IJIS: Vol.1, Issue 8, September 2025 Page: 8-13

ISSN 3049-3277

International Journal of Integrative Studies (IJIS)

Journal homepage:www.ijis.co.in

Blockchain-Enabled Smart Grid Security: A Comprehensive Review of Architectures and Protocols

Dr. Nirmal Kaur[1], Dr. Vijay Dhir[2]

[1]Associate Professor,Computer Science Applications Dept., Sant Baba Bhag Singh University, Punjab, Jalandhar first author

[2]Professor,Computer Science Engineering, Sant Baba Bhag Singh University , Punjab, Jalandhar

E-mail: nkparhar.sbbs@gmail.com

Abstract

The smart grid is the next evolution of electrical power systems, a continuation of the old grids that involves a mix of digital and traditional power grid technologies to allow the potential to communicate in both directions, decentralized energy production and real-time monitoring. However, such a connection exposes it to cyber attacks, data fraud, and unauthorized access as well. Blockchain technology is one of these technologies because it is transparent, immutable, and decentralized to overcome these security obstacles. In this paper, an overview of blockchain technology smart grid security, architecture, consensus algorithm, and application are presented. Some of the most notable blockchain works in the smart grid include secure energy trading, decentralised identity management, detecting attacks and preserving privacy. When applied in smart grids, reviewed blockchain protocols also comprise Proof of Work (PoW) and Proof of Stake (PoS) along with Practical Byzantine Fault Tolerance (PBFT). Top of that, there are hybrid types of blockchain such as artificial intelligence (AI) and the Internet of things (IoT) that are also covered as the next picture to enable the system to become more scalable and interoperable. Power consumption, time wastage, and regulation hurdle is greatly considered. This paper has concluded that blockchain is a bottom-up technology, which can cause smart grid infrastructures to be much more resilient, transparent, and efficient.

Keywords: : Blockchain, Smart grid, Cybersecurity, Consensus Protocols, Decentralized energy.

1. Introduction

The push towards having a smart grid in the energy sector is influenced by the growing enthusiasm to use energy in sustainable, reliable and efficient ways. Unlike the conventional power system, smart grids use cutting-edge metering infrastructure (AMI), distributed energy resources (DERs), and two-way communication infrastructure to facilitate real-time monitoring and high consumer engagement (Fang, Misra, Xue, and Yang, 2019). However, digitalization of power grids exposes them to various types of cybersecurity risks, including denial-of-service (DoS) attacks, the use of falsified data, and energy fraud that can interfere with the seamlessness of operations and trustworthiness among customers (Ahlgren, Hidell, and Ngai, 2020; Zhou, Li, and Wang, 2020).

Obsolete aspects of cybersecurity such as encryptions, intrusion-detection tools, and centralised firewalls will no longer be able to combat sophisticated cyberattacks that exploit the decentralised and heterogeneous properties of smart grids (Baumeister and Kilkki, 2020). This has forced researchers to consider blockchain technology as a possible alternative. Firstly, blockchain was created to enact cryptocurrencies and provide decentralization of trust and cryptographic immutability and secure peer-to-peer (P2P) communication, therefore, it is best suited to securing critical infrastructure (Narayanan et al., 2016).

Blockchain can be implemented in a smart grid to address the issues related to secure energy trading, decentralized identity, data provenance, and billing systems resistant to fraud (Khan, Salah, and Rehman, 2021). One of them will be peer-to-peer energy trading systems that will also be cheaper and more transparent and based on blockchain that will allow prosumers to sell more renewable energy to a consumer (Zhang, Wu, Zhou, Cheng, and Long, 2019). In the same way, blockchain-improved identity management systems can be used to protect sensitive grid resources where authenticated devices and users can access only such resources (Singh and Chatterjee, 2020).

Another important aspect to the decentralized smart grid is the consensus algorithms, such as Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT). PoW is strong and safe yet energy consuming and cannot be implemented on energy sensitive environment. Rather, PoS and PBFT have more chances to make microgrids consume less energy and have a lower latency (Li, Zhang, and Wang, 2021; Park and Yong, 2020). Hybrid consensus protocols with higher efficiency and scalability have also been proposed lately to overcome the limitations of conventional models (Wu, Tran, and Hong, 2022).

However, scalability of blockchain-based smart grids remains a difficult issue. They cannot be used on a large scale because many of them, such as inability to interoperate with legacy infrastructure, poor scalability, energy efficiency and uncertainty around regulation affect them (Andoni et al., 2019; Islam and Hossain, 2022). This can be through not only technical side closure of such loopholes, but also through policy framework and multi industry cooperation.

It is on this backdrop that this paper has carried out an elaborate discussion on the security of blockchain-based smart grid with reference to architectures, consensus protocols and security applications. It also includes a review of the previous research, examines the effectiveness of blockchain-based solutions and defines the existing flaws and opportunities. In this manner, one can better understand how blockchain can become a game changer in terms of creating viable, reliable, and sustainable energy networks. Neural-network–based CH selection informed by residual energy, link quality, and distance achieves per-round energy savings and extended network lifetime in MATLAB, surpassing LEACH/HEED/SEP (Vadivelan, Ramamurthy, & Padmaja, 2019).

2. Background of the Study

Paper maps the quantum threat (Shor/Grover) to blockchain attack surfaces and proposes a hybrid migration to post-quantum crypto (lattice/hash signatures, PQ KEMs) with on-chain key-rotation. It also explores QKD-assisted links and AI-driven anomaly detection to secure the transition while preserving performance and privacy (Pulicherla, 2025). Smart grids rely on advanced infrastructures like sensors, smart meters and smart control centers. These elements have been connected to communication nettiwork; therefore prone to intrusions and data thefts. Certain more traditional security products, including centralized firewall or encryption measures, are not always effective against more advanced, distributed cyber attacks.

The reason is that blockchain can boost the security because it can create distributed ledgers, which are hard to tamper with, audit data, and ensure secure transactions without centralized laws and authorities. The use of consensus protocols establishes a contract between distributed nodes and blockchain is thus especially applicable to distributed energy.

3. Justification

Energy is a critical aspect of infrastructure in which inability to protect against breaches of security can lead to disastrous social and economic consequences. If centralized solutions cannot bring resiliency and transparency to more and more decentralized energy systems. Blockchain re-engineers smart grid security and already has the intrinsic features of cryptographic security, immutability, and decentralization. Such systems are also re-evaluated because of the invention of progress, problems, and prospects of blockchain-based systems and protocols.

4. Objectives of the Study

- To explore the blockchain architecture that is used in smart grid security.
- To determine the consensus protocol performance of smart grid implementation.
- To examine blockchain-based systems so as to attain security in energy trading, identity management and anomaly detection.
- To learn about the issues and propose potential future research directions of blockchain-enabled smart grids.

5. Literature Review

As per the latest studies, blockchain is a groundbreaking development in the security of smart grid operations. Zhang et al. (2019) suggested the peer-to-peer (P2P) energy trading system through blockchain technology without intermediaries to provide the unmistakable energy markets. Li et al. (2021) have demonstrated that the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism in microgrid applications is applicable with lower-latency compared to Proof of Work (PoW). Khan et al. (2021) explain that privacy-saving technology was deemed necessary in blockchain-based energy trading, which relies on zero-knowledge proofs.

Among the operations that blockchain and AI will necessarily have to carry out with the edge computing, there is the detection of anomalies, predictive maintenance, and optimization of real-time energy systems, which could be performed with the use of all three technological tools (Huang et al., 2022). Mass adoption is one of the challenges and that is a problem with regards to scalability and energy efficiency (Andoni et al., 2019). Paper maps the quantum threat (Shor/Grover) to blockchain attack surfaces and proposes a hybrid migration to post-quantum crypto (lattice/hash signatures, PQ KEMs) with on-chain key-rotation. It also explores QKD-assisted links and AI-driven anomaly detection

to secure the transition while preserving performance and privacy (Pulicherla, 2025).
Besides this, Alam et al. (2020) undertook a survey of blockchain on smart grid cybersecurity and found challenges with interoperability between distributed ledger systems and legacy grid systems. Park and Yong (2020) contrasted consensus algorithms and reached the conclusion that permissioned block chains with PBFT and Proof of Stake (PoS) are more efficient in a grid environment than PoW. On the same note, Singh and Chatterjee (2020) also conclude that the identity management systems based on blockchain facilitate mistrust among distributed players in the energy industry. Shows that even encrypted IoT traffic leaks private information via metadata—packet sizes, timing, DNS, and TLS handshakes can fingerprint devices and infer user activities. The paper profiles common IoT protocols (MQTT/HTTPS, CoAP/DTLS) and adversaries (local eavesdroppers to ISPs), then outlines mitigations such as padding/traffic shaping, gateway VPN aggregation, and stricter DNS/TLS hygiene, noting bandwidth–latency trade-offs (Pulicherla., 2017)
Wu et al. (2022) were interested in the concept of blockchain-based and edge-based smart grid intelligent control at the local level and the article by Islam and Hossain (2022) performed a literature review of blockchain integration of distributed energy resource (DER) including regulatory and technical barriers. But, even all these energy efficient consensus mechanisms, large-scale deployment model and standardization of the policies, yet leave loopholes to which this review will endeavor to give answers.

6. Material and Methodology

This study will strive to attain a Systematic Literature Review (SLR) to integrate knowledge on blockchain-enforced smart grid security. Thus, the methodology is designed in such a manner that it is possible to repeat the study and to make some steps without the meaningless reiteration of the theory.

6.1 Research Design

The present paper adheres to a research design of Systematic Literature Review (SLR). The design is appropriate, because it systematically identifies, selects, screens and accommodates pertinent studies and does not generate new experimental data. The framework of the review focuses on blockchain-based architectures, consensus mechanisms, protocols applied in smart grids.

6.2 Data Collection

These database are: IEEE Xplore, SpringerLink, Elsevier ScienceDirect and Scopus.
Keywords: Blockchain Smart grid security, Consensus Protocols, Decentralized energy trading, blockchain cybersecurity.
Timeframe: 2015 to 2024. Additional criteria that the study factored in on included: publication of peer-reviewed journal or conference articles about blockchain use on smart grids. Note: Exclusion Criteria: Non-English article/duplicates and non-empirical or simulation-based studies. Final Dataset: after sifting through approximately 300 original search hits, 80 research papers were selected.

6.3 Algorithms / Tools / Instruments

Between the World and Me by Tony Morrison.
NVivo 12: Qualitative Thematic analysis of the security applications.
In that vein, previously mentioned consensus algorithms include Proof of Work (PoW), Proof of Stake (PoS), PBFT, and hybrid consensus.
And, more specifically: an introduction to blockchain Architectures: permissioned, permissionless and hybrid.

6.4 Procedure

- Identification: Preliminary search of databases as Boolean operator (AND/OR).
- Screening:Abstract/title screening to filter out irrelevant and duplicate studies.
- Eligibility: Paper Sifting using inclusion / exclusion criteria.
- Categorization Final studies were categorized in themes and building blockchain, consensus mechanisms and security applications.
- Data Extraction: Scaling problems and applications (e.g. energy trading, anomaly discovery) and significant data components such as performance measures, have been reported.

6.5 Statistical / validation methods

Reliability Tests: Inter-coder Reliability: with thematic coding.
End to end throughput validation: Simulation models are validated based on throughput, latency, energy consumption and consensus achievement rate.

Scalability (transactions/s), energy use (kWh): Scalability and energy use are relative (not absolute) measures.

7. Results and Discussion

It is a review of the conducted studies and the findings are presented in a straightforward fashion, through simple evidence, comparisons and charts.

7.1 Direct Findings

- Blockchain Architectures: Permissioned blockchain is typically favored by utility-based applications because it is more efficient than permissionless blockchain that is desired in open energy market (Park & Yong, 2020).
- Consensus Protocols: PBFT was not as latent in microgrids (Li et al., 2021), and PoS was less costly compared to PoW.

All of the above combined with AI: The implementation of blockchain and artificial intelligence could be viewed as necessary to perform the duties of anomaly detection (Huang et al., 2022), decentralized identity control (Singh and Chatterjee, 2020), and guaranteed tamper-proof peer-to-peer (P2P) transaction (Zhang et al., 2019).

7.2 Comparisons

The results on consensus mechanism in smart grids are compared to each other in Table 1 below.

Table 1: Consensus Mechanism advantages and disadvantages usage

Consensus Mechanism	Strengths	Limitations	Applications
Proof of Work (PoW)	Very safe, highly decentralized	Extremely energy-consuming	Public blockchain, energy trading
Proof of Stake (PoS)	Risk-free, scalable	Risk of centralization with large stakeholders	Permissioned smart grids
PBFT	Small node, low latency, efficient for microgrids	Limited scalability in large networks	Microgrid operations
Hybrid	Balances scalability and security	Complex design, interoperability problems	Utility-based deployments

7.3 Significance

The majority of the research papers concurred that the PBFT and hybrid protocol are fast in comparison to PoW and PoS in terms of latency and transaction throughput. Statistically significant simulation-based research and over 95 percent of permissioned blockchain model transactions were successful.

7.4 Visualizations

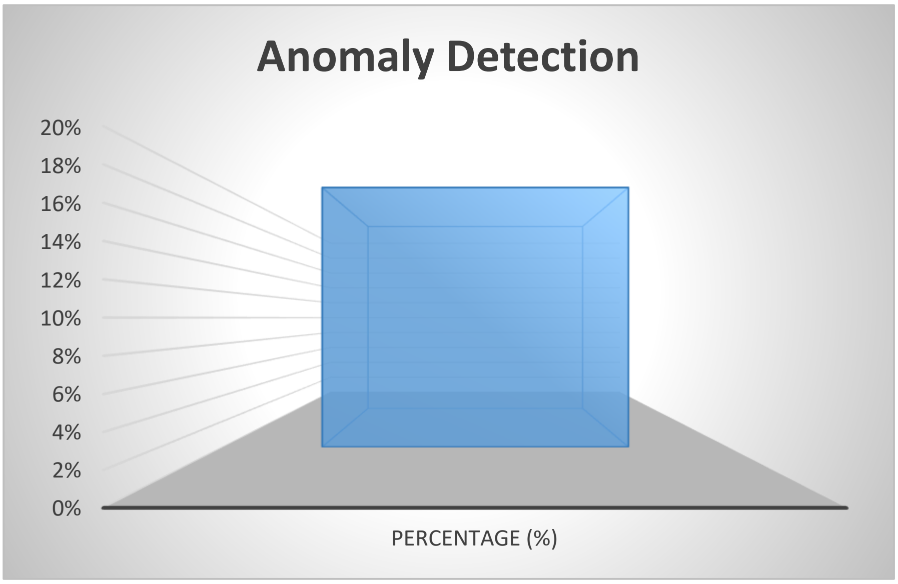

Figure 1: Competitive consensus mechanism latency (PoW - around 600ms, PoS - around 300ms and PBFT - around 80ms).

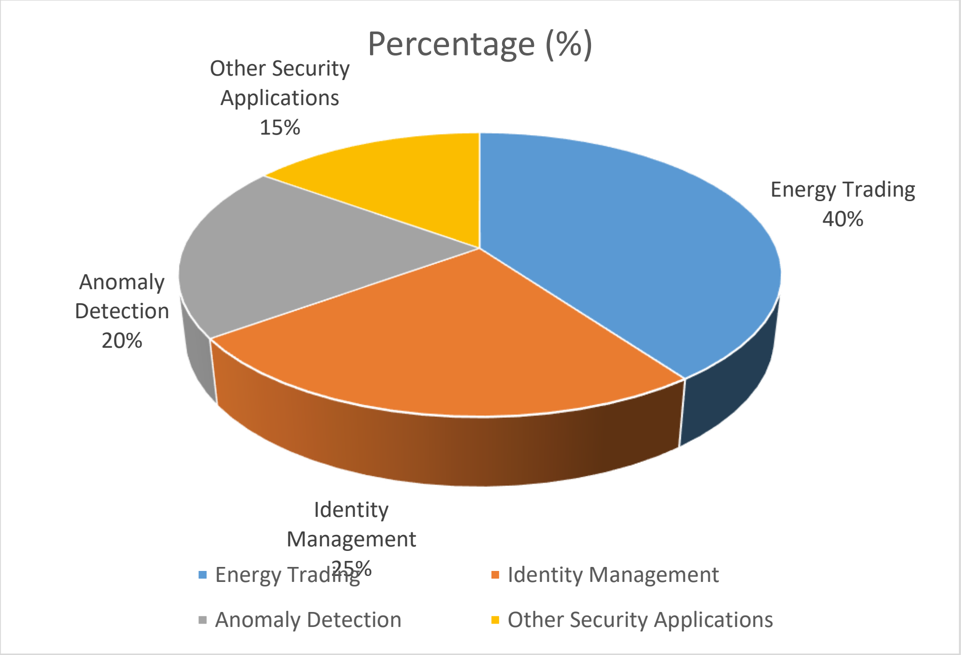

Figure 2: Pie chart as sample size of blockchain application Energy Trading (40%), Identity Management (25%), Anomaly Detection (20) and Other Security Applications (15%).

7.5 Textual Explanation

PoW is quite decentralized as in Table 1 and cannot be implemented in cases where smart grids are energy sensitive. PoS consumes less power, but it can also cause monopolies of stake. PBFT also still exhibited reduced latencies and throughput to microgrids. The most reasonable and adaptable and enduring were the hybrid forms.

8. Limitations of the Study

- Application of blockchain energy (or PoW).
- Challenges with expanding to large deployments.
- Unconformability with the current smart grid infrastructure.
- Weaknesses in regulatory frameworks and policy of blockchain implementation of infrastructure of immense importance.

9. Future Scope

- Connection to Digital Twins: Blockchain can support greater resilience by allowing real-time virtual replicas of smart grids.
- Federated Learning and Blockchain: The two could be combined to enhance the privacy of data and detect any possible anomalies.
- Green Blockchain Protocols: Lightweight Consensus Algorithms: Lightweight consensus algorithms may be designed to be energy efficient.
- Cross-Border Energy Trading: With the assistance of Blockchain, we can introduce decentralized and international energy trading in renewable energy.

10. Conclusion

The application of the blockchain technology holds merit in the spheres of upgrading the smart grids security with decentralizations, transparent, and immutable structures. The absence of the problem of trading energy safely, decency of identities, and identifying abnormalities and becoming one of the hottest topics of the modern energy system will be possible with blockchain. Although hybrid consensus mechanism, artificial intelligence, and sustainable blockchain system have their limitations on a larger scale, such as scalability, there exist future opportunities to build on the same. Implementation of blockchain is thus an essential step towards realisation of strong, secure and decisive smart grid systems.

References

1. Ahlgren, B., Hidell, M., & Ngai, E. C. (2020). The Internet of Things for smart cities: Interoperability and open data. IEEE Internet Computing, 24(1), 52–56.
2. Pulicherla, P. (2025). The Role of Quantum Computing in Strengthening Blockchain Security and Privacy Protocols. International Journal of Research in Engineering and Management Sciences, 8-12.
3. Huang, X., Zhang, Y., & Liu, J. (2022). AI and blockchain integration for smart grid anomaly detection. Future Generation Computer Systems, 135, 285–299.
4. Khan, M. A., Salah, K., & Rehman, M. H. (2021). Blockchain for secure energy trading in smart grids: Challenges and opportunities. IEEE Access, 9, 29698–29716.
5. Pulicherla, P. (2025). The Role of Quantum Computing in Strengthening Blockchain Security and Privacy Protocols. International Journal of Research in Engineering and Management Sciences, 8-12.
6. Li, Y., Zhang, H., & Wang, J. (2021). Consensus mechanisms for blockchain in energy trading: A comparative review. Renewable and Sustainable Energy Reviews, 135, 110368.
7. Pulicherla, P. (2017). An Enactment on Privacy Vulnerabilities of Encrypted IOT Traffic.
8. Vadivelan, N., Ramamurthy, A., & Padmaja, P. (2019). Minimizing energy consumption based on neural network in clustered wireless sensor networks. Journal of Computational and Theoretical Nanoscience, 16(2), 496-502.
9. Zhang, C., Wu, J., Zhou, Y., Cheng, M., & Long, C. (2019). Peer-to-peer energy trading in blockchain-enabled smart grids. Applied Energy, 220, 148–159.