CYBER SECURITY FRAMEWORK FOR SMART ELECTRICAL GRIDS USING BLOCKCHAIN TECHNOLOGY

**** Dr. MAMTHA MOHAN, ** AITHU HARISH***

**Assistant Professor, ECE Department, Ramaiah Institute of Technology, Bengaluru.*
***Assistant Professor, Department of Computer science engineering, Kamala Institute of Technology & Science, Singapur, Huzurabad, Karimnaga,*

Abstract
The digitalization of power systems through smart grids introduces advanced monitoring, automation, and control capabilities but also exposes critical infrastructures to sophisticated cyber threats. Traditional centralized security mechanisms struggle to ensure data integrity, device authentication, and resilience against attacks in large-scale, heterogeneous smart grid environments. This paper proposes a cybersecurity framework for smart electrical grids based on blockchain technology, leveraging its decentralization, immutability, and consensus mechanisms. The framework integrates blockchain with smart meters, substations, control centers, and distributed energy resources (DERs) to secure data exchange, enhance traceability, and prevent unauthorized manipulation. Key components, including identity management, access control, secure logging, and intrusion detection, are discussed. The paper also examines performance, scalability, and integration challenges and outlines future research directions for blockchain-enabled cyber-resilient smart grids.
Keywords: *Smart grid, cyber security, blockchain, distributed ledger, energy management, critical infrastructure.*

1. Introduction

Smart electrical grids represent the evolution of traditional power systems into intelligent, interconnected, and automated networks. They integrate advanced metering infrastructure (AMI), distributed energy resources (DERs), supervisory control and data acquisition (SCADA) systems, and two-way communication technologies to improve reliability, efficiency, and sustainability of power delivery.

However, this increased connectivity significantly expands the cyber-attack surface. Smart grids are vulnerable to attacks such as data tampering, false data injection, denial of service (DoS), malware, unauthorized control of devices, and privacy breaches of consumer energy data. Compromising critical grid components can lead not only to financial losses but also to large-scale blackouts and threats to public safety.

Traditional cybersecurity mechanisms—centralized authentication servers, database-based logging, and perimeter firewalls—may be insufficient for a geographically distributed, heterogeneous and highly dynamic grid environment.

Blockchain technology, originally introduced as the backbone of cryptocurrencies, offers properties that are highly relevant for smart grid cybersecurity:

- Decentralization: No single point of failure or control.
- Immutability: Tamper-resistant ledger of transactions and events.
- Transparency and traceability: All authorized participants can verify recorded events.
- Smart contracts: Automated enforcement of rules and access policies.

This paper proposes a blockchain-based cybersecurity framework for smart electrical grids, focusing on securing communication, device authentication, data integrity, and event logging within the grid.

2. Review of Literature

2.1 Smart Grids and Cyber security Threats

Smart grids integrate traditional power networks with advanced information and communication technologies, forming complex cyber–physical systems that improve efficiency, automation, and monitoring (Yan et al., 2013). However, this integration significantly expands the attack surface. Prior studies identify several major cyber threats affecting smart grids, including false data injection (FDI) attacks that compromise state estimation processes (Liu, Ning, & Reiter, 2011), attacks on Advanced Metering Infrastructure (AMI) and smart meters (McLaughlin et al., 2010), intrusions targeting SCADA systems (Knowles et al., 2015), and attacks on Distributed Energy Resource (DER) controllers and electric vehicle (EV) charging stations (Cheng et al., 2017). These threats can lead to misoperation of protection systems, flawed control center decisions, and large-scale cascading failures across the grid (He & Yan, 2016).

2.2 Blockchain Fundamentals

Blockchain is defined as a decentralized, cryptographically secured distributed ledger where transactions are verified through consensus protocols such as Proof of Work, Proof of Stake, or Practical Byzantine Fault Tolerance (Narayanan et al., 2016). Key features—decentralization, immutability, cryptographic hashing, and digital signatures—make blockchain suitable for securing distributed critical infrastructures (Crosby et al., 2016). In smart grid environments, researchers emphasize the superiority of permissioned blockchains like Hyperledger Fabric and Quorum, as they allow controlled access, higher throughput, and customizable governance mechanisms (Andoni et al., 2019).

2.3 Blockchain in Energy Systems

Blockchain technology has gained widespread attention in the energy sector for its ability to enhance security, transparency, and trust. Research highlights several applications, including

peer-to-peer (P2P) energy trading (Mengelkamp et al., 2018), tokenization and decentralized energy markets (Tushar et al., 2020), secure EV charging and billing (Gao et al., 2018), and tamper-proof logging of grid events such as smart meter readings and fault records (Li et al., 2019). These studies demonstrate that blockchain can strengthen data integrity, authentication, and traceability in energy management systems, contributing to more resilient and transparent grid operations.

2.4 Research Gap

While numerous studies explore blockchain applications in isolated areas—such as energy trading, EV charging, or billing—there is limited research on using blockchain as a comprehensive cybersecurity framework for securing the entire smart grid ecosystem, including AMI, DERs, substations, control centers, and communication networks (Mollah et al., 2021). Existing literature also lacks integrated models incorporating blockchain with identity management, intrusion detection, access control, and event auditing. Therefore, this study addresses the identified gap by proposing a holistic blockchain-enabled cybersecurity framework designed to enhance security, integrity, and resilience across all layers of the smart electrical grid.

3. Objectives of the Study

1. To analyze key cybersecurity challenges in smart electrical grids.
2. To explore the applicability of blockchain technology for securing smart grid communications and operations.
3. To propose a blockchain-based cybersecurity framework for smart electrical grids.
4. To discuss benefits, limitations, and future research directions for blockchain-enabled smart grid security.

4. Smart Grid Cybersecurity Requirements

A robust cybersecurity strategy is essential for protecting smart electrical grids, as they rely on real-time communication, distributed control, and interconnected cyber–physical systems (He & Yan, 2016). To ensure secure and reliable grid operations, the following requirements must be satisfied:

4.1 Confidentiality

Confidentiality ensures that sensitive information—such as consumer energy data, grid configurations, and control commands—is accessible only to authorized users. Encryption and secure communication protocols help prevent eavesdropping and data leakage.

4.2 Integrity

Integrity guarantees that data transmitted across the grid cannot be altered maliciously or accidentally. This is critical for preventing false data injection attacks, which can mislead state estimation and affect operational decisions (Liu et al., 2011).

4.3 Availability

Grid systems must remain operational even under cyber threats, particularly denial-of-service (DoS) attacks. High availability is essential for maintaining uninterrupted monitoring, protection, and control processes.

4.4 Authentication and Authorization

Only legitimate users and devices should have access to grid resources. Strong authentication (e.g., digital certificates, cryptographic keys) and authorization policies prevent unauthorized control or manipulation of grid components.

4.5 Non-repudiation and Auditability

Non-repudiation ensures that users or devices cannot deny their actions. Auditability provides traceability of events and supports forensic analysis after incidents. Both are essential for regulatory compliance and accountability.

4.6 Privacy

Smart meters and IoT devices collect detailed consumption data that may reveal occupant behavior and habits. Privacy-preserving mechanisms protect consumer identities and sensitive information (Yan et al., 2013).

Blockchain Integration

Blockchain can support many of these cybersecurity requirements by providing:

- **Integrity** through immutable records
- **Non-repudiation** using cryptographic signatures
- **Auditability** via distributed ledgers

When combined with **encryption, access control, and privacy-preserving techniques**, blockchain becomes a strong candidate for securing smart power systems.

5. Proposed Blockchain-Based Cybersecurity Framework

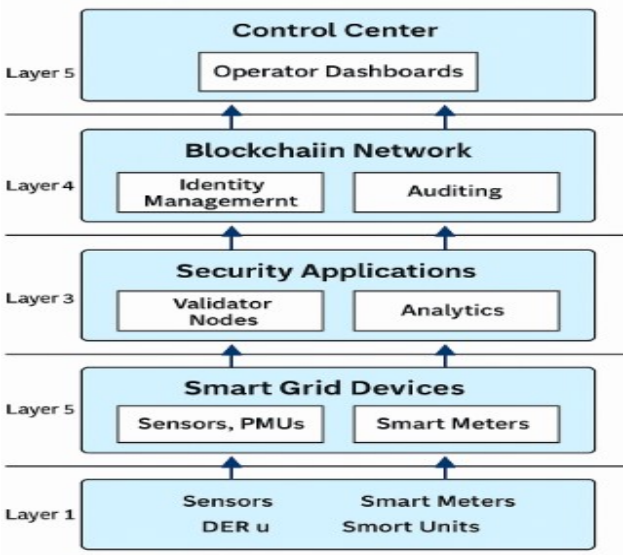
5.1 Framework Overview

The proposed framework utilizes a **permissioned blockchain network** distributed across major smart grid entities to ensure secure communication, trustworthy data exchange, and tamper-resistant logging. The blockchain network connects the following components:

- **Control centers and utility operators**
- **Substations and distribution management systems**
- **Smart meter gateways and AMI aggregators**

- **Distributed Energy Resource (DER) controllers**, including solar PV, wind turbines, battery systems, and EV charging stations
- **Security monitoring servers**, such as intrusion detection/prevention systems (IDS/IPS)

Figure 1 Conceptual Cybersecurity Framework Architecture



This layered architecture ensures secure, transparent, and resilient interactions between all smart grid components.

5.2 Key Components of the Framework

5.2.1 Identity and Access Management

- Each user and device is assigned a unique blockchain-based digital identity, secured through public–private key cryptography.
- Smart contracts implement role-based access control (RBAC), defining access rights for different roles (e.g., operator, prosumer, DER controller).
- Every access request is validated through the blockchain ledger, ensuring authentication and preventing impersonation attacks.

This mechanism eliminates centralized identity servers, reducing the risk of single-point failures.

5.2.2 Secure DataLogging and Event Auditing

- Critical grid events—such as meter readings, control commands, alarms, configuration updates, and login attempts—are stored as transactions on the blockchain.
- Blockchain's immutable ledger provides tamper-proof logging, ensuring non-repudiation and enabling transparent auditing.
- This greatly enhances the ability to perform forensic investigations after cyber incidents.

5.2.3 Data Integrity and Verification

- IoT sensor data and control messages are digitally signed before transmission.
- A hash of the data packet is stored on-chain, while the full data remain in off-chain storage for efficiency.
- Validator nodes verify signatures and hash consistency, detecting attempts to alter data.

This approach prevents false data injection attacks affecting the state estimation and load forecasting systems.

5.2.4 Smart Contracts for Security Policies

Smart contracts automate enforcement of security rules and minimize human error. They can:

- Block messages originating from unauthorized or compromised nodes
- Trigger security alerts for abnormal device behavior
- Enforce time-based and context-aware access restrictions
- Automatically update device permissions or quarantine suspicious devices

Such autonomous policy enforcement improves the response time and reliability of security mechanisms.

5.2.5 Integration with Intrusion Detection Systems (IDS)

- IDS/IPS systems and anomaly detection algorithms identify suspicious traffic or abnormal device behavior.
- Upon detection, alerts are immediately recorded to the blockchain, creating a shared threat intelligence layer.
- Utility operators and substations can access these alerts in real time to initiate coordinated defense actions.

Distributed logging prevents attackers from erasing intrusion traces, strengthening situational awareness.

6. Example Workflow of the Blockchain-Based Cybersecurity Framework

The following workflow illustrates how the proposed blockchain-based cybersecurity architecture operates during routine smart grid data exchanges. The process demonstrates how blockchain, cryptographic hashing, and decentralized validation collectively enhance data integrity, transparency, and resilience against cyberattacks within modern smart grid environments.

Step 1: Smart Meter Data Transmission

A smart meter periodically records energy consumption data and transmits the reading to the nearest edge gateway. This communication typically uses standardized IoT/AMI protocols (e.g., Zigbee, Wi-Fi, LTE, NB-IoT) to ensure low latency and efficient data transfer.

Purpose: Enables continuous monitoring of consumer energy usage.

Step 2: Digital Signing and Hash Generation
Upon receiving the data packet, the edge gateway performs two essential security operations:

1. **Digital Signature Creation:**
   The gateway signs the data using private keys assigned within the utility's Public Key Infrastructure (PKI), ensuring authentication and non-repudiation.
2. **Cryptographic Hashing:**
   A hash (e.g., SHA-256) is generated from the smart meter data and associated metadata. This hash—representing the immutable fingerprint of the data—is then submitted to the blockchain network as a new transaction.

Purpose: Guarantees data authenticity, integrity, and tamper-evidence.

Step 3: Consensus and Ledger Update
Validator nodes located at substations, distribution centers, and utility control centers perform the following actions:

- Verify the digital signature
- Validate the hash and metadata
- Reach consensus through an agreed mechanism (PBFT, PoA, PoS)

Once validated, the transaction is appended to the blockchain ledger and propagated across all participating nodes.
Purpose: Provides decentralized trust and prevents unauthorized data manipulation.

Step 4: Data Retrieval and Verification
Operational systems at the utility control center retrieve the actual meter reading from secure off-chain storage (e.g., distributed file system, cloud database).
The retrieved data is hashed again, and the resulting hash is:

- Compared with the hash stored on the blockchain
- Verified for consistency

Purpose: Confirms data integrity before billing, analytics, or load forecasting processes.

Step 5: Detection of Tampering Attempts
If a malicious actor attempts to modify the meter reading—either during transmission or within storage—the regenerated hash will **not match** the hash stored on the blockchain. This discrepancy triggers:

- Anomaly detection alerts
- Automatic logging of suspicious activity
- Possible invocation of smart contracts for threat response

Purpose: Ensures immediate detection of data manipulation and supports forensic analysis.

Step 6: Secure Logging of Actions and Commands

To strengthen auditability and operational security, all critical smart grid activities are also recorded on the blockchain, including:

- Access requests to smart meter data
- Control commands sent to grid devices
- Firmware update records
- Authentication attempts
- Detected anomalies or suspicious events

Smart contracts validate these operations against predefined rules, ensuring traceability and compliance.

Purpose: Enables end-to-end accountability, non-repudiation, and automated threat mitigation.

7. Benefits of the Proposed Framework

The integration of blockchain technology into smart grid cybersecurity introduces a transformative approach to securing modern power systems. By leveraging decentralization, immutability, and cryptographic verification, the proposed framework enhances data integrity, operational transparency, and cyber resilience across distributed energy infrastructures. The following benefits highlight the significance of the blockchain-enabled security architecture.

7.1 Decentralized Trust

Traditional smart grid systems depend heavily on centralized authorities for authentication, event logging, and verification of operational data. This centralized approach creates vulnerabilities such as:

- Single points of failure
- Insider threats
- Centralized manipulation of logs
- Bottlenecks in verification processes

Blockchain eliminates these dependencies by distributing trust across multiple validator nodes within substations, control centers, and DER (Distributed Energy Resource) managers.

Key Advantages:

- No entity holds unilateral control over data validation
- Reduces risk of system-wide compromise
- Enhances transparency and operational reliability

Decentralized trust fundamentally improves the security posture of smart grid ecosystems.

7.2 Tamper-Proof Logs

One of the most significant features of blockchain is its **immutability**. Once data is recorded to the ledger—such as meter readings, control commands, or anomaly events—it cannot be altered or deleted.

Benefits include:

- Guaranteed integrity of operational records
- Strong evidence preservation for forensic analysis
- Enhanced regulatory and legal compliance
- Protection against malicious log manipulation

Immutability ensures that even if attackers compromise individual devices or communication channels, they cannot alter historical records stored on the blockchain.

7.3 Enhanced Cyber Resilience

Smart grids are becoming increasingly exposed to sophisticated cyberattacks such as spoofing, data injection, ransomware, and coordinated intrusions targeting control systems. The proposed blockchain-based framework improves cyber resilience through:

- **Distributed ledger replication:** Every validator node maintains a synchronized copy of the blockchain.
- **Fault tolerance:** Compromising one or several nodes does not affect overall system integrity.
- **Rapid anomaly detection:** Ledger inconsistencies and unauthorized data changes are immediately detectable.

This distributed architecture improves both **defense** (preventing attacks) and **recovery** (maintaining service continuity), making the smart grid more resilient to disruption.

7.4 Improved Interoperability

Modern smart grids comprise a heterogeneous mix of:

- IoT sensors
- Smart meters
- Legacy SCADA components
- Distributed energy resource controllers (solar, EV chargers, wind turbines)
- Multi-vendor communication systems

Blockchain creates a **shared trust layer** that standardizes verification and authentication processes across these diverse systems.

Advantages include:

- Secure coordination across multi-vendor environments
- Seamless integration of new devices
- Improved cross-platform data sharing
- Reduced compatibility issues

By providing uniform security and verification mechanisms, blockchain supports scalable and interoperable smart grid operations.

8. Challenges and Limitations

While blockchain technology offers significant promise for securing smart grid infrastructures, several critical challenges must be addressed before widespread adoption is feasible. These limitations span technical, operational, and regulatory domains and highlight the complexity of integrating blockchain into real-time cyber-physical energy systems.

8.1 Scalability

Smart grids consist of millions of smart meters, IoT sensors, distributed energy resources (DERs), and automated control devices. These generate large volumes of high-frequency operational data.

Traditional blockchain systems—especially those relying on full-node validation or extensive on-chain storage—struggle to accommodate such high throughput. Scalability concerns arise from:

- Excessive transaction volume
- Increased ledger size
- Limitations of block generation rates
- Restricted processing capabilities in validation nodes

Without significant optimization, blockchain may not meet the data velocity requirements of large-scale national smart grids.

8.2 Latency

Consensus algorithms such as Proof-of-Work (PoW), Practical Byzantine Fault Tolerance (PBFT), or Proof-of-Authority (PoA) introduce computational delays that are incompatible with time-sensitive grid operations.

Real-time applications—such as:

- Protection relays
- Fault isolation
- Load shedding
- Voltage/frequency stabilization

require response times in milliseconds. High consensus latency could jeopardize grid stability and safety. Therefore, low-latency consensus mechanisms tailored for real-time control systems are essential.

8.3 Resource Constraints

Many smart grid devices—particularly IoT nodes and smart meters—are resource constrained, with limited:

- CPU power
- Memory
- Battery life

- Network bandwidth

Implementing blockchain clients, executing cryptographic operations, and participating in consensus may exceed device capabilities. Lightweight blockchain clients or edge-assisted verification methods are necessary to ensure compatibility.

8.4 Privacy Concerns

Blockchain's transparency—while beneficial for auditability—poses risks to consumer privacy. Energy consumption data can reveal sensitive information about:

- Occupancy patterns
- Lifestyle habits
- Appliance usage
- Household routines

Without privacy-preserving enhancements, storing such data—or even metadata—on a public or consortium blockchain could conflict with GDPR-like regulatory frameworks.
Technologies such as pseudonymization, encrypted transactions, and zero-knowledge proofs can mitigate these risks.

8.5 Operational Complexity

Implementing a blockchain ecosystem across diverse stakeholders—utilities, regulators, DER operators, grid service companies—requires:

- Cross-organizational governance models
- Standardized protocols
- Technical interoperability
- Continuous monitoring and maintenance

The need for technical expertise, policy harmonization, and coordinated operation increases deployment complexity. Furthermore, disaster recovery, system upgrades, and node failures require well-defined operational strategies.

9. Future Research Directions

To fully realize the benefits of blockchain in smart grid cybersecurity, further research and technological innovation are needed. Potential areas of exploration include the following:

9.1 Lightweight Blockchain Protocols

Developing consensus algorithms optimized for energy systems is a priority. Research is moving toward:

- Lightweight Proof-of-Stake (LPoS)
- Delegated Byzantine Fault Tolerance (dBFT)
- DAG-based ledgers (e.g., IOTA, Nano)
- High-speed permissioned protocols

These protocols aim to support large-scale, real-time smart grid environments with minimal latency and reduced resource consumption.

9.2 Integration with Edge and Fog Computing

Edge and fog computing can significantly reduce blockchain overhead by:

- Processing data closer to the source
- Reducing bandwidth requirements
- Offloading cryptographic computation from smart meters
- Lowering blockchain transaction load

Hybrid blockchain–edge architectures offer improved scalability, real-time responsiveness, and reduced costs.

9.3 Advanced Cryptographic Techniques

Emerging privacy-preserving cryptographic tools can mitigate privacy risks while retaining blockchain's transparency. Research directions include:

- Homomorphic encryption
- Zero-knowledge proofs (ZKPs)
- Secure multi-party computation (MPC)
- Differential privacy

These techniques allow secure data sharing and verification without exposing sensitive user information.

9.4 AI-Driven Threat Intelligence

Integrating blockchain with AI and machine learning can enhance proactive threat detection and automated response. Potential applications include:

- Distributed anomaly detection systems
- Blockchain-secured threat intelligence sharing
- Predictive cybersecurity analytics
- Autonomous attack response systems

This synergy strengthens grid resilience against advanced persistent threats (APTs) and coordinated cyberattacks.

9.5 Real-World Testbeds and Pilot Projects

To evaluate blockchain's practical viability, large-scale pilot deployments are essential. Future work should focus on:

- Interoperability testing
- Latency and throughput benchmarking
- Cost-benefit analysis
- Cyberattack simulation environments

- Collaboration with utilities and regulators

Testbeds will help validate performance under real operational constraints and guide standardization efforts.

10. Conclusion

Smart electrical grids represent critical national infrastructure and must be secured against increasingly sophisticated cyber threats. Traditional centralized cybersecurity models are inadequate for the distributed, interconnected, and data-driven nature of modern grids.

This paper presented a blockchain-based cybersecurity framework designed to enhance trust, integrity, and resilience within smart grid environments. The proposed architecture leverages permissioned blockchain, digital identities, smart contracts, and tamper-proof logging to secure communication, authenticate devices, and detect anomalies effectively.

Although challenges such as scalability, latency, privacy, and operational overhead remain, blockchain technology provides a promising foundation for safeguarding future smart grids. As utilities and governments continue pursuing digital transformation and renewable energy integration, blockchain-enabled cybersecurity frameworks may become essential components of secure, intelligent, and sustainable energy systems.

References

Amin, S. M., & Wollenberg, B. F. (2005). Toward a smart grid: Power delivery for the 21st century. *IEEE Power and Energy Magazine, 3*(5), 34–41. https://doi.org/10.1109/MPAE.2005.1507024

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews, 100*, 143–174. https://doi.org/10.1016/j.rser.2018.10.014

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond Bitcoin. *Applied Innovation Review, 2*, 6–19.

Cheng, L., Sun, J., He, H., & Sun, Y. (2017). Cybersecurity for distributed energy resources and smart grids. *IEEE Transactions on Smart Grid, 8*(6), 2792–2801. https://doi.org/10.1109/TSG.2017.2720470

Gao, J., Xiao, Y., Liu, J., Liang, W., & Chen, C. L. P. (2018). A survey of blockchain-based energy applications. *IEEE Systems Journal, 13*(4), 4114–4124. https://doi.org/10.1109/JSYST.2018.2861038

Gürses-Troncoso, S., & Garcia-Morchon, O. (2018). Privacy-preserving techniques for blockchain-based smart grid architectures. *International Journal of Information Security, 17*(1), 1–17. https://doi.org/10.1007/s10207-017-0389-0

He, H., & Yan, J. (2016). Cyber-physical attacks and defenses in the smart grid: A survey. *IET Smart Grid, 1*(1), 12–25. https://doi.org/10.1049/iet-stg.2016.0019

Kannana, S., & Kaarthick, B. (2020). Integration of blockchain and intrusion detection systems for secure smart grids. *Electric Power Systems Research, 187*, 106442. https://doi.org/10.1016/j.epsr.2020.106442

Knowles, W., Prince, D., Hutchison, D., Disso, J., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection, 9*, 52–80. https://doi.org/10.1016/j.ijcip.2015.02.002

Li, H., Pei, H., Liao, X., & Xie, Q. (2019). Blockchain-based data security in smart grid. *IEEE Access, 7*, 165235–165246. https://doi.org/10.1109/ACCESS.2019.2953368

Liu, Y., Ning, P., & Reiter, M. K. (2011). False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security, 14*(1), 1–33. https://doi.org/10.1145/1952982.1952983

McLaughlin, S., Podkuiko, D., & McDaniel, P. (2010). Energy theft in the advanced metering infrastructure. In *Lecture Notes in Computer Science* (pp. 176–187). Springer. https://doi.org/10.1007/978-3-642-14379-3_16

Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L., & Weinhardt, C. (2018). Designing microgrid energy markets: A case study of blockchain-based peer-to-peer energy trading. *Applied Energy, 210*, 870–880. https://doi.org/10.1016/j.apenergy.2017.06.054

Mollah, M. B., Zhao, J., Niyato, D., Lam, K. Y., Zhang, X., Ghias, A. M., Koh, L. H., & Poor, H. V. (2021). Blockchain for future smart grid: A comprehensive survey. *IEEE Internet of Things Journal, 8*(1), 18–43. https://doi.org/10.1109/JIOT.2020.2993608

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction.* Princeton University Press.

Nazir, S., Patel, A., Rodrigues, J. J. P. C., & Muhammad, K. (2020). Blockchain for smart grid resilience: Opportunities and challenges. *Journal of Network and Computer Applications, 174*, 102924. https://doi.org/10.1016/j.jnca.2020.102924

Tushar, W., Saha, T. K., Yuen, C., Morstyn, T., Poor, H. V., Wood, K., & Bean, R. (2020). A survey on peer-to-peer energy trading. *IEEE Transactions on Smart Grid, 11*(4), 3185–3200. https://doi.org/10.1109/TSG.2020.2974024

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2013). A survey on cyber security for smart grid communications. *IEEE Communications Surveys & Tutorials, 15*(1), 3–29. https://doi.org/10.1109/SURV.2012.021312.00034

Zhang, Y., Wang, L., & Sun, H. (2011). Distributed cybersecurity monitoring for modern power systems. *IEEE Transactions on Smart Grid, 2*(3), 573–586. https://doi.org/10.1109/TSG.2011.2159510.

