Dandao Xuebao/Journal of Ballistics
ISSN: 1004-499X
Vol. 37 No. 1 (2025)

Blockchain-Secured and VPN Integrated Power Systems Management

[1]Revanth P S B.E., M.E., [2]Dr. Satheeshkumar M.E., Ph.D., [3]Dr. G. Karthikeyan M.E., Ph.D., [4]Dr. G. Suresh M.E., Ph.D., [5]Dr. C. Santhanalakshmi M.E., Ph.D.

[1]Sona College of Technology, Salem.

[2]Assistant Professor – Sona College of Technology, Salem.

[3]Associate Professor– Sona College of Technology, Salem.

[4]Assistant Professor – Sona College of Technology, Salem.

[5]Assistant Professor (Sr.Gd) – Sona College of Technology, Salem.

Abstract: - Integration VPN and blockchain technology for power system management provides a transformative approach to the user by addressing obstacles of data security transparency and efficiency with the help of decentralized energy grids. As a modern power system, it enhances its dependency on distributed renewable energy sources and integrated smart grids which require robust protection of data and operation integrity. Blockchain provides a decentralized immutable laser for securely recording energy transaction monitoring performance and protecting from unauthorized access. This ensures transparency by promoting trust among multiple stakeholders and reducing the risk of Cybercrime. Along with blockchain VPN integration ensures encrypted communication across the power grid and ensures encrypted data transmission between nodes. It is also capable of preventing authorized access and allowing the users to remote monitor securely with the help of a dual layout framework and real-time system optimization. It supports critical applications including energy trading platform demand response programs and improves data privacy and security. Integration with VPN-encrypted connectivity and blockchain-decentralized security power systems can achieve excellent resilience against cybercrime and operational disruptions. This integrated approach created an effective way for efficient and sustainable energy management that supports innovation and trust in a rapidly transforming energy landscape. The present study is going to explore the potential of the blockchain and VPN for securing power systems.

Keywords: VPN, Blockchain technology, Cybercrime, VPN encrypted connectivity , blockchain-decentralized security power, blockchain VPN integration

1.Introduction: - The modern power system underwent a significant transformation through the enhanced integration of renewable energy sources, coupled with decentralized energy resources and cutting-edge smart grid technologies. This transformation also introduces several complexities including data security risk in the efficiency of the system and managing the overall power system integrating with various enhanced technologies. In this situation, reliable decentralized management is required to manage modern power systems integrated with blockchain and VPN. Power systems have critical infrastructure that is vulnerable to cyber-attack disruptions and data breaches that require the adoption of effective security and management mechanisms. This particular research paper will explore the integration of virtual private network solutions and blockchain technology as a comprehensive framework to address all kinds of challenges within modern power system management.

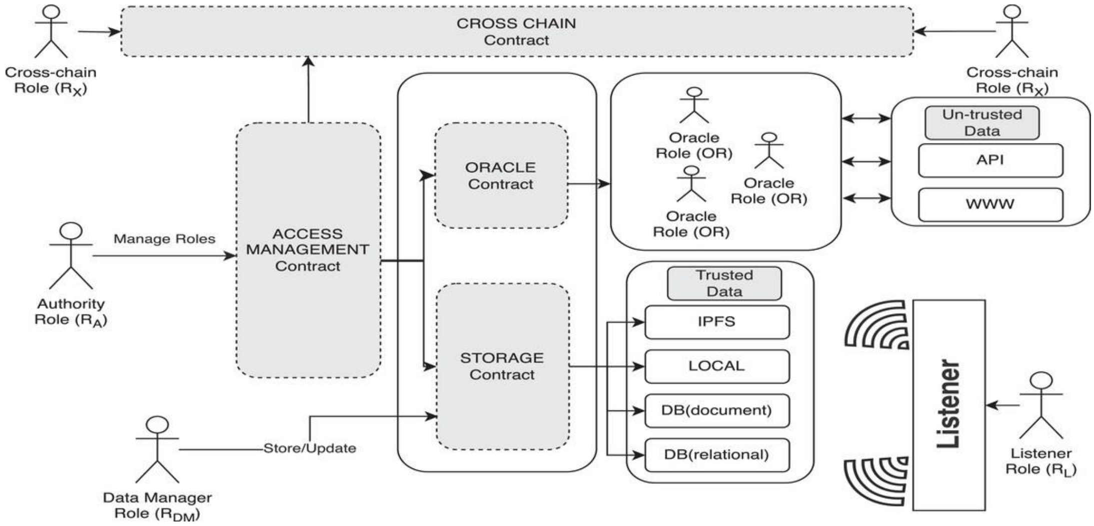


Figure 1 Structure of Cross Chain Contract

Blockchain technology is decentralized tamper-proof laser systems that provide effective transparency and Data integrity. Blockchain technology enables an Organisation to record its power system transactions securely. It is also capable of recording energy generation and distribution. Automatic agreements are embedded in the blockchain that are identified as smart contracts that are capable of streamlining the process including energy trading, load balancing, and bill generation.

Decentralization of the power system operation enhances reliability and also allows peer-to-peer energy trading by promoting sustainability and reducing operational costs. Along with blockchain technology VPN technology is also capable of providing secure communication channels among the distributed power it also safeguards sensitive operational data with the help of communication encryption between devices. Along with communication encryption it also controls centers and other system components to ensure a secure communication channel. Incorporating VPN technology into power system management safeguards data transmission integrity and secrecy, thereby reducing the threat of unauthorized system access by cybercriminals. VPN technology highlights the potential of the system by enhancing scalability security and operational resilience of the system while addressing the challenges of conventional centralized systems. The study is going to evaluate the methods used for power system management by integrating with the VPN promotion and blocks in technology. It is also going to identify the contribution of the ongoing development of a secure and efficient energy system to ensure sustainable critical power infrastructure which is developing in a digital and interconnected world.

2. Literature Review: -

2.1. Research Philosophy:- Research philosophy and its basic assumptions are important because they facilitate data gathering, analysis, and interpretation. Research philosophy is the primary component of gathering and analysing data and its results. This study's scientific position is developed using the "Positivism research philosophy" on which it is founded. In order to examine every step and preventative method for blockchain security and VPN-integrated power systems management, positivism is taken into consideration [1]. The research must be scientifically studied because it will provide and analyse integrated power systems management for blockchain security and VPN.

2.2. Research Approach: - The development and creation of a research design that depends on the formulation of a research design requires a research method. It serves a crucial function in facilitating the advancement of the research and its methodological framework.This research will be conducted using an inductive approach, which consists of specific observations and the initiation of a particular pattern [2]. Establishing a connection between VPN-integrated power systems management and blockchain security can be facilitated by an inductive approach. Therefore, it is crucial to have a research approach to build a concept for the study design.

2.3. Research Design: This research utilized a descriptive design, one of the three primary research approaches that also include explanatory and exploratory methods. Opting for a descriptive design proves beneficial as it facilitates the creation of foundational data, which can act as a springboard for guiding and shaping future research initiatives. It also helps to explore and explain an individual phenomenon of a group or a situation by describing characteristics and functions [16]. The overall design is rigid and structured which helps to complete the result in a structured way. It also supports probability sampling which enhances the possibility to acquire samples without bias. These specific designs assist the researcher in creating pre-planned statistical designs for analysis.

2.4. Search Strategy: - In order to search reliable and related data boolean search strategies have been used. This practice is effective for provide search results faster with more accuracy. General boolean operators like and, or and not have been used in the study. These logic-based operators help the search engine to narrow down the wide search results related to the topic [17].

2.5 Inclusion Criteria:- Articles and journals have been used that were acquired from Google Scholar and Scopus. With the help of the search strategy, 25 related articles have been acquired but among them, only 15 articles were used in this study. Several criteria have been followed for selecting the articles included in the study and they are mentioned below

- Articles that were published after 2019 have been included in this study.
- Articles with proper information about the author have been included
- Articles that have proper abstracts, introductions, methodology, outcomes, and conclusions have been included in the study
- Selected articles have proper references are information about the source

2.6 Ethical Consideration:- Ethical concerns are an essential element of the research because they develop the user about the reliability and innovation of the data offered. Research technique is a crucial component of research since it is necessary to go in a relevant direction when researching to continue the study on track and focus entirely on the subject without moving from it. This basis of study is a detailed examination of VPN Integrated Power Systems Management and blockchain security. A research paper on the assigned topic must uphold and adhere to the privacy and values that are necessary for appropriate ethics:

- *Ethical awareness:* Everything that has been collected is real and unedited. The journal articles are collected based on the necessary information for a secondary examination of the topic. Each journal article was collected from reliable and authentic sources. The statistics and substance of the articles are therefore reliable and authentic. The journals offer accurate and reliable information because they are all full-text and peer-reviewed.
- *Real and authentic searches:* All filters and search strategies are regarded as authentic and reliable. Databases require filtering, and papers that are rejected are eliminated and not considered for additional study.
- *Adequate information:* The facts and data collected for the report are real and provide accurate and genuine information. Every article was gathered from trustworthy and legitimate internet databases. They can be found freely on websites and in other public places.

3. Result

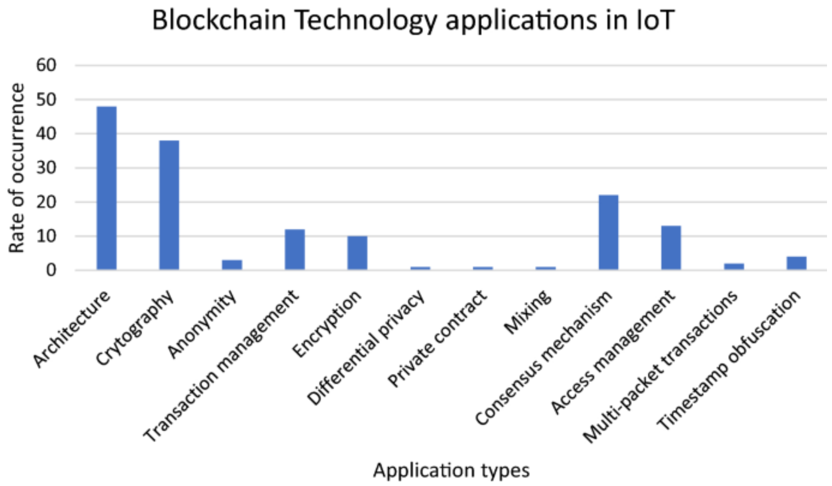
3.1. Importance of Blockchain Security– Blockchain security is one of the important aspects of blockchain-secured and VPN-integrated power system management as it enhances transparency, security, and accountability. Currently, power systems that incorporate decentralized renewable energy sources are becoming more complex. It is because the system becomes more distributed, that it needs a robust security protocol for ensuring reliable operation and safety from cybercrime. Blockchain is capable of offering an immutable, decentralized ledger that can record the transactions in power system management securely. Apart from transactions, it is also capable of recording energy exchange, metering, and smart grid data [15]. The characteristic of immutability ensures that data cannot be altered after it is recorded which provides a reliable audit trail for every activity in the system.

Integration with virtual private network technology also enhances the strength of blockchain security because it is capable of providing an encrypted communication channel within both public and private networks.

VPN ensures that the data exchange between decentralized Nodes including energy generators, consumers, and distributors is completed securely by ensuring data safety. Encrypted communication through VPN also reduces a risk related to data interception and unauthorized access which ensures that sensitive data and system control information about energy transactions remains secure [7]. A combination of VPN integration and blockchain security is capable of creating a decentralized resilient system for power system management. It also helps to enhance the trustworthiness of data transformation by ensuring real-time system updates and lowering the risk of Cyber-attacks which can disrupt grade operations that result in financial loss. The integration of these two technologies is vital in power systems that include multiple stakeholders. It also supports the framework of a power system with private enterprise government entities and customers as it provides secure efficient and transparent energy infrastructure.

3.2. Application of VPN Integrated Power System- Application of VPN integrated power systems becomes vital because the power grid transition is shifting to smart interconnected decentralized systems. Krrish because it provides secure encrypted communication by maintaining the confidentiality of data while it is exchanged within the power grid. It is very important in an environment where multiple stakeholders are included like energy production grid operations and consumers who interact in real time [9]. VPN ensures safe remote access for control of the system in smart grids by allowing the operators to monitor and manage energy distribution consumption and great performance from any location. It also ensures that the sensitive data is encrypted because remote access is essential for enhancing grid efficiency by responding to flaws and conducting predictive management without compromising system security. It also creates secure tunnels over public networks for preventing unauthorised access to complex infrastructures which is essential when a power system is distributed across diverse geographic areas.

It is also effective in renewable energy integration where diverse power sources are used including wind energy, solar energy, and energy storage systems are continuously increasing toward decentralization.Virtual Private Networks (VPNs) enable these systems to establish secure connections with central management hubs, facilitating real-time monitoring of energy production and usage. Maintaining equilibrium between supply and demand, as well as enhancing energy distribution, is crucial. In addition, it allows the operators a secure energy trading platform for consumers and producers who can exchange energy without the risk of data breaches [8].It is helpful for the system to manage supply and demand by supporting demand response programs by enabling secure encrypted communication between energy providers and consumers. It allows consumers to adjust their energy utilization according to the requirement, and financial incentive without compromising data privacy.



3.3 Importance for Blockchain-Based Secure Framework for Data Management: -

In today's digital environment, where data security, transparency, and integrity are crucial, there is a growing necessity for a blockchain-based system to manage data securely. This approach is highly valuable and essential for companies, as it addresses the increasing demand for robust data protection in the current technological landscape. Centralized data management systems are vulnerable to database and cyber-attacks because of the excessive possibility of unauthorized access and hacking. Blockchain technology has characteristics like decentralization and immutable which offer more robust solutions for data safety and it also ensures that data cannot be altered or tampered with when it is once recorded. It is currently used in different sectors including accounts, supply chain management and healthcare where data privacy is critical. In this sector, blockchain-based frames provide secure data transmission by lowering the risk of manipulation of the data [13]. The cryptography characteristic of blockchain ensures that all data transactions and exchanges are encrypted by protecting sensitive information. Moreover, blockchain provides real-time tracking of data with auditable history enhancing accountability and transparency. Blockchain technology enables consumers to engage in peer-to-peer electricity trading without relying on a centralized provider. Additionally, blockchain utilizes energy cryptocurrency, which offers anonymity and confidentiality for cryptocurrency transactions [12].

3.4 Drawbacks:- Decentralization, a fundamental aspect of blockchain technology, comes with inherent costs that significantly impact energy systems. Among the various blockchain platforms utilized in energy-related applications, Ethereum and Bitcoin stand out as prominent examples. Both of these platforms employ Proof of Work (PoW) as their consensus mechanism. This approach necessitates that network nodes tackle complex hash puzzles, a process that substantially increases energy consumption and associated expenses. Blockchain is a decentralization system that requires redundant data storage therefore each blockchain node requires a copy of the data that enhances the storage cost. High cost of the fully decentralized power system impacts the practice of blockchain-based energy systems. In addition, slow mining for consensus is also a limitation of blockchain in the power system [14]. Low query speed is also a challenge for the Blockchain because the Blockchain size grows continuously and the search strategy is required to adopt accordingly and slowly becomes much slower than the rate of growth. Limited block size is also a challenge for blockchain and VPN-integrated power systems.

The scalability of blockchain systems is hindered by their consensus mechanism, which limits their ability to manage increased workloads effectively. While blockchain technology purports to offer key security features such as immutability, resistance to single points of failure, and anonymity, it remains vulnerable to various cyber threats. The use of decentralized blocks in system information enables transparency through the sharing of ledgers among all participants using cryptographic methods [11]. However, the privacy and transparency aspects of blockchain are not flawless and may conflict with each other. Additionally, blockchain faces challenges in addressing real-world trust issues. Although blockchain data is difficult to alter, there is no guarantee of the reliability and authenticity of information before it is recorded in the blockchain.

4. Discussion

4.1. Importance of Blockchain Security: - Blockchain security is the application of cybersecurity best practices, technologies, and principles to reduce risk and prevent unauthorised access and harmful attacks on blockchain networks. Although "Distributed Ledger Technology (DLT)" powers all blockchains, not all of them are equally safe or functional. Although both public and private blockchains have positive and negative aspects of their own, the open versus restricted nature of their networks results in fundamentally different security models [3]. Crypto phishing attacks take advantage of people by tricking them into disclosing confidential information, including passwords or private keys, usually by using a fake website or message that looks real. Blockchain bridges are instruments that improve the “Decentralised Finance (DeFi)” ecosystem by enabling the smooth transfer of assets across various blockchain networks.

The substantial network latency undermines consistency guarantees, making HLF version 1.2.1 unsuitable for critical applications like banking or trading. A performance analysis of private blockchain Ethereum focused primarily on the Pow-based Geth and PoA-based Parity clients. Parity demonstrated superior performance, processing transactions 89.82% faster across various workload fluctuations [19]. The effect of significant network delays on fabric performance was examined. A method utilizing Palladio Workbench and simulation was employed to predict the latency of blockchain-based applications [19]. The evaluation of latency in a private Ethereum (Geth) testing environment achieved a low relative error in response time of approximately 10%. Following the development of Blockbench, three cryptocurrencies were evaluated: Ethereum (geth v1.4.18), Parity (v1.6.0), and HLF (v0.6.0-preview). HLF outperformed Ethereum and Parity in both macro and micro benchmarks [19]. However, HLF encountered scaling issues at 16 nodes. Additionally, it was noted that Ethereum and HLF faced challenges due to consensus mechanisms.

A custom-designed workload was used to successfully evaluate HLF v0.6 with PBFT, HLF v1.0 with BFT-SMaRt, and Ripple [19].This action was taken to address the challenges of comparing multiple blockchains. Bridges are a popular target for hackers since they store a lot of valuables and are not as secure as blockchains. An ecosystem attack is more likely to affect a blockchain with fewer servers than one with many, evenly spaced nodes. On blockchains like Bitcoin or Ethereum, for example, Sybil assaults or 51% attacks are now nearly hard to execute because of the amount of computational ability or assets needed [3]. However, it is important to be aware of the entire range of dangers, especially when the company is thinking about creating its blockchain or using smaller, emerging models.

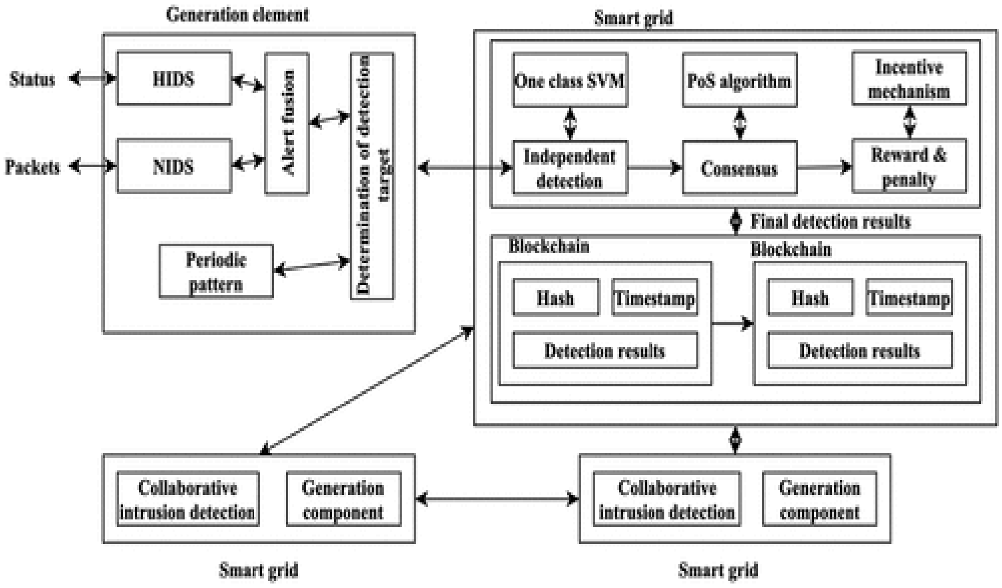
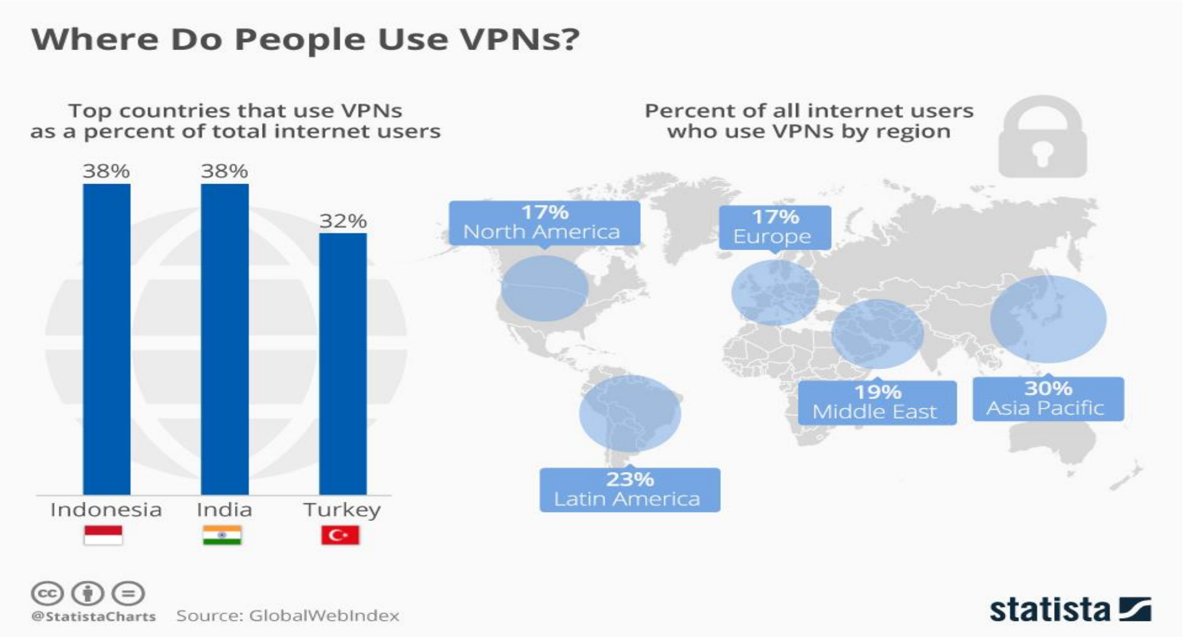


Figure 3 Blockchain Based Collaborative for Smart Grid Security

4.2. Application of VPN Integrated Power Systems Management: - A Virtual Private Network (VPN) serves as an intermediary between users and the internet, concealing their IP address and providing a secure connection through a private service rather than their usual Internet Service Provider (ISP). This encrypted pathway safeguards users' locations, personal information, and other data while enabling internet access. All network communications are routed through the VPN instead of the user's computer, ensuring a protected connection [4]. Emerging security frameworks prioritize trust verification at every step, offering robust defense against evolving cyber threats. Advanced encryption techniques are employed to shield VPNs from potential quantum threats, thereby securing business networks. The integration of artificial intelligence and machine learning enhances VPN capabilities, providing proactive security measures and adaptive threat detection. VPNs are being revolutionized by blockchain technology, which offers decentralized, impenetrable solutions for enhanced privacy and secure data transmission. It is crucial to evaluate the impact of these advancements on corporate security and compliance, ensuring VPNs adhere to legal requirements. Streaming platforms like Netflix, Hulu, and Amazon Prime Video offer different content to users in various countries [4]. By utilizing a VPN, streaming customers can access content intended for viewers in other regions.

4.3. Necessity of Blockchain-Based Secure Data Management Framework:- Blockchain technology creates a flexible framework to ensure safe management of data in the unmanned systems, IoT, and aviation industries. The framework's distinctive clustered architecture developed intentionally to fill in research gaps, improve scalability, and effectively handle the complexity of component interactions in major networks. Custom consensus mechanisms to meet the framework's operating requirements are integrated due to architectural development [6]. The system protects data from internal and external threats using an exact approach. DU uses V_{key} and Algorithm 1 to calculate QK and uses the API to deliver it as a requests message to the framework. When the number of access times surpasses n or the access time surpasses t, the permission verification cannot be passed, suggesting that the DU is unable to pass the data access permission verification [18]. The framework uses authentication and authorisation methods and role-based access control, to meet the security needs for handling sensitive data. This highlights the framework's dedication to ensure complete security by combining various technology, such as drones, IoT devices, and aircraft, offering range in processing power and blockchain technology access and perform specific jobs [5]. This means the entire process; all participants must adhere to unalterable regulations. establishing a unique, restricted-access blockchain system intended especially for identity management.

Blockchain technology's decentralised infrastructure could strengthen the security and legitimacy of IoT data management. Blockchain can improve system stability and reduce centralised management issues because it does not rely upon specific centralised nodes for data storage and processing, compared to traditional centralised designs [18]. It also has the qualities of non-repudiation, accountability, and trust, which makes it an attractive option for increasing data exchange while resolving issues with trust. an access-control system built on blockchain that gives data owners the ability to safely grant, audit, and remove access privileges. It is inappropriate for complex blockchain issues because of its high execution costs, which result from the need of advanced cryptographic processes.



Source: GlobalWebIndex

Figure 4 Necessity of VPNs

5. Challenges of Blockchain and VPN Integration in Power Systems Management:-

The combination of blockchain and VPN technologies presents notable benefits for managing power systems, but there are hurdles to overcome before their full potential can be realized. A key issue is the substantial expense linked to decentralization. For instance, the consensus mechanisms employed by blockchain platforms such as Ethereum and Bitcoin rely on computationally demanding processes like Proof of Work (PoW). These mechanisms require extensive calculations and consume considerable amounts of energy. This naturally increases operational costs but also brings into the spotlight the environmental aspect behind blockchain systems. Moreover, a decentralized system like blockchain requires redundant data storage at each node, as it necessitates a copy of the ledger at each node, thereby making storage costs astronomical. The financial and environmental challenges can discourage the widespread use of blockchain technology by power systems, especially in resource-constrained environments [14].

Another major challenge for blockchain systems is scalability. As the blockchain's size increases so does the time to process and validate transactions. The query speed then slows down. This could be a significant issue in real-time applications such as power systems management, especially where real-time data process is of prime importance. Moreover, the inherent consensus mechanisms of blockchain systems limit their ability to handle increased workloads, which makes it difficult to scale these systems to meet the demands of large, complex power grids. It is essential to address these scalability issues so that blockchain technology can support the growing complexity of modern power systems [11].

Privacy and transparency are also major challenges in blockchain-based systems. Transparency in blockchain assures that all the transactions are made visible and also auditable; however, that can conflict with the need to maintain data privacy, especially within sensitive applications, such as in energy trading. Therefore, finding a way through which blockchain systems can balance their transparency with a certain level of privacy is highly essential in fostering trust among its stakeholders.Moreover, while blockchain technology ensures data immutability and resistance to tampering, it cannot guarantee the authenticity of information prior to its entry into the blockchain system. This makes it question the reliability of blockchain systems in practice applications, wherein data accuracy and integrity are of paramount importance [11].

6. Advantages of Blockchain and VPN Integration in Power Systems Management:-

Despite these difficulties, the convergence of blockchain and VPN technologies can provide significant advantages in power system management. Enhanced security and transparency are among the most important advantages. The blockchain technology offers a distributed, unalterable record-keeping system that securely logs all transactions in a way that prevents modification. This creates a dependable trail of evidence for every event occurring within the power network. This transparency is particularly valuable in environments with multiple stakeholders, such as energy producers, grid operators, and consumers, as it fosters trust and accountability. Moreover, the integration of VPN technology further strengthens security by providing encrypted communication channels, ensuring that data exchanged between decentralized nodes remains confidential and protected from unauthorized access [7].

Enhanced operational efficiency is another significant advantage. The use of blockchain technology facilitates direct peer-to-peer (P2P) energy trading. Through this technology, consumers can directly sell electricity to producers without the need for intermediaries, resulting in reduced transaction costs and increased flexibility and resilience in power systems. To do this efficiently, VPN plays a critical role in providing real-time data interexchange between involved stakeholders through its secure, encrypted communication channels. This combination of blockchain and VPN technologies creates a decentralized, resilient system that can adapt to the dynamic demands of modern power grids, improving overall system efficiency and reliability [8].

The integration of blockchain and VPN technologies also supports the transition to renewable energy. As power systems increase their utilization of decentralized energy sources such as wind, solar, and energy storage systems, there is an ever-increasing demand for the management of secure data. The application of blockchain technology provides a safe platform for recording and managing energy transactions. This is supplemented by VPNs to ensure confidentiality and protection of data exchanged between decentralized energy sources and central management hubs. This provides for real-time monitoring of energy production and consumption, which helps balance the supply and demand while optimizing the energy flow. Also, blockchain-based frameworks support the use of energy cryptocurrencies, which guarantee anonymity and privacy of transactions of data further enhancing the security and efficiency of renewable energy systems [12].

7. Future Directions for Blockchain and VPN Integration in Power Systems Management:-

The integration of blockchain and VPN in future power systems presents significant opportunities for advancement and change. Key areas of focus include creating energy-efficient consensus mechanisms to address the high energy usage and operational expenses associated with blockchain systems. Traditional methods like Proof of Work (PoW) are unsustainable due to their resource-intensive nature. Future research should explore alternative approaches such as Proof of Stake (PoS) or Delegated Proof of Stake (DPoS), which require significantly less energy and computational resources. These mechanisms could reduce the environmental impact of blockchain systems while preserving security and decentralization, making large-scale implementation in power systems management more feasible [14].

Another promising avenue is combining blockchain with cutting-edge technologies like Artificial Intelligence (AI) and Internet of Things (IoT). AI can bolster the security and efficiency of blockchain systems through advanced threat detection and predictive analytics. For example, AI algorithms could be employed to identify and counteract potential cyberattacks on blockchain networks, safeguarding data integrity and security. Blockchain technology enables IoT devices to securely exchange data, offering real-time monitoring and control capabilities for decentralized energy sources. This system, in terms of combining blockchain, AI, and IoT, can result in a smart power system that can be both safe and efficient by adapting to modern energy grids dynamic demands [18].

One important challenge is related to scalability with blockchain systems and large complex power grids. Future research should be directed toward scalable blockchain architectures that can handle increased workloads without degrading performance. One such technique is sharding, which splits the blockchain into smaller, more manageable segments that can be processed in parallel, thereby improving the scalability of blockchain systems and making them more suitable for real-time applications in power systems management. In addition, layer-2 solutions, such as Lightning Network, can improve the scalability of blockchain systems by allowing off-chain transactions that are later settled on the main blockchain [11].

Lastly, the ethical and regulatory implications of blockchain and VPN integration in power systems management must be considered. As these technologies become more widespread, clear guidelines and regulations must be established to ensure their ethical use. One of the issues is data privacy, transparency, and accountability. Policymakers and industry stakeholders have to come together to develop frameworks that will move together in consideration of the benefits and threats of blockchain and VPN technologies, in protecting user privacy, and ensuring fair and equitable access to energy resources. It has the potential to transform power systems management by bringing a more secure, efficient, and sustainable energy future through tackling such challenges and opportunities in blockchain and VPN technologies [19].

8.Conclusion:- The integration of blockchain and VPN technologies has significant prospects for the revolutionization of the management of power systems, with regard to safety, transparency, and efficiency. Blockchain ensures an immutable and decentralized ledger, where data integrity can be guaranteed; VPNs secure communication channels and allow data to be exchanged efficiently. These two technologies combine a resilient and adaptable system that matches the dynamic demand of modern power grids. However, it's still full of challenges and areas that are challenging in cost, scalability, and privacy for all these technologies.

Future studies and research need to be made more energy efficient at consensus mechanisms in blockchain, enhancing the scalability in blockchain, as well as implementing blockchain integration into emerging technologies, such as AI and IoT, while careful thought must go to the ethics and regulations governing both blockchain and VPN integration in all their forms of use. The revolution in blockchain and VPN technologies will determine the crucial role they will play by providing a platform of secured, efficient, and sustainable power systems to a resilient energy future.

References

1. C. A. Saliya, *Social Research Methodology and Publishing Results: A Guide to Non-Native English Speakers: A Guide to Non-Native English Speakers*. IGI Global, 2023.
2. Mohajan and Mohajan, “Constructivist Grounded Theory: a new research approach in social science,” *Research and Advances in Education*, no. 1(4), pp. 8–16, 2022, [Online]. Available: https://www.paradigmpress.org/rae/article/download/256/223
3. C. Team, “The Importance of Blockchain Security,” *Chainalysis*, May 15, 2024. https://www.chainalysis.com/blog/blockchain-security/
4. “How does a VPN work? Advantages of using a VPN | Fortinet,” *Fortinet*. https://www.fortinet.com/resources/cyberglossary/how-does-vpn-work

5. O. Zorlu and A. Ozsoy, “A blockchain-based secure framework for data management,” *IET Communications*, vol. 18, no. 10, pp. 628–653, May 2024, doi: 10.1049/cmu2.12781.

6. H. M. S. E. MSi, M. M. S. E. Cwm M. Si. ,. Cipm. ,., S. E. M. M. Cokki, and S. S. S. E. MSi, *Marketing Digital: Konsep Entrepreneurship UMKM*. Nas Media Pustaka, 2023.

7. Suo, S., Chen, L., Cheng, R., Kuang, X., & Zou, J. (2021, December). Design of secure access to distributed load resources of a virtual power plant based on a virtual communication private network. In *2021 IEEE Sustainable Power and Energy Conference (iSPEC)* (pp. 4142-4149). IEEE.https://ieeexplore.ieee.org/abstract/document/9735489/

8. Akinsanya, M. O., Ekechi, C. C., & Okeke, C. D. (2024). Virtual private networks (VPN): a conceptual review of security protocols and their application in modern networks. *Engineering Science & Technology Journal*, *5*(4), 1452-1472.https://www.fepbl.com/index.php/estj/article/view/1076/1300

9. Baran, P., Varetsky, Y., Kidyba, V., Pryshliak, Y., Sabadash, I., & Franchuk, O. (2022). VPN-based monitoring power system facilities. *Przegląd Elektrotechniczny*, *98*(5), 16-19.http://pe.org.pl/articles/2022/5/3.pdf

10. Zadsar, M., Abazari, A., Ameli, A., Yan, J., & Ghafouri, M. (2022). Prevention and detection of coordinated false data injection attacks on integrated power and gas systems. *IEEE Transactions on Power Systems*, *38*(5), 4252-4268.https://drive.google.com/file/d/1zqRdQD2CZ2gd0IQsJM5Qr-uaTSXt_NZP/view

11. Gawusu, S., Zhang, X., Ahmed, A., Jamatutu, S. A., Miensah, E. D., Amadu, A. A., & Osei, F. A. J. (2022). Renewable energy sources from the perspective of blockchain integration: From theory to application. *Sustainable Energy Technologies and Assessments*, *52*, 102108.https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4071207

12. Livingston, D., Sivaram, V., Freeman, M., & Fiege, M. (2022). *Applying blockchain technology to electric power systems*. Council on Foreign Relations.http://www.ourenergypolicy.org/wp-content/uploads/2018/07/Discussion_Paper_Livingston_et_al_Blockchain_OR_0.pdf

13. Wang, T., Hua, H., Wei, Z., & Cao, J. (2022). Challenges of blockchain in new generation energy systems and future outlooks. *International Journal of Electrical Power & Energy Systems*, *135*, 107499.http://jcao.org/pub/doc/jcao_j_blockchainsurvey.pdf

14. Adeyemi, A., Yan, M., Shahidehpour, M., Botero, C., Guerra, A. V., Gurung, N., ... & Paaso, A. (2020). Blockchain technology applications in power distribution systems. *The Electricity Journal*, *33*(8), 106817.https://fardapaper.ir/mohavaha/uploads/2021/04/Fardapaper-Blockchain-technology-applications-in-power-distribution-systems.pdf

15. Siedlecki, S. L. (2020). Understanding descriptive research designs and methods. *Clinical Nurse Specialist*, *34*(1), 8-12.https://www.academia.edu/download/114343622/nur.0000000000000493 20240509-1-tfem8r.pdf

16. Scells, H., Zuccon, G., Koopman, B., & Clark, J. (2020, April). Automatic boolean query formulation for systematic review literature search. In *Proceedings of the web conference 2020* (pp. 1071-1081). https://ielab.io/publications/pdfs/scells2020conceptual.pdf

17. T. Hu *et al.*, “N-Accesses: A Blockchain-Based Access Control Framework for Secure IoT Data Management,” *Sensors*, vol. 23, no. 20, p. 8535, Oct. 2023, doi: 10.3390/s23208535. Available: https://doi.org/10.3390/s23208535

18. Y. Y. Ghadi *et al.*, “The role of blockchain to secure internet of medical things,” *Scientific Reports*, vol. 14, no. 1, Aug. 2024, doi: 10.1038/s41598-024-68529-x. Available: https://doi.org/10.1038/s41598-024-68529-x