Blockchain-Enabled Cyber-Secure Microgrid Control Using Consensus Algorithm

Preprint

Rasel Mahmud and Gab-Su Seo

National Renewable Energy Laboratory

Presented at the IEEE Workshop on Control and Modeling for Power Electronics
November 2–5, 2021

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Conference Paper
NREL/CP-5D00-78958
November 2021

Blockchain-Enabled Cyber-Secure Microgrid Control Using Consensus Algorithm

Preprint

Rasel Mahmud and Gab-Su Seo

National Renewable Energy Laboratory

Suggested Citation
Mahmud, Rasel, and Gab-Su Seo. 2021. *Blockchain-Enabled Cyber-Secure Microgrid Control Using Consensus Algorithm: Preprint*. Golden, CO: National Renewable Energy Laboratory. NREL/CP-5D00-78958. https://www.nrel.gov/docs/fy22osti/78958.pdf.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Conference Paper
NREL/CP-5D00-78958
November 2021

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored in part by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Solar Energy Technologies Office grant number DE-EE0009026. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

Cover Photos by Dennis Schroeder: (clockwise, left to right) NREL 51934, NREL 45897, NREL 42160, NREL 45891, NREL 48097, NREL 46526.

Blockchain-Enabled Cyber-Secure Microgrid Control Using Consensus Algorithm

Rasel Mahmud and Gab-Su Seo
Power Systems Engineering Center, National Renewable Energy Laboratory, Golden, CO 80401, USA
email: {Rasel.Mahmud, Gabsu.Seo}@nrel.gov

***Abstract*—This paper proposes a distributed control method based on a consensus algorithm for distributed energy resources (DERs) using blockchain as a secure communication medium for cyber resilience. Each DER communicates with a local blockchain server that is maintained by the distributed ledger technology to allow for securely sharing local measurements among neighbouring assets to achieve the global control objectives, i.e., voltage and frequency regulation as well as accurate power sharing among the DERs, including collective grid-forming capability. To prove that the distributed control can retain system stability under a blockchain-induced variable communication delay, Lyapunov function-based stability analysis is carried out. This paper demonstrates the concept on an 11-bus test case developed in MATLAB Simulink, which has been modified from the IEEE 9-bus test case, to study dynamic operations of the five inverter-based DERs working with a blockchain-induced variable delay. The results validate the superior performance of the proposed control method, compared to heavily compromised operations of the other test cases without the security measure, affected by heavy communication delays and communication interruptions.**

I. Introduction

Electric grids are experiencing exceptional changes in generation and load as increasing numbers of distributed energy resources (DERs), usually interfaced through power electronics converters, have been deployed, posing multifaceted technical challenges [1], [2]. These fundamentally challenging changes are mainly twofold from the control point of view: i) the number of assets to control is exponentially increasing because DERs, in general, are scaled at relatively lower power levels; and, ii) because of this, the control system is forced to heavily depend on the communication system. This causes not only scalability issues—how to effectively control a large system with multiple assets—but also security issues—how to operate such a large system depending on communication in a cyber-secure manner [3], [4].

To effectively coordinate multiple generators to achieve the global control objectives, such as voltage and frequency control, a distributed control method is desirable because a centralized control method might expose a single point of failure, potentially leading to a cascading generation failure and system-wide blackout [5]. Droop control is the most widely accepted concept to operate multiple inverters in parallel, allowing for collective voltage and frequency control as well as power sharing due to its simple implementation and backward compatibility [6], [7], allowing inherent communication-free operation, and inspiring advanced grid-forming technologies [8], [9]. In a power system where multiple power sources with different underlying characteristics should coordinate to maintain the system-level objectives, however, additional functionalities are essential, which cannot be obtained from the conventional droop, such as secondary and tertiary controls for frequency recovery and long-term energy balance and operation.

It is debatable how to achieve system-level objectives in a tractable manner. To achieve the system-level objectives, for example, frequency recovery, a secondary control using varying control set points from a low-bandwidth controller, a hierarchical control system can be used [10]. It is beneficial to achieve the system-level objectives with less reliance on communication; however, this increases vulnerability to cyberattack due to the centralized communication structure. To make such a system more resilient, consensus algorithm-based control for AC microgrids [11], DC microgrids [12], and hybrid AC-DC microgrids [13] have been proposed. By avoiding a dedicated or centralized control center for the system-level control, the consensus algorithm can achieve the control objectives in a distributed manner, [14], [15].

One key decisions in implementing consensus-based control is to choose the right communication that can provide a high level of cybersecurity and data privacy. Blockchain technology has a huge potential to be used for both hierarchical and distributed control systems, but it needs to address the concerns of limited network bandwidth, security, and privacy [16]. In the context of the electric grid, however, blockchain has been proposed mostly for peer-to-peer energy trading [17] using its cryptocurrency concept, but its use in power system control has not been given full attention because it is less popular in the community [18]. A recent work reported in [19] proposed the use of blockchain for the secondary control from a hierarchical control perspective, focusing on the impact of the delay on voltage and reactive power control in an inverter. To elucidate the use of blockchain for distributed

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U. S. Department of Energy Office of Energy Efficiency and Renewable Energy Solar Energy Technologies Office grant number DE-EE0009026. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. U.S. Government work not protected by U.S. copyright

controls, this paper proposes a concept to not only exploit the inherent benefits of blockchain to ensure cybersecurity in the system using the distributed ledger technology but also explore the control design aspects of the technology for use in the field. Specifically, although the blockchain network can equip multiple layers of state-of-the-art security measures, control nodes using it (DERs, in this case), as a result, have to compromise latency. Because the secure measure leads to a trade-off between security and latency, this paper studies the effect of the realistic parameters. The authors in [19] showed that the blockchain-based communication can be modeled as a communication delay. Few works in the literature have addressed the communication delay or blockchain for consensus-based microgrid control. A distributed secondary and optimal active power sharing control considering delay was proposed in [20] without providing a control mechanism for reactive power control. The impact of the sampling effect on multi-agent-based secondary control for microgrids was investigated in [21]. This paper, however, did not address the delay or blockchain for consensus-based microgrid control.

Motivated by the aforementioned limitations and potential of the blockchain technology in implementing consensus-based control, this paper envisions incorporating blockchain technology with the consensus algorithm for AC microgrid control. The main contributions reported in this paper include i) an analysis of the blockchain technology for modeling purposes in the consensus-based microgrid control design, ii) the proposal of a delay-tolerant, blockchain-enabled, consensus-based microgrid controller for voltage and frequency regulation as well as active and reactive power sharing, and iii) the Lyapunov function-based stability analysis of the proposed controller. The paper is structured as follows: Section II discusses the blockchain technology for the consensus-based control. Section III proposes the consensus-based control with the proof of stability for the proposed controller using Lyapunov function. Section IV presents and demonstrates the efficacy of the proposed controller with a simulation for a modified IEEE 9-bus system. Finally, Section V concludes the paper.

II. Blockchain for Consensus-based control

This study envisions that blockchain is used as a secure and resilient means of communication for a consensus-based distributed control for microgrid operation, as illustrated in Fig. 1. The blockchain nodes are connected to DERs and controllable assets, such as smart switches and controllable loads, as well as measurement and monitoring devices to gather the operational data in a distributed manner and to enable the distributed control to the system assets based on the blockchain. The data reported to the blockchain can include measurements, the status of the distributed devices, and diagnostic and identification information. Since the blockchain nodes maintain the same database in a secure manner by nature, using the distributed ledger technology, they can be programmed to provide the control system with intelligence and autonomy, via a smart contract. The distributed assets

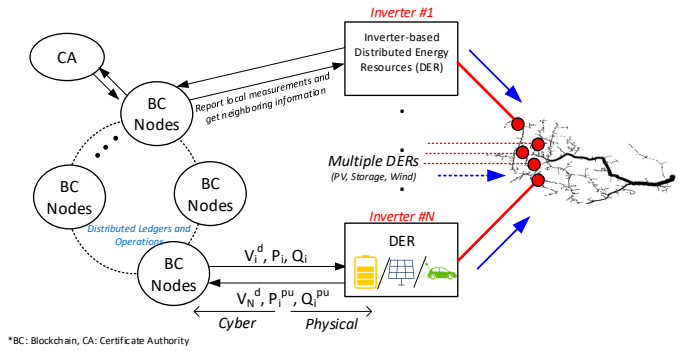


Fig. 1. Blockchain-enabled distributed control based on the consensus algorithm. Each DER communicates with a blockchain node to securely share local measurements with the other DERs and/or controllable assets through the distributed ledger and to resiliently achieve system-level objectives.

can obtain commands and maintain optimal operation based on these promising features [22]. The concept can be used to achieve system resilience under cyberattacks and natural disasters that can compromise the operation of a fraction of or an entire electric power system because the blockchain can sustain its operation even under a severe partial failure.

In this paper, a permissioned blockchain, Hyperledger Fabric (HLF), is investigated for use in the DER control system; HLF blockchain is used as a secure medium for secondary and tertiary control. HLF features privacy—only certified assets (inverters and measurement devices, in this case) can use the network; modularity for customization and performance; and relatively low latency resulting from the lack of proof of work, which is required for public blockchain, such as bitcoin. Under the HLF framework, a blockchain network for the DER-dominant power system control can be implemented with multiple blockchain nodes for resilience. The HLF blockchain provides read (query) and write (invoke) functions to the clients (DERs) for exchanging local measurements and commands for DER control in the concept. As shown in Fig. 2, the read action, query, takes three steps since it does not require blockchain generation, i.e., no ordering service is needed. The read action only needs to refer to the database, World State, which stores the latest information on the assets, whereas the write action would incur a higher latency because of the additional steps needed for the ordering service and for recording the transaction information on the blockchain. In the decentralized microgrid concept, both actions would be involved in the inverter control, i.e., each DER recording its local measurements and reading others to achieve global objectives with the consensus algorithm. In addition, because of the inherent sequence of the processes for authentication, HLF may show a degree of randomness in its delay.

To study the effect of the blockchain-induced delay on the microgrid control, this paper uses a blockchain model developed to represent the variable delay of the HLF based on a benchmark that characterizes its performance under various conditions, including data size, endorsement policy, consensus

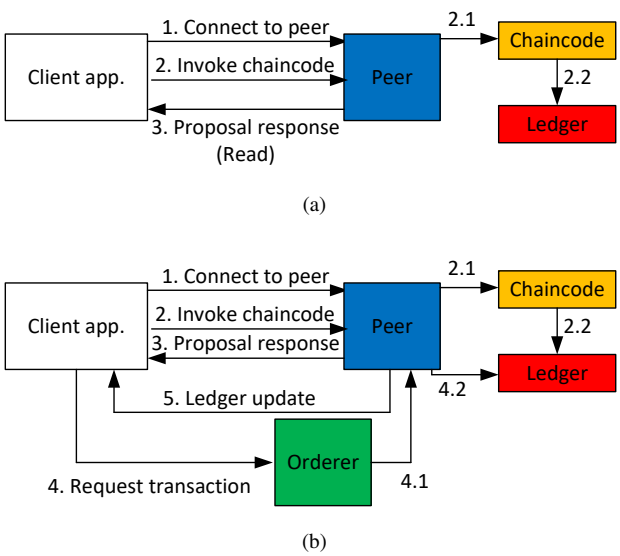


Fig. 2. Simplified diagrams for HLF blockchain operation of read and write (query and invoke): (a) to read the information from the blockchain for secondary control and (b) to write the measurement/command on the blockchain. Since the invoke operation requires additional steps to update the blockchain, it incurs greater latency.

process, database type, and batch size for blockchain. The latency varies with randomness and is dependent on the blockchain operation mechanism, including batch size and time-out, to generate a block and to process the queries. Based on the benchmark, a time-varying delay model with a Gaussian distribution is developed for the performance evaluation in the experiments. A standard deviation of 100 ms with a mean of 47.6 ms have been used for the delay distribution. More details can be found in [19].

III. Blockchain-Enabled Consensus Algorithm for Microgrid Control

Fig. 1 shows the conceptual diagram for the blockchain technology application for the power system control using the consensus-based algorithms. A key concern of the distributed control using the blockchain is the time delay introduced by the additional communication security layers. In this paper, we propose a droop-free distributed voltage and reactive power control as well as a distributed frequency and active power control that tolerates communication delays.

The objective of the distributed voltage controller is to i) regulate the DER point of common coupling (PCC) voltage to nominal voltage, and ii) ensure accurate reactive power sharing among the DERs. The distributed voltage controller is expressed by:

$$\begin{aligned} V_i^d(t) &= V_n + \delta V_i^1(t) + \delta V_i^2(t) \\ V_i^q(t) &= 0 \end{aligned} \tag{1}$$

where $i = 1, 2, ..., N$, and N is the total number of DER; V_n is the nominal inverter output voltage magnitude; and V_i^d and V_i^q are the d- and q-axis voltage magnitude of the ith DER in the synchronous reference frame, respectively. δV_i^1 and δV_i^2 are two voltage correction terms for the ith DER and are defined as follows:

$$\begin{aligned} \delta \dot{V}_i^1(t) &= \sum_{j \in N_i} a_{ij}\left(V_i(t) - V_j(t-\tau_d)\right) + \left(V_n - V_i(t)\right) \\ \delta \dot{V}_i^2(t) &= b \sum_{j \in N_i} a_{ij}\left(Q_i^{pu}(t) - Q_j^{pu}(t-\tau_d)\right) \end{aligned} \tag{2}$$

Here, Q_i^{pu} the is per-unit reactive power of the ith DER defined as $Q_i^{pu} = \frac{Q_i}{Q_i^{max}}$, where Q_i is the reactive power output, and Q_i^{max} is the maximum reactive power rating of the ith DER. $b \in \Re^+$ is the control parameter. Also, τ_d represents the time delay caused by communication and others, and $a_{ij} = 1$ if the information is being exchanged from the ith DER to the jth DER, and $a_{ij} = 0$ if otherwise. If the communication topology is balanced, then $a_{ij} = a_{ji}$.

The objective of the distributed frequency controller is to i) regulate the microgrid frequency within an acceptable boundary, and ii) ensure accurate active power sharing among the DERs. The distributed frequency controller is given by:

$$\omega_i(t) = \omega_n + \delta\omega_i(t) \tag{3}$$

where ω_i is the frequency of the ith DER, and ω_n is the nominal frequency. $\delta\omega_i$ is the frequency correction term for the ith DER, and it is defined as follows:

$$\delta\dot{\omega}_i(t) = c \sum_{j \in N_i} a_{ij}\left(P_i^{pu}(t) - P_j^{pu}(t-\tau_d)\right) \tag{4}$$

Here, P_i^{pu} is the per-unit active power of the ith DER defined as $P_i^{pu} = \frac{P_i}{P_i^{max}}$, where P_i is the active power output, and P_i^{max} is the maximum active power rating of the ith DER.

Remark 1: Mathematically, the control objectives can be defined as follows:

$$\begin{aligned} \lim_{t\to\infty}\left(\omega_i(t) - \omega_n\right) &= 0 \\ \lim_{t\to\infty}\left(V_i^d(t) - V_n\right) &= 0 \\ \lim_{t\to\infty} P_1^{pu}(t) = \lim_{t\to\infty} P_2^{pu}(t) &= \ldots = \lim_{t\to\infty} P_N^{pu}(t) \\ \lim_{t\to\infty} Q_1^{pu}(t) = \lim_{t\to\infty} Q_2^{pu}(t) &= \ldots = \lim_{t\to\infty} Q_N^{pu}(t) \end{aligned} \tag{5}$$

A. Stability of Distributed Frequency Control with Time Delay

The proposed distributed frequency control is based on the following two assumptions:

Assumption 1: The communication graph is balanced.

Assumption 2: There is a proportional relationship between the per-unit active power output of each DER and the frequency of the voltage at the PCC of the DER. The slope of the per-unit active power versus the frequency curve is negative.

Assumption 1 is achievable with a careful design of the sparse communication topology. On the other hand, *Assumption 2* is true for most microgrids having a high $\frac{X}{R}$ ratio. Now, the main result related to the distributed frequency control is as follows:

Theorem 1: All agents in the system (3) under *Assumption 1* and *Assumption 2* with the control (4) synchronize to the

reference frequency, ω_n, and the per-unit power output of each agent will have the same equilibrium even with the communication delay.

Proof: Rearranging (3) and taking the derivative,

$$\begin{aligned}\delta\dot{\omega}_i(t) &= \dot{\omega}_i(t) - \dot{\omega}_n \\ &= \dot{\omega}_i(t) = c\sum_{j\in N_i} a_{ij}\left(P_i^{pu}(t) - P_j^{pu}(t-\tau_d)\right),\end{aligned} \tag{6}$$

Using assumption 2, (6) can be expressed as:

$$\begin{aligned}\delta\dot{\omega}_i(t) &= ck\sum_{j\in N_i} a_{ij}\left(\omega_j(t-\tau_d) - \omega_i(t)\right) \\ &= ck\sum_{j\in N_i} a_{ij}\left(\delta\omega_j(t-\tau_d) - \delta\omega_i(t)\right),\end{aligned} \tag{7}$$

where $k \in \Re^+$. Now, consider following Lyapunov function:

$$V(t) = \sum_{i=1}^{N}\left(\delta\omega_i(t)\right)^2 + ck\sum_{i=1}^{N}\sum_{j\in N_i}\int_{t-\tau_j}^{t} a_{ij}\left(\delta\omega_j(s)\right)^2 ds \tag{8}$$

Observing (8), it can be said that $V(t) \geq 0$. Because the communication graph is assumed to be balanced in Assumption 1, we have:

$$\sum_{i=1}^{N}\sum_{j\in N_i} a_{ij}\left(\delta\omega_i(t)\right)^2 = \sum_{i=1}^{N}\sum_{j\in N_i} a_{ij}\left(\delta\omega_j(t)\right)^2 \tag{9}$$

After some mathematical manipulation and using (9), the time derivative of $V(t)$ is as follows:

$$\dot{V}(t) = -ck\sum_{i=1}^{N}\sum_{j\in N_i} a_{ij}\left(\delta\omega_i(t) - \delta\omega_j(t-\tau_j)\right)^2 \leq 0 \tag{10}$$

So the system (3) is asymptotically stable, and $\lim_{t\to\infty}\left(\omega_i(t) - \omega_n(t)\right) = 0$, and $\lim_{t\to\infty} P_i^{pu}(t) = \lim_{t\to\infty} P_j^{pu}(t)$. This completes the proof. ■

B. Stability of Distributed Voltage Control with Time Delay

Assumption 3: There is a proportional relationship between the per-unit reactive power output of each DER and the d-axis magnitude of the voltage at the PCC of the DER. The slope of the per-unit reactive power versus the $d-axis$ voltage magnitude curve is negative.

Assumption 3 is true for the case where the phase angle of the DER PCC voltage does not vary with a significant margin from one DER to another. Now, the stability assessment for the distributed voltage control is as follows:

Theorem 2: All agents in the system (1) under *Assumption 1* and *Assumption 3* with the control (2) synchronize to the reference voltage magnitude, V_n, and the per-unit reactive power output of each agent will have the same value even with the communication delay.

Proof: Assuming the voltage difference between the ith node from the nominal voltage as $\delta V_i(t)$, i.e., $\delta V_i(t) = V_i(t) - V_n$, (1) can be rewritten as:

$$\delta V_i^1(t) + \delta V_i^2(t) = V_i^d(t) - V_n = V_i(t) - V_n = \delta V_i(t) \tag{11}$$

Using *Assumption 3* and with some manipulations, (2) can be written as:

$$\begin{aligned}\delta\dot{V}_i^1 &= \sum_{j\in N_i} a_{ij}\left(\delta V_i(t) - \delta V_j(t-\tau_d)\right) - \delta V_i(t) \\ \delta\dot{V}_i^2 &= bm\sum_{j\in N_i} a_{ij}\left(V_j(t-\tau_d) - V_i(t)\right) \\ &= bm\sum_{j\in N_i} a_{ij}\left(\delta V_j(t-\tau_d) - \delta V_i(t)\right)\end{aligned} \tag{12}$$

where $m \in \Re^+$. Now, consider following Lyapunov function:

$$\begin{aligned}V(t) = &\sum_{i=1}^{N}\left(\delta V_i^1(t) + \delta V_i^2(t)\right)^2 \\ &+ (1+bm)\sum_{i=1}^{N}\sum_{j\in N_i}\int_{t-\tau_j}^{t} a_{ij}\left(\delta V_j(s)\right)^2 ds\end{aligned} \tag{13}$$

Observing (13), it can be said that $V(t) \geq 0$. Taking the derivative of both sodes of (13),

$$\begin{aligned}\dot{V}(t) = &2\sum_{i=1}^{N}\left(\delta V_i^1(t) + \delta V_i^2(t)\right)\left(\delta\dot{V}_i^1(t) + \delta\dot{V}_i^2(t)\right) \\ &+ (1+bm)\sum_{i=1}^{N}\sum_{j\in N_i} a_{ij}\left(\left(\delta V_j(t)\right)^2 - \left(\delta V_j(t-\tau_d)\right)^2\right)\end{aligned} \tag{14}$$

Using (11) in (14),

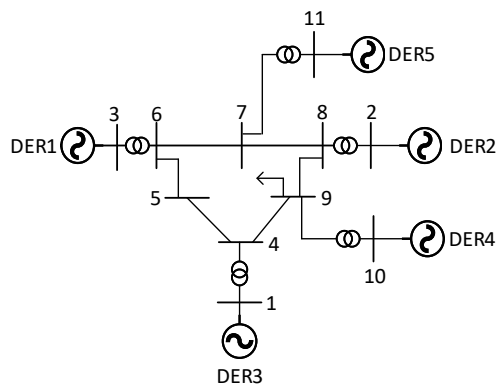
$$\begin{aligned}\dot{V}(t) = &2\sum_{i=1}^{N}\delta V_i(t)\left(\delta\dot{V}_i^1(t) + \delta\dot{V}_i^2(t)\right) \\ &+ (1+bm)\sum_{i=1}^{N}\sum_{j\in N_i} a_{ij}\left(\left(\delta V_j(t)\right)^2 - \left(\delta V_j(t-\tau_d)\right)^2\right)\end{aligned} \tag{15}$$

The relations expressed in (12) can be used in (15) to get the expression for $\dot{V}(t)$ as follows:

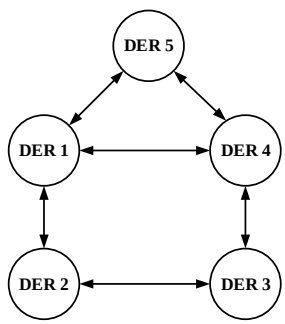
$$\begin{aligned}&\dot{V}(t) = \\ &(1+bm)\sum_{i=1}^{N}\sum_{j\in N_i} a_{ij}\left(2\delta V_i(t)\,\delta V_j(t-\tau_d) - 2\left(\delta V_j(t)\right)^2\right) \\ &-2\sum_{i=1}^{N}\left(\delta V_i(t)\right)^2 \\ &+ (1+bm)\sum_{i=1}^{N}\sum_{j\in N_i} a_{ij}\left(\left(\delta V_j(t)\right)^2 - \left(\delta V_j(t-\tau_d)\right)^2\right)\end{aligned} \tag{16}$$

Because the communication graph is assumed to be balanced in Assumption 1, we have:

$$\sum_{i=1}^{N}\sum_{j\in N_i} a_{ij}\left(\delta V_i(t)\right)^2 = \sum_{i=1}^{N}\sum_{j\in N_i} a_{ij}\left(\delta V_j(t)\right)^2 \tag{17}$$



(a)



(b)

Fig. 3. Simulation setup to evaluate the performance of the proposed distributed controller: (a) modified IEEE 9-bus system, and (b) communication topology for communication among the DERs.

After some mathematical manipulation and using (17) in (16), the time derivative of $V(t)$ is as follows:

$$\dot{V}(t) = -(1+bm)\sum_{i=1}^{N}\sum_{j\in N_i} a_{ij}\left(\delta V_i(t) - \delta V_j(t-\tau_j)\right)^2 - 2\sum_{i=1}^{N}\left(\delta V_i(t)\right)^2 \leq 0 \tag{18}$$

So the system (1) is asymptotically stable, and $\lim_{t\to\infty}(V_i(t) - V_n(t)) = 0$, which implies $\lim_{t\to\infty}\delta V_i^1(t) = 0$ and $\lim_{t\to\infty}\delta V_i^2(t) = 0$. From (2), $\lim_{t\to\infty} Q_i^{pu}(t) = \lim_{t\to\infty} Q_j^{pu}(t)$. This completes the proof. ■

Remark 2: Assumption 3 is a weak assumption: Reactive power is not only a function of voltage magnitude but also a function of the phase angle of the PCC voltage. Thus, the network impedance plays a crucial role in the reactive power generation from the DER. Hence, *Theorem 2* is as good as the *Assumption 3*.

IV. Simulation Results

The performance of the proposed blockchain-enabled distributed control using the consensus algorithm is verified in a modified IEEE 9-bus network, converted to an 11-bus network to accommodate five DERs, as shown in Fig. 3(a). All DERs are rated at 10 MVA, and they are supposed to evenly share the active and reactive powers through the consensus algorithm-based control. The communication topology of the system is illustrated in Fig. 3(b). Four cases were tested for the performance evaluation for the system under different communication conditions, as discussed next.

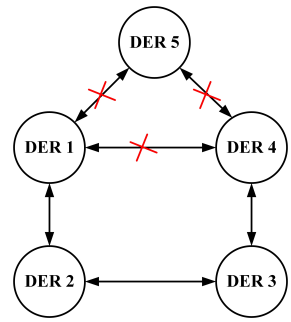


Fig. 4. Communication interruption for Case #2.

- *Case #1–Baseline*: It serves as the baseline, operation with the proposed distributed controller and no interruption. To emulate a delay that may be minimal without a security measure, a universal delay of 0.1 ms is used in this case: No blockchain-induced delay is applied in this case.
- *Case #2–Communication interruption*: In this test case as shown in Fig. 4, the three communication links connecting DER #1, DER #4, and DER #5 are interrupted at $t = 34.5$ seconds, making DER #5 islanded, though it is still physically connected to the grid, and loosening the connections among the other DERs as well. It is to investigate the impact of cyberattacks that could disable a fraction of the communication links, such as a denial-of-service attack.
- *Case #3–Heavy communication delay*: A heavy communication delay is imposed on the communication channels that emulates a cyberattack attempt to cause a sub-optimal or detrimental operation. A delay of 1 second is used in this test case.
- *Case #4–Blockchain-protected system*: This case emulates the system whose communication is protected by the blockchain as proposed in this paper. It is expected that the system may retain the communications among DERs, and stay resilient against the cyberattacks emulated in *Case #2 and Case #3*, but the security measure would induce a sizable communication delay with randomness, as explained in Section II.

For all test cases, a load transient occurs at $t = 35$ seconds to evaluate the system performance for the voltage and frequency regulation and the power rebalancing after the transient.

Fig. 5 shows the simulation results of the four test cases. From the result of the baseline case and the other cases,

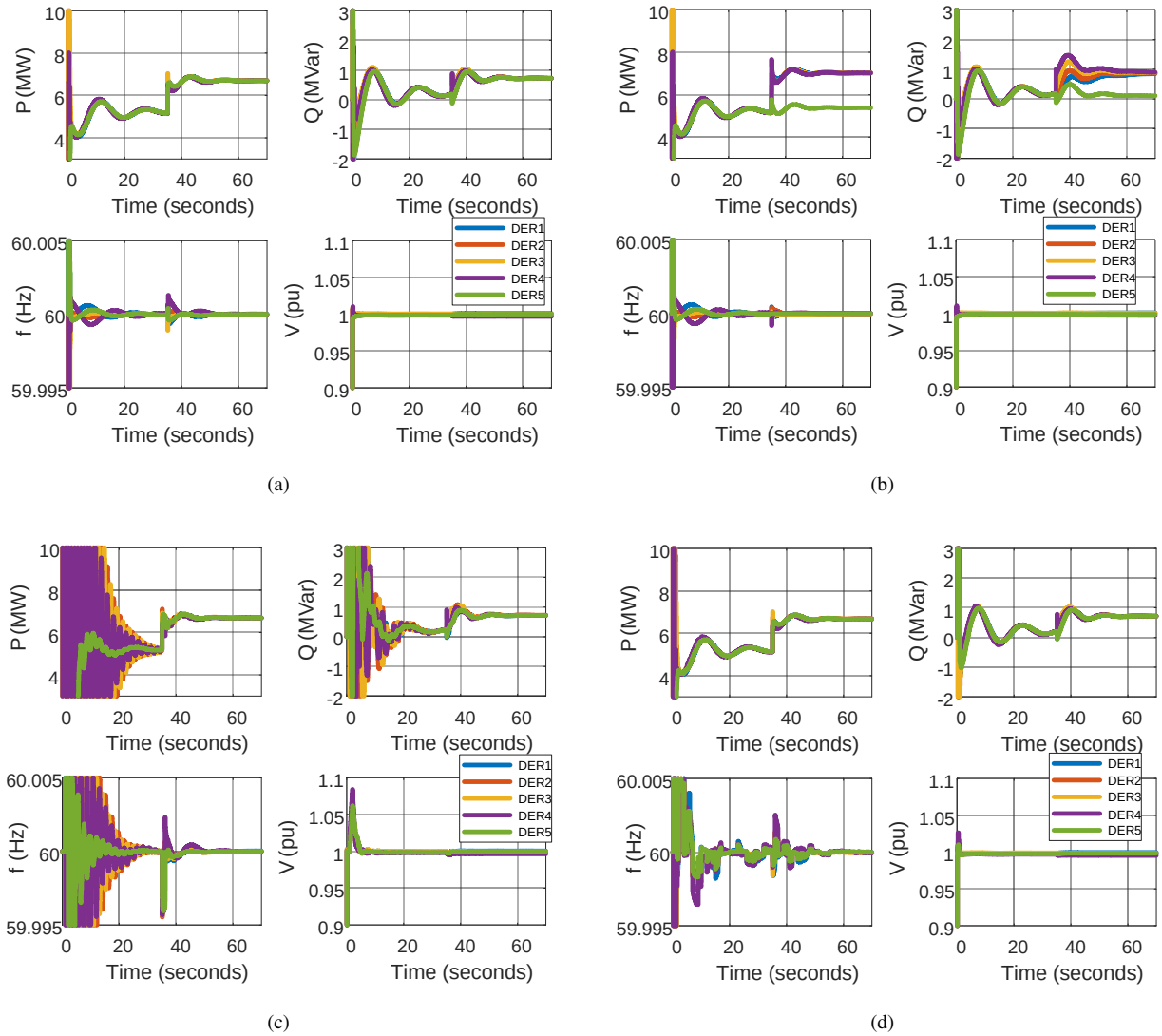


Fig. 5. Comparison of the system performances of test cases with different communication measures and contingencies: (a) baseline without any communication delay, interruption, or blockchain; (b) communication interruption at 34.5 seconds isolating DER #5; (c) heavy communication delay of 1 second, and (d) operation with communication secured by blockchain and therefore the blockchain-induced delay, proposed in this paper. A load transient occurs at 35 seconds.

it is confirmed that the consensus-based controller achieves the control objectives as described in (5), even under severe constraints, and communication delays, maintaining stability, as proved in Section III. Noticeably, Fig. 5(b), for the communication interruption, implies that a severe cyberattack, e.g., a denial-of-service attack, might cause suboptimal operation of the system, disabling key system functionalities, as well as longer settling times or undesirable oscillations after a disturbance due to reduced visibility. From Fig. 5(c), it is clear that the communication delay would play a critical role in the control dynamic, and it could be detrimental. The 1-second delay, blocking the measurement data flow among the DERs, substantially affect the regulation performance. It also implies that the proper communication system design would be critical to guarantee the system performance; the trade-off between the security measure to protect the system and the resultant delay or compromise should be properly considered in the design stage. Finally, Fig. 5(d) demonstrates the performance of the proposed blockchain-based system. The result shows slighted compromised regulation performance with an increased settling time and increased system parameter excursions in the transients; however, importantly, it would survive under severe cyberattacks avoiding the severe suboptimal operations shown in the other results.

V. Conclusion

A blockchain-enabled, cyber-secure distributed controller based on the consensus algorithm for voltage and frequency regulation has been proposed in this paper. The HLF blockchain can provide high security in the DER communications at the cost of increased latency, inducing a variable delay. By constructing a suitable Lyapunov function, it was proved

that the proposed controller can retain stability even under the communication delay. The consensus-based control can restore the microgrid voltage and frequency to the respective nominal values; and, by doing so, it can achieve accurate active and reactive power sharing. To evaluate its performance and compare with conventional systems without security measures, four test cases using MATLAB Simulink have been developed, including load transients, communication interruptions, a heavy communication delay, and a blockchain-induced variable delay to emulate the proposed system. Simulation results imply that the proposed consensus-based control reinforced by the blockchain can achieve the system-level control objectives, securing high resilience against cyberattacks and thus preventing system failure or suboptimal operation, which are simulated in the other test cases.

ACKNOWLEDGMENT

The authors would like to thank Dr. Abdullah Al Hadi for his assistance in the Hyperledger Fabric characterization.

REFERENCES

[1] B.-M. S. Hodge, H. Jain, C. Brancucci, G.-S. Seo, M. Korpås, J. Kiviluoma, H. Holttinen, J. C. Smith, A. Orths, A. Estanqueiro *et al.*, "Addressing technical challenges in 100% variable inverter-based renewable energy power systems," *Wiley Interdisciplinary Reviews: Energy and Environment*, vol. 9, no. 5, p. e376, 2020.

[2] S. Chakraborty, B. Kramer, and B. Kroposki, "A review of power electronics interfaces for distributed energy systems towards achieving low-cost modular design," *Renewable and Sustainable Energy Reviews*, vol. 13, no. 9, pp. 2323–2335, 2009.

[3] J. Ye, A. Giani, A. Elasser, S. K. Mazumder, C. Farnell, H. A. Mantooth, T. Kim, J. Liu, B. Chen, G.-S. Seo, W. Song, M. D. Roig Greidanus, S. Sahoo, F. Blaabjerg, J. Zhang, L. Guo, B. Ahn, M. B. Shadmand, N. R. Gajanur, and M. A. Abbaszada, "A review of cyber-physical security for photovoltaic systems," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, early access, September 10, 2021, doi: 10.1109/JESTPE.2021.3111728.

[4] Energy Sector Control Systems Working Group (Sep. 2011), "Roadmap to achieve energy delivery systems cybersecurity."

[5] M. S. Golsorkhi and M. Savaghebi, "A decentralized control strategy based on vi droop for enhancing dynamics of autonomous hybrid ac/dc microgrids," *IEEE Transactions on Power Electronics*, vol. 36, no. 8, pp. 9430–9440, 2021.

[6] M. C. Chandorkar, D. M. Divan, and R. Adapa, "Control of parallel connected inverters in standalone ac supply systems," *IEEE transactions on industry applications*, vol. 29, no. 1, pp. 136–143, 1993.

[7] S. Wang, Z. Liu, J. Liu, D. Boroyevich, and R. Burgos, "Small-signal modeling and stability prediction of parallel droop-controlled inverters based on terminal characteristics of individual inverters," *IEEE Transactions on Power Electronics*, vol. 35, no. 1, pp. 1045–1063, Jan. 2019.

[8] Y. Lin, J. H. Eto, B. B. Johnson, J. D. Flicker, R. H. Lasseter, H. N. Villegas Pico, G.-S. Seo, B. J. Pierre, and A. Ellis, "Research roadmap on grid-forming inverters," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2020.

[9] G.-S. Seo, M. Colombino, I. Subotic, B. Johnson, D. Groß, and F. Dörfler, "Dispatchable virtual oscillator control for decentralized inverter-dominated power systems: Analysis and experiments," in *Proc. IEEE Applied Power Electron. Conf.* IEEE, 2019, pp. 561–566.

[10] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. De Vicuña, and M. Castilla, "Hierarchical control of droop-controlled ac and dc microgrids—a general approach toward standardization," *IEEE Transactions on industrial electronics*, vol. 58, no. 1, pp. 158–172, Jan. 2010.

[11] V. Nasirian, Q. Shafiee, J. M. Guerrero, F. L. Lewis, and A. Davoudi, "Droop-free distributed control for ac microgrids," *IEEE Transactions on Power Electronics*, vol. 31, no. 2, pp. 1600–1617, Feb, 2015.

[12] R. Mahmud, A. Nejadpak, and R. Ahmadi, "Cooperative Load Sharing in V2G Application," in *Proc. IEEE International Converence on Electro/Information Technology*, 2015.

[13] R. Mahmud and A. Nejadpak, "Distributed Cooperative Control of Hybrid AC/DC Microgrid," in *Proc. IEEE Photovoltaic Specialists Conference*, 2019, pp. 2950–2955.

[14] D. He, D. Shi, and R. Sharma, "Consensus-based distributed cooperative control for microgrid voltage regulation and reactive power sharing," in *Proc. IEEE PES Innovative Smart Grid Technologies, Europe*, 2014, pp. 1–6.

[15] E. Espina, R. Cárdenas-Dobson, J. W. Simpson-Porco, D. Sáez, and M. Kazerani, "A consensus-based secondary control strategy for hybrid ac/dc microgrids with experimental validation," *IEEE Transactions on Power Electronics*, vol. 36, no. 5, pp. 5971–5984, 2020.

[16] A. Stanciu, "Blockchain Based Distributed Control System for Edge Computing," *Proc. IEEE International Conference on Control Systems and Computer*, pp. 667–671, jul 2017.

[17] M. L. Di Silvestre, P. Gallo, J. M. Guerrero, R. Musca, E. R. Sanseverino, G. Sciumè, J. C. Vásquez, and G. Zizzo, "Blockchain for power systems: Current trends and future applications," *Renewable and Sustainable Energy Reviews*, vol. 119, p. 109585, 2020.

[18] A. A. Hadi, G. Bere, T. Kim, J. J. Ochoa, J. Zeng, and G.-S. Seo, "Secure and cost-effective micro phasor measurement unit PMU-like metering for behind-the-meter BTM solar systems using blockchain-assisted smart inverters," in *Proc. IEEE Applied Power Electron. Conf.* IEEE, 2020, pp. 2369–2375.

[19] N. Gajanur, M. Greidanus, G.-S. Seo, S. K. Mazumder, and M. A. Abbaszada, "Impact of blockchain delay on grid-tied solar inverter performance," in *Proc. IEEE International Symposium on Power Electronics for Distributed Generation Systems*, 2021, pp. 1–7.

[20] G. Chen and Z. Guo, "Distributed secondary and optimal active power sharing control for islanded microgrids with communication delays," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2002–2014, Mar. 2019.

[21] M. J. Park, S. H. Lee, O. M. Kwon, and S. G. Choi, "Sampling Effect on Secondary Control of Microgrids via Consensus Protocol of Multi-Agent Systems," *IEEE Access*, vol. 6, pp. 38 535–38 543, Jul. 2018.

[22] Y. Li, W. Yang, P. He, C. Chen, and X. Wang, "Design and management of a distributed hybrid energy system through smart contract and blockchain," *Applied Energy*, vol. 248, pp. 390–405, 2019.