N} ((\frac{1}{V_{i,\max}^{org}} |\tilde{y}_i^V(t) - y_i^{V,org}(t)| + \frac{1}{I_{ti,\max}^{org}} |\tilde{y}_i^I(t) - y_i^{I,org}(t)| \\ + \frac{1}{u_{i,\max}^{org}} |\tilde{u}_i(t) - u_i^{org}(t)|)) \end{aligned} \tag{49}$$

where $\tilde{y}_i^I(t)$ and $\tilde{y}_i^V(t)$ represent voltage and current values of DGU i actually used by the centralized controller, respectively, the meanings of the other variables are the same as those in Supplementary Table 8. In order to evaluate the performance of various secondary control methods for accomplishing the regulation tasks given by (12) and (13), the control performance metric is defined as

$$J_{task,pfc} = \sum_{t=t_{\text{sec}}}^{t_{\text{sec}}+T} (\sum_{i=1}^{N} (\frac{1}{V_{i,\max}^{org}} | \frac{1}{N} \sum_{i=1}^{N} V_i(t) - V^{ref} | + \sum_{j \in \mathcal{N}_i^c} (\frac{1}{I_{tj,\max}^{org}} | \frac{I_{tj}^{org}(t)}{\theta_j^s} - \frac{I_{ti}^{org}(t)}{\theta_i^s} |))) \tag{50}$$

where the meanings of the variables are shown in Supplementary Table 8 and Supplementary Table 9. ”

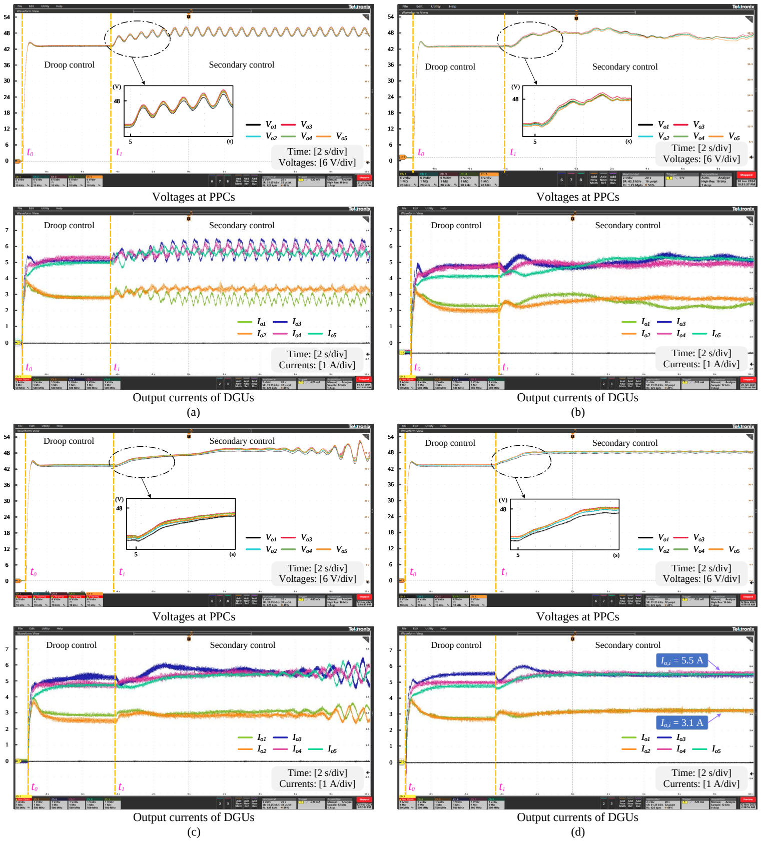


Fig. 8: Microgrid responses under (a) the resilient method in [13], (b) the blockchain-based method in [56], (c) the PoT-based method without delay compensation, and (d) the PoT-based method.

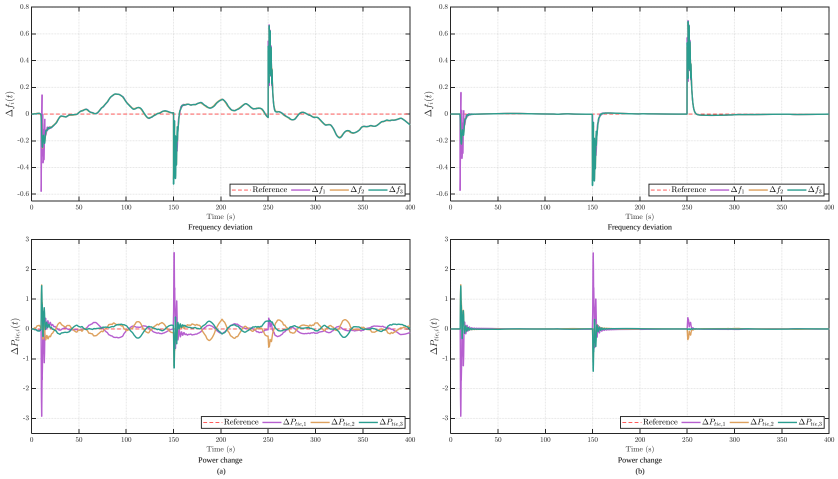
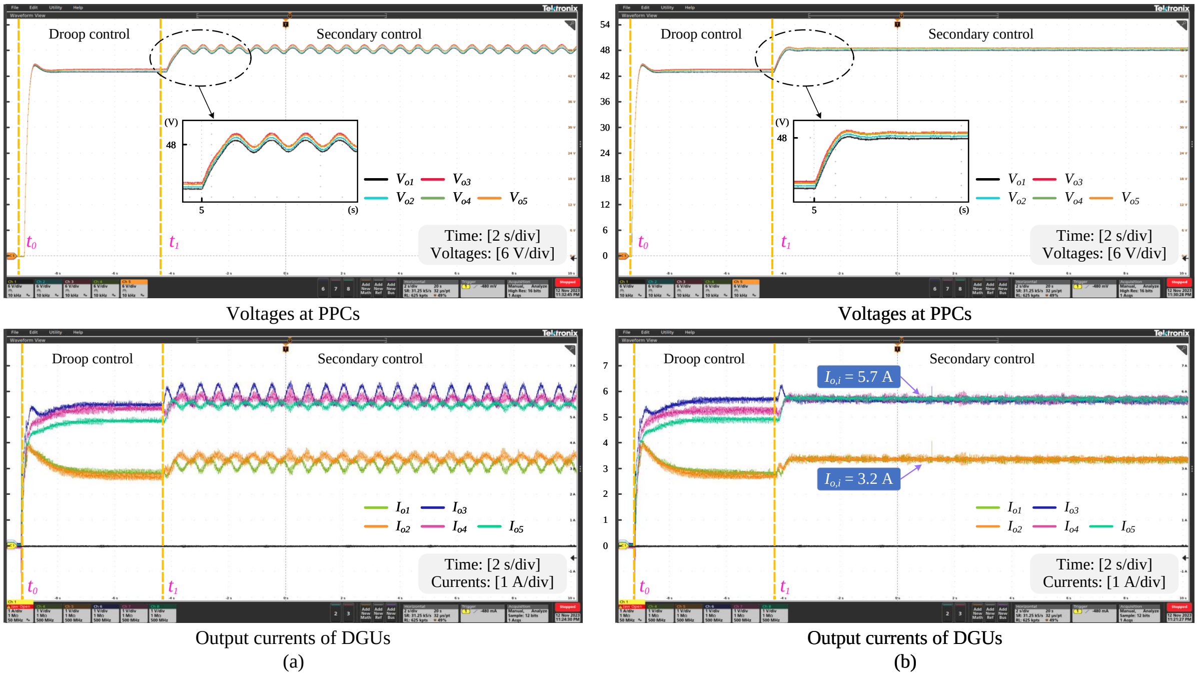


Fig. 16: Responses of the three-area power system for (a) the existing resilient method in [57] and (b) PoT-based LFC scheme.



Voltages at PPCs

Voltages at PPCs

Output currents of DGUs

(a)

Output currents of DGUs

(b)

Fig. 18: Microgrid responses under (a) the existing method in [58] and (b) the PFC-based approach.

TABLE IV: Probability of secure data transmission in the microgrid system with different approaches

Methods\ DGUs	DGU 1	DGU 2	DGU 3	DGU 4	DGU 5
Method 1*	0.53	0.54	0.63	0.55	0.58
Method 2*	0.81	0.77	0.75	0.80	0.79
Method 3*	**0.94**	**0.96**	**0.95**	**0.95**	**0.97**

Method 1*, Method 2* and Method 3* refer to the approach proposed in [13], [56] and this paper, respectively.

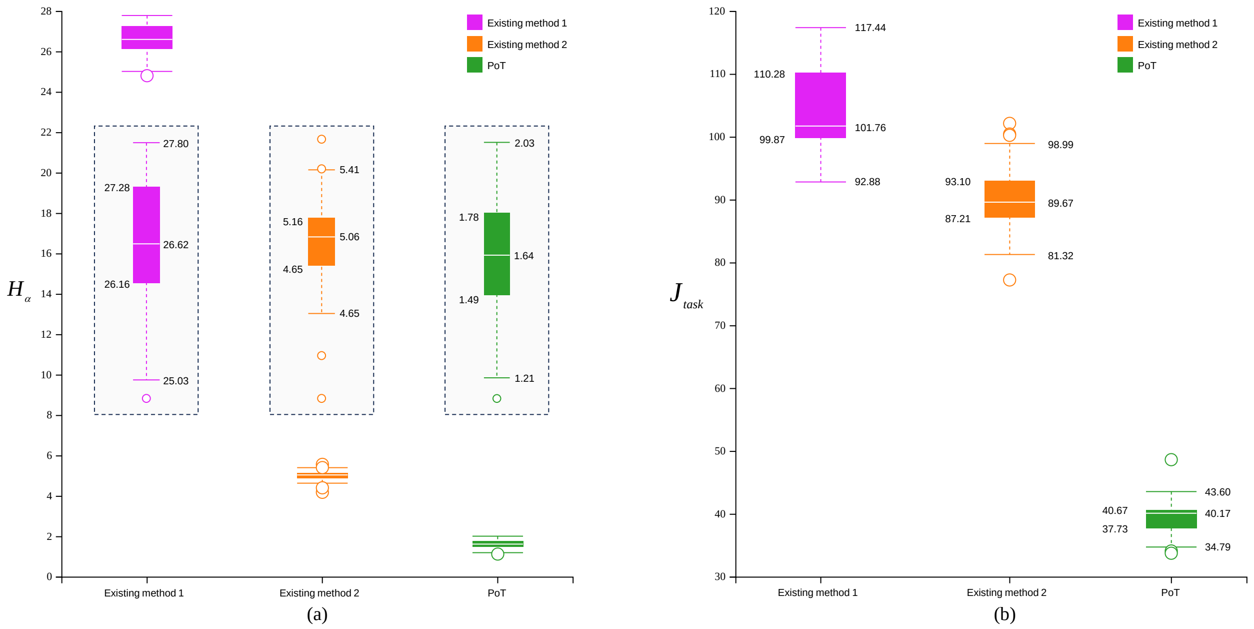


Fig. 11: Comparison of the performance metrics of the tested microgrid system under different approaches: (a) the security performance metric H_α, (b) the control performance metric J_{task}. The middle part of (a) shows three enlarged subplots. The methods labeled as 'Existing method 1' and 'Existing method 2' correspond to the approaches in [13] and [56], respectively.

Supplementary Table 8: Meanings of the variables in equation (30)

Variable	Meaning
t_{sec}	Moment activating the secondary control strategy
T	Action time of the secondary control strategy
N	Number of DGUs contained in the microgrid
$y_j^{V,org}(t)$	Ideal voltage value of DGU j in the microgrid
$y_j^{I,org}(t)$	Ideal current value of DGU j in the microgrid
$u_i^{org}(t)$	Ideal control command of DGU i in the microgrid
$\tilde{y}_{ij}^{I}(t)$	Voltage value actually used by the controller in the microgrid, which received by DGU i from DGU j
$\tilde{y}_{ij}^{V}(t)$	Current value actually used by the controller in the microgrid, which is received by DGU i from DGU j
$\tilde{u}_i(t)$	Control command actually used by the actuator of DGU i in the microgrid
$V_{j,\max}^{org}$	Maximum ideal voltage value of DGU j during secondary control period
$I_{tj,\max}^{org}$	Maximum ideal current value of DGU j during secondary control period
$u_{i,\max}^{org}$	Maximum ideal control command of DGU i during secondary control period

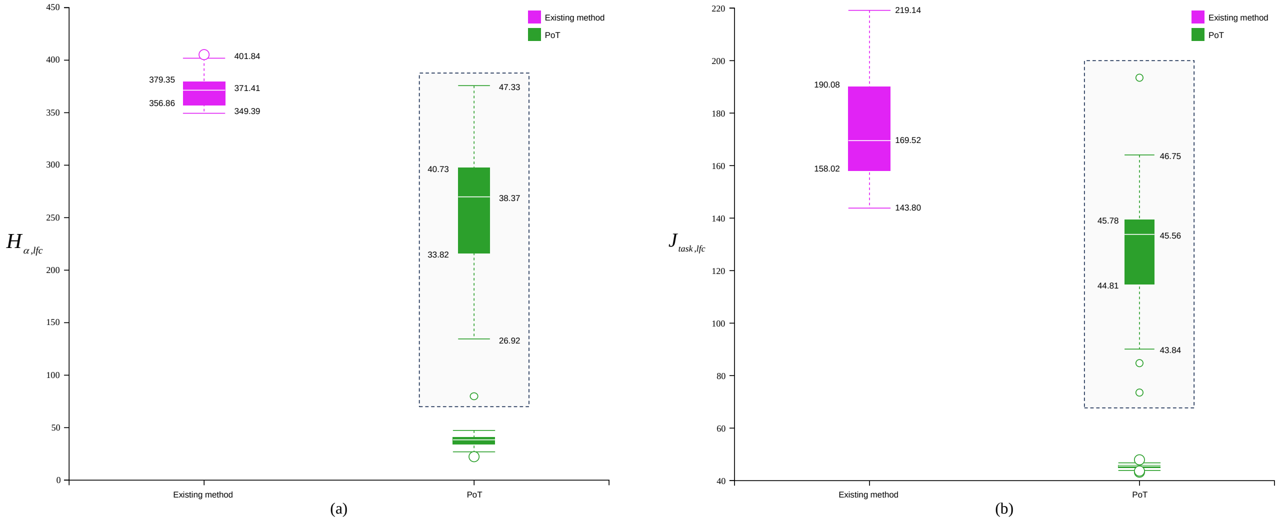
Supplementary Table 9: Meanings of the variables in equation (31)

Variable	Meaning
$\bar{V}_{i,\max}^{org}$	Maximum ideal estimated voltage value of DGU i during secondary control period
$I_{tj,\max}^{org}$	Maximum ideal current value of DGU j during secondary control period
$I_{tj}^{org}(t)$	Ideal/measured current value of DGU j in the microgrid

Supplementary Table 4: Probability of secure data transmission in the multi-area power system with different approaches

Methods\Areas	Area 1	Area 2	Area 3
Method 1*	0.54	0.57	0.61
Method 2*	**0.96**	**0.93**	**0.97**

Method 1* and Method 2* refer to the approach proposed in [57] and the PoT-based LFC method in this paper, respectively.



(a)

(b)

Supplementary Fig. 9: Comparison of the performance metrics of the tested three-area power system under different approaches: (a) the security performance index $H_{\alpha,lfc}$, (b) the control performance index $J_{task,lfc}$. The middle part of the figure shows two enlarged subplots. The method labeled as ‘Existing method’ corresponds to the approach in [57] of the paper.

Supplementary Table 10: Meanings of the variables in equation (46)

Variable	**Meaning**
t_0	Moment activating the specific load frequency control
T	Action time of the load frequency control strategy
N	Number of subsystems contained in the three-area power system
$x_j^{P,org}(t)$	Ideal power deviation value (i.e., ideal $\Delta P_{tie,j}(t)$) of subsystem j in the three-area power system
$x_j^{f,org}(t)$	Ideal frequency deviation value (i.e., ideal $\Delta f_j(t)$) of subsystem j in the three-area power system
$\tilde{x}_{ij}^{P}(t)$	Power deviation value actually used by the controller in the power system, which received by subsystem i from subsystem j
$\tilde{x}_{ij}^{f}(t)$	Frequency deviation value actually used by the controller in the power system, which received by subsystem i from subsystem j
$\tilde{u}_i(t)$	Control command actually used by the actuator of subsystem i in the power system
$u_i^{org}(t)$	Ideal control command of subsystem i in the power system
$\Delta P_{tie,j,\max}^{org}$	Maximum ideal power deviation value of subsystem j during power system operation
$\Delta f_{j,\max}^{org}$	Maximum ideal frequency deviation value of subsystem j during power system operation
$u_{i,\max}^{org}$	Maximum ideal control command of subsystem i during power system operation

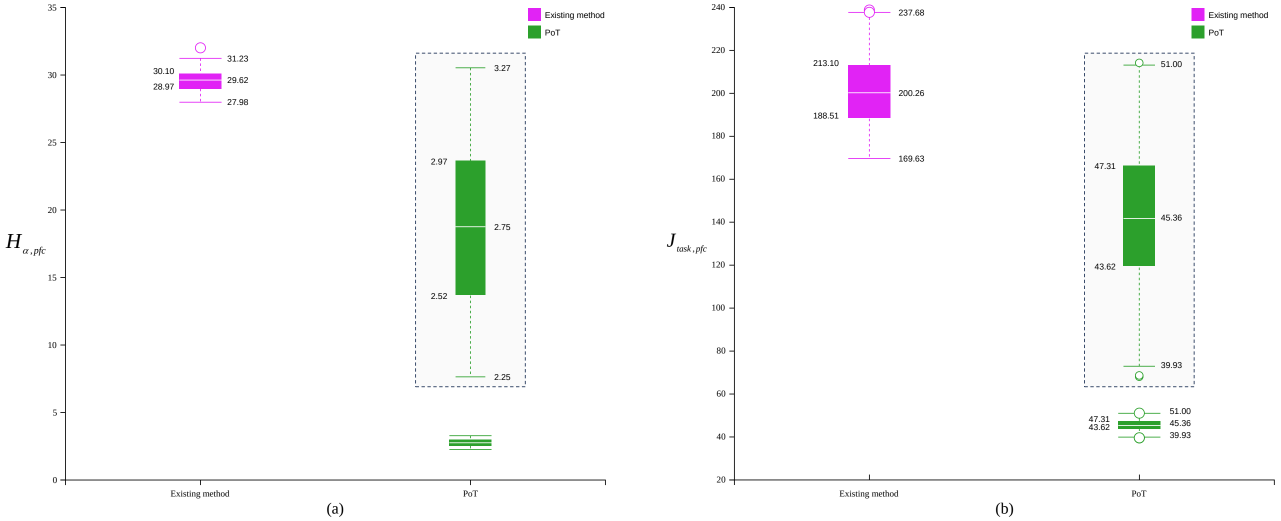
Supplementary Table 11: Meanings of the variables in equation (47)

Variable	**Meaning**
$ACE_{i,\max}^{org}$	Maximum ideal area control error of subsystem i during power system operation
$ACE_i^{org}(t)$	Ideal area control error of subsystem i in the three-area power system, which is calculated from the measured power deviation and frequency deviation values

Supplementary Table 5: Probability of secure data transmission in the dc microgrid system with different approaches

Methods\DGUs	DGU 1	DGU 2	DGU 3	DGU 4	DGU 5
Method 1*	0.48	0.47	0.47	0.48	0.51
Method 2*	**0.90**	**0.91**	**0.91**	**0.92**	**0.92**

Method 1* and Method 2* refer to the approach proposed in [58] of the paper and the PFC-based secondary control in this paper, respectively.



Supplementary Fig. 11: Comparison of the performance metrics of the microgrid system under different centralized approaches: (a) the security performance index $H_{\alpha,pfc}$, (b) the control performance index $J_{task,pfc}$. The middle part of the figure shows two enlarged subplots. The method labeled as ‘Existing method’ corresponds to the approach in [58] of the paper.

References

[1] J. Yang, J. Dai, H. B. Gooi, H. D. Nguyen, and A. Paudel, "A proof-of-authority blockchain-based distributed control system for islanded microgrids," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 8287–8297, 2022.

[2] Y. Yu, G.-P. Liu, H. Xiao, and W. Hu, "Design of networked secure and real-time control based on blockchain techniques," *IEEE Transactions on Industrial Electronics*, vol. 69, no. 4, pp. 4096–4106, 2022.

[3] Y. Yu, G.-P. Liu, and W. Hu, "Learning-based secure control for multichannel networked systems under smart attacks," *IEEE Transactions on Industrial Electronics*, vol. 70, no. 7, pp. 7183–7193, 2023.

[4] Y. Huang, G.-P. Liu, Y. Yu, and W. Hu, "Data-driven distributed predictive tracking control for heterogeneous nonlinear multi-agent systems with communication delays," *IEEE Transactions on Automatic Control*, 2024.

[5] G.-P. Liu, "Coordinated control of networked multiagent systems with communication constraints using a proportional integral predictive control strategy," *IEEE Transactions on Cybernetics*, vol. 50, no. 11, pp. 4735–4743, 2020.

[6] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE symposium on security and privacy*, pp. 104–121. IEEE, 2015.

[7] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE transactions on knowledge and data engineering*, vol. 30, no. 7, pp. 1366–1385, 2018.

[8] S. Chen *et al.*, "A blockchain consensus mechanism that uses proof of solution to optimize energy dispatch and trading," *Nature Energy*, vol. 7, no. 6, pp. 495–502, 2022.

[9] H. M. Khalid *et al.*, "Wams operations in power grids: A track fusion-based mixture density estimation-driven grid resilient approach toward cyberattacks," *IEEE Systems Journal*, 2023.

[10] Q. Tang, C. Deng, Y. Wang, F. Guo, and S. Fan, "Iterative observer-based resilient control for energy storage systems in microgrids under fdi attacks," *IEEE Transactions on Smart Grid*, 2024.

[11] M. Andoni *et al.*, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renewable and sustainable energy reviews*, vol. 100, pp. 143–174, 2019.

[12] M. B. Mollah *et al.*, "Blockchain for future smart grid: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 18–43, 2020.

[13] D. K. Mishra, P. K. Ray, L. Li, J. Zhang, M. Hossain, and A. Mohanty, "Resilient control based frequency regulation scheme of isolated microgrids considering cyber attack and parameter uncertainties," *Applied Energy*, vol. 306, p. 118054, 2022.

[14] Z. Liu and L. Wang, "A distributionally robust defender-attacker-defender model for resilience enhancement of power systems against malicious cyberattacks," *IEEE Transactions on Power Systems*, 2022.

[15] A. Aljohani, M. AlMuhaini, H. V. Poor, and H. Binqadhi, "A deep learning-based cyber intrusion detection and mitigation system for smart grids," *IEEE Transactions on Artificial Intelligence*, 2024.

[16] M. Kesici, B. Pal, and G. Yang, "Detection of false data injection attacks in distribution networks: A vertical federated learning approach," *IEEE Transactions on Smart Grid*, 2024.

[17] S. Xu, D. Ye, G. Li, and D. Yang, "Globally stealthy attacks against distributed state estimation in smart grid," *IEEE Transactions on Automation Science and Engineering*, 2024.

[18] X. Luo, R. Gao, X. Li, Y. Fu, Q. Xu, and X. Guan, "Event-based attack detection and mitigation for dc microgrids via adaptive lqr approach," *IEEE Transactions on Smart Grid*, 2024.

[19] X. Ran, W. P. Tay, and C. H. Lee, "Robust data-driven adversarial false data injection attack detection method with deep q-network in power systems," *IEEE Transactions on Industrial Informatics*, 2024.

[20] T. Tabassum, S. Lim, and M. R. Khalghani, "Artificial intelligence-based detection and mitigation of cyber disruptions in microgrid control," *Electric Power Systems Research*, vol. 226, p. 109925, 2024.

[21] M. K. AlAshery *et al.*, "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.

[22] Y. Yu, G.-P. Liu, X. Zhou, and W. Hu, "Blockchain protocol-based predictive secure control for networked systems," *IEEE Transactions on Industrial Electronics*, vol. 70, no. 1, pp. 783–792, 2023.

[23] A. B. Masood, A. Hasan, V. Vassiliou, and M. Lestas, "A blockchain-based data-driven fault-tolerant control system for smart factories in industry 4.0," *Computer Communications*, vol. 204, pp. 158–171, 2023.

[24] V. Veerasamy, Z. Hu, H. Qiu, S. Murshid, H. B. Gooi, and H. D. Nguyen, "Blockchain-enabled peer-to-peer energy trading and resilient control of microgrids," *Applied Energy*, vol. 353, p. 122107, 2024.