nature communications

Article

https://doi.org/10.1038/s41467-024-54626-y

A blockchain consensus mechanism for real-time regulation of renewable energy power systems

Received: 11 March 2024

Accepted: 13 November 2024

Published online: 05 December 2024

Check for updates

Yi Yu [1,2,3], Guo-Ping Liu [1,2] ✉, Yi Huang [4], Chi Yung Chung [3] & Yu-Zhong Li [5]

With the ongoing development of renewable energy sources, information technologies and physical energy systems are further integrated, which leads to challenges in ensuring the secure and stable operation of renewable energy power systems in the face of potential cyber threats. The strengths of blockchain in cybersecurity make it a promising solution to these challenges. However, existing blockchains are not well-suited for control tasks due to their low real-time performance. Here, we present a consensus mechanism that enables real-time security control of systems, called Proof of Task. Instead of solving meaningless hash puzzles in Proof of Work, Proof of Task addresses problems closely related to the stable operation and control performance of these systems. With the proposed verification mechanism, Proof of Task significantly enhances the real-time performance of blockchain while mines its computational resources for tasks of interest. To demonstrate the effectiveness and necessity of Proof of Task, it is deployed across three renewable energy power systems. The results show that Proof of Task markedly fortifies the security and computing capability of these systems, ensuring their reliable and stable operation. This work highlights the promise of blockchain to facilitate security control and trusted computing of large-scale, complex-dynamic systems.

Renewable clean energy resources are gaining attention for their immense potential to mitigate the environmental detriments associated with fossil fuel consumption[1,2]. Increasing advances in technologies such as solar, wind, and hydrogen power have brought the sustainability to power systems, but they have also endowed the systems with strong uncertainty and vulnerability[3,4]. To achieve large-scale resource integration, the Renewable Energy Power Systems (REPSs) will take the form of coordinated transmission from multiple resources with huge quantities and wide geographical distribution. The low inertia, limited overload tolerance, and high stochasticity of generation units based on renewable energy resources, interfaced with power electronic devices, make it necessary for the generation subsystems to interact frequently during the regulation process[4,5]. In a non-ideal communication environment, ensuring the secure and uninterrupted operation of REPSs, amid pervasive data exchanges, presents a formidable challenge[6,7].

Incidents, such as the 2015 Ukraine blackout caused by an attack[8], illustrate the importance of cybersecurity for the stable operation of power systems[9]. REPSs consisting of massive amounts of distributed energy resources[10,11] also face significant security risks from external network intrusions, if not worse[12,13]. 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[14–19]. Specifically, various control strategies for attack

[1]Shenzhen Key Laboratory of Control Theory and Intelligent Systems, Southern University of Science and Technology, Shenzhen, China. [2]Center for Control Science and Technology, Southern University of Science and Technology, Shenzhen, China. [3]Department of Electrical and Electronic Engineering and Research Centre for Grid Modernisation, The Hong Kong Polytechnic University, Hong Kong SAR, China. [4]School of Electrical Engineering and Automation, Wuhan University, Wuhan, China. [5]School of Computer Science and Engineering, Huizhou University, Huizhou, China. ✉e-mail: liugp@sustech.edu.cn

prevention[16], attack detection[17], and attack mitigation[18] 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 often depend on an understanding of the dynamic properties of the threats and may not ensure the captured data of the system is as trustworthy as possible[16]. The reason is that most of these strategies implement countermeasures that passively tolerate negative impacts after an attack occurs or rely on detection-based packet discarding to protect systems from specific types of attacks[19]. As a result, current resilient methods are insufficient and limited in their defensive capabilities.

The emerging blockchain technology holds the promise of addressing the security issues at the root[20,21]. Among its numerous characteristics, decentralization, security, and a single source of truth stand out for their high compatibility with the demands of power systems[22,23]. Specifically, the decentralization of blockchain complements the distributed control strategy of REPSs, which is also robust to a single point of failure, prompting possibilities for blockchain-enabled control[24]. The control algorithm generates control commands based on measurements received via the communication network, making the control effects susceptible to network anomalies. The security features of blockchain will offer a guarantee of the integrity of measurement data during interactions[25]. Furthermore, the single source of truth strengthens the security of the control strategy as it allows the system to adjust the transmission strategy based on observed results.

Critical elements of the blockchain technology include Peer-to-Peer (P2P) networks, consensus mechanisms, and smart contracts[22]. Detailed descriptions of the roles of these components are provided in Supplementary Note 1. Among these, the consensus mechanism mainly determines the security and processing speed of blockchain, making it a focal point of extensive research[26]. Due to its success in underpinning Bitcoin[27] and Ethereum[28], Proof of Work (PoW) is often regarded as the most popular consensus mechanism. Besides, Proof of Stake is popularly known for eliminating the high energy consumption associated with PoW and is utilized in Ethereum 2.0, etc[29]. Due to varying evaluation criteria, the compelling aspects of various consensus algorithms differ, while they also expose different flaws[30]. Consequently, many advanced alternative mechanisms have emerged, including Delegated Proof of Stake[31], Delegated Byzantine Fault Tolerance[32], Proof of Capacity[33], etc. It is an endless quest to design an effective consensus mechanism that balances speed, scalability, decentralization, and security.

Blockchain technology is shining in some areas such as finance, energy management, and supply chain management[34,35]. 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. However, it inherits the limitations of PoW, such as high resource consumption for solving hash puzzles and long waiting times for usable solutions. Subsequently, AlAshery et al. suggested a mechanism called Proof of Clearance (PoC)[37], which replaces the hash puzzle in PoW with a winner determination problem in the energy trading market. PoC has been applied in dispatch of energy power systems and trading of energy markets, but it does not explicitly specify the conditions for verifying whether a candidate solution is optimal, which is an aspect worth further improvement. Additionally, a consensus mechanism, Proof of Solution (PoSo), which substitutes the meaningless mathematical puzzle in PoW with a meaningful optimization problem, was proposed[38]. PoSo has achieved impressive results in energy dispatch and trading due to its well-designed verification mechanism. However, its applicability is limited to optimization problems where optimal solutions can be verified using the Karush–Kuhn–Tucker conditions and the second-order sufficient conditions, which may not be suitable for certain applications. Beyond these contributions, numerous studies are exploring the use of blockchain to enhance the efficiency, security, and reliability of energy dispatch and trading in power systems[39–43].

However, the control of REPSs has unique characteristics compared with aforementioned energy dispatch and trading, such as numerous state constraints, complex multi-objective problems, and high real-time requirements with a short time scale[44]. These nuances pose significant challenges for classical consensus mechanisms. Consequently, there are ongoing efforts to tap the potential of blockchain in the area of control for dynamical systems[45–49]. Specifically, the authors of ref. 45 introduced the blockchain consensus mechanism into networked control systems 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 enhance the suitability of blockchain for the security control of networked systems[46], their work remains at the level of combining blockchain with control systems and mitigating the drawbacks that blockchain brings to systems, rather than proposing a consensus mechanism that integrates the unique characteristics of real-time control and the multi-party nature of blockchain. Blockchain was applied to microgrid control in ref. 47. However, similar to ref. 46, this work applied existing consensus mechanisms to the security control framework without designing a consensus protocol exclusively for the control of REPSs. Abdullah et al. proposed a blockchain-based fault-tolerant control framework aimed at enhancing the response of Industry 4.0 smart factories in the event of anomalies such as cyberattacks[48]. However, for systems with short sampling periods, such as REPSs, this method may be inadequate, as it assumes minute-level sampling for industrial control systems.

To sum up, most existing studies have treated blockchain merely as a means of data interaction in power energy systems, without actually engaging it into the achievement of control tasks. Furthermore, existing research has only leveraged the multi-party verification nature of blockchain, while its other inherent capabilities remain underutilized. As a result, research on blockchain for the control of power energy systems is still at an embryonic stage. In this work, we suggest a blockchain consensus mechanism called Proof of Task (PoT) for real-time control of REPSs. In PoT, the term “task” refers to various control tasks of REPSs relevant to actual application scenarios. Essentially, PoT determines which data will be adopted based on the contributions made by peers in completing these control tasks. This blockchain consensus mechanism features several distinctive characteristics as follows.

(1) Similar to the mathematical puzzles in PoW, the problems to be solved by the peers under PoT are also computationally intensive. However, we have assigned 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 criteria for the published solutions are closely related to the stability of the system. This approach could enable better integration of blockchain into the REPSs, which has not been explored in previous work on blockchain-based security control[46–48].

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

(3) Unlike existing consensus mechanisms[37,38], PoT protects both source data (measurements) and target data (control commands). This dual protection not only defends against malicious nodes within the

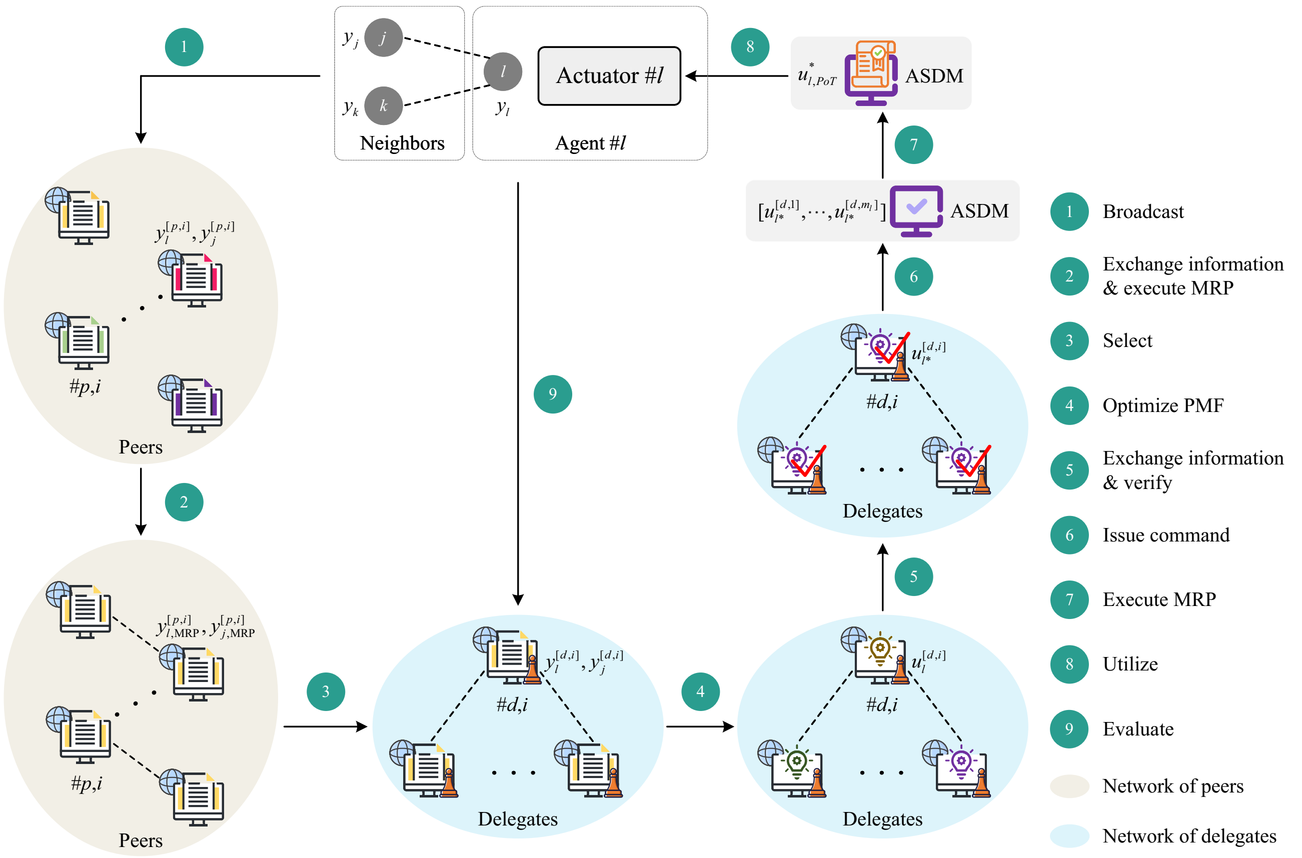

Fig. 1 | Architecture of the PoT consensus protocol. Step 1: Agents l, j and k send raw interaction data to the P2P network. Step 2: Nodes in the P2P network exchange their data and perform the Majority Rule Principle (MRP) on raw interaction data belonging to each node. Step 3: Choose representative nodes to form a delegation. Step 4: Delegates obtain their respective candidate control command by solving a constrained optimization problem on the regulation Performance Metric Function (PMF). Step 5: Delegates exchange solutions, validate viable control inputs through stability criteria, and choose a relatively optimal one on the PMF. Step 6: Each delegate issues the locally validated command to the Actuator-Side Decision Maker (ASDM). Step 7: The ASDM selects the final control input $u^*_{l,PoT}$ based on the MRP. Step 8: The actuator takes input $u^*_{l,PoT}$. Step 9: Score delegates based on their performance in the round.

network, but also enhances the resilience of the system against external cyber-attacks. By combining the practical verification mechanisms mentioned above, it can be seen that PoT imparts attractive attributes to REPSs, including 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 solely on software algorithms[15,17], 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.

Ultimately, the effectiveness of PoT is demonstrated through its application in a renewable energy resource-based microgrid system and a multi-area interconnected power system. These results show that blockchain could bring promising possibilities for real-time control of complex dynamic systems.

Results

Methodology of Proof of Task

Blockchain has the potential to enhance the security of data interactions within the system. However, characteristics such as low real-time performance have hindered the widespread adoption of blockchain technology in the control of REPSs. In addition, taking into account the internal and external challenges, i.e., simultaneously guaranteeing the integrity of the nodes inside blockchain and defending against outside attacks, the full exploitation of the computational resources of blockchain has not yet been well realized. To this end, a PoT consensus mechanism that enables real-time regulation is proposed in this paper, as shown in Fig. 1.

First, a meaningful optimization problem associated with the control task is issued for each peer to solve. To be specific, the cost function serves as a performance metric linked to the regulation objective, while the constraints play a critical role in ensuring the stable operation of REPSs. In this way, the computing capabilities of each blockchain node are fully unleashed, providing abundant computational resources in addition to security guarantees for the control of REPSs.

Second, the verification mechanism of PoT is original and compatible with regulation objectives of REPSs. Here, a combination of stability-related conditions and optimality-based relative verification is proposed to validate the published solutions. The stability conditions are designed to ensure that the acquired control commands meet fundamental requirements for system operation, while the optimality-based relative verification improves consensus efficacy. This verification approach provides each blockchain node with the opportunity to participate in the realization of the control task, facilitating the integration of blockchain into real-time control systems.

For this matter, Fig. 2 demonstrates the utilization of computational resources under different blockchain consensus mechanisms. Whether every peer participates in the solving process in PoW or only one peer performs the computation in PoSo, there is only one

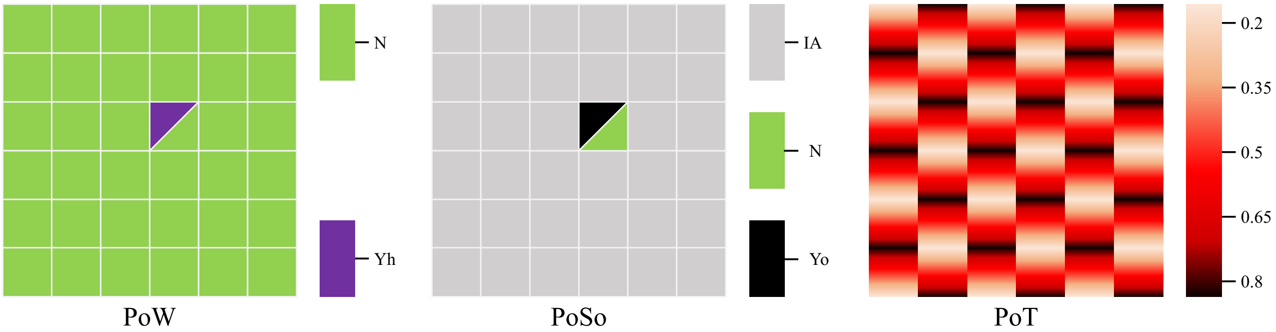

Fig. 2 | Schematic for the exploitation of computing resources of blockchain nodes in different consensus algorithms. Each small square represents the computational resource of a node, and the color on it indicates whether its resource is utilized and whether a valid result is obtained. The occurrence of multiple colors on a square indicates the presence of multiple situations. N denotes that the node gets a solution that does not pass local validation. Yh means that the node gets the solution to the issued meaningless problem. Yo indicates that the node gets the solution to the issued meaningful problem. IA means that the node is not activated to solve the issued problem. The interval (0, 1) represents that the node gets a feasible solution to the meaningful optimization problem, and the magnitude of this value represents the optimality of the solution, where 0 and 1 indicate the node with no feasible and an optimal solution, respectively.

submitted candidate solution waiting for validation. Besides, in the absolute verification method they employ, only when the submitted solution or its hash value is exactly equal to a desired value can it pass validation. It is likely that multiple rounds of consensus will not yield a trusted winner, which would significantly increase time delays. In contrast, the PoT mechanism gathers all the candidate solutions generated by peers and selects the best one based on the performance index function. This optimality-based relative verification enables the system to obtain a trusted solution in each round of consensus, which is one of the key endeavors of PoT to improve its real-time performance. Furthermore, blockchain nodes participate in consensus as both data publishers and validators, thus tapping into the computing power of the vast majority of blockchain nodes.

Third, at the end of the fixed waiting time in each round of solving, all blockchain nodes must simultaneously broadcast the current solution obtained for the assigned optimization problem throughout the delegation network. The simultaneous release of data ensures that the time taken to solve the optimization problem is consistent across all blockchain nodes, and determines the time delay imposed on the system by the solving process in PoT. In this way, specialized techniques, such as predictive control, can be designed to compensate for these communication delays. In addition, this practice makes the time required for problem solving and solution broadcasting controllable. By setting a reasonable waiting time, PoT will take far less time to run compared to other blockchain consensus mechanisms. This represents an improvement of the PoT mechanism to accommodate the demands for high real-time performance in control systems.

Finally, not all blockchain nodes within the P2P network participate in the consensus process under PoT. Instead, appropriate delegates are intelligently and dynamically selected to engage in the consensus through a hybrid policy derived from a game. This reflects the intelligence of the PoT mechanism and further improves the security of the system. A blockchain network that remains static is more vulnerable to attacks. For example, in ref. 50, a malicious adversary could devise an efficient stealthy attack scheme against the system with a static communication mode. In both PoW and PoC mechanisms, full participation is involved in problem solving. Nevertheless, the PoSo mechanism selects a delegation, from which a single leader is further chosen, allowing only one node to participate in the computation. All of these factors suggest that existing consensus algorithms may not be sufficiently intelligent or robust against cyber-attacks.

In summary, the nodes in PoT will solve an optimization problem related to the control tasks of REPSs, while the validation of candidate solutions determines the stability of the system (Supplementary Note 2). Therefore, the successful completion of PoT will be closely tied to the secure and stable operation of REPSs. In addition, PoT utilizes a simpler problem, rather than the complex and time-consuming hash puzzles found in traditional blockchain, to meet the requirements of real-time control. Although PoT may not be as secure as PoW, the combination of problem-solving related to control tasks and a slightly more complex verification mechanism than PoW makes PoT suitable and competent for real-time security control of REPSs.

Proof of Task-based secure real-time regulation

From the perspective of the owned blockchain elements, the comparison between the proposed PoT consensus mechanism and existing typical mechanisms is summarized in Table 1. As can be seen, the current consensus algorithms are unsuitable for the regulation of REPSs because none of them involves the conversion of transaction data (measurements) into terminal data (control commands). It is this conversion that imposes significant security and real-time requirements, which are not met by existing mechanisms, such as PoC and PoSo.

Instead, the PoT mechanism not only protects data throughout the entire control cycle against both external malicious attacks and internal dishonest nodes, but also ensures real-time performance through a specialized validation mechanism, etc. Consequently, the PoT framework outperforms the existing work in this regard.

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. On the other hand, the advantages possessed by blockchain are fully unleashed through a two-pronged approach of reducing the induced delays of PoT and compensating for delays that cannot be further eliminated. These advantages include rich computational resources and high security. A real-time output regulation scheme based on PoT is no longer merely a simple combination of blockchain technology and the control system. Instead, the system dynamically influences the elections within the PoT mechanism, while the execution of the PoT mechanism, in turn, determines the dynamic behavior of the system.

In addition, the advantages and disadvantages of the PoT-based regulation framework, compared to the existing output regulation methods for REPSs, particularly regarding the robustness to a single point of failure, etc., are summarized in Table 2. As can be seen from the table, the proposed PoT-based output regulation scheme offers significant advantages over existing methods owing to two key factors, namely its multi-node structure and its elaborate consensus mechanism. Moreover, in the proposed framework, the regulation strategy is deployed and executed in a distributed manner, which follows the characteristics of distributed power resources in REPSs.

Table 1 | Characteristics of different consensus mechanisms

Consensus mechanism	Protected data	Consensus value*	Meaningful solution	Operation center	Real-time	Security	Complexity	Efficiency
PoW	Transaction	No	No	No	Low	High	High	Low
PoC	Solution	No	Yes	No	Low	High	Low	High
PoSo	Solution	No	Yes	Yes	Medium	High	Low	High
PoT	Measurement and solution	Yes	Yes	No	High	High	Medium	High

Consensus value* denotes that there must be a value under a round of consensus.

Table 2 | Comparison of different regulation architectures

Regulation architecture	Centralized	Decentralized	Distributed resilient	Blockchain-based distributed	PoT-based
Tolerance of single point of failures	No	Yes	Yes	Yes	Yes
Defend against cyber-attacks	No	No	Yes	Yes	Yes
Optimality of regulation	No	No	No	No	Yes
Intelligence of regulation	No	No	No	No	Yes
Examples	57,58	51,59	60,61	47,52	This article

Representative extensions of Proof of Task

PoT improves the system security while releasing computational resources of the P2P network. As a result, there are two main directions for PoT variants. From the point of view of computational resources, the P2P network can either take on more computation tasks associated with the controller or none at all. From a security standpoint, there is potential to either add or reduce the authentication elements within the PoT framework.

Based on the above discussion, two highly representative variants can be shaped. To be specific, a variant called Degraded PoT (DPoT) can be derived by centralizing the PoT mechanism and excluding the P2P network from the computation tasks. At this point, DPoT would facilitate secure transmission. Similarly, by incorporating local verification into the actuator, another variant known as Upgraded PoT (UPoT) can be evolved. It can be seen DPoT is easier to deploy in REPSs, while UPoT further improves the security of REPSs against cyber-attacks. These two distinctive variants are described in detail below.

(1) Upgraded PoT Mechanism. Here, the UPoT mechanism with re-verification at the actuator is proposed for a kind of adverse scenarios where more than 50% of nodes in the blockchain network suffer attacks. In such cases, the broken data arriving at the ASDM will dominate, and the actuator will use that corrupted signal based on the MRP under PoT. To address this issue, the re-verification process is implemented. When the actuator receives different control commands, it not only counts which one occurs the most times, but also verifies whether these values meet the stability conditions and compares their performance functions after the control commands pass the initial verification.

Counting is simpler for the ASDM than verifying conditions, calculating performance functions, and making comparisons. Therefore, the ASDM will first judge if all the received control commands are the same during this control period. The best situation is that all the commands presented to the ASDM are the same, then the data will pass unanimously without the need for local validation. Notice that attackers and dishonest nodes will try their best to generate consistent misleading data in order to maximize the damage to the system. In other words, there are at most two types of data arriving at the ASDM: one is real data, and the other is corrupted data. When two different control commands arrive, it is not the one with more votes that wins under UPoT, but the one that performs better after verification and comparison of the performance functions. The specific procedure of UPoT described above is detailed in Supplementary Algorithm 1.

Although a slight increase in workload, the newly added comparative validation makes UPoT more secure than PoT. The following example supports this statement. It is assumed that the communication environment is such that there are no dishonest nodes in the blockchain network and that the system only encounters external cyber-attacks. In this scenario, the system based on PoT executes the compromised control command as soon as attackers disrupt more than half of the communications. Instead, UPoT can identify the correct candidate solution for the system as long as not all communications are corrupted.

(2) Degraded PoT Mechanism. PoT provides excellent security and rich computational resources for accomplishing the regulation task of REPSs. It can be seen that both PoT and UPoT maintain distributed architectures that necessitate a P2P network for each generation unit. While this architecture guarantees advantages such as the plug-and-play functionality, it also incurs high costs. As illustrated in Fig. 1, certain operations in PoT, such as the MRP, are executed more than once in order to protect measurement signals and control commands separately. Although PoT provides powerful computational resources for REPSs, it simultaneously imposes demands on the computational capability of participating peers. In some specific scenarios, these peers may not possess sufficient computational resources, or it may be inaccessible to free up their computational resources.

In order to develop a DPoT mechanism with a simpler structure and reduced demands on P2P nodes, steps like delegation selection, optimization problem solving, etc., are removed from original PoT, and the distributed generation units share a public P2P network. In this way, the DPoT mechanism can also be called as Proof-Free Consensus (PFC). The architecture of the REPS under the PFC is given in Supplementary Fig. 1. As can be seen, the PFC provides a paradigm for secure data transmission since the P2P network is used only for data delivery. In such a secure transmission mode, the computation of control commands is not undertaken by the P2P network, but by a given device. PFC-based regulation is centralized and is a minimalist variant of PoT.

In all, variant operations of the PoT mechanism include changing, removing, and adding components. The key elements of PoT are: (C1) the selection of the delegation, (C2) the consensus on measurements, (C3) the optimality proof and (C4) the smart contract. New actions that can be incorporated include the re-verification at the actuator. Removing certain elements from (C1), (C2), (C3), and (C4), as well as adding an extra action, could form different variants of PoT. The

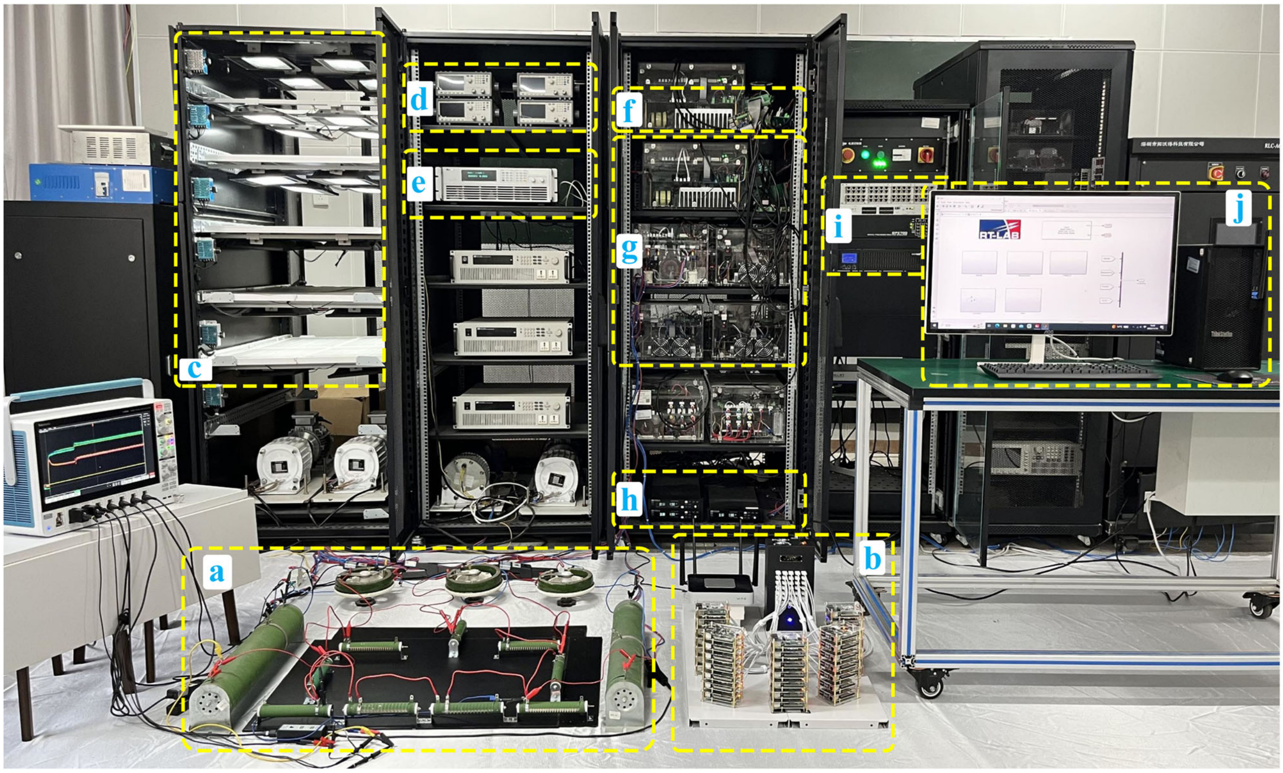

Fig. 3 | Panoramic view of the converter-based IEEE 9-bus microgrid platform, featuring five distributed generation units, alongside the OPAL-RT-based Hardware-in-the-Loop (HIL) platform for the multi-area interconnected power system. a Line impedance of the 9-bus and five local loads. **b** Raspberry Pi-based blockchain implementation. **c** Photovoltaic (PV) panels. **d** Energy storage units. **e** Photovoltaic simulator. **f** Raspberry Pi-based ASDM and actuators. **g** DC converters. **h** DC sources. **i** Real-time digital simulator. **j** Upper computer.

characteristics of UPoT and DPoT from the point of view of elements increasing and decreasing are summarized in Supplementary Table 1.

In addition, depending on whether the blockchain nodes are involved in generating control signals, the key applications of the PoT mechanism can be summarized into the following two aspects. The first is a blockchain-assisted real-time regulation scheme with high security and powerful computational capability to serve complex control tasks. The second is a blockchain-enabled security real-time regulation scheme that serves general control tasks, where PoT only plays a role in providing security. Thus, PoT, as a basic architecture, comes with many variants that can be adapted to different application scenarios.

Application 1: Proof of Task-based security regulation for DC microgrids

Given the widespread distribution of renewable energy source-based generation units, communication-based distributed regulation strategies are prevalent in DC microgrid systems. However, the integration of communication networks introduces potential cyber threats. Research on secure regulation strategies for DC microgrid systems has garnered significant attention and can be found in ref. 51 and references therein. Most current efforts focus on detecting cyber-attacks or tolerating the impact of damage to the maximum extent possible after attacks. Therefore, it is imperative to develop regulation strategies to proactively defend against attacks. In addition, optimization of the control cost is also expected while ensuring the power quality, which requires controllers with abundant computational resources. The suggested PoT scheme, which allows interconnected Distributed Generation Units (DGUs) to implement online optimal control algorithms and guarantee regulation security, has the potential to address the above challenges. This promotes the necessity of the PoT-based secondary regulation strategy.

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 trustworthy control commands by solving the optimization problem for a DC microgrid suffering from cyber-attacks, to achieve distributed secondary security regulation. The structure of the islanded DC microgrid system with PoT-based secondary regulation strategy is presented in Supplementary Fig. 2. Detailed implementation, including the DC microgrid system model, prediction compensator, and optimization problem, is given in Supplementary Note 3. In addition, the flowchart of the PoT-based secondary regulation strategy is shown in Supplementary Fig. 3.

The testbed used in this case is a scaled-down IEEE 9-bus system with five generation units developed in the laboratory, as shown in Fig. 3. The prototype includes actual photovoltaic power generation, storage batteries, photovoltaic simulators, and DC sources. Each power source, along with the converter and filter, forms a distributed generation unit connected to the bus. These buses are interconnected by transmission lines to form the system shown in Supplementary Fig. 4. Blockchain nodes are implemented on Raspberry Pi with appropriate computational and storage resources, as marked in Fig. 3.

The PoT-based method offers effective defense against various types of attacks. As an example, assume that a malicious adversary initiates a false data injection attack on data interactions within a DC microgrid. In line with typical practices, in this experiment, the launched attacks are described as $\tilde{y}_l^i(t) = y_l^i(t) + \alpha_l^i(t)\zeta_l^{i,y}(t)$ and $\tilde{u}_l^i(t) = u_l^i(t) + \beta_l^i(t)\zeta_l^{i,u}(t)$, $\forall i \in \mathcal{B}_l$, where $y_l(k) = x_l(k) = [\Delta V_l(k), \Delta I_{tl}(k), \Delta\phi_l(k), \Delta\gamma_l(k), e_l^V(k), \varepsilon_l^I(k)]^{\mathrm{T}}$, $\mathcal{B}_l$ denotes the set of nodes in the blockchain network belonging to the lth generation unit, $\alpha_l^i(t) = \operatorname{diag}\{\alpha_{l,1}^i(t), \alpha_{l,2}^i(t), \cdots, \alpha_{l,6}^i(t)\} \in \mathbb{R}^{6\times 6}$ and $\beta_l^i(t) \in \mathbb{R}$ are Bernoulli random variables indicating whether an attack has occurred, $\zeta_l^{i,y} = [\zeta_{l,1}^{i,y}, \zeta_{l,2}^{i,y}, \cdots, \zeta_{l,6}^{i,y}]^{\mathrm{T}} \in \mathbb{R}^{6\times 1}$ and $\zeta_l^{i,u} \in \mathbb{R}$ are contaminated data injected by the attacker. Specifically, $\zeta_{l,m}^{i,y}(t) = A_y \sin(\omega t)$ for

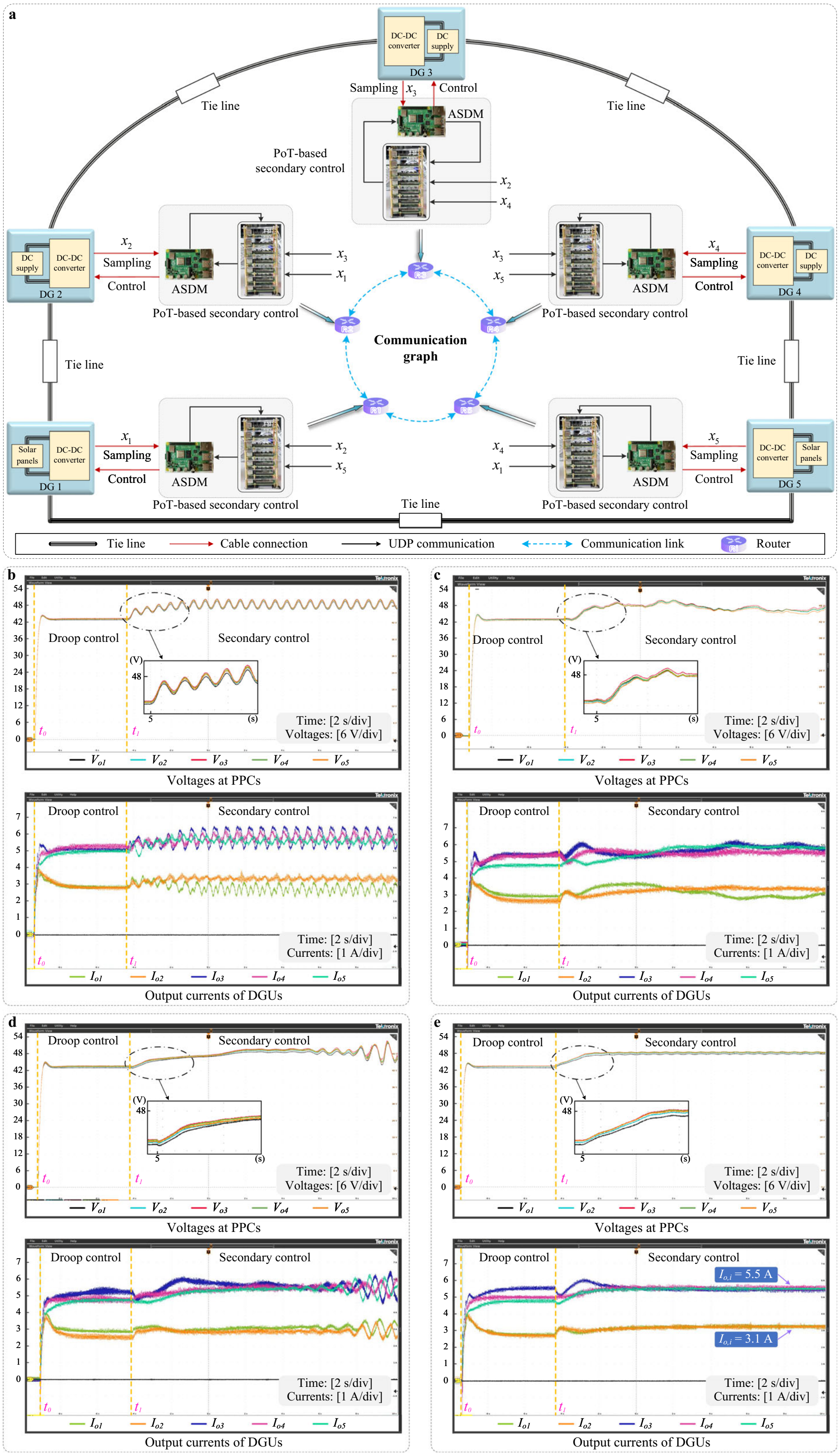

Fig. 4 | Application of the PoT-based secondary control strategy in a DC microgrid (Application 1). a Data flow of the IEEE 9-bus test bench with PoT-based blockchain, which also presents the deployment architecture of the microgrid under PoT-based secondary control. Communication between the generation units at the information layer forms a ring topology, in which the User Datagram Protocol (UDP) is utilized. Only part of the tie lines are shown. **b** Responses of the resilient method in ref. 14. **c** Responses of the blockchain-based method in ref. 52. **d** Responses of the PoT-based method without delay compensation. **e** Responses of the PoT-based method.

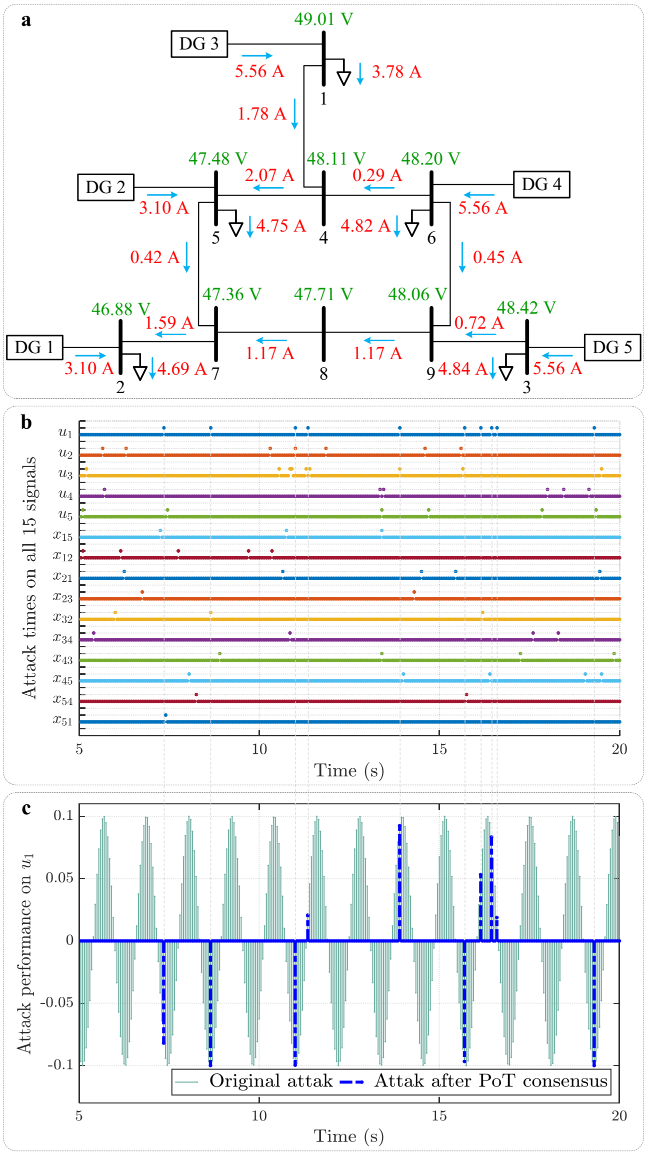

Fig. 5 | Data analyses of Application 1. a Power flow of the IEEE 9-bus microgrid system with PoT-based secondary control. **b** Moment of occurrence of cyber-attacks on all 15 signals of the DC microgrid. **c** Defend performance against attacks on the control signal u_1 of the DC microgrid with PoT-based secondary control. Near dense and sparse points in **b** form one 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 PoT, respectively. The meanings of the variables in the figure are available in Supplementary Table 2.

$m = 1, 2, \cdots, 6$, and $\zeta_l^{i,u}(t) = A_u \sin(\omega t)$, where A_y and A_u are the amplitudes of the attack signals and ω is the angular frequency of the sinusoidal signal. Aforementioned parameters are available at https://github.com/blockchainer01/PoTREPSs.git. The five generation units communicate using a ring topology as shown in Fig. 4a, and the upper bound of communication delays is 40 ms. Further explanations of the variables are provided in Supplementary Note 3.

Now, the PoT-based distributed secondary regulation strategy is tested and deployed on the hardware as shown in Fig. 4a, which also illustrates the data flow of the DC microgrid with PoT-based control. The structure of the code for PoT-based distributed secondary security regulation is depicted in Supplementary Fig. 5. Further deployment details are available at https://github.com/blockchainer01/PoTREPSs.git. In this scenario, each blockchain network is implemented using seven Raspberry Pi with Wi-Fi-based communication, as presented in Fig. 3. According to the time required to solve the optimization problem, the waiting time for each node to issue the candidate control command is set to 40 ms.

Table 3 | 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 refs. 14,52, and this paper, respectively. The bold value in each column shows the probability of secure data transmission corresponding to the method with the best performance.

For comparison, the traditional cooperation-based resilient controller in ref. 14 and the existing blockchain-based security control method in ref. 52 are employed in the testbed first. Figure 4b, c display the output responses of the two controllers subject to attacks and communication delays, respectively. The waveform results indicate that, under the combined influence of attacks and delays, the existing resilient secondary control approach fails to achieve the desired regulation performance and may even lead to system divergence, which is unacceptable. Similarly, the existing blockchain-based approach is also inadequate for the distributed security control of DC microgrids. This is primarily because the method in ref. 52 only defends against external attacks and does not account for disloyal nodes within the blockchain network. Additionally, it cannot effectively compensate for communication constraints in a distributed manner.

Moreover, the responses of the DC microgrid under the PoT-based distributed secondary regulation strategy without and with the delay compensation mechanism are presented in Fig. 4d, e, respectively. It can be seen that the output voltages of the microgrid are regulated to around 48 V and the currents are precisely allocated among the distributed generation units in the set ratio of 1:1:1.8:1.8:1.8 under the PoT-based secondary control. Comparing Fig. 4b–d demonstrates that PoT significantly mitigates the negative impact of attacks on the DC microgrid. Furthermore, comparing Fig. 4d, e reveals that the prediction algorithm in PoT effectively compensates for the inevitable time delays caused by data communication and the consensus mechanism. Additionally, the power flow of the DC microgrid corresponding to the steady state shown in Fig. 4e is presented in Fig. 5a.

In addition to the waveform results and associated discussion above, quantitative comparisons and analyses are provided. Specifically, Table 3 presents the probability of secure data transmission in the microgrid system under the three methods. The moments of the original attacks and those of the effective attacks after PoT on all 15 signals in the microgrid system are shown in Fig. 5b. Taking the control signal u_1 of the first DGU as an example, the original attack signal and the attack signal under PoT are given in Fig. 5c. To 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 in (30) and (31) in Supplementary Note 3, respectively. Figure 6a displays the results of H_α for the REPSs across 20 independent trials under three different methods to demonstrate their effectiveness in defending against cyber-attacks. Figure 6b presents the results of J_{task} in the same scenario to show how well different methods accomplish the control task. The ratio of the probability of successful defense w.r.t. probability of unsuccessful defense for PoT over 20 independent trials is illustrated in Supplementary Fig. 6, providing an intuitive demonstration of PoT's defensibility against cyber-attacks. This figure highlights the long-term stable defense performance of the PoT-based approach.

Based on the data presented in the above results, the defense role imparted by PoT at the physical level significantly reduces the

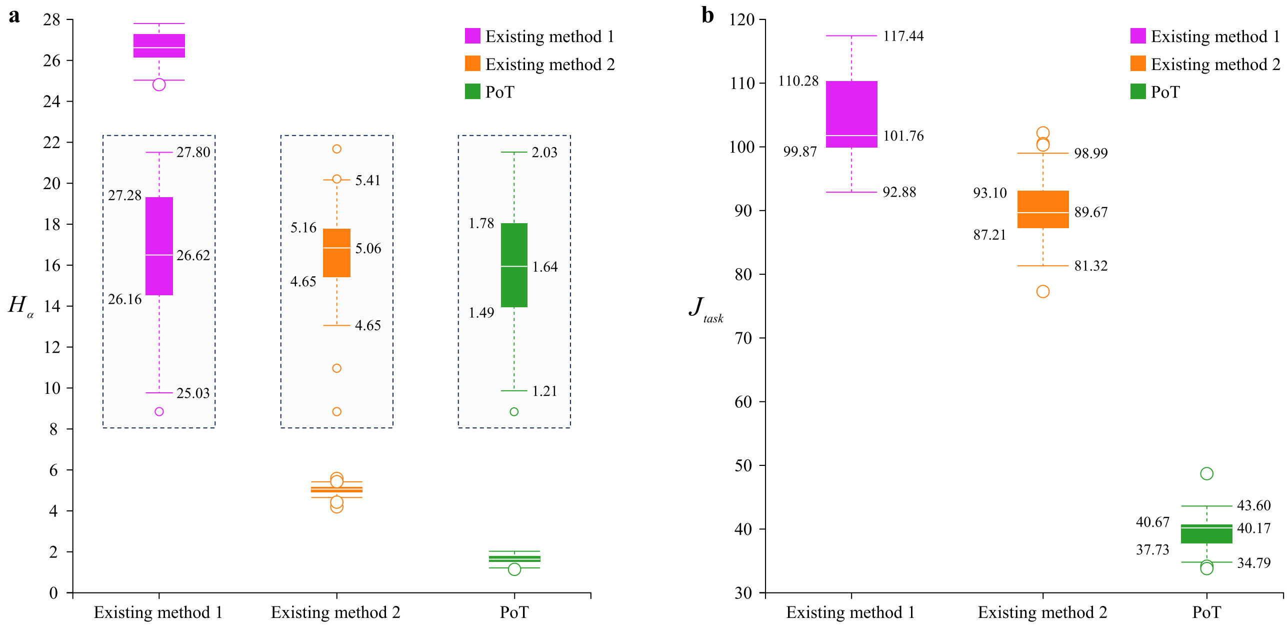

Fig. 6 | Comparative data analyses of Application 1. a Comparison results based on the security performance metric H_α. **b** Comparison results based on the control performance metric J_{task}. The middle part of **a** displays three enlarged subplots. The methods labeled as "Existing method 1" and "Existing method 2" correspond to the approaches in refs. 14,52, respectively.

likelihood of REPSs being attacked compared to existing real-time control methods. As shown in Table 3, the security of the microgrid system with the proposed method reaches 95%, which surpasses existing methods. While the security improvements PoT offers over the existing blockchain-based security control method are less pronounced than those over traditional resilient methods, this highlights blockchain's effectiveness in enhancing data security. However, in terms of performance metrics shown in Fig. 6, the proposed PoT-based control method still outperforms the existing blockchain-based security control method.

In addition, the performance of the nodes with different optimization solvers during the operation of the DC microgrid under PoT is given in Supplementary Figs. 7 and 8. By considering both solution optimality and solving time, there is not a particular solver that is used all the time throughout the system operation. Instead, different types of solvers alternately win the PoT consensus. From the data shown in the figures, under PoT, the distinct characteristics of different types of solvers are explored, which improves the computing power of the controller.

To further illustrate the effectiveness of the proposed PoT-based regulation strategy, plug-and-play characteristics are evaluated. It is assumed that the PV unit disconnects from the microgrid due to a fault at t_2 and restores its power capacity at t_3. Supplementary Fig. 9 gives the voltage and current responses of the DC microgrid under the unplugging and plugging actions of the 5th DGU. The results indicate that the PoT-based regulation method exhibits plug-and-play capability while effectively defending against cyber-attacks.

The above results demonstrate that the PoT mechanism makes it possible to simultaneously solve complex optimization problems and achieve secure distributed control for microgrids. Although the multi-node nature of blockchain introduces some unavoidable latency, the distributed prediction in PoT addresses this flaw. Consequently, the PoT-based distributed secondary regulation approach maintains the inherent security and trustworthiness of blockchain while leveraging the computational capabilities of nodes in the P2P network. Meanwhile, the low real-time nature that previously hindered blockchain's application in power generation control systems is eliminated.

Application 2: Proof of Task-based security load frequency control

In power grids, mismatches between the power supply and demand can cause frequency deviations from its rated value, thereby inducing destabilization. Therefore, mitigating these deviations is crucial for grid reliability. Load Frequency Control (LFC) aims to maintain frequency fluctuations within a predefined range. However, due to the rapid frequency response, LFC systems struggle with complex data authentication algorithms such as encryption and decryption, making them vulnerable to jamming and cyber-attacks. Therefore, it is necessary to design a PoT-based distributed LFC 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. Details on the optimization problem to be solved by the blockchain network, the attack patterns, etc., are provided in Supplementary Note 4.

The performance of the PoT-based approach in the presence of step load changes will be evaluated in a three-area power system with turbines and synchronous generators. The logic structure of this power system is illustrated in Supplementary Fig. 10, where each area is equipped with an automatic generation control system. Figure 7a displays the data flow of the PoT-based interconnected power system, along with the deployment architecture of the system. The structure of the code for PoT-based distributed security LFC and architecture of the HIL test system are provided in Supplementary Figs. 11 and 12, respectively. Deployment details of PoT in the three-area power system are available at https://github.com/blockchainer01/PoTREPSs.git. In this test, the load in area 1 increases by 0.02 P.U. at $t = 10$ s, the loads in areas 2 and 3 increase by 0.02 P.U. at $t = 150$ s, and the loads in all three areas decrease by 0.02 P.U. at $t = 250$ s. It is worth noting that all load changes $\Delta P_{L,i}$ decay to zero after five seconds. 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 target system. Here, it is set to 5 µs. In general, a smaller time step results in a more accurate simulation.

For comparison, the PoT-based LFC approach and the classical cooperation-based resilient LFC strategy in ref. 53 are tested under

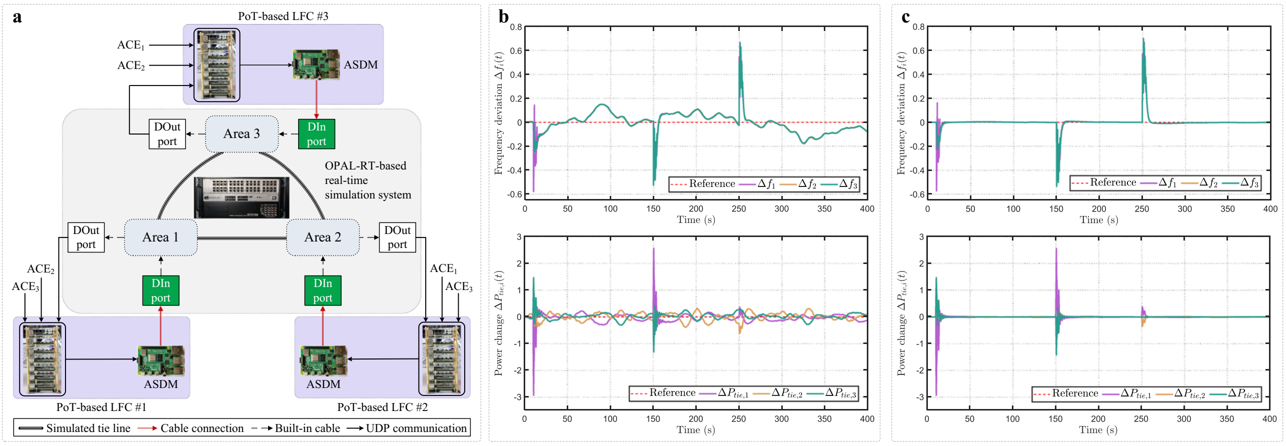

Fig. 7 | Application of the PoT-based LFC scheme in a three-area power system (Application 2). **a** Data flow of the HIL interconnected power system. **b** Responses of the existing resilient method in ref. 53. **c** Responses of the PoT-based LFC scheme.

cyber-attacks. System responses are shown in Fig. 7b, c. The results indicate that the system becomes unstable under a cyber-attack when utilizing the traditional resilient LFC approach. In contrast, the PoT-based LFC ensures a smooth response in the multi-area power system subjected to the cyber-attack, adhering to generation rate and load reference setpoint constraints. Additionally, the quantitative results, including performance metrics for both the existing and PoT-based methods, are presented in Supplementary Table 3 and Supplementary Fig. 13. Definitions of these metrics are provided 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. 14 demonstrates the consistent performance of the PoT method over multiple trials. In summary, the above analysis confirms that the proposed PoT-based distributed LFC algorithm can ensure the security of the system while optimizing its operation.

Application 3: Degraded Proof of Task-based security regulation for DC microgrids

The PFC is a DPoT mechanism introduced in the degraded PoT mechanism part. Unlike Application 1, 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, as shown in Supplementary Fig. 1. It can be found that the P2P network in the PFC no longer performs any mathematical problems related to control tasks, but is only used for data transmission.

In this application, the PFC-based secondary control strategy is implemented on the Ethereum platform. Ethereum is deployed on each Raspberry Pi. During the operation of the system, the PFC on Ethereum manages data transfer between the generation unit and the controller. Besides, post-consensus data forms a new block added to the chain. Considering the long-distance communication between the central controller and each generation unit as well as the operation time of the Ethereum, there is still a delay in the execution of PFC. Therefore, the PFC-based secondary secure control with delay compensation is designed as (48) in Supplementary Note 5. The architecture of the DC microgrid under PFC-based secondary control is presented in Supplementary Fig. 15. The logical structure of the Ethereum platform and microgrid system is shown in Fig. 8a. The structure of the code for the PFC-based secondary control is provided in Supplementary Fig. 16. The corresponding deployment details can be found in https://github.com/blockchainer01/PoTREPSs.git.

The effectiveness of the control strategy in this case is also verified on the experimental platform shown in Fig. 3. Unlike PoT, where data interaction is implemented directly in Raspberry Pi, this application uses Ethereum. The attacks are consistent with those in the previous case. During experiments, the round trip time delay measured by the timestamping technique ranges from 12 to 13 steps. As can be seen from Fig. 4e, the networked prediction mechanism in PoT can compensate for this communication delay. However, the prediction mechanism cannot handle arbitrary time delays. The number of time steps it can compensate for depends on factors such as 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. The status and performance of the Ethereum are demonstrated in Supplementary Fig. 17.

To evaluate the effectiveness of the proposed method, it is compared with the typical semiconsensus resilient control method in ref. 54. As illustrated in Fig. 8b, the existing resilient method results in varying degrees of oscillations in output voltages and currents, and fails to achieve the expected current sharing. In contrast, the PFC-based secondary control method, as depicted in Fig. 8c, regulates the average output voltages to the desired level around 48 V and accurately shares output currents in the ratio of 1:1:1.8:1.8:1.8. In addition, some quantitative results are provided in Supplementary Table 4, Supplementary Figs. 18 and 19, including comparisons of the security probability as well as performance metrics with established methods. These results demonstrate that PFC-based secondary control is still capable of realizing the desired regulation goals for DC microgrids and actively defending against cyber-attacks. In practice, the appropriate PoT method can be selected based on the requirements for security and regulation performance, as well as budget considerations.

Discussion

Security at the information layer becomes increasingly important for the control, dispatch, and trading of power energy systems. With the access to a large number of renewable energy resources, the increasing level of power electronification and informatization in power energy systems, traditional control methods in a passive way would be sluggish in the face of network imperfections. Developed PoT is a blockchain consensus mechanism tailored for real-time control tasks, providing reliable and desired regulation effects for REPSs in the presence of cyber threats. The performance in the test validates that PoT not only effectively improves the security and computing capability of power energy systems, but also facilitates the accomplishment of complex control tasks under various physical constraints. Furthermore, three different applications suggest that the proposed

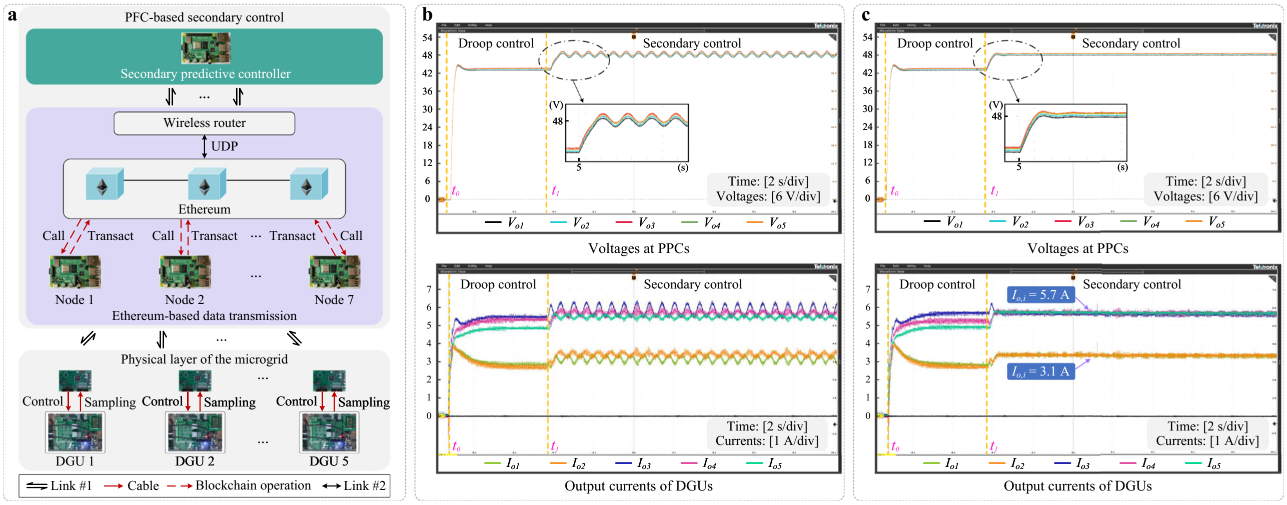

Fig. 8 | Application of the PFC-based secondary control strategy in a DC microgrid (Application 3). a Data flow of the PFC-assisted microgrid system based on the Ethereum platform. Links #1 and #2 refer to the communication link between external data and the Ethereum platform, and the communication link between Ethereum nodes, respectively. **b** Responses of the existing method in ref. 54. **c** Responses of the PFC-based approach.

consensus protocol is both effective and generalizable for various configurations of REPSs.

PoT has been successfully applied to the distributed secondary control of renewable energy resources-based DC microgrids and load frequency control for multi-area interconnected power systems. In addition, the PFC, a kind of degraded PoT consensus mechanism, provides a feasible and simplified solution for applying PoT in the centralized control of DC microgrids. The superiority of PoT lies in its real-time performance, multi-pattern data protection, and computational resource extraction, combined with the intelligence to perceptually adjust consensus participants. These characteristics allow PoT to provide a trusted and fast computing paradigm. Besides being able to provide abundant computational resources, PoT also possesses the innate property of trustworthiness, which is not available in other computing modes. This technology is promising to broaden the application scope of blockchain, and facilitate the development of smart energy.

Regardless of the size, REPSs would first determine their physical topology, which may include common structures such as star, ring, and mesh configurations. In certain topologies, the number of neighbors that are electrically connected to a generation unit increases as the system expands. However, these changes in the electrical layer faced when scaling up to large-scale REPSs will not pose additional challenges for the applications of PoT. This is because PoT does not require the information layer and the electrical layer to be connected in the same manner. At this point, REPSs need to focus on the mode of data communication within the information layer, as this will directly influence the deployment and control performance of PoT. If a fully distributed communication is adopted, PoT deployment and application will remain unaffected by the scale-up to large REPSs, since 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 would necessitate 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.

In essence, PoT enables the trusted real-time transmission and rapid optimization problem solving. Within PoT, the control task is formulated as an optimization problem, while the stability requirement of the system is transformed into a validation condition for candidate solutions. In addition, multi-node computation and relative optimality verification unleash the computational resources of the blockchain network. While realizing the system stability and given control objectives, PoT provides complex dynamic systems with higher security and powerful computing capabilities. These attributes allow PoT to be seamlessly suitable for the control of large-scale REPSs. Besides, PoT can also be applied to the dispatch and trading of power energy systems, as well as scenarios beyond the energy sector.

PoT offers interesting perspectives for both the blockchain and control communities, but it also has certain limitations. First, the quantitative mathematical relationship among the size of P2P networks, system security, and real-time performance is not revealed systematically. Second, the trade-off between the optimality, security, and the real-time nature of blockchain-enabled control needs further investigation. Moreover, to facilitate real-time control of REPSs, PoT makes certain compromises in security compared to traditional consensus mechanisms. In PoT, for example, the problems solved by peers 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 maintaining its real-time nature. 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 optimization problems 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.

Methods

Algorithm of Proof of Task-based regulation

PoT, as a lightweight, highly real-time, and efficient consensus algorithm, is able to facilitate the secure output regulation of REPSs. The meaningful mathematical problem and the exclusive verification mechanism make blockchain-based real-time control a computationally effective solution for secure data transfer and security control. The secure cooperative regulation framework based on the PoT mechanism consists of nine steps as shown in Fig. 1. Taking a large-scale REPS containing *N* 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.

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 generation subsystem in step 1, the consensus on each $y_j^{[p,i]}$ in step 2 involves all these nodes as this operation is straightforward. It should be noted that the local raw interaction data y_l refers to the measurements of the subsystem l, and neighbors' raw interaction data refers to the predicted future states sent by the neighboring generation subsystems over the communication network. These states contain physical quantities required for regulation, such as output voltages and currents in REPSs. At this stage, the MRP is executed, protecting the source data (i.e., measurements) in a manner analogous to a practical Byzantine fault tolerance protocol. In this way, $y_j^{[p,i]}$ with the superior number will be kept by each blockchain node, denoted as $y_{j,\mathrm{MRP}}^{[p,i]}$.

In step 3, m_l nodes are selected from the P2P network using a game-derived strategy. This strategy provides a guideline for dynamically authorizing blockchain nodes that will participate in subsequent processes during each control cycle. Since this strategy is obtained offline, its execution introduces no additional delay to the system. Numerous studies have explored game-based approaches, with Supplementary Algorithm 2 offering one viable specific process. The rigorous proof of the optimality and convergence of the algorithm can be found in ref. 55. It should be mentioned that only peers authorized as delegates are responsible for solving the optimization problem. This practice 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 historical loyalty. Moreover, it also introduces additional uncertainties into the system, making it more difficult for malicious adversaries to launch attacks, thus improving the security of the system.

In step 4, we leverage the nodes in the delegation selected in the previous step to optimize the performance metric function under hard conditions of system stability. Many online optimization algorithms are faced with the problem of requiring large amount of computational resources and failing to respond in real time due to the complexity of searching for the optimal solution. On the one hand, the large number of idle nodes in blockchain provides attractive computational resources. On the other hand, the mechanism of fixed waiting time for each round of solving enables PoT to retain an excellent real-time performance.

It is worth mentioning that the consensus mechanism operates over communication networks. Along with the complex calculation and data transmission, there are inevitably communication constraints such as time delays and packet losses. For this problem, which is particularly challenging in some application scenarios sensitive to communication constraints, we 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 system modeling, an effective distributed prediction algorithm, and an appropriate compensation mechanism. Details of these steps can be found in Supplementary Notes 3–5. For scenarios where components like constant power loads introduce nonlinear characteristics to REPSs, simpler models can significantly reduce the solution difficulty, while reflecting more dynamics can improve the control performance. The fully actuated system approach offers a promising option to effectively cope with this conflict[56]. The prediction technique ensures that the PoT consensus mechanism effectively balances security and real-time performance, with security achieved through multi-party verification and real-time performance enhanced by state prediction.

In step 5, the control commands obtained by solving the constrained optimization problem on each node are exchanged among the delegates and campaigned based on relative optimality. Such a practice skillfully integrates the blockchain technology with the control tasks of REPSs. Specifically, a theoretical analysis first derive the sufficient conditions that can guarantee the stability of the system and the completion of the control objective. These conditions function as a preliminary filter during the verification of candidate solutions. Solutions that do not meet these conditions are discarded, as their use may lead to control failure or even system collapse. Among the filtered solutions that satisfy the conditions, they are further ranked by the designed performance metric function to identify the relatively optimal solution. In this way, it is guaranteed that at least one control command that allows the system to operate stably can be produced in each period. This is another key of PoT to improve its real-time responsiveness.

Subsequently, in step 6, all delegates send their relatively optimal solutions, obtained after verification and comparison in the previous step, to the decision maker on the actuator side. In the PoT mechanism presented in Fig. 1, the detailed implementation process for steps 4–6 is shown in Box 1. Furthermore, in step 7, the MRP is performed to protect the target data (control commands) from potential attacks or disloyalty, thereby ensuring a trusted control input. This control signal is then applied to the actuator in step 8 to complete the regulation of the REPSs. Finally, in step 9, a smart contract is developed to calculate 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 probabilities given by the prior knowledge of the vulnerabilities of different nodes to cyber-attacks. In addition, the smart contract further evaluates these delegate nodes and decides whether any should be removed from the delegation. The election mechanism and the smart contract both complement each other to form a comprehensive 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.

Hardware and software

The converter used in Section Application 1: Proof of Task-based security regulation for DC microgrids is a buck circuit where each single phase switching circuit consists of an IGBT PM50RL1A120T01-CA3G. The oscilloscope used in the experiments is Tektronix MSO 2024B, and the current probe is A622 AC/DC current probe. A Raspberry Pi model B with 2GB RAM is used as the hardware implementation of the blockchain node. As shown in Fig. 3, there are five groups of Raspberry Pi in the experimental platform to form the blockchain networks. The Raspberry Pi runs the program written in C code, including the PoT-based secondary control algorithm and the communication module. The distributed nodes communicate with each other using the UDP.

The PoT-based PFC mechanism in Section Application 3: Degraded Proof of Task-based security regulation for DC microgrids is verified with a HIL system. The corresponding multi-area power system is developed using the SIMULINK environment and run in OPAL-RT, i.e., OP5700 and OP4512 shown in Fig. 3. The PoT-based LFC strategy operates in the Raspberry Pi platform shown in Fig. 3. Then, HIL simulations are performed using the wind turbine model in the hardware FPGA of OPAL-RT and the control signals obtained from the Raspberry Pi. The VNC Viewer software is used to access and take remote control of Raspberry Pi. The blockchain network consists of Raspberry Pi loaded with Ethereum client, and the details of the softwares involved are available in Supplementary Table 5. There are five optimization solvers used in the PoT implementation and their details are available in Supplementary Table 6.

BOX 1

Operations for delegates

```
Input: Optimization problem to be solved, etc.
Delegate $i$ ($\forall i \in D$) solves the issued optimization problem based on authentic interaction data until a given waiting time is reached
Send the obtained solution $u^i_{l,i}(t)$ to the other delegates
Receive candidate solutions $u^i_{l,k}(t)$ from other delegates
For $k = 2, \cdots, m_l$
    Verify the candidate solution $u^i_{l,k}(t)$ using the stability condition
    If $u^i_{l,k}(t)$ satisfies the stability condition then
        Let the optimal PMF as $J^{i*}_l = J(u^i_{l,1}(t), \cdot)$
        If $J(u^i_{l,k}(t), \cdot) < J^{i*}_l$ then
            Update the optimal PMF as $J^{i*}_l = J(u^i_{l,k}(t), \cdot)$
            Obtain the local optimal solution $u^{i*}_l(t) = u^i_{l,k}(t)$
        end if
    else
        Discard $u^i_{l,k}(t)$
    end if
end for
Package the feasible optimal solution $u^{i*}_l(t)$ with the index $i$ and send it to the decision maker on the actuator side
Let $t \leftarrow t+1$
```

where D denotes the set of delegates, l the lth DGU in REPSs, i the index of ith delegate, m_l is the size of the delegation affiliated with lth DGU.

Data availability

Data analyses are primarily conducted using MATLAB software. The relevant data used in this study are available in the Figshare database at https://doi.org/10.6084/m9.figshare.25375105. Source data are provided with this paper.

Code availability

Information about the software code and hardware requirements for this study is available on Github at https://github.com/blockchainer01/PoTREPSs.git (also accessible via https://doi.org/10.5281/zenodo.14055476). More details can be obtained from the corresponding author upon request.

References

1. Brockway, P. E., Owen, A., Brand-Correa, L. I. & Hardt, L. Estimation of global final-stage energy-return-on-investment for fossil fuels with comparison to renewable energy sources. *Nat. Energy* **4**, 612–621 (2019).
2. Gielen, D. et al. The role of renewable energy in the global energy transformation. *Energy Strat. Rev.* **24**, 38–50 (2019).
3. Sajadi, A., Kenyon, R. W. & Hodge, B.-M. Synchronization in electric power networks with inherent heterogeneity up to 100% inverter-based renewable generation. *Nat. Commun.* **13**, 2490 (2022).
4. Impram, S., Nese, S. V. & Oral, B. Challenges of renewable energy penetration on power system flexibility: a survey. *Energy Strat. Rev.* **31**, 100539 (2020).
5. He, X., Wang, R., Wu, J. & Li, W. Nature of power electronics and integration of power conversion with communication for talkative power. *Nat. Commun.* **11**, 2479 (2020).
6. Mahmud, K., Khan, B., Ravishankar, J., Ahmadi, A. & Siano, P. An internet of energy framework with distributed energy resources, prosumers and small-scale virtual power plants: an overview. *Renew. Sustain. Energy Rev.* **127**, 109840 (2020).
7. Vosughi, A., Tamimi, A., King, A. B., Majumder, S. & Srivastava, A. K. Cyber–physical vulnerability and resiliency analysis for der integration: a review, challenges and research needs. *Renew. Sustain. Energy Rev.* **168**, 112794 (2022).
8. Case, D. U. Analysis of the cyber attack on the Ukrainian power grid. *Electricity Inf. Shar. Anal. Cent.* **388**, 3 (2016).
9. Haes Alhelou, H., Hamedani-Golshan, M. E., Njenda, T. C. & Siano, P. A survey on power system blackout and cascading events: research motivations and challenges. *Energies* **12**, 682 (2019).
10. Yu, Y., Liu, G.-P., Huang, Y. & Guerrero, J. M. Distributed data-driven secondary regulation for the conflict between voltage recovery and accurate current sharing in DC microgrids. *IEEE Trans. Power Electron.* **38**, 9617–9634 (2023).
11. Yang, Q., Wang, G., Sadeghi, A., Giannakis, G. B. & Sun, J. Two-timescale voltage control in distribution grids using deep reinforcement learning. *IEEE Trans. Smart Grid* **11**, 2313–2323 (2020).
12. Li, Y. & Yan, J. Cybersecurity of smart inverters in the smart grid: a survey. *IEEE Trans. Power Electron.* **38**, 2364–2383 (2023).
13. Zografopoulos, I., Hatziargyriou, N. D. & Konstantinou, C. Distributed energy resources cybersecurity outlook: vulnerabilities, attacks, impacts, and mitigations. *IEEE Syst. J.* **17**, 6695–6709 (2023).
14. Kachhwaha, M., Modi, H., Nehra, M. K. & Fulwani, D. Resilient control of DC microgrids against cyber attacks: a functional observer based approach. *IEEE Trans. Power Electron.* **39**, 459–468 (2024).
15. Presekal, A., Ştefanov, A., Rajkumar, V. S. & Palensky, P. Attack graph model for cyber-physical power systems using hybrid deep learning. *IEEE Trans. Smart Grid* **14**, 4007–4020 (2023).
16. Khalid, H. M. et al. WAMS operations in power grids: a track fusion-based mixture density estimation-driven grid resilient approach toward cyberattacks. *IEEE Syst. J.* **17**, 3950–3961 (2023).
17. Tabassum, T., Lim, S. & Khalghani, M. R. Artificial intelligence-based detection and mitigation of cyber disruptions in microgrid control. *Electr. Pow. Syst. Res.* **226**, 109925 (2024).
18. Rahiminejad, A. et al. A resilience-based recovery scheme for smart grid restoration following cyberattacks to substations. *Int. J. Electr. Power Energy Syst.* **145**, 108610 (2023).

19. Liu, M. et al. Enhancing cyber-resiliency of der-based smart grid: a survey. *IEEE Trans. Smart Grid* **15**, 4998–5030 (2024).
20. Andoni, M. et al. Blockchain technology in the energy sector: a systematic review of challenges and opportunities. *Renew. Sustain. Energy Rev.* **100**, 143–174 (2019).
21. Mollah, M. B. et al. Blockchain for future smart grid: a comprehensive survey. *IEEE Internet Things J.* **8**, 18–43 (2020).
22. Belotti, M., Božić, N., Pujolle, G. & Secci, S. A vademecum on blockchain technologies: when, which, and how. *IEEE Commun. Surv. Tutor.* **21**, 3796–3838 (2019).
23. Malla, T. B. et al. Status, challenges and future directions of blockchain technology in power system: a state of art review. *Energies* **15**, 8571 (2022).
24. Xiao, Y., Zhang, N., Lou, W. & Hou, Y. T. A survey of distributed consensus protocols for blockchain networks. *IEEE Commun. Surv. Tuts.* **22**, 1432–1465 (2020).
25. Ahmed, M. M. et al. A peer-to-peer blockchain based interconnected power system. *Energy Rep.* **7**, 7890–7905 (2021).
26. Abdella, J. et al. Hicoob: hierarchical concurrent optimistic blockchain consensus protocol for peer-to-peer energy trading systems. *IEEE Trans. Smart Grid* **14**, 3927–3943 (2023).
27. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System.* (Bitcoin, 2008).
28. Etherscan (Etherscan, 2015). https://etherscan.io/.
29. Kiayias, A., Russell, A., David, B. & Oliynykov, R. Ouroboros: a provably secure proof-of-stake blockchain protocol. In *Proc. Annual International Cryptology Conference* 357–388 (Springer, 2017).
30. Bouraga, S. A taxonomy of blockchain consensus protocols: a survey and classification framework. *Expert Syst. Appl.* **168**, 114384 (2021).
31. Larimer, D. *Delegated Proof-of-Stake (dpos)* Bitshare whitepaper (2014), retrieved March 31, 2019. http://docs.bitshares.org/bitshares/dpos.html.
32. Fan, X. & Chai, Q. Roll-dpos: a randomized delegated proof of stake scheme for scalable blockchain-based internet of things systems. In *Proc. 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services* 482–484 (Association for Computing Machinery, 2018).
33. Miller, A., Juels, A., Shi, E., Parno, B. & Katz, J. Permacoin: repurposing bitcoin work for data preservation. In *Proc. 2014 IEEE Symposium on Security and Privacy* 475–490 (IEEE, 2014).
34. Danish, S. M. et al. Blockchain for energy credits and certificates: a comprehensive review. *IEEE Trans. Sustain. Comput.* **9**, 727–739 (2024).
35. Morstyn, T., Farrell, N., Darby, S. J. & McCulloch, M. D. Using peer-to-peer energy-trading platforms to incentivize prosumers to form federated power plants. *Nat. Energy* **3**, 94–101 (2018).
36. Shibata, N. Proof-of-search: combining blockchain consensus formation with solving optimization problems. *IEEE Access* **7**, 172994–173006 (2019).
37. AlAshery, M. K. et al. A blockchain-enabled multi-settlement quasi-ideal peer-to-peer trading framework. *IEEE Trans. Smart Grid* **12**, 885–896 (2021).
38. Chen, S. et al. A blockchain consensus mechanism that uses proof of solution to optimize energy dispatch and trading. *Nat. Energy* **7**, 495–502 (2022).
39. Di Silvestre, M. L. et al. Blockchain for power systems: current trends and future applications. *Renew. Sustain. Energy Rev.* **119**, 109585 (2020).
40. Yang, Q. et al. Blockchain-based decentralized energy management platform for residential distributed energy resources in a virtual power plant. *Appl. Energy* **294**, 117026 (2021).
41. Wu, Y., Wu, Y., Cimen, H., Vasquez, J. C. & Guerrero, J. M. Towards collective energy community: potential roles of microgrid and blockchain to go beyond P2P energy trading. *Appl. Energy* **314**, 119003 (2022).
42. Ali, L. et al. Integrating forecasting service and gen2 blockchain into a local energy trading platform to promote sustainability goals. *IEEE Access* **12**, 2941–2964 (2024).
43. Huang, C.-T. & Scott, I. J. Peer-to-peer multi-period energy market with flexible scheduling on a scalable and cost-effective blockchain. *Appl. Energy* **367**, 123331 (2024).
44. Molzahn, D. K. et al. A survey of distributed optimization and control algorithms for electric power systems. *IEEE Trans. Smart Grid* **8**, 2941–2962 (2017).
45. Yu, Y., Liu, G.-P., Xiao, H. & Hu, W. Design of networked secure and real-time control based on blockchain techniques. *IEEE Trans. Ind. Electron.* **69**, 4096–4106 (2022).
46. Yu, Y., Liu, G.-P., Zhou, X. & Hu, W. Blockchain protocol-based predictive secure control for networked systems. *IEEE Trans. Ind. Electron.* **70**, 783–792 (2023).
47. Yang, J., Dai, J., Gooi, H. B., Nguyen, H. D. & Paudel, A. A proof-of-authority blockchain-based distributed control system for islanded microgrids. *IEEE Trans. Ind. Inform.* **18**, 8287–8297 (2022).
48. Masood, A. B., Hasan, A., Vassiliou, V. & Lestas, M. A blockchain-based data-driven fault-tolerant control system for smart factories in industry 4.0. *Comput. Commun.* **204**, 158–171 (2023).
49. Veerasamy, V. et al. Blockchain-enabled peer-to-peer energy trading and resilient control of microgrids. *Appl. Energy* **353**, 122107 (2024).
50. Pang, Z., Fu, Y., Guo, H. & Sun, J. Analysis of stealthy false data injection attacks against networked control systems: three case studies. *J. Syst. Sci. Complex.* **36**, 1407–1422 (2023).
51. Mohammadi, F. et al. Robust control strategies for microgrids: a review. *IEEE Syst. J.* **16**, 2401–2412 (2022).
52. Yu, Y., Liu, G.-P. & Hu, W. Blockchain protocol-based secondary predictive secure control for voltage restoration and current sharing of DC microgrids. *IEEE Trans. Smart Grid* **14**, 1763–1776 (2023).
53. Zhang, Y., Peng, C., Cheng, C. & Wang, Y.-L. Attack intensity dependent adaptive load frequency control of interconnected power systems under malicious traffic attacks. *IEEE Trans. Smart Grid* **14**, 1223–1235 (2023).
54. Lin, P., Deng, C., Yang, Y., Lee, C. H. T. & Tay, W. P. Resilience-oriented control for cyber-physical hybrid energy storage systems using a semiconsensus scheme: design and practice. *IEEE Trans. Ind. Electron.* **70**, 2508–2519 (2023).
55. Yu, Y., Liu, G.-P. & Hu, W. Learning-based secure control for multichannel networked systems under smart attacks. *IEEE Trans. Ind. Electron.* **70**, 7183–7193 (2023).
56. Duan, G.-R. Fully actuated system approach for control: an overview. *IEEE Trans. Cybern.* 1–22 https://doi.org/10.1109/TCYB.2024.3457584 (2024).
57. Espín-Sarzosa, D., Palma-Behnke, R. & Núñez-Mata, O. Energy management systems for microgrids: Main existing trends in centralized control architectures. *Energies* **13**, 547 (2020).
58. Callegari, J. M. S., Vitoi, L. A. & Brandao, D. I. VFD-based coordinated multi-stage centralized/decentralized control to support offshore electrical power systems. *IEEE Trans. Smart Grid* **14**, 2863–2873 (2023).
59. Alhasnawi, B. N., Jasim, B. H., Sedhom, B. E., Hossain, E. & Guerrero, J. M. A new decentralized control strategy of microgrids in the internet of energy paradigm. *Energies* **14**, 2183 (2021).
60. Sadabadi, M. S., Sahoo, S. & Blaabjerg, F. Stability-oriented design of cyberattack-resilient controllers for cooperative DC microgrids. *IEEE Trans. Power Electron.* **37**, 1310–1321 (2022).
61. Ghiasi, M. et al. A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: past, present and future. *Electr. Pow. Syst. Res.* **215**, 108975 (2023).

Acknowledgements

This work is partially supported by the Shenzhen Science and Technology Program under grant KQTD20221101093557010 (G.P.L.), the Shenzhen Key Laboratory of Control Theory and Intelligent Systems under grant ZDSYS20220330161800001 (G.P.L.), and the National Natural Science Foundation of China under grants 62403235 (Y.Y.), 62173255 (G.P.L.), and 62188101 (G.P.L.).

Author contributions

Y.Y. conceived the key idea for this paper. Y.Y. and Y.H. developed the methods and designed the experiments. Y.Y., Y.H., and Y.Z.L. performed the experiments. Y.Y. and Y.H. developed the theoretical model and carried out data analysis. Y.Y., G.P.L., and Y.H. prepared the manuscript with the input from all authors. Y.Y., G.P.L., Y.H., C.Y.C., and Y.Z.L. discussed the results and proofread the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41467-024-54626-y.

Correspondence and requests for materials should be addressed to Guo-Ping Liu.

Peer review information *Nature Communications* thanks Mohammad Ghiasi, Thongchart Kerdphol, and Renuka Loka for their contribution to the peer review of this work. A peer review file is available.

Reprints and permissions information is available at http://www.nature.com/reprints