Review of Blockchain Algorithms for Security and Power Management in 6G

S.Janani[1], S.G.Hymlin Rose[2], Ms. Manju.K[3] ,Ms. Sujitha.S[4] ,Ms. Sruthi Rega K[5]
[1]Associate Professor, Department of ECE, Periyar Maniammai Institute of Science & Technology,Vallam,drsjananiece@gmailcom
[2]Associate Professor,Department of ECE,R.M.D. Engineering College, Kavaraipettai, India, hymlinrose@gmail.com
[3,4,5] UG Student,Department of ECE,Periyar Maniammai Institute of Science & Technology,Vallam

Abstract.
While 6G networks promise unprecedented advances in communication technologies, they also pose challenges in ensuring robust security and efficient power management. Blockchain, with its decentralized architecture and tamper-proof nature, represents a promising alternative for improving security and optimizing power management in 6G. This paper looks at various blockchain algorithms and their applications for tackling important security challenges and power efficiency requirements in 6G networks. We discuss the most recent developments, problems, and future directions for incorporating blockchain into 6G.
Keywords. Blockchain-technology, blockchain algorithm, Power-management, security, 6

[1] INTRODUCTION

The proliferation of wireless devices in recent decades, particularly smartphones, has caused LTE networks to reach saturation and 5G to develop. 5G uses large MIMO and ultra-dense networks to fulfill the demands of 20 Gbps speeds, high connection density, and low latency. Sixth-generation (6G) network research attempts to outperform 5G in terms of dependability, connectivity, and spectrum efficiency. Nonetheless, there are still issues with energy efficiency, security, and network complexity [1].

Blockchain technology, known for its decentralization and security features, has emerged as a viable answer to 6G's security and power management concerns. This research looks at blockchain algorithms designed for safeguarding 6G networks and improving power management [2]. An even larger number of Internet of Things (IoT) devices—which are frequently vulnerable to security flaws—will be supported by 6G.

According to several predictions, 6G will be mostly used for commercial, industrial, and military uses, with a few consumer uses like immersive entertainment [4]. Higher frequencies in the wireless spectrum are used by both 5G and 6G to deliver data more quickly. With 6G, speeds up to 1000 times faster than 5G will be possible, as the technology will operate at frequencies ranging from 95 GHz to 3 terahertz (THz), while 5G runs in the sub-6 GHz and over 24.25 GHz bands (lower and big band frequencies) [5].

One of the most important metrics for 5G and 6G is latency, or the amount of time it takes for data to move across a network. In 4G, latency is roughly 50 milliseconds, whereas in 5G, it lowers to 5 milliseconds—a tenfold reduction. Massive data transmission will be made possible by 6G's estimated 1 millisecond latency, which will enable almost instantaneous data transfers[6].

[2] LITERATURE SURVEY

Blockchain and hybrid cryptography solutions can successfully handle the security concerns posed by the convergence of satellite and wireless communications in 6G networks. Blockchain technology is crucial to maintaining data security and integrity in 6G, especially for AI-powered apps that improve intelligent services like self-driving cars and indoor location. Blockchain greatly enhances the integrity of sensitive data in intelligent transportation systems by decreasing data tampering and boosting credibility [17][22].

Furthermore, effective energy trading and decentralized energy management depend on blockchain's capacity to improve security and transparency in energy transactions, promoting wise power use and low energy consumption. Blockchain's position in smart grids and renewable energy management is part of its rapidly growing applications in energy trading and power management within 6G networks [10].

[3] BLOCKCHAIN ALGORITHMS FOR SECURITY IN 6G

3.1 Consensus Algorithms

Blockchain integration with 6G networks relies on consensus techniques to offer secure, efficient, and dependable communication systems. In the context of 6G networks, high-performance and efficient consensus algorithms are required to meet the high data rates and demands of next-generation communication systems. One interesting technique is to combine Directed Acyclic Graph (DAG) with sharding, which greatly increases transaction throughput by processing several transactions simultaneously, boosting resource use and scalability [11][12].

On the security front, Post-Quantum Blockchain Consensus (PQBC) algorithms are intended to protect blockchain systems from quantum computing threats, assuring data integrity and privacy in the face of potential quantum adversaries [14]. Choosing the right blockchain types and consensus algorithms is particularly crucial for addressing the security requirements of 6G applications, such as data integrity, non-repudiation, and auditability [10].

3.2 Smart Contracts

Blockchain smart contracts, which provide decentralized and trust-free solutions, can help address 6G's security challenges. The incorporation of blockchain technology into 6G networks offers a compelling answer to the privacy and security concerns connected with these sophisticated communication technologies. One novel method is the creation of a Blockchain Radio Access Network (B-RAN) model, which promises to increase both efficiency and security in 6G networking by exploiting blockchain technology's unique qualities [17][19].

3.3 Hybrid Cryptographic Approaches

The merging of wireless and satellite communications in 6G networks creates security concerns that can be addressed using blockchain and hybrid cryptographic techniques. Blockchain technology is critical to assuring data integrity and security in 6G networks, especially for AI applications that improve intelligent services like indoor location and autonomous vehicles. Blockchain improves the integrity of sensitive information in intelligent transportation systems by reducing data tampering and increasing credibility [22][23]. To improve data privacy and security in blockchain-based storage systems, hybrid cryptographic techniques combining several cryptographic algorithms, including as RC6, AES, and DES, are being investigated; nevertheless, scalability and performance issues remain crucial [19].

4. BLOCKCHAIN FOR POWER MANAGEMENT IN 6G

Blockchain's potential to increase security and transparency in energy transactions has led to its consideration for power management in 6G networks. Energy trading may become more effective as a result. The decentralized, transparent, and secure characteristics of blockchain enhance energy systems' dependability and efficiency, which is critical as demand rises and more renewable energy is used. The DE-BFT algorithm is one technique that lowers communication costs and boosts throughput, making it more appropriate for energy applications [23]. In distributed energy systems, hybrid techniques that combine algorithms such as Raft and IBFT help to improve security, scalability, and reliability.

5. FUTURE DIRECTION OF 6G NETWORKS

In order to meet the demands of a fully connected society by 2030 and beyond, as well as to address the limits of 5G, 6G networks are being developed. Global coverage, increased efficiency, greater intelligence, and higher security are the goals of 6G.

Integration and Worldwide Coverage of Non-Terrestrial Networks: In order to create a space-air-ground-sea communication network, 6G will combine terrestrial, satellite, and unmanned Aerial Vehicle (UAV) networks [24]. Use of Broader Spectrum Bands: In order to boost data rates and connection density, 6G will investigate all accessible spectra, including sub-6 GHz, millimeter wave (mmWave), terahertz (THz), and optical frequency bands [22]. Learning and Artificial Intelligence: In 6G, AI and ML will be essential for intelligent transceivers, network automation, adaptive communication environments, and real-time network status learning. Reflecting Surfaces with Intelligence (IRS): Wireless communication channels will be managed by IRS technology, improving spectrum and energy efficiency. New Use Cases and Applications: 6G will enable new applications such as extended reality (XR), high-fidelity mobile holograms, and the Internet of Space Things [19]

6. Conclusion

The integration of non-terrestrial networks, the use of broader spectrum bands, and the integration of cutting-edge AI, ML, and quantum technologies define the future trajectory of 6G networks. Network performance will be further enhanced by cell-free massive MIMO, intelligent reflecting surfaces, and enhanced security. The demands of a fully connected world will be met by 6G thanks to edge computing, network slicing, and an emphasis on sustainability, enabling new and creative applications. Thus it is going to be a standard parameter for transmission in all upcoming trends in technologies.

References

[1] E. Oughton, Z. Frias, T. Russell, D. Sicker, and D. D. Cleevely, "Towards 5G: Scenario-based assessment of the future supply and demand for mobile telecommunications infrastructure," Technological Forecasting and Social Change, vol. 133, pp. 141-155, 2018, doi: 10.1016/j.techfore.2018.03.016.

[2] A. Kumari, R. Gupta, and S. Tanwar, "Amalgamation of blockchain and IoT for smart cities underlying 6G communication: A comprehensive review," Comput. Commun., vol. 172, pp. 102–118, 2021.

[3] Z. Yang, M. Chen, K. K. Wong, H. V. Poor, and S. Cui, "Federated learning for 6G: Applications, challenges, and opportunities," Engineering, vol. 8, pp. 33–41, 2022.

[4] S. B. Prathiba et al., "Federated learning empowered computation offloading and resource management in 6G-V2X," IEEE Trans. Netw. Sci. Eng., 2022.

[5] L. Mucchi, "Physical-layer security in 6G networks," IEEE Open J. Commun. Soc., 2021.

[6] N. Nomikos et al., "A survey on reinforcement learning-aided caching in heterogeneous mobile edge networks," IEEE Access, 2022.

[7] Z. Zhang et al., "A many-objective optimization based intelligent intrusion detection algorithm for enhancing security of vehicular networks in 6G," IEEE Trans. Veh. Technol., 2021.

[8] J. Li et al., "Joint virtual network topology design and embedding for cyber-twin-enabled 6G core networks," IEEE Internet Things J., 2021.

[9] Y. Sun et al., "When machine learning meets privacy in 6G: A survey," IEEE Commun. Surv. Tutor., vol. 22, pp. 341–366, 2020.

[10] A. Khan et al., "Blockchain and 6G: The Future of Secure and Ubiquitous Communication," IEEE Wireless Commun., vol. 29, no. 1, pp. 194-201, 2021.

[11] J. Xie, K. Zhang, Y. Lu, and Y. Zhang, "Resource-Efficient DAG Blockchain with Sharding for 6G Networks," IEEE Network, vol. 36, pp. 189-196, 2022.

[12] X. Fu, H. Wang, and P. Shi, "A survey of Blockchain consensus algorithms: mechanism, design and applications," Science China Information Sciences, vol. 64, 2020.

[13] S. Bamakan, A. Motavali, and A. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," Expert Syst. Appl., vol. 154, p. 113385, 2020.

[14] J. Gomes, S. Khan, and D. Svetinovic, "Fortifying the Blockchain: A Systematic Review and Classification of Post-Quantum Consensus Solutions for Enhanced Security and Resilience," IEEE Access, vol. 11, pp. 74088-74100, 2023.

[15] J. Yusoff, Z. Mohamad, and M. Anuar, "A Review: Consensus Algorithms on Blockchain," Journal of Computer and Communications, vol. 10, no. 9, pp. 1-7, 2022.

[16] F. Yang et al., "Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism," IEEE Access, vol. 7, pp. 118541-118555, 2019.

[17] V. S. et al., "Blockchain Based Privacy Preserving Framework for Emerging 6G Wireless Communications," IEEE Transactions on Industrial Informatics, vol. 18, pp. 4868-4874, 2022.

[18] A. Singh et al., "Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities," Comput. Secur., vol. 88, p. 101654, 2022

[19] J. Wang, X. Ling, Y. Le, Y. Huang, and X. You, "Blockchain-enabled wireless communications: a new paradigm towards 6G," National Science Review, vol. 8, 2021.

[20] S. Wang et al., "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, pp. 2266-2277, 2019.

[21] A. Lone and R. Mir, "Applicability of Blockchain smart contracts in securing Internet and IoT: A systematic literature review," Comput. Sci. Rev., vol. 39, p. 100360, 2021.

[22] S. Kushwaha et al., "Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract," IEEE Access, vol. 10, pp. 1-1, 2022.

[23] R. Zhang, R. Xue, and L. Liu, "Security and Privacy on Blockchain," ACM Computing Surveys (CSUR), vol. 52, no. 1, pp. 1 - 34, 2019.

[24] S. Kushwaha et al., "Ethereum Smart Contract Analysis Tools: A Systematic Review," IEEE Access, vol. 10, pp. 1-1, 2022.

[25] T. Maksymyuk et al., "Blockchain-Empowered Framework for Decentralized Network Management in 6G," IEEE Communications Magazine, vol. 58, pp. 86-92, 2020.

Biographies

Dr.S.Janani is working as Associate Professor in Department of Electronics and Communication Engineering in Periyar Maniammai Institute of Science & Technology. She did her B.E. Degree (ECE) in Kumaraguru college of Technology, Coimbatore and M.E Degree (Communication systems) in Sri Sivasubramaniya Nadar college of Engineering, Chennai. She pursued her Ph.D. from Annamalai University. She has more than 15 years of teaching experience and her area of interest include RF & Microwave Engineering, wireless communication and networks. She presented many papers in various International Conferences, published 25 International Journals and 14 books. She is a member of ISTE, IEI and IEEE.

S.G. Hymlin Rose graduated from Noorul Islam College of Engineering, Kumaracoil, Anna University, Chennai, in Electronics and Communication Engineering during the year 2007. She obtained her Master degree in Communication Systems from Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam, Anna University, Chennai, during the year 2009. From 2009 to 2011 She has completed PhD in Information and Communication, Anna University in the year 2021. At present she is working as Associate Professor in the Department of Electronics and Communication Engineering at R.M.D Engineering College, Chennai, Tamil Nadu, India Her current area of research is security issues in wireless sensor networks. She is a Life member of ISTE.

Sujitha is an engineering student with a B.Tech (Hons.) in Electronics and Communication Engineering (ECE) from Periyar Maniammai Institute of Science & Technology, Vallam. She has expertise in advanced automation technologies, control systems, and robotics applications for industrial processes.

Manju is an engineering student with a B.Tech (Hons.) in Electronics and Communication Engineering (ECE) from Periyar Maniammai Institute of Science & Technology, Vallam. She has expertise in advanced automation technologies, control systems, and robotics applications for industrial processes.

Sruthirega is an engineering student with a B.Tech (Hons.) in Electronics and Communication Engineering (ECE) from Periyar Maniammai Institute of Science & Technology, Vallam. She has expertise in advanced automation technologies, control systems, and robotics applications for industrial processes.