IET Smart Grid

Research Article

IET Journals
The Institution of Engineering and Technology

ISSN 1751-8644
doi: 0000000000
www.ietdl.org

Enhancing Power Grid Management and Incident Response Mechanisms Through Consortium Blockchain

Md. Mainul Islam[1], *Rachad Atat*[2], *Muhammad Ismail*[3], *Katherine R. Davis*[1], *Erchin Serpedin*[1]*

[1] *Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843, USA*
[2] *Department of Computer Science and Mathematics, Lebanese American University, Beirut, Lebanon*
[3] *Department of Cybersecurity Education, Research and Outreach Center (CEROC) and Computer Science, Tennessee Tech University, Cookeville, TN 38505, USA*
E-mail: mdmainul11@tamu.edu, rachad.atat@lau.edu.lb, mismail@tntech.edu, katedavis@tamu.edu, eserpedin@tamu.edu
**Corresponding author: eserpedin@tamu.edu*

Abstract: Enhancing the resilience and reliability of power grids is crucial amid rising cyber threats and system complexities. To address these challenges, this paper proposes an energy-efficient, consortium blockchain-based global alarm system for power grid management. Using smart contracts and the proof-of-authority consensus algorithm, the alarm system triggers global alarms upon detecting local anomalies, ensuring a prompt response to partition the power grid and mitigate failures. The effectiveness is validated by simulating the Iberian power system with 15 providers from various regions. Key metrics, such as load shedding, damage reduction, energy consumption, latency, and transaction costs, are used to assess the performance. Simulation results show that the blockchain-based system effectively limits the damage propagation and the load shedding during cascading failures by delaying the onset of instability and maintaining lower damage levels compared to non-blockchain scenarios. Our investigations reveal that the proposed global alarm mechanism reduces the damage and load shedding by up to 29% and 87%, respectively, showcasing its potential for preventing widespread outages.

Keywords: Power grid management, cascading failures, cyber attacks, blockchain, smart contracts, grid partitioning, damage reduction

Acknowledgments

This research was supported by the National Science Foundation under Grants 2220347 and 2220346.

1 Introduction

Modern power grids are critical infrastructures that underpin the functionality of virtually every aspect of contemporary life. Ensuring their reliable operation is paramount, particularly in the face of potential failures and attacks. Recent high-profile power blackouts, such as the Texas blackout in February 2021 [1], have highlighted the devastating economic and social impacts of large-scale cascading failures. These events underline the importance of robust power grid management, reliable operation, and the ability to respond quickly to failures and attacks. [2].

Power grids are complex networks composed of generation, transmission, and distribution systems. The interdependence of these components means that a failure in one part can propagate rapidly, causing widespread disruptions [3]. The growing incorporation of renewable energy sources and the rise of smart grid technologies add further layers of complexity to power grid management. These developments, while beneficial, also introduce new challenges, particularly in terms of maintaining grid stability and reliability amidst variable power inputs and sophisticated cyber threats [4].

Effective power grid management involves several key aspects: monitoring and control, fault detection and isolation, and restoration and recovery [5]. Monitoring and control systems continuously assess the state of the grid, detecting anomalies and ensuring balance between supply and demand [6]. Fault detection and isolation are crucial for identifying and isolating faults to prevent their spread. Finally, restoration and recovery processes aim to restore the power grid's normal operation as quickly as possible. The integration of these functions is essential for maintaining power grid reliability and preventing large-scale blackouts [2, 7].

One crucial aspect of power grid management is the timely detection and response to anomalies, which can prevent localized issues from escalating into widespread outages. Traditional centralized defence systems, where monitoring and response activities are managed by a central authority, are seen as inadequate. These systems face several issues:

- **Single Point of Failure:** Centralized systems create a single point of failure, making the entire power grid's response mechanisms vulnerable if compromised [8].
- **Vulnerability to Cyber-Attacks:** Centralized systems are prime targets for cyber-attacks. A successful attack can disrupt monitoring and response, potentially leading to large-scale outages [9].
- **Latency in Communication:** Delays in data transmission to the central system can result in delayed responses, exacerbating rapidly evolving failure scenarios. Even small delays in response can lead to significant damage to the power system.

A large-scale power grid can comprise numerous system providers, each with its own infrastructure and operational domain. For instance, in the United States, the power grid is segmented into three main regions: the Eastern, the Western, and Texas interconnections. These interconnections consist of multiple utility companies and independent system operators managing the grid within their specific regions. Each provider independently owns and operates its infrastructure, including generation, transmission, and distribution assets. This diverse ownership structure complicates cohesive and reliable power grid management. The core problem is that these providers, each with its own sub-network or power transmission system, require a way to coordinate effectively among themselves. Traditionally, this coordination has depended on a centralized entity that all providers can trust to manage responses during anomalies. This entity alerts providers to disconnect tie lines between sub-networks

to prevent cascading failures. However, reliance on a centralized authority introduces vulnerabilities, as previously mentioned [10].

Blockchain technology offers a solution to the challenges of centralized grid management by removing the need for a single controlling authority while still ensuring secure, coordinated actions across multiple providers through the use of consensus algorithms. Blockchain functions as a tamper-proof distributed ledger that records transactions in an immutable sequence of cryptographically linked blocks, allowing for real-time, verifiable data sharing and automation via smart contracts, which are self-executing programs embedded within the ledger [11]. This decentralized structure strengthens trust and resilience against cyber threats by eliminating single points of failure.

When implementing blockchain technology for power grid management, it is essential to select the appropriate type: public, private, or consortium blockchain. Public blockchains, which permit open access and decision-making participation, are not suitable for power grid management because power system providers need to retain control over their infrastructures. Moreover, public blockchains often employ high-resource consensus algorithms such as proof of work (PoW), which consume significant energy and involve substantial processing time, unsuitable for the rapid responses required in grid management [4]. Although some public blockchains, such as Ethereum, have adopted the proof of stake (PoS) consensus algorithm to reduce energy use, PoS remains inefficient for critical grid applications due to its lower throughput and bias toward wealthy validators with significant stakes.

Conversely, private and consortium blockchains limit access to approved participants and designate specific nodes for transaction validation, resulting in faster consensus and reduced energy consumption. The key difference is that private blockchains are managed by a single entity, while consortium blockchains involve multiple entities in decision-making. Consortium blockchains are particularly effective, as they support coordinated yet independent actions by multiple grid providers, enabling more efficient and secure grid management. Given that the failure response process involves individual providers managing their own buses, a consortium blockchain is the most appropriate option. Through a decentralized global alarm system based on a consortium blockchain, providers can autonomously detect anomalies and execute necessary actions, such as closing tie switches, without depending on a central entity.

In this paper, we aim to limit the spread of failures in interconnected power grids and enhance power grid resilience against cyber attacks by enabling collaboration among providers through a consortium blockchain-based global alarm system. By conducting a comparative analysis, we show that decentralized coordination among power system providers significantly reduces the risk of cascading failures and widespread outages compared to conventional centralized approaches.

2 Related Work

Studies on cascading failures have focused on centralized techniques, with recent research shifting towards blockchain technology for improving power grid security and resilience.

2.1 Centralized Approaches to Cascading Failures

Cai et al. [12] examined the impact of network topology on cascading failures, revealing double-star networks were more resistant to random attacks but less so to intentional ones. Wang et al. [13] developed a detection and isolation framework for false data injection attacks (FDIAs) against smart grids, enhancing accuracy and minimizing false alarms. Shuvro et al. [7] introduced a three-layer model to analyze the interplay among power grids, communication networks, and human operators, emphasizing how failures in these components can exacerbate cascading failures. Tootaghaj et al. [2] proposed a twofold approach using a consistent failure set algorithm and a minimum cost flow assignment for mitigating and recovering from cascading failures.

A dynamic model incorporating communication networks and battery backups was developed by Gharebaghi et al. [3], with a centralized controller used for load shedding and system reliability. Wei et al. [9] highlighted the importance of robust communication infrastructure. Babalola et al. [14] proposed an adaptive multi-agent system for preventing cascading failures without load shedding, using historical economic dispatch data and heuristic strategies. Liu et al. [15] reviewed cascading failure modeling in future power grids, addressing technological impacts and new failure modes. Zhao et al. [16] introduced a "Learning-to-Infer" strategy for real-time outage identification using Monte Carlo simulations and offline training. Atat et al. [17] optimized the joint partitioning of mutually dependent power and communication systems to mitigate large-scale cascading failures, aiming to minimize load shedding while ensuring power flow stability and connectivity. Their investigations revealed that optimal partitioning can significantly reduce the overall damage.

2.2 Blockchain-Based Power System Management

Cybersecurity challenges in multimicrogrid (MMG) systems were addressed by Hu et al. [18] using a collaborative intrusion detection method based on blockchain. Their approach leverages blockchain's consensus and incentive mechanisms to enhance the accuracy and reliability of intrusion detection without relying on a trusted central authority. They introduced an enhanced delegated PoS algorithm to decentralize decision-making, although this algorithm risks centralizing power among the wealthiest nodes, posing security risks such as biased prioritization. Yang et al. [19] proposed a PoA-based distributed control system to secure islanded microgrids against cyber-attacks, such as false data injection, while maintaining control quality. The system uses a private blockchain to secure data transmission between microgrid components. Smart contracts are used to compute and send control feedback to secondary controllers.

Ghiasi et al. [8] focused on enhancing cybersecurity in smart DC microgrids using blockchain technology and the Hilbert Huang transform to detect FDIAs. This approach analyzes voltage and current signals in sensors and controllers, offering a robust FDIA detection mechanism through signal processing and threshold-based identification. A blockchain-enabled community detection framework is used for secure data exchange, providing fine-grained data-sharing services that ensure only authenticated agents access information. Dai et al. [20] proposed a blockchain-enabled framework to enhance cyber-resilience in microgrid distributed secondary control, securing against FDIAs. Using enterprise-level HyperLedger blockchain with smart contracts, the framework supports secure exchanges and computations, providing distributed control and self-healing in a zero-trust environment. It leverages the Practical Byzantine Fault Tolerance (PBFT) consensus for resilience under severe FDIA conditions, although PBFT is more resource-intensive than PoA.

Gao et al. [21] proposed a sovereign blockchain-based approach with smart contracts to enhance the security and transparency of smart grid systems, focusing on data integrity and consumer trust. They aimed to create an immutable ledger for electricity usage data, preventing unauthorized alterations and enforcing agreements between consumers and utilities. However, the paper lacks details on the consensus mechanism used, leaving the energy efficiency of their blockchain approach unclear. Guo et al. [22] introduced BEcontractor, a blockchain-driven electronic contract management system designed for commodity procurement in the electronic power industry. They addressed the inefficiencies of traditional paper-based contracts by leveraging blockchain technology to enhance contract security, traceability, and efficiency. BEcontractor restricts access to selected nodes (power grid enterprises) to ensure contract integrity and privacy, improving management efficiency within the power grid industry.

Liang et al. [23] proposed a distributed blockchain-based framework to strengthen power system defenses against cyber-attacks. By using smart meters as nodes that encapsulate measurements as blocks, the framework enhances grid security, making data manipulation difficult without compromising a majority of nodes. Miners

are selected from pre-specified or random nodes to balance efficiency and security. However, this framework provides probabilistic security and requires substantial storage capacity to accommodate a large amount of meter data on the blockchain, potentially leading to network overhead. Wang et al. [24] presented a secure and auditable private data sharing scheme for smart grids, utilizing a blockchain-based framework to enable trustless data computation and transparent usage tracking. This framework, operating under data processing-as-a-service, employs smart contracts to define specific data usage policies and maintains a transparent ledger for data transactions. The scheme applies contract theory to design optimal data sharing contracts that balance utility and incentives, thereby encouraging participation and enhancing data quality.

Keshk et al. [25] developed a privacy-preserving framework using blockchain and deep learning to secure smart power networks against data privacy threats. The framework features a two-level privacy module integrating an enhanced proof-of-work blockchain for data integrity and a variational autoencoder to encode data, protecting against data poisoning and inference attacks. Nasiri et al. [26] propose a distributed state estimation framework for power systems that integrates blockchain for ensuring data consistency and countering malicious injections. Their trust management strategy allows nodes to assess each other's reliability and effectively detect and isolate anomalous behavior. Ramanan et al. [27] proposed a blockchain-based scheme to detect coordinated replay attacks in large-scale power systems, emphasizing sensor data privacy and employing Bayesian inference for analyzing locally reported attack probabilities. The scheme integrates regional and network-level detection models that trigger global alarms when multiple regional anomalies are detected.

Recent studies [28–31] explored the use of blockchain technology in the energy sector to facilitate peer-to-peer energy trading, improve transaction transparency, and reduce operational costs. These approaches eliminate the need for trusted intermediaries in various scenarios such as vehicle-to-grid networks and microgrids. Abouyoussef et al. [32] introduced a private blockchain-based framework for dynamic charging of electric vehicles (EVs), which supports charging coordination, authentication, and billing. The framework employs a group signature scheme and a distributed random number generation mechanism for protecting the privacy of EV owners when interacting with the charging service provider.

2.3 Research Gap and Our Contribution

One significant drawback of the centralized approaches is their reliance on a single central authority to coordinate responses during anomalies, which can create bottlenecks in the decision-making process. This centralization can lead to delays in response times, especially in critical situations where rapid action is necessary to prevent cascading failures. If the central authority is overwhelmed or compromised, it can slow down the entire coordination process, exacerbating the risk of widespread outages. Moreover, the traditional centralized model complicates collaboration among multiple utility companies and independent system operators, each managing their own infrastructure. This diverse ownership structure makes it challenging to achieve cohesive and reliable power grid management, as each provider may have different operational protocols and priorities. A centralized system is not only inefficient but also susceptible to cyber-attacks, as the central authority could be targeted by malicious actors seeking to disrupt the power grid.

While existing blockchain-based solutions have made progress in improving data security and management within power systems, they primarily focus on detecting cyber attacks. However, as defense mechanisms advance, attackers also adapt their strategies, constantly looking for weaknesses in the systems. The risk of severe damage underscores the need not only for preventing attacks but also for implementing robust mitigation strategies to handle attacks if the systems are compromised. This is especially important when it comes to cascading failures in interconnected power systems, which is a problem that current solutions often do not fully address. Managing the aftermath of attacks, including power grid partitioning and limiting damage propagation, remains a significant gap. Preventing cascading failures is critical because they can quickly lead to widespread blackouts with serious economic consequences. This requires fast and coordinated action across various parts of the systems. While data security is important, it becomes less of a priority when there is an urgent need to stop cascading failures. Unlike data breaches, which usually affect specific parts of a power grid and can be managed locally, cascading failures impact the entire power grid, requiring quick and strategic responses to prevent further damage.

Additionally, blockchain systems based on PoS and PoW are not ideal for the quick responses needed in interconnected power systems. Blockchains that focus on user privacy often add delays and complexity, slowing down the real-time responses needed during a failure. As more users join, scalability issues arise, creating network overhead. In a blockchain-based alarm system, only authorized system providers, acting as consensus nodes, report alarms. Since only the consensus nodes are involved in conducting transactions, user privacy is not a concern; therefore, complex cryptographic mechanisms such as anonymization and randomization are not required. However, strong access controls are still necessary to prevent unauthorized access to alarm data.

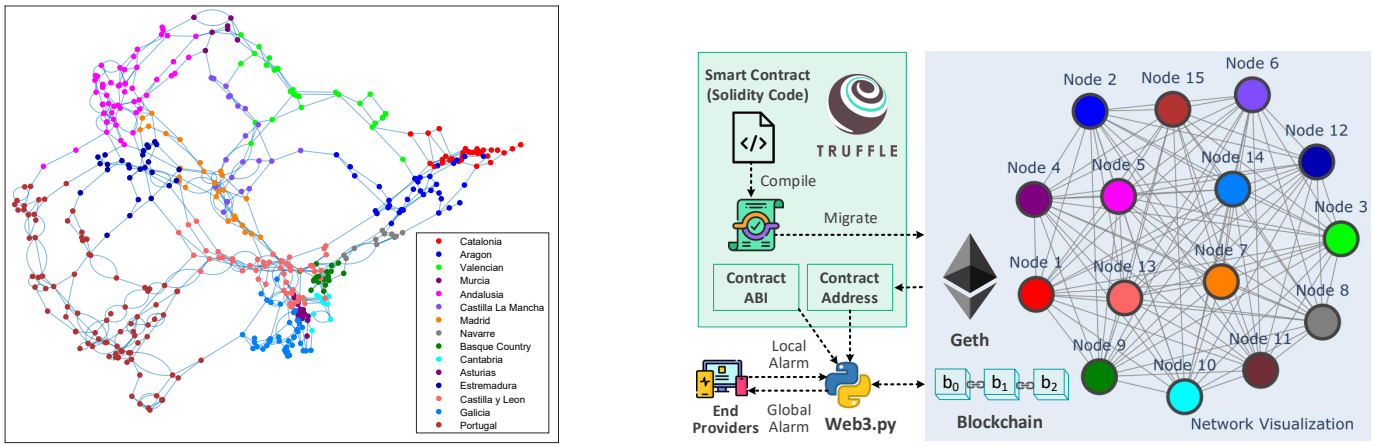
To bridge this gap, we introduce an energy-efficient cooperative global alarm system for interconnected power grids using a consortium blockchain. This system enhances reliability and resilience by enabling collaboration among authorized bus providers and promptly isolating damaged buses from the operational power grids. The contributions of the paper are summarized as follows:

- We propose a consortium blockchain-based global alarm system to mitigate cascading failures in interconnected power grids, where power system providers serve as consensus nodes. Our approach decentralizes failure response management, eliminates single points of failure, and enhances resilience against cyber-attacks. The consortium network provides a common platform for sharing information among independent system operators managing the power grid within their respective regions.
- We implement local alarm units to monitor critical parameters and securely transmit anomalies to the blockchain network using a smart contract. Upon receiving a predefined number of local alarms, determined through extensive simulations, the smart contract automatically triggers a global alarm so that the system providers can isolate failures by power grid partitioning and prevent damage propagation across buses.
- We adopt the PoA consensus algorithm for rapid alarm triggering, ensuring fast transaction processing, low latency, high scalability, and low energy consumption, making it suitable for large-scale power grids.
- We validate the effectiveness of the proposed alarm system through simulations, demonstrating that decentralized failure response management reduces damage and load shedding by up to 29% and 87%, respectively, compared to conventional centralized management. Our simulations also reveal that the decentralized approach slows damage progression and maintains power grid stability over time, thereby reducing the risk of widespread outages.

3 Proposed Global Alarm System

The proposed global alarm system is designed to enhance the resilience and security of interconnected power grids through a robust, decentralized framework. As depicted in Fig. 1a,b, the overall system architecture comprises: (a) *local alarm units*, (b) *a consortium blockchain network*, and (c) *a smart contract*. This setup ensures that alerts generated by local alarm units are securely transmitted and recorded on the blockchain, where the smart contract validates and aggregates these alarms to issue global alarms if necessary.

The system uses the Iberian Peninsula's power grid because we have access to a comprehensive dataset for this power grid. The dataset allows to thoroughly test and validate our approach under realistic conditions. However, the design of our consortium blockchain network and smart contract is not limited to this specific



(a) The Iberian transmission system topology.

(b) Consortium blockchain network.

Fig. 1: Overall architecture of the proposed power grid management system.

power grid configuration. They are flexible architectures that may be applied to other power grids with different structures. While this study utilizes the Iberian power system as a proof of concept, the system can be implemented with other power system cases, provided that sufficient attack data or relevant operational data are available for testing.

The components of the system are separately described next.

3.1 Local Alarm Units

Local alarm units are strategically deployed alongside each power provider to continuously monitor critical parameters such as voltage levels and abnormal power flows. These units are equipped with advanced anomaly detection algorithms that can identify irregularities indicative of potential power grid failures. Upon detecting an anomaly, the local alarm units generate alerts, which are then securely transmitted to the blockchain network. Each alert is time-stamped and includes detailed information about the anomaly, such as the real and apparent power, damaged bus number, bus region, and provider ID.

Fig. 1a depicts the complex topology of the Iberian transmission system, which interconnects Spain and Portugal. Nodes in the graph represent different buses, and edges represent the transmission lines connecting them. Each region within the grid is color-coded to show the distinct areas managed by different providers. This visual representation helps understanding how local alarm units are distributed and how they interact within their regions to detect and respond to anomalies.

Fig. 2 maps the geographical locations of the Iberian power grid regions based on GPS coordinates. Each dot represents a bus within the power grid, and the color coding corresponds to the different regions (Catalonia, Aragon, Andalusia, etc.). This geographical mapping provides a spatial understanding of the power grid's layout, highlighting the regional distribution and the extensive coverage of the local alarm units across the grid.

3.2 Consortium Blockchain Network

The proposed system operates on a permissioned Ethereum blockchain called Go Ethereum (Geth), providing a reliable platform for decentralized operations [33]. The choice of blockchain technology and its configuration play a crucial role in the system. Ethereum was selected due to its robust smart contract capabilities and the extensive support available within the developer community. The implementation of a permissioned network ensures that only authorized participants can engage with the system, thereby maintaining a high level of security and control over the network's operations.

The blockchain network is managed by several consensus nodes, each representing a provider. Alarm data are stored in sequential blocks, creating a tamper-proof and transparent historical record.

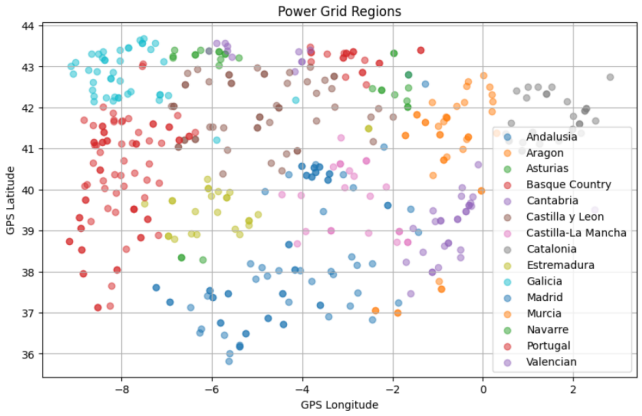


Fig. 2: GPS locations of the Iberian transmission system.

This record can be audited and analyzed to enhance future power grid management practices. Each provider maintains a copy of the blockchain, and there is no central data server. The network uses the Clique consensus algorithm [34], a form of PoA, to ensure data consistency across all local ledgers, making them identical. Clique is chosen for its energy efficiency and scalability. This algorithm is particularly suited for consortium networks as it requires lower computational resources compared to PoW, and it enables faster block validation [19, 27].

Our Geth implementation uses Truffle [35], a development environment, to compile the smart contract source code written in Solidity, migrate the contract ABI (application Binary Interface) to the network, and deploy the contract into the blockchain. Upon deployment, the blockchain provides a unique address, essential for invoking the functions within the contract. Web3.py [36], a Python library for interacting with Ethereum, facilitates interaction with the blockchain using the contract address and ABI. This process ensures seamless integration of the smart contract with the blockchain network, enabling efficient communication between the local alarm units and the smart contract. Fig. 1b illustrates this process.

Security and privacy are paramount in the design of the global alarm system. All communications among providers are encrypted using TLS [37] to prevent man-in-the-middle attacks, ensuring data confidentiality. The Elliptic Curve Digital Signature Algorithm (ECDSA) [38] is utilized in the smart contract to ensure the integrity and authenticity of alarm data. The access control mechanism is built around signature-based authentication, where providers must sign transactions with their private keys and the signatures must be verified with their public keys [39]. This ensures that only authorized providers can register or submit alarms, preventing unauthorized actions.

IET Smart Grid, pp. 1–10

3.3 Smart Contract

Central to the system is a smart contract, which is responsible for managing the alarm data received from the local units. This self-executing contract validates the authenticity of each alarm using cryptographic signatures and aggregates alarms from different power system providers.

The smart contract implementation for the proposed global alarm system is developed in Solidity and deployed on the Geth blockchain. The primary components of the smart contract include the registration of power grid providers, reporting of local alarms, and the issuance of global alarms based on a threshold mechanism.

Algorithm 1 is a key component of the contract, responsible for aggregating local alarms and issuing global alarms. The process begins with the detection of anomalies by local alarm units. Upon detecting anomalies, providers submit alarm transactions to the network. Each transaction T includes essential details, such as the damaged bus number b_d, bus region r, type of the alarm a_t (local or global), and a timestamp t. Once the local alarm transaction is submitted to the blockchain network, the smart contract takes over. It validates the authenticity of the alarm by ensuring that the sender's Ethereum address $\mathcal{P}$ belongs to a registered provider in the network and verifying that the cryptographic signature $\mathcal{S}$ generated by the sender matches $\mathcal{P}$. This validation ensures that only legitimate alarms are considered. Once the number of local alarms reaches a predefined threshold k, such as receiving local alarms from k different providers in a cycle, the smart contract issues a global alarm. The value of k is adjustable and it is set by the network based on the local alarm throughput and the cost of global alarm issuance.

The smart contract includes the following main features:

• **Provider Registration**: Providers must register on the blockchain network by submitting their region details and a valid cryptographic signature for authentication. The `registerProvider` function handles this process by verifying the signature and storing the provider's details (region and registration timestamp). This ensures that only authorized providers can participate in the system, enhancing security and trust.
• **Alarm Reporting**: The `reportAlarm` function allows registered providers to submit alarms when an anomaly is detected in the grid. Each alarm includes details such as real power (P), reactive power (Q), the region, and a timestamp. The contract verifies the authenticity of the alarm using signature validation before storing it on the blockchain. Each alarm is logged and associated with the reporting provider and region.
• **Global Alarm Issuance**: The smart contract aggregates the local alarms from different providers. Once the number of local alarms reaches a predefined threshold k (e.g., receiving alarms from k different providers in a cycle), a `issueGlobalAlarm` function is triggered, and a global alarm is issued. This threshold is adjustable and set by the network, based on local alarm throughput and the cost of global alarm issuance. The issuance of a global alarm prompts neighboring providers to take predefined response actions, such as isolating their grid segments to contain the impact of the detected failure or attack. This coordinated response helps to minimize disruption and maintain grid stability.
• **Security and Verification**: The smart contract employs ECDSA [38] for signature verification, ensuring data integrity and authentication. The functions `getEthSignedMessageHash`, `splitSignature`, and `verifySignature` collectively handle the validation of provider-submitted transactions, preventing unauthorized actions and maintaining the reliability of reported data.
• **Data Storage and Retrieval**: The smart contract maintains a transparent and tamper-proof record of alarms, accessible via functions such as `getAlarmDetails`, `getAlarmsByRegion`, `getAlarmsByProvider`, and `getGlobalAlarms`. This enables easy auditing and analysis to improve future response strategies.

The implementation of the smart contract in this system brings several key advantages. The use of a consortium blockchain facilitates decentralized coordination, allowing multiple power grid providers to actively participate without relying on a central authority. This setup eliminates single points of failure and enhances the resilience of the overall system. Additionally, the signature-based authentication mechanism ensures efficient verification of alarm submissions, maintaining data authenticity and preventing tampering. This security measure upholds the integrity of reported data and restricts unauthorized actions. Moreover, the system's scalability is supported by the use of the Clique consensus algorithm, which enables rapid and energy-efficient block validation. This feature makes the solution suitable for managing large-scale power grids effectively, ensuring prompt responses and maintaining grid stability.

Algorithm 1 Reporting Local Alarms and Issuing Global Alarms

Network parameter: Number of local alarms threshold k
Input: Local alarm $T = [b_d, r, a_t, t]$, transaction signature $\mathcal{S}$
Output: Local alarm status, global alarm issuance
Define provider list of past local alarms: $l = []$
Recover provider's address: $\mathcal{P} = \text{ecrecover}(hash(T), \mathcal{S})$
if $\mathcal{P}$ is registered and $\mathcal{S}$ is verified **then**
  Store T in the blockchain
  if $\mathcal{P} \notin L$ **then**
    Append T into the provider list: $l.append(\mathcal{P})$
    if $length(l) \geq k$ **then**
      Issue a global alarm
      Nullify l for the next cycle: $del\ l$
      return (Accepted, Issued)
    end if
  end if
  return (Accepted, Wait)
end if

3.4 Clique Consensus Algorithm

Clique is a PoA consensus algorithm implemented in Geth that operates in permissioned network environments where participant nodes are known and trusted [33]. This algorithm is designed to prioritize network efficiency, eliminating the need for energy-intensive computations. It relies on the identity of pre-approved participants to propose and validate blocks, creating a more streamlined and efficient consensus mechanism.

Fig. 3a,b provide a visual representation of the Clique consensus process, detailing the block proposal, validation, and chain selection workflow among the network's authorities. The figure is divided into two panels, which illustrate key aspects of the algorithm's operation.

• **Authority Rotation:** The authorities labeled A_0 to A_7 in Fig. 3a represent the signers, which are trusted nodes authorized to propose and validate blocks. These nodes participate in a round-robin rotation for block proposal rights, ensuring that all signers share the responsibility of block creation. The dashed lines between nodes (e.g., from A_1 to A_2) indicate the transition of proposal rights, showing that A_1 has finished its turn and A_2 is now responsible for proposing the next block. This structured rotation prevents any single node from monopolizing block proposals and maintains a fair distribution of responsibilities.

Clique operates by rotating block proposal rights among the signers, with a defined set of signers established in the genesis block configuration. At each step, $N/2 - 1$ signers among N total signers can propose blocks. Therefore, a signer takes its turn after every $N/2 + 1$ steps. When a signer proposes a block during its turn (in-turn), that block has a higher likelihood of being accepted by the network. Out-of-turn proposals, which occur when a signer steps in to propose a block outside of its designated turn (e.g., due to a scheduled signer's unavailability), are permitted but are given a lower priority.
• **Block Proposal, Commit, and Chain Selection:** Fig. 3b illustrates the process of broadcasting block proposals and the subsequent validation and commitment by other signers. The arrows

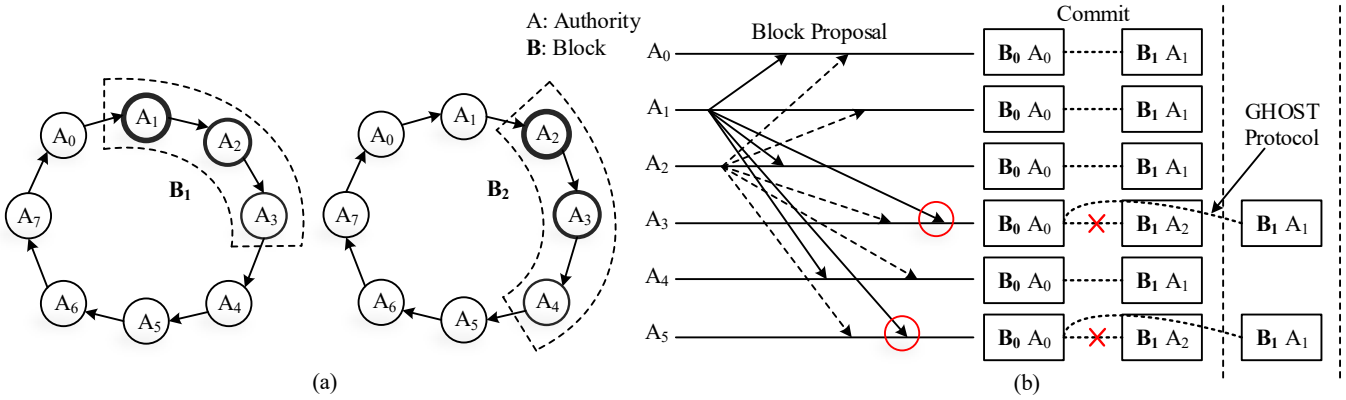


Fig. 3: Clique consensus algorithm [40].

originating from a single node (e.g., A_0 proposing block B_0) represent the dissemination of the block proposal to other signers for validation. Each signer independently verifies the block, ensuring that the proposer's identity is legitimate, the block's timestamp is valid, and the transactions are accurate. Once the block passes validation, it is appended to the local blockchain, depicted in the stacked blocks under each authority node (e.g., B_0 under A_0 and B_1 under A_1). This visual indicates that the nodes have agreed on the block and committed it to their copies of the blockchain.

Clique uses difficulty values to differentiate between in-turn and out-of-turn blocks. In-turn blocks have a difficulty of `2`, while out-of-turn blocks have a difficulty of `1`. This mechanism helps the network prioritize in-turn proposals and maintain orderly consensus. Forks in the network are resolved using a simplified version of the Greedy Heaviest Observed Subtree (GHOST) protocol [41]. The GHOST protocol assists the network in determining the canonical chain by selecting the one with the highest total cumulative difficulty [34]. This is illustrated with crossed-out blocks, such as B_0 under A_2, which signify rejected branches. This approach ensures that the network eventually converges on a single version of the chain, even when temporary forks appear. Clique also allows for chain reorganization up to a depth of 7 blocks, enabling the network to manage delays and synchronization issues effectively.

Security Features: Clique has built-in security measures to enhance its resilience:

- **Checkpoint Blocks**: These are inserted periodically to solidify the blockchain's history and prevent modification beyond these checkpoints. This feature ensures that past transactions remain immutable and tamper-proof.
- **Protection Against Eclipse Attacks**: The rotation of block proposal rights among a known set of signers reduces the risk of eclipse attacks, in which an attacker attempts to isolate and dominate the block production of certain nodes.
- **Fault Tolerance**: Fault tolerance is ensured by a supermajority $(2/3)$ of signers operating honestly.

Efficiency and Performance: Clique is optimized for efficiency by reducing computational demands and allowing rapid block propagation and verification. This makes it especially suitable for private or test networks where transaction throughput and low latency are key requirements.

4 Simulation Models

To highlight the significance of blockchain in minimizing cascading failures, the damage impact is simulated with and without blockchain integration.

Algorithm 2 simulates the propagation of cascading failures without blockchain integration. The process begins by loading power flow data collected at 15-minute intervals from the Iberian transmission system, covering a 13-hour period. The simulations leverage a comprehensive dataset that includes both normal and abnormal power flows. Arrays are initialized to track cumulative damage over multiple time steps. At each time step, the algorithm identifies attacked buses b_d with abnormal power levels and evaluates their damage impact. To quantify the damage on the affected buses, several key metrics are calculated, contributing to an overall damage score.

4.1 Damage Assessment

Firstly, *Load Shedding* (L) refers to the fraction of electrical load that needs to be shed or is lost due to cascading failures in the power grid. It quantifies the total apparent power following a node failure and is computed as follows [17]:

$$L = 1 - \frac{\sum_{i=1}^{N} (P'^2_{D_i} + Q'^2_{D_i})^{1/2}}{\sum_{i=1}^{N} (P^2_{D_i} + Q^2_{D_i})^{1/2}}, \tag{1}$$

where P'_{D_i} and Q'_{D_i} indicate the active and reactive power loads that remain connected following the failure of node i, and P_{D_i} and Q_{D_i} represent the active and reactive power loads prior to the node failure, respectively.

Next, the *Effective Graph Resistance* (R_G) that quantifies the overall cost of transferring power flow between two nodes is measured. A lower effective graph resistance indicates a more robust power grid against failures. R_G is calculated as follows [17]:

$$R_G = \sum_{i=1}^{N} \sum_{j=i+1}^{N} R_{ij}, \tag{2}$$

where R_{ij} denotes the impedance between nodes i and j. It is derived from the inverse of the non-singular admittance matrix Y_{bus} of the power grid:

$$R_{ij} = \left| Y_{\text{bus}}^{-1} \right|_{ij}. \tag{3}$$

The electrical degree centrality indicates the number of power flows that directly influence the status of node i. It is expressed as $\text{CD}_i^{\text{elec}} = \sum_{i \sim j} P_{ij}/(N-1)$, where $i \sim j$ means that node i is connected to node j and P_{ij} is the maximum electrical power flowing between nodes i and j.

Additionally, the *Connectivity Impact* (CI) is calculated, which indicates the proportion of nodes that remain operational after a node failure [17]:

$$\text{CI} = 1 - \frac{N'}{N}, \tag{4}$$

where N' is the number of nodes that remain connected after the failure.

Algorithm 2 Cascading Failure Propagation Without Blockchain

Input: caseIberian power flow data, attacked buses
Output: Damage impact
Load power flow case: mpc = loadcase('caseIberian')
Set simulation time steps τ
Initialize damage: $D = zeros(1:\tau)$
Initialize previous damaged buses: $b'_d = []$
for $t = 1$ **to** τ **do**
    Check for damaged buses: $b_d = get\_attacked\_buses(t)$
    Aggregate all damaged buses for cumulative operation: $b_d = b_d + b'_d$
    Measure damage $D(t)$ by passing (b_d, mpc) into (9)
    Update previous attacked buses: $b'_d = b_d$
end for
return D

Algorithm 3 Cascading Failures Propagation with Blockchain

Input: caseIberian power flow data, providers' bus lists $\forall b$
Output: Damage impact
Load power flow case: mpc = loadcase('caseIberian')
Let G be the graph representation of the power system
Set simulation time steps τ
for $t = 1$ **to** τ **do**
    Initialize vector: $D = zeros(1:\tau)$
    Find the indices of attacked buses from $\forall b$
    for $i = 1$ **to** 15 **do**
        Identify damaged buses b_d belong to provider i
        Report local alarms using **Algorithm 1**
        if A global alarm is notified **then**
            Make partition $\mathcal{C}_p$ to isolate b_d from the power system
        end if
        Measure damage score D_i for provider i using Eq. (5)
    end for
    Aggregate individual damage values for the current time step: $D(t) = \sum_{i=1}^{15} D_i * length(\forall b(i))/size(G)$
end for
return D

Finally, after normalizing the metrics using a min-max scaler, we compute the overall damage score, denoted as D, using the following weighted expression:

$$D = w_1 \cdot \mathrm{L} + w_2 \cdot \mathrm{R_G} + w_3 \cdot \mathrm{CD^{elec}} + w_4 \cdot \mathrm{CI}, \qquad (5)$$

where w_1, w_2, w_3, and w_4 are weights assigned to each metric. The weights assigned to each term reflect their relative importance in determining the overall damage from cascading failures. For simplicity, we assume $w_1 = w_2 = w_3 = 1/6$ (electrical) and $w_4 = 1/2$ (topological).

In the case when the nodes fail completely, we use Eq. (5) for damage assessment. In the case when nodes are only electrically affected by the attack, i.e., they are not isolated from the rest of the network, we compute damage by setting $w_1 = w_2 = w_3 = 1/3$ and CI to 0.

The results are stored, and the list of previously attacked buses is updated. If no new attacks occur, the damage values from the previous time step are carried forward. This process ensures that the cumulative impact of attacks is tracked over time, providing a clear picture of how damage propagates in the absence of a blockchain-based coordination system.

Algorithm 3 simulates cascading failure propagation in the Iberian power grid with blockchain integration, aiming to provide a more granular and coordinated response to anomalies. Initially, power flow data from the *caseIberian* is loaded, and power flow analysis is performed.

The simulation runs over a set number of time steps τ. For each time step t, the algorithm initializes a vector D for damage assessment. For each provider, the algorithm identifies the damaged buses belonging to them, and local alarms are reported using Algorithm 1. Upon notifying a global alarm, the transmission system is divided into 15 partitions by creating subgraphs based on predefined bus numbers and switching off the transmission lines that connect the affected provider's power system to the others. Each partition represents a different provider's area. This strategy prevents the damage from propagating across bridges or tie lines, keeping the cascading failure contained within the affected partition instead of spreading globally. The algorithm computes the damage score for each provider.

The cumulative damage impact for the current time step is computed by accumulating the individual damage values from all providers, considering the case partition scenarios. The process repeats for each time step, resulting in comprehensive arrays of cumulative damage over the simulation period, which is then returned as the final output. This approach provides a detailed, partitioned view of how damage propagates in the power grid under attacked conditions.

5 Results and Discussion

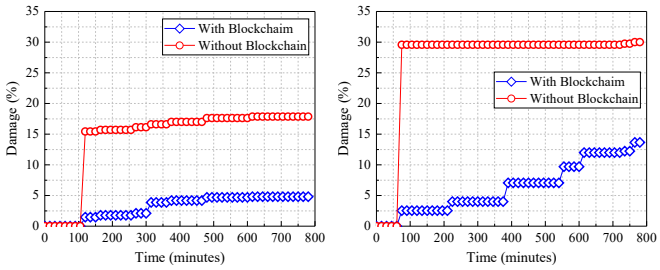
The proposed system was implemented on a laptop (CPU: AMD Ryzen 7 4700U @ 2.0 GHz, RAM: 16 GB), and MATLAB R2022a was used to simulate the MATPOWER case of Iberian power system. This specific case was chosen due to the availability of a detailed dataset for this power system, allowing us to thoroughly test our approach. However, our proposed algorithms and smart contract are not limited to this specific case. The method is designed to be reproducible and flexible, and it can be applied to other MATPOWER cases, provided that sufficient attack data or relevant event data are available for those cases.

Fig. 4a,b illustrate the damage progression in the worst-case scenario where attacked nodes fail completely and become isolated from the power grid. We compare single and multiple providers with and without blockchain. For a single provider, the damage rapidly surpasses 15% without blockchain but stays under 5% with blockchain. For fifteen providers, the damage rises to 30% without blockchain, while blockchain limits it to below 15%. This comparison highlights how blockchain's decentralized coordination mitigates rapid damage escalation by enabling providers to isolate affected nodes promptly, effectively containing damage within specific partitions.

The extensive damage in scenarios involving multiple providers results from cascading failures, where an initial fault triggers subsequent failures in interconnected buses. Each provider typically operates within its own partition or subsystem. Without blockchain-enabled collaborative partitioning, centralized systems struggle to counter sustained attacks effectively, leading to a rapid escalation of damage. Blockchain allows for a controlled, stepwise progression of damage by facilitating decentralized decision-making, which is particularly valuable in multi-provider scenarios where communication and coordination are critical for containment.

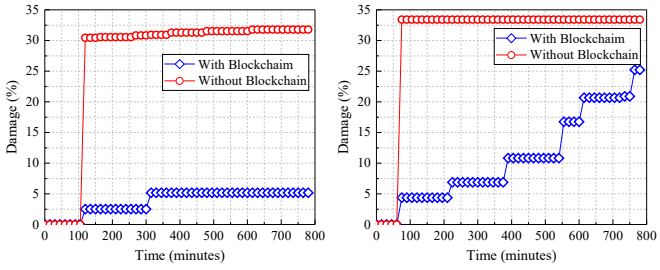
Conversely, with blockchain, the damage increases gradually with each new attack, allowing the system to endure more attacks within the same timeframe. This controlled escalation gives providers more time to isolate affected buses before the power system becomes unstable, helping to contain damage within the affected partition and prevent it from spreading globally. Thus, blockchain's decentralized coordination among providers helps to effectively mitigate cascading failures. This aspect is especially important for real-time grid management, as it enables providers to act promptly on localized faults, preventing them from impacting the broader network.

Fig. 5a,b present the electrical damage progression for the case when buses are electrically damaged but are still operating in the power grid. With one provider, the damage escalates to 31% without blockchain but stabilizes at 5% with blockchain. For fifteen



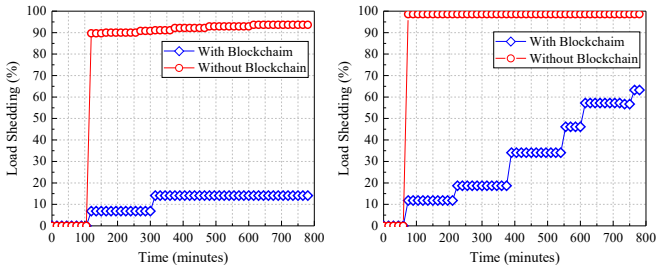
(a) Single provider (b) 15 providers

Fig. 4: Damage over time with and without blockchain for single and multiple providers with fully damaged nodes.



(a) Single provider (b) 15 providers

Fig. 5: Damage over time with and without blockchain for single and multiple providers with partially damaged nodes.

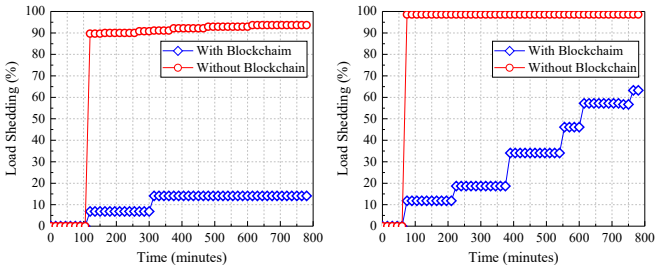


(a) Single provider (b) 15 providers

Fig. 6: Load shedding over time with and without blockchain for single and multiple providers with fully damaged nodes.

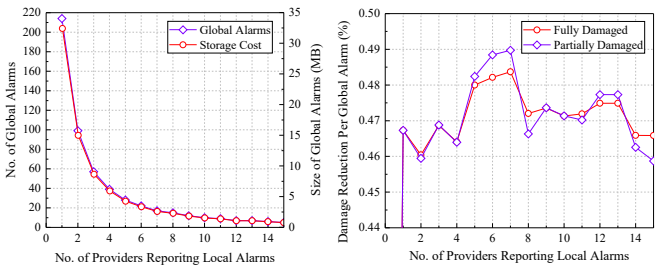
providers, the damage reaches 33% without blockchain but remains at 25% with blockchain after 13 hours. These figures collectively highlight the effectiveness of blockchain in limiting damage propagation under different conditions and enhancing the resilience of the power grid. They demonstrate that blockchain not only delays the onset of instability by partitioning but also maintains a lower overall damage level compared to the non-blockchain scenario, showing blockchain's effectiveness in real-time damage control.

Fig. 6a,b and Fig. 7a,b illustrate load shedding progression for the topologically damaged (worst case) and electrically damaged scenarios, respectively, comparing single and multiple providers with and without blockchain. In both figures, load shedding reaches 90% and 100% rapidly without blockchain for a single and fifteen providers, respectively. However, with blockchain, load shedding increases more gradually and stabilizes around 15% for a single provider and reaches 65% after 13 hours for fifteen providers. These results demonstrate blockchain's effectiveness in mitigating load shedding. Blockchain's integration distributes response efforts, leading to a more controlled and gradual increase in load shedding compared to the rapid escalation observed without blockchain. This controlled load shedding progression illustrates blockchain's role in balancing grid stability, as it prevents abrupt losses that could destabilize the network.



(a) Single provider (b) 15 providers

Fig. 7: Load shedding over time with and without blockchain for single and multiple providers with partially damaged nodes.



(a) Global alarms and storage cost for variable k (b) Damage reduction per global alarm for variable k

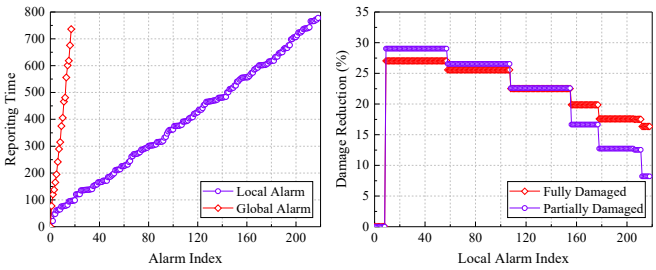
Fig. 8: Effect of varying the number of providers reporting local alarms k.

Fig. 8a,b illustrate the sensitivity of the threshold k in the smart contract. To issue each global alarm, local alarms must be received from k different providers. Fig. 8a shows that as the number of providers reporting local alarms k increases from 1 to 15, the number of global alarms decreases from 218, and storage cost for the global alarms correspondingly drops from 32.4 MB to 0.8 MB, with each global alarm occupying 155 bytes of memory. The reductions occur because the smart contract automatically issues a global alarm only when local alarms are received from k different providers. This efficient aggregation of local alarms minimizes unnecessary global alarms, saving memory. However, a larger k value means global alarms are triggered less frequently, potentially delaying responses to some incidents.

Issuing global alarms more frequently results in greater damage reduction but also leads to higher costs. To find the optimal threshold, we measure damage reduction per global alarm by varying the value of k. As shown in Fig. 8b, damage reduction per global alarm initially fluctuates with increasing k, then rises sharply when k exceeds 4, peaking at $k = 7$. This indicates that the smart contract is most effective at issuing global alarms when $k = 7$ in this system. Optimizing k is essential for balancing between response time and resource efficiency, as higher k values lead to fewer global alarms but risk slower responses.

Fig. 9a,b demonstrate the alarm timing and damage reduction at the optimal threshold setting (i.e., $k = 7$) for 15 providers. As shown in Fig. 9a, local alarms are reported consistently, while global alarms are less frequent due to aggregation from 7 different providers. This aggregation delays global alarms compared to local ones but ensures more accurate and meaningful alerts, reducing the likelihood of false alarms and making each global alert more actionable.

Fig. 9b illustrates the damage reduction percentages achieved through the implementation of local and global alarm mechanisms. The graph demonstrates that the proposed system effectively reduces damage, with initial reductions up to 27% for the worst-case scenario and up to 29% for the electrically damaged buses scenario. However, as the local alarm index increases over time, the damage reduction decreases. This decrease occurs because, without blockchain, the damage quickly saturates at a high level, whereas with blockchain,



(a) Global and local alarm timing. (b) Damage reduction.

Fig. 9: Alarm timing and damage reduction at the optimum threshold setting ($k = 7$) for 15 providers.

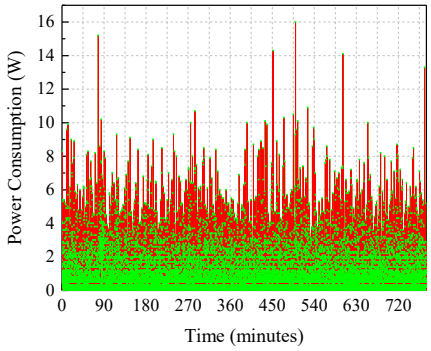


Fig. 10: Power consumption over time.

the damage saturates more slowly and at a lower level, reflecting blockchain's capacity to sustain damage mitigation over extended periods.

Fig. 10 shows the power consumption over a 720-minute period, with notable spikes occurring at various intervals. These spikes indicate the moments when alarms were generated, transmitted, verified, and stored. The processing of alarms likely requires additional computational resources, leading to these temporary increases in power consumption. The maximum and average power consumption by the blockchain network were 16 and 1.38 W, respectively. The observed power consumption is manageable in light of the resilience improvements gained, affirming that blockchain's energy overhead is justifiable given its contributions to grid stability.

Table 1 Blockchain implementation summary.

Parameter	Value
Block time	5 s
Contract deployment cost	2.5M gas units
Transaction cost per local alarm	243 gas units
Local alarm size	458 bytes
Latency per local alarm	52 ms
Global alarm size	155 bytes
Transaction throughput	20
Total simulation time	13 hours
Total energy consumptions	64584 J or 17.94 Wh

Table 1 summarizes key metrics for the blockchain implementation in the global alarm system for power grid management. The block time was 5 seconds. The transaction cost and size per local alarm were 243 gas units and 464 bytes, respectively. The average latency to report a local alarm was 52 ms. The system is capable of processing 20 transactions per second. The total simulation time was 13 hours, with a total energy consumption of 64584 J (17.94 Wh). These results confirm the feasibility of blockchain-based power grid management even for real-time applications, as the system supports high throughput and maintains low latency.

6 Limitations and Scopes

While the current blockchain-based system demonstrates strong capabilities in reducing damage and mitigating load shedding, it operates in a reactive manner by responding to failures after they occur. The consensus algorithm introduces a minimum block time delay (5 seconds in this case), meaning that the response to failures is not instantaneous. During this delay, additional damage can accumulate, especially in cases of fast-spreading faults.

To address this, future enhancements could incorporate more proactive approaches. Leveraging advanced deep learning models could help reduce the time it takes to respond to failures and improve system resilience. Further research could focus on developing predictive and adaptive algorithms that seamlessly integrate with blockchain technology, balancing reactive and proactive measures to enhance grid stability and minimize disruptions.

7 Conclusions

This study presented a blockchain-based approach to enhance resilience in power grid management. Utilizing the Go-Ethereum platform with the Clique consensus algorithm and smart contracts, the proposed system enables secure, decentralized alarm aggregation and dissemination, eliminating single points of failure and reducing cyber-attack vulnerabilities.

The results demonstrate that this system can significantly limit damage, achieving up to a 27% reduction in high-impact scenarios and 29% in moderate cases. By enabling coordinated, decentralized responses, the system helps prevent cascading failures and manages load shedding more effectively. This approach is particularly valuable for real-time interconnected power system management, where rapid, reliable, and collaborative action among providers is essential to maintaining grid stability under stress.

Future research will focus on enhancing this framework with predictive capabilities, using machine learning to identify and isolate vulnerabilities proactively. This addition aims to reduce response delays further, supporting a proactive and resilient power system management approach that can adapt to potential threats while avoiding unnecessary disruptions.

Conflict of Interest

The authors declare that they have no conflict of interest.

Data Availability Statement

The data that support the findings of this study are available from the authors upon reasonable request.

Author Contributions

Md. Mainul Islam: Data curation, Formal analysis, Methodology, Software, Visualization, Writing - original draft.

Rachad Atat: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Supervision, Validation, Writing - review & editing.

Muhammad Ismail: Investigation, Writing - review & editing.

Katherine Davis: Funding acquisition, Project administration.

Erchin Serpedin (Corresponding Author): Funding acquisition, Investigation, Project administration, Resources, Supervision.

8 References

1 Busby, J.W., Baker, K., Bazilian, M.D., Gilbert, A.Q., Grubert, E., Rai, V., et al.: 'Cascading risks: Understanding the 2021 winter blackout in Texas', *Energy Res*

Soc Sci, 2021, **77**, (102106), pp. 102106.
2 Tootaghaj, D.Z., Bartolini, N., Khamfroush, H., He, T., Chaudhuri, N.R., Porta, T.L.: 'Mitigation and recovery from cascading failures in interdependent networks under uncertainty', *IEEE Trans Control Netw Syst*, 2019, **6**, (2), pp. 501–514.
3 Gharebaghi, S., Chaudhuri, N.R., He, T., Porta, T.F.L.: 'Dynamic modeling and mitigation of cascading failures in power grids with interdependent cyber and physical layers', *IEEE Trans Smart Grid*, 2024, **15**, (3), pp. 3235–3247.
4 Zhuang, P., Zamir, T., Liang, H.: 'Blockchain for cybersecurity in smart grid: A comprehensive survey', *IEEE Trans Industr Inform*, 2021, **17**, (1), pp. 3–19.
5 Aklilu, Y.T., Ding, J.: 'Survey on blockchain for smart grid management, control, and operation', *Energies*, 2021, **15**, (1), pp. 193.
6 Srivastava, I., Bhat, S., Vardhan, B.V.S., Bokde, N.D.: 'Fault detection, isolation and service restoration in modern power distribution systems: A review', *Energies*, 2022, **15**, (19), pp. 7264.
7 Shuvro, R.A., Wangt, Z., Das, P., Naeini, M.R., Hayat, M.M. 'Modeling cascading-failures in power grids including communication and human operator impacts'. In: 2017 IEEE Green Energy and Smart Systems Conference (IGESSC). (Milan, Italy: IEEE, 2017. pp. 1–11.
8 Ghiasi, M., Dehghani, M., Niknam, T., Kavousi.Fard, A., Siano, P., Alhelou, H.H.: 'Cyber-attack detection and cyber-security enhancement in smart DC-microgrid based on blockchain technology and Hilbert Huang transform', *IEEE Access*, 2021, **9**, pp. 29429–29440.
9 Wei, M., Lu, Z., Wang, W.: 'On characterizing information dissemination during city-wide cascading failures in smart grid', *IEEE Syst J*, 2018, **12**, (4), pp. 3404–3413.
10 North American Electric Reliability Corporation (NERC). '2021 state of reliability'. (, 2021. accessed: 14-Jul-2024. Available from: `https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2021.pdf`
11 Alladi, T., Chamola, V., Rodrigues, J.J.P.C., Kozlov, S.A.: 'Blockchain in smart grids: A review on different use cases', *Sensors (Basel)*, 2019, **19**, (22), pp. 4862.
12 Cai, Y., Cao, Y., Li, Y., Huang, T., Zhou, B.: 'Cascading failure analysis considering interaction between power grids and communication networks', *IEEE Trans Smart Grid*, 2016, **7**, (1), pp. 530–538.
13 Wang, X., Luo, X., Zhang, Y., Guan, X.: 'Detection and isolation of false data injection attacks in smart grids via nonlinear interval observer', *IEEE Internet Things J*, 2019, **6**, (4), pp. 6498–6512.
14 Babalola, A.A., Belkacemi, R., Zarrabian, S.: 'Real-time cascading failures prevention for multiple contingencies in smart grids through a multi-agent system', *IEEE Trans Smart Grid*, 2018, **9**, (1), pp. 373–385.
15 Liu, D., Zhang, X., Tse, C.K.: 'A tutorial on modeling and analysis of cascading failure in future power grids', *IEEE Trans Circuits Syst II Express Briefs*, 2021, **68**, (1), pp. 49–55.
16 Zhao, Y., Chen, J., Poor, H.V.: 'A learning-to-infer method for real-time power grid multi-line outage identification', *IEEE Trans Smart Grid*, 2020, **11**, (1), pp. 555–564.
17 Atat, R., Ismail, M., Serpedin, E.: 'Limiting the failure impact of interdependent power-communication networks via optimal partitioning', *IEEE Trans Smart Grid*, 2023, **14**, (1), pp. 732–745.
18 Hu, R., Wang, J., Zhou, Y., Cao, Y., Cao, Y.: 'A collaborative intrusion detection approach using blockchain for multimicrogrid systems', *IEEE Trans Ind Appl*, 2019, **55**, (6), pp. 7210–7219.
19 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 Industr Inform*, 2022, **18**, (11), pp. 8287–8297.
20 Dai, J., Yang, J., Wang, Y., Xu, Y.: 'Blockchain-enabled cyber-resilience enhancement framework of microgrid distributed secondary control against false data injection attacks', *IEEE Trans Smart Grid*, 2024, **15**, (2), pp. 2226–2236.
21 Gao, J., Asamoah, K.O., Sifah, E.B., Smahi, A., Xia, Q., Xia, H., et al.: 'Grid-Monitoring: Secured sovereign blockchain based monitoring on smart grid', *IEEE Access*, 2018, **6**, pp. 9917–9925.
22 Guo, L., Liu, Q., Shi, K., Gao, Y., Luo, J., Chen, J.: 'A blockchain-driven electronic contract management system for commodity procurement in electronic power industry', *IEEE Access*, 2021, **9**, pp. 9473–9480.
23 Liang, G., Weller, S.R., Luo, F., Zhao, J., Dong, Z.Y.: 'Distributed blockchain-based data protection framework for modern power systems against cyber attacks', *IEEE Trans Smart Grid*, 2019, **10**, (3), pp. 3162–3173.
24 Wang, Y., Su, Z., Zhang, N., Chen, J., Sun, X., Ye, Z., et al.: 'SPDS: A secure and auditable private data sharing scheme for smart grid based on blockchain', *IEEE Trans Industr Inform*, 2021, **17**, (11), pp. 7688–7699.
25 Keshk, M., Turnbull, B., Moustafa, N., Vatsalan, D., Choo, K.K.R.: 'A privacy-preserving-framework-based blockchain and deep learning for protecting smart power networks', *IEEE Trans Industr Inform*, 2020, **16**, (8), pp. 5110–5118.
26 Nasiri, S., Seifi, H., Delkhosh, H.: 'A secure power system distributed state estimation via a consensus-based mechanism and a cooperative trust management strategy', *IEEE Trans Industr Inform*, 2024, **20**, (2), pp. 3002–3014.
27 Ramanan, P., Li, D., Gebraeel, N.: 'Blockchain-based decentralized replay attack detection for large-scale power systems', *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2022, **52**, (8), pp. 4727–4739.
28 Ding, S., Zeng, J., Hu, Z., Yang, Y.: 'A peer-2-peer management and secure policy of the energy Internet in smart microgrids', *IEEE Trans Industr Inform*, 2022, **18**, (8), pp. 5689–5697.
29 Di.Silvestre, M.L., Gallo, P., Ippolito, M.G., Sanseverino, E.R., Zizzo, G.: 'A technical approach to the energy blockchain in microgrids', *IEEE Trans Industr Inform*, 2018, **14**, (11), pp. 4792–4803.
30 Huang, H., Miao, W., Li, Z., Tian, J., Wang, C., Min, G.: 'Enabling energy trading in cooperative microgrids: A scalable blockchain-based approach with redundant data exchange', *IEEE Trans Industr Inform*, 2022, **18**, (10), pp. 7077–7085.
31 Ji, H., Jian, J., Yu, H., Ji, J., Wei, M., Zhang, X., et al.: 'Peer-to-peer electricity trading of interconnected flexible distribution networks based on distributed ledger', *IEEE Trans Industr Inform*, 2022, **18**, (9), pp. 5949–5960.
32 Abouyoussef, M., Ismail, M.: 'Blockchain-based privacy-preserving networking strategy for dynamic wireless charging of EVs', *IEEE Trans Netw Serv Manag*, 2022, **19**, (2), pp. 1203–1215.
33 Ethereum Foundation. 'Geth documentation'. (, 2024. accessed: 2024-11-10. Available from: `https://geth.ethereum.org/docs`
34 Angelis, S.D., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., Sassone, V. 'Pbft vs proof-of-authority: Applying the cap theorem to permissioned blockchain'. In: Proc. Italian Conf. Cyber Secur. (Milan, Italy, 2018. pp. 1–11.
35 Bhaskar, N.: 'Truffle Quick Start Guide: Learn the fundamentals of Ethereum development'. (Birmingham, England: Packt Publishing, 2018)
36 Lee, W.M. 'Developing web3 dapps using python'. In: Beginning Ethereum Smart Contracts Programming. (Berkeley, CA: Apress, 2023. pp. 215–239.
37 Rescorla, E.. 'The Transport Layer Security (TLS) Protocol Version 1.3'. (RFC Editor, 2018. RFC 8446. Available from: `https://www.rfc-editor.org/info/rfc8446`
38 Johnson, D., Menezes, A., Vanstone, S.: 'The elliptic curve digital signature algorithm (ECDSA)', *Int J Inf Secur*, 2001, **1**, (1), pp. 36–63.
39 Antonopoulos, A.M., Wood, G.: 'Mastering ethereum: Building smart contracts and DApps'. (Stanford University Press, 2021)
40 Islam, M.M., IN, H.P.: 'A privacy-preserving transparent central bank digital currency system based on consortium blockchain and unspent transaction outputs', *IEEE Trans Serv Comput*, 2023, **16**, (4), pp. 2372–2386.
41 Sompolinsky, Y., Zohar, A. 'Secure high-rate transaction processing in bitcoin'. In: Proceedings of the International Conference on Financial Cryptography and Data Security. (, 2015. pp. 507–527.