Journal of Science and Technology – Smart Systems and Devices
Volume x, Issue x, Month Year, ppp-ppp

Using the Ethereum Blockchain Platform for Data Storage and Protection in Model Predictive Frequency Control System of Microgrid

Duong Minh Hai, Le Ngoc Dung, Nguyen Duc Tuyen*
Hanoi University of Science and Technology, Ha Noi, Vietnam
**Corresponding author email: tuyen.nguyenduc@hust.edu.vn*

Abstract
Microgrids with high penetration of renewable energy sources (REs) require secure, transparent, and reliable data exchange to maintain stable operation. However, communication delays and False Data Injection Attacks (FDIA) can severely degrade system performance and compromise control reliability. To address these issues, this paper proposes a blockchain-assisted Distributed Model Predictive Control (DMPC) framework using the Ethereum platform and smart contracts to enhance data storage security and integrity verification in microgrid operation. The primary control layer employs Finite Control Set Model Predictive Control (FCS-MPC) with harmonic suppression and virtual-impedance-based droop control, while the secondary layer implements a DMPC strategy to achieve frequency consensus and coordinated power sharing among Distributed Generators (DGs). All control signals and measurement data are encrypted, transmitted, and immutably stored on the blockchain through Ganache and Web3.js, enabling transparent data logging and integrity verification of operational data in microgrid communication networks. Simulation results on a four-DGs microgrid in MATLAB/Simulink show that the proposed method maintains identical control performance compared to the conventional system, demonstrating that blockchain integration enhances transparency and cybersecurity without degrading dynamic response or control accuracy.

Keywords: Blockchain technology, ethereum, microgrid, model predictive control, smart contract.

1. Introduction

The integration of REs and distributed generation is becoming increasingly prevalent in modern power systems, fostering the development of microgrids. These small-scale power networks enhance efficiency and reliability, particularly in scenarios involving grid disturbances [1]. However, communication latency and data security have emerged as common challenges in microgrids, and blockchain technology has gained prominence as a potential solution to address these issues. In study by Tuyen *et al.* [2], cybersecurity challenges in microgrid control were analyzed, and several countermeasures such as access control, encryption, and intrusion detection were proposed. Nour et al. [3] discussed the potential and challenges of applying blockchain technology in the power sector. Veerasamy *et al.* [4] developed a blockchain-based peer-to-peer energy trading framework with resilient control, maintaining frequency stability and data privacy under cyberattacks. Similarly, Yang *et al.* [5] proposed a blockchain-based security framework that ensures secure communication and data integrity within microgrids. In our previous research, Dung *et al.* [6] also proposed integrating blockchain technology using the IOTA platform, but their work did not verify the integrity of the data once it was uploaded to the blockchain. Therefore, this paper introduces a novel approach to implementing Model Predictive Frequency Control (MPFC) on the Ethereum blockchain platform while addressing key cybersecurity challenges. The proposed method employs Solidity smart contracts, Web3.js, Ganache and encryption techniques to securely record system data on the blockchain, which is subsequently decrypted to verify data integrity. This process ensures both data security and privacy while enhancing the integrity and traceability of operational data in microgrid communication networks.

2. Model Predictive Frequency Control for Microgrid

Model Predictive Control (MPC) has become one of the most advanced and flexible control strategies for modern microgrids due to its predictive capability and ability to explicitly handle operational constraints. MPC utilizes a discrete-time mathematical model of the system to forecast its future behavior over a specified prediction horizon. At each sampling instant, the controller determines the optimal control action by minimizing a cost function that reflects key objectives such as minimizing frequency deviation or ensuring power balance, while satisfying system constraints. Only the first control action of the computed sequence is applied, and the optimization process is repeated at the next time step, allowing continuous adaptation to dynamic operating conditions. In Liu *et al.* [7], proposed a MPC approach for frequency regulation in networked microgrids, which effectively maintains voltage constraints and enhances coordination among microgrids using limited communication. In Lou *et al.*

p-ISSN 3093-3285
e-ISSN 3093-3315
https://doi.org/10.51316/jst.xxx.ssad.xxxx.xx.x.x
Received: ...../..../.....; Revised: ...../..../.....;
Accepted: ...../..../.....; Online: ...../..../.....

[8], proposed a MPC strategy for secondary voltage regulation in islanded microgrids, which incorporates input–output feedback linearization to handle system nonlinearities and enhance voltage and frequency stability under communication delays and uncertainties. In Zhao *et al.* [9], presented a model predictive secondary frequency control method for islanded microgrids using an unknown input observer and virtual synchronous generator deloading control, which enhances frequency stability under stochastic wind and solar conditions. In this study, we propose to apply MPC to the secondary frequency control layer of a microgrid. Unlike the primary droop control, which cannot remove steady-state deviations, the MPC-based strategy predicts system dynamics and optimizes the power output of controllable sources and loads under given constraints. The objective is to minimize frequency deviation from the nominal value, formulated as a Quadratic Program (QP) that can be efficiently solved using numerical optimization methods.

3. Ethereum Blockchain Platform

Ethereum, launched in 2015 by Vitalik Buterin and collaborators, is an open-source, decentralized blockchain platform designed not only for peer-to-peer payments but also for deploying and executing smart contracts on a global computing infrastructure. Unlike Bitcoin, Ethereum supports a wide range of decentralized applications (dApps), including Decentralized Finance (DeFi), Decentralized Autonomous Organizations (DAOs), Non-Fungible Tokens (NFTs), and peer-to-peer energy trading. The Ethereum Virtual Machine (EVM) provides a secure environment for running smart contracts written in Solidity, ensuring transparency and immutability. Compared with other distributed ledger technologies such as IOTA, which relies on the Tangle structure but lacks mature smart-contract functionality, or Hyperledger, which supports permissioned networks but requires more complex configuration and offers limited public accessibility, Ethereum delivers a more flexible, widely adopted, and developer-friendly ecosystem. The availability of robust development tools including Ganache, Truffle, and Web3.js enables rapid prototyping, straightforward deployment, and convenient testing, making Ethereum an effective platform for evaluating blockchain-enhanced control architectures. Initially operating under a Proof-of-Work (PoW) mechanism, Ethereum has since transitioned to Proof-of-Stake (PoS) to improve scalability and energy efficiency.

3.1. Proof of Stake Method

Ethereum now employs the PoS consensus mechanism as a replacement for the energy-intensive PoW, eliminating the need for computationally demanding mining processes. In PoS, validators are selected based on their staked ETH to propose or confirm new blocks, receiving rewards for honest behavior while malicious actions can lead to slashing of staked assets. This approach enhances security by making attacks economically impractical, while also improving scalability, reducing operational costs, and promoting greater decentralization. Following The Merge in 2022, Ethereum's energy consumption decreased by more than 99%, addressing long-standing environmental concerns and aligning the platform with sustainable technology goals. Overall, PoS provides Ethereum with a secure, efficient, and environmentally responsible foundation suitable for modern decentralized applications.

3.2. Ganache

Ganache is a personal blockchain platform developed by Truffle Suite to simulate the Ethereum network for research, development, and testing of smart contracts and dApps. It provides fast, low-latency block generation independent of external network conditions and initializes with preloaded ETH accounts so contracts can be executed without real transaction fees. Supporting the JSON-RPC protocol, Ganache is fully compatible with Web3.js, Ethers.js, and other Ethereum development tools. It also offers flexible state management features such as snapshots, state reversion, timestamp adjustment, and manual block generation, which are useful for testing time-dependent contracts. In addition, Ganache supports network forking from mainnet or testnets, allowing developers to replicate real blockchain states safely while enabling controlled experimentation through unlocked accounts with visible private keys. Overall, it provides a reproducible, safe, and efficient environment for evaluating blockchain consensus, transactions, and smart-contract behavior prior to real deployment.

3.3. Ethereum Smart Contract

A smart contract is a self-executing program stored on the blockchain that automatically runs when predefined conditions are satisfied, enabling the enforcement and verification of agreements without intermediaries. Written in Solidity and deployed as immutable entities with unique addresses, smart contracts are executed by all nodes in the Ethereum network to ensure consensus and prevent unauthorized modification. When triggered by user-initiated transactions or interactions between contracts, they require a gas fee proportional to computational cost, which helps deter unnecessary computation and network abuse. Smart contracts contain functions, state variables, and events that support a wide range of decentralized applications including decentralized finance protocols, token standards such as ERC-20 and ERC-721, and governance mechanisms in decentralized autonomous organizations. Their core properties of automation, transparency, and immutability reduce the risk of fraud, increase trust among participants, and improve transactional efficiency across the blockchain ecosystem.

4. Utilizing Blockchain for Distributed Model Predictive Frequency Control for Microgrids

Fig. 1 illustrates the overall architecture of the proposed blockchain-integrated DMPC framework for microgrids. The system includes two main parts: the distributed model predictive control strategy and the blockchain-based data management layer.

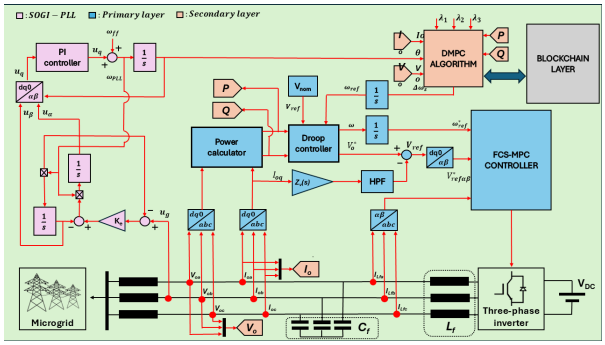

Fig. 1. Blockchain-Integrated Control Architecture for Microgrids

4.1. Distributed Model Predictive Frequency Control

The proposed fully distributed model predictive frequency control operates under a hierarchical two-layer architecture, consisting of a primary layer and a secondary layer. The primary layer governs local dynamics, maintaining stability of voltage and frequency at each DG, while the secondary layer coordinates among DGs to guarantee global synchronization of the microgrid frequency and power sharing.

4.1.1. Primary control layer

The primary layer serves as the local control mechanism, responsible for regulating the output voltage and frequency of each inverter-based DG within the permissible operating range. It consists of two main components:

1) FCS-MPC with Harmonic Suppression: In this context, the finite control set model predictive control (FCS-MPC) requires a cost function to optimize the control law. The conventional FCS-MPC system for voltage regulation can be developed with calculations performed in the α–β reference frame, as examined in [10]:

$$g_{\text{conv}} = \left(V^*_{\text{ref}\alpha} - V^p_{cf\alpha}(k+n)\right)^2 + \left(V^*_{\text{ref}\beta} - V^p_{cf\beta}(k+n)\right)^2 \tag{1}$$

where g_{conv} is the cost function, $V^*_{\text{ref}\alpha}$ and $V^*_{\text{ref}\beta}$ are the real and imaginary components of the voltage reference signal, and $V^p_{cf\alpha}(k+n)$ and $V^p_{cf\beta}(k+n)$ are the predicted voltage components corresponding to each switching configuration. The variable k denotes the prediction step. In this study, $n = 2$ is selected to suppress harmonic distortions.

The influence of this secondary objective is captured by introducing the weighting factor λ_d, resulting in the modified cost function:

$$g_{\text{conv}} = \left(V^*_{\text{ref}\alpha} - V^p_{cf\alpha}(k+n)\right)^2 + \left(V^*_{\text{ref}\beta} - V^p_{cf\beta}(k+n)\right)^2 + \lambda_d\, g_I \tag{2}$$

For simplification, the weighting factor λ_d is set to unity in this work.

The control algorithm proposed for the primary layer is based on the FCS-MPC principle, where the control cost function is minimized by evaluating all possible switching states and selecting the one that yields the smallest cost. Each switching state corresponds to a unique vector of inverter output voltage in the space vector modulation plane. By employing this predictive control scheme, the system achieves fast dynamic response and reduced steady-state error in frequency and voltage regulation.

2) Virtual-Impedance-Enhanced Droop Controller: The droop control strategy is commonly used for power sharing among inverter-based DGs. In this approach, a virtual impedance loop is incorporated to adjust the inverter's output impedance, thereby enhancing the microgrid's apparent inertia, improving voltage quality under weak-grid conditions, and enabling more precise active and reactive power sharing. By embedding harmonic suppression within the primary FCS-MPC stage, the proposed model ensures high-quality voltage regulation and robust harmonic performance without additional filtering components.

4.1.2. Secondary control layer

The secondary layer operates at a higher hierarchical level and ensures system-wide frequency restoration and coordinated power sharing across the entire microgrid. Unlike the local primary controllers, the secondary layer relies on communication among DGs to achieve distributed consensus. Its main components are as follows:

1) Distributed Generator Model: In the context of a three-phase microgrid without a neutral line, the frequency dynamics of each DG can be represented using the droop control law:

$$\omega_i(t) = \omega^* - M_{p\omega,i} P_i(t) + \omega_{s,i}(t) \tag{3}$$

$$\delta\theta_i(t) = \theta_i(t) - \theta^*_i(t) = \int_0^t \left[\omega_i(\tau) - \omega^*_i(\tau)\right] d\tau \tag{4}$$

$$P_i(t) = M_i V_i(t) V^*_i(t) \sin\left(\delta\theta_i(t)\right) \tag{5}$$

$$M_i = \frac{1}{L_i\,\omega_0} \tag{6}$$

In these equations, $\omega_i(t)$ denotes the inverter operating frequency, which determines the normalized active power output $P_i(t)$. The term $M_{p\omega,i}$ corresponds to the droop coefficient that defines the frequency–power relationship, whereas $\omega_{s,i}$ represents the secondary control signal. The coupling inductance L_i provides the interconnection between the inverter and the microgrid, thereby influencing the phase-angle deviation $\delta\theta_i(t)$.

2) DMPC Strategy: To enable coordination among DGs, the communication network is modeled by an adjacency matrix defined as:

$$a_{ij} = \begin{cases} 1, & \text{if } i \neq j \text{ and data from } j \text{ to } i, \\ 0, & \text{if } i \neq j \text{ and no data from } j \text{ to } i, \\ 0, & \text{if } i = j. \end{cases} \tag{7}$$

This matrix describes the connectivity of the distributed communication graph. Each DG formulates a local MPC problem based on its own dynamics and the information received from its neighbors, avoiding reliance on a centralized controller. By embedding the graph topology into the predictive optimization, the DMPC framework ensures that frequency regulation and active power sharing are achieved in a fully distributed manner across the microgrid.

3) Equality Constraints: To guarantee that the system frequency converges to the nominal reference ω_0 within the prediction horizon N_y, equality constraints are imposed on the predictive model. A key feature is the explicit incorporation of communication delay estimates $\hat{\tau}_{ij}$:

$$\bar{\omega}_i(t_{n+k}) = \frac{\omega_0 + \omega_i(t_{n+k}) + \sum_{j=N_i}^{p} a_{ij}(t_n)\,\omega_j(t_{n+k-\hat{\tau}_{ij}})}{2 + \sum_{j=N_i}^{p} a_{ij}(t_n)} \tag{8}$$

$$\bar{\omega}_i(t_{n+N_y}) = \omega_0 \tag{9}$$

This enables the predictive model to remain robust against time delays in information exchange across the communication network.

4) Inequality Constraints: To respect physical limitations, the active power output of each DG must remain within its rated capacity:

$$0 < P_i(t_{n+k}) < P_{i,\max} \tag{10}$$

5) DMPC Optimization Problem: Each distributed generator (DG) solves a convex quadratic programming (QP) problem that minimizes a cost function $C_i(t_n)$ consisting of three weighted objectives:

$$\begin{aligned} C_i(t_n) = &\sum_{k=1}^{N_y} \lambda_{1i}\big(\bar{\omega}_i(t_{n+k}) - \omega_0\big)^2 \\ &+ \sum_{k=1}^{N_y} \lambda_{2i}\big(\Delta\omega_{s,i}(t_{n+k-1})\big)^2 \\ &+ \sum_{j=1,\,j\neq i}^{p} \sum_{k=1}^{N_y} \lambda_{3i}\,a_{ij}(t_n)\left(\frac{P_i(t_{n+k})}{P_{i,\max}} - \frac{P_j(t_{n+k-\hat{\tau}_{ij}})}{P_{j,\max}}\right)^2 \end{aligned} \tag{11}$$

where λ_{1i}, λ_{2i}, and λ_{3i} are the weighting factors for frequency regulation accuracy, control effort minimization, and consensus on normalized active power sharing, respectively.

The optimization problem is convex and can therefore be solved efficiently at each step. The fully distributed design ensures scalability, plug-and-play capability, and resilience against single points of failure. Moreover, the modularity of this architecture provides a natural interface for integration with blockchain-based mechanisms to enhance security and trust in data communication.

4.2. Blockchain-Integrated Framework for Distributed Model Predictive Frequency Control

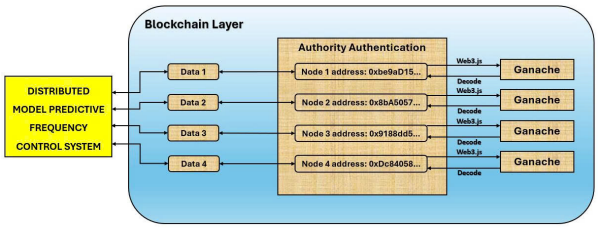

Fig. 2. Diagram of a blockchain-based system

In the proposed architecture, the blockchain layer operates asynchronously and in parallel with the control system. The primary and secondary control algorithms, including FCS-MPC and DMPC, are executed locally within the controllers to maintain frequency regulation and power sharing among DGs. As shown in Fig. 2, the blockchain platform serves as the second layer of the proposed architecture and exchanges data continuously with the DMPC-based secondary controller. At each sampling interval, DGs send their state variables to the blockchain, where the data are encrypted, encoded, validated, and stored as transactions for secure logging and integrity verification. The overall communication workflow consists of four stages:

1) Data acquisition and communication: All DGs establish communication through the network and transmit their local state variables, including frequency and normalized active power, to the blockchain layer. In the proposed implementation, these data are first transmitted from the control system to a blockchain interface through a local communication link. The measured signals are then received by an external module, where they are prepared and converted into transaction data for blockchain interaction. Every piece of exchanged information is recorded and prepared for secure encapsulation.
2) Authentication and address assignment: Each inverter is assigned a unique Ethereum address associated with a corresponding private key. This address is used to authenticate the identity of each distributed generator when submitting transactions to the blockchain network. In the present implementation, data integrity and authenticity are ensured through the inherent cryptographic mechanisms of Ethereum, including transaction signing using private keys and hash-based immutability of recorded data. The transaction hash generated by the blockchain ensures that any modification of the transmitted data during communication would result in a different hash value, allowing the system to detect potential tampering in transit. All measurement and control-related data considered in this study are directly stored on-chain through smart contract functions for simplicity and transparency.
3) Transaction encoding, hashing, and blockchain storage: The collected data are encoded into blockchain transactions using Web3.js and submitted to the Ganache network. Each transaction is validated, assigned a unique hash, and inserted into a block whose hash is cryptographically linked to its predecessor, ensuring data immutability and traceability. A smart contract is deployed to manage the storage and retrieval of operational data. The contract accepts input data including the identifier, corresponding measured variables of each DG and stores them on-chain. The output of this process is the transaction hash, which serves as a reference for data tracking and verification. Access to the smart contract is limited to authorized nodes through their Ethereum addresses, so only valid participants can send data. Each transaction generates a record with its corresponding identifier for tracking. Data storage consumes gas, while data retrieval requires very little cost when executed locally. Possible issues include unauthorized access, invalid data, or insufficient gas, which are handled by the blockchain system.
4) Data retrieval, decoding, and integrity verification: Stored data are retrieved through the smart contract's ABI, decoded, and compared with a reference dataset obtained from the microgrid simulation operating under normal conditions without blockchain integration. In this study, the reference dataset is used only as a benchmark for experimental validation in order to evaluate whether the operational data recorded on the blockchain remain consistent with the expected system behavior. This comparison is not intended to represent the operational workflow of a real power system. In practical deployment, measurement data generated by distributed generators would be transmitted directly to supervisory control systems, while the blockchain layer would mainly serve as an immutable logging and verification mechanism. Any discrepancy between the retrieved data and the reference values immediately indicates potential tampering, thereby ensuring reliable end-to-end integrity.

By integrating this four-step pipeline into the control architecture, the blockchain layer provides transparent, tamper-proof, significantly enhancing cybersecurity within the microgrid.

5. Simulation Setup and Results

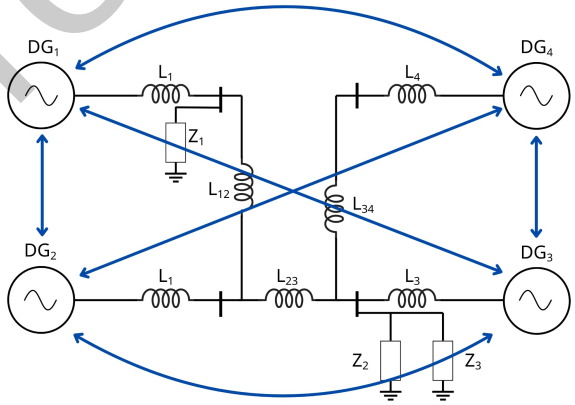

Fig. 3. Microgrid model used for simulation

In the proposed implementation, a microgrid with four-DGs is simulated in MATLAB/Simulink. The overall diagram and communication network among four-DGs are illustrated in Fig. 3. Each DG includes a primary control layer with virtual impedance and the designed FCS-MPC algorithm, along with a secondary control layer whose output serves as input to the droop controller. The measurement signals from the four DG units are transmitted through the network using the "Horizontal Matrix Concatenate" block in Simulink. Furthermore, communication latency among the microgrid inverters is modeled by incorporating the "Unit Delay" block. A full switching inverter model is adopted to ensure simulation accuracy, and the detailed configuration and performance metrics are summarized

in Table 1. The blockchain layer functions as an external data management module that records the operational data generated by the controllers. Consequently, the blockchain operations, including transaction submission and block generation, do not participate in the real-time control loop and therefore do not influence the dynamic control behavior of the microgrid. The software tools and development environment used for the blockchain implementation are listed in Table 2.

Table 1. Configuration Parameters of the Simulation System

Description	Parameter	Value
DC Voltage	V_{DC}	600 (V)
Simulation Sample Time	T_s	$10e^{-6}(s)$
Nominal Frequency	Ω_0	$2\pi \times 50$ (rad/s)
Three-phase Load 1	Z_1	3×5.239 (Ω)
Three-phase Load 2	Z_2	3×5.239 (Ω)
Three-phase Load 3	Z_3	3×5.239 (Ω)

Table 2. Facilities Information for Blockchain implementation

Facility	Version
Node.js	22.14.0
Solidity Smart Contract	0.8.0
Web3.js	1.10.0
Address	.json
Static-nodes	.json
Truffle	5.11.5
Ganache	2.7.1
MATLAB	2023b

In the process of transmitting data from DGs to the blockchain, each DG is assigned a public address to facilitate authentication and subsequent transaction retrieval. Moreover, every piece of data exchanged among the DGs is treated as a transaction, which, once recorded on the blockchain, is permanently stored within a block. The detailed contents of a block are presented in Fig. 4, including the transaction hash (TX Hash), the sender's Ethereum account address, and the contract address of the DG transmitting the transaction. This information is used for encryption and subsequent retrieval of submitted transactions, while also ensuring transaction integrity and mitigating FDIA. In addition, the block records the timestamp of when the transaction was submitted, along with the amount of gas consumed for its execution. Similarly, the transaction information is also recorded. It still contains the information already represented in the storage block, along with the amount of ETH transferred to execute the transaction. Although the displayed ETH value is 0.00, in practice, a small amount of ETH is indeed consumed to complete the transaction. The data sent to the contract is encrypted and represented as TX Data, which ensures that all information is thoroughly protected against potential hacker attacks aimed at data modification.

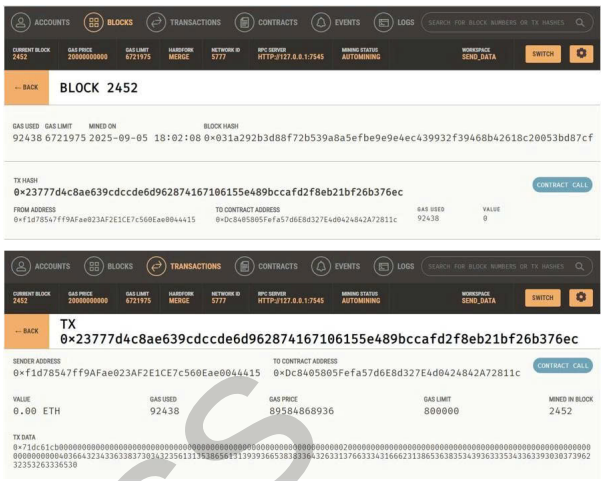

Fig. 4. Block and Transaction Information

The signals transmitted within this blockchain-based system are recorded through the blockchain layer, whose operation relies on a consensus mechanism, as previously described. In total, there are eight output signals: four correspond to the frequencies of the inverters, while the remaining four represent the normalized active power of the DMPC system. These signals are transmitted to the blockchain layer via a local host and Web3.js, where they are recorded on-chain and later retrieved for verification. The retrieved data are subsequently compared with the corresponding data obtained directly from the control system during operation.

As shown in Fig. 5 and Fig. 6, the inverter frequencies exhibit no difference between the cases without blockchain and with blockchain. After the frequencies drop, the DMPC is activated at 0.5s, restoring the frequencies of the four inverters to 50 Hz. Similarly, the normalized active power in both cases is identical, as illustrated in Fig. 7 and Fig. 8, increasing to approximately 0.27 p.u. and then maintaining stability around that value. This indicates that the off-chain control process and the on-chain data recording process remain consistent with each other, while the blockchain layer does not alter the dynamic response of the microgrid. Therefore, the main advantage demonstrated by these figures is that blockchain integration can provide transparent data recording and integrity verification of operational data without degrading the frequency regulation and power-sharing performance of the control system.

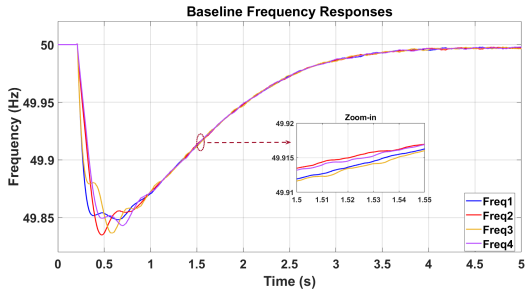

Fig. 5. Frequency Responses without Blockchain

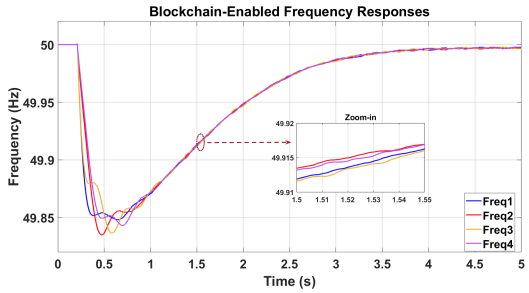

Fig. 6. Frequency Responses with Blockchain Integration

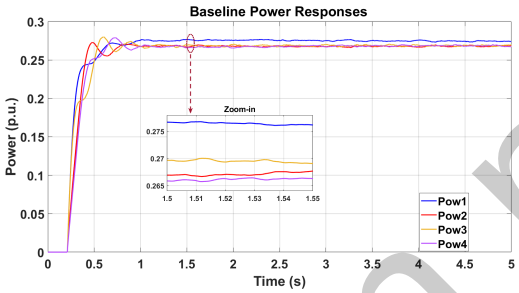

Fig. 7. Power Responses without Blockchain

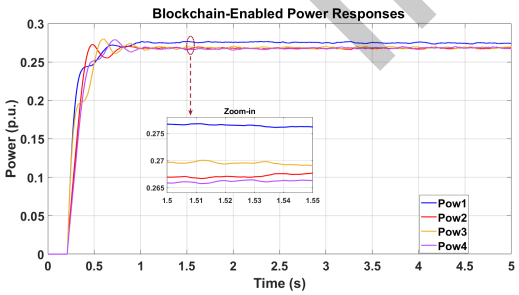

Fig. 8. Power Responses with Blockchain Integration

6. Future Work

The proposed blockchain system has demonstrated stability as well as compatibility with the control system. However, it still exhibits several limitations that need to be addressed in future work. The issue of resource consumption in blockchain remains a major challenge. Although the consensus mechanism significantly reduces resource usage compared to traditional approaches, the demand still becomes substantial under a large volume of transactions. Future research may explore novel consensus mechanisms and hybrid on-chain/off-chain architectures to further mitigate this issue and improve scalability under high data throughput conditions. A detailed timing analysis should also be conducted to evaluate the impact of blockchain-related operations, including data transmission, transaction processing, and block confirmation latency, particularly under realistic network conditions, in order to assess the feasibility of large-scale deployment in practical microgrid systems. Furthermore, certain FDIA should be carried out to demonstrate the high level of security and the ability to maintain system stability when integrating blockchain technology, while Hardware-in-the-Loop (HIL) testing can be incorporated to validate the proposed approach under realistic operating conditions, including communication delays and hardware constraints. Advanced encryption techniques, such as homomorphic encryption, could also be explored to enhance data confidentiality while ensuring that the control performance remains unaffected, together with more comprehensive key management and data protection strategies to improve the practical security level of the system. These research directions will help strengthen the scalability, security, and practical applicability of blockchain-assisted predictive control in modern microgrids.

7. Conclusion

This paper presents a blockchain-integrated DMPC framework that effectively combines predictive control and decentralized data management in microgrids. Simulations on a four-DGs system verify that the two-layer control structure, comprising FCS-MPC for local regulation and DMPC for global coordination, successfully stabilizes frequency and ensures accurate power sharing despite communication delays. The obtained results demonstrate that the proposed control architecture maintains stable operation and coordination among distributed generators under practical communication constraints. The integration of Ethereum blockchain and smart contracts secures all data exchanges, providing transparency and data integrity without affecting control performance. In particular, the blockchain layer enables reliable data recording and verification, ensuring that the information used in the control framework remains consistent and traceable throughout operation. These results confirm blockchain's role as a trust-enabling infrastructure for distributed control in microgrid systems. Future work will focus on evaluating system performance under cyber-attack scenarios and conducting experimental validation under realistic operating conditions, while also addressing scalability and computational challenges through the development of lightweight consensus mechanisms and fault-injection analyses to enhance system resilience and responsiveness.

Acknowledgments

This research is partly funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 31/2025/TN.

References

[1] M. H. Saeed, W. Fangzong, B. A. Kalwar, and S. Iqbal, A review on microgrids' challenges and perspectives, IEEE Access, vol. 9, pp. 166502–166514, Dec. 2021. https://doi.org/10.1109/ACCESS.2021.3135083

[2] N. D. Tuyen, N. S. Quan, V. B. Linh, V. Van Tuyen, and G. Fujita, A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy, IEEE Access, vol. 10, pp. 35846–35875, Mar. 2022. https://doi.org/10.1109/ACCESS.2022.3163551

[3] M. Nour, J. P. Nour, J. P. Chaves-Ávila, and A. Sánchez-Miralles, Review of blockchain potential applications in the electricity sector and challenges for large-scale adoption, IEEE Access, vol. 10, pp. 47383–47432, Apr. 2022. https://doi.org/10.1109/ACCESS.2022.3171227

[4] V. Veerasamy, Z. Hu, H. Qiu, S. Murshid, H. B. Gooi, and H. D. Nguyen, Blockchain-enabled peer-to-peer energy trading and resilient control of microgrids, Applied Energy, vol. 353, pp. 122107, Jan. 2024. https://doi.org/10.1016/j.apenergy.2023.122107

[5] J. Yang, J. Dai, H. B. Gooi, H. D. Nguyen, and P. Wang, Hierarchical blockchain design for distributed control and energy trading within microgrids, IEEE Transactions on Smart Grid, vol. 13, no. 4, pp. 3133–3144, Feb. 2022. https://doi.org/10.1109/TSG.2022.3153693

[6] L. N. Dung, N. S. Quan, H. T. Linh, T. T. Son, G. Fujita, and N. D. Tuyen, Utilizing IOTA distributed ledger platform for security in model predictive frequency control system of microgrid, in Proceedings of the 2024 11th International Conference on Power and Energy Systems Engineering (CPESE), 2024, pp. 91–96.

[7] K. Liu, T. Liu, Z. Tang, and D. J. Hill, Distributed MPC-based frequency control in networked microgrids with voltage constraints, IEEE Transactions on Smart Grid, vol. 10, no. 6, pp. 6343–6354, Mar. 2019. https://doi.org/10.1109/TSG.2019.2902595

[8] G. Lou, W. Gu, W. Sheng, X. Song, and F. Gao, Distributed model predictive secondary voltage control of islanded microgrids with feedback linearization, IEEE Access, vol. 6, pp. 50169–50178, Sep 2018. https://doi.org/10.1109/ACCESS.2018.2869280

[9] Z. Zhao, X. Zhang, and C. Zhong, Model predictive secondary frequency control for islanded microgrid under wind and solar stochastics, Electronics, vol. 12, no. 18, pp. 3972, Sep. 2023. https://doi.org/10.3390/electronics12183972

[10] N. D. Tuyen, N. S. Quan, V. B. Linh, L. N. Dung, and T. M. Khoi, Two-level distributed fully-predictive frequency control scheme for inverter-based AC microgrid considering communication delay, Electric Power Systems Research, vol. 222, pp. 109471, Sep. 2023. https://doi.org/10.1016/j.epsr.2023.109471