Transactions on Engineering and Computing Sciences - Vol. 13, No. 03
Publication Date: June 12, 2025
DOI:10.14738/tmlai.1303.18933.
Hassan, A. & Ketel, M. (2025). Blockchain and Wireless Network Security: A Comprehensive Review of Techniques, Challenges, and Future Prospects. *Transactions on Engineering and Computing Sciences*, 13(03). 112-126.

Blockchain and Wireless Network Security: A Comprehensive Review of Techniques, Challenges, and Future Prospects

Abshir Hassan
Applied Information Technology Department
University of Baltimore, Baltimore, MD 21201, USA

Mohammed Ketel
Applied Information Technology Department
University of Baltimore, Baltimore, MD 21201, USA

ABSTRACT

In the history of digital ecosystems, security has always been and will continue to be a primary issue. Newer fields of study, such as blockchain and wireless networks, continue to confront the difficulties that are exclusive to them despite technological breakthroughs. This article provides an assessment of these two important domains, diving into their relevance and fundamental security methodologies, primary research, unsolved challenges, and prospective future paths. This article covers the key components of blockchain security and emphasizes the importance of wireless network security. A comparative study of the security of blockchain technology and wireless networks elucidates the distinctive qualities, difficulties, and solutions that each one presents. This paper also explores the synergistic integration of AI and blockchain to address the multifaceted security challenges in modern wireless networks.

Keywords: Blockchain, Wireless Networks, Security, AI, Wi-Fi, IoT, 5G/6G.

INTRODUCTION

Wireless networks and blockchain technology have completely changed how we communicate, connect, and do business in the digital age. Blockchain has revolutionized many industries because of its decentralized and transparent structure, making it possible to create safe, immutable transaction records. Wireless networks have simultaneously provided unrestricted connection and mobility, enabling people and things to remain linked on a global scale. However, as our dependence on these technologies increases, it is more important that they be secure.

Blockchain security guarantees the authenticity, clarity, and confidentiality of information stored on distributed ledgers. It is very safe and robust since it eliminates the need for centralized organizations and protects against hacking or data tampering [4]. Blockchain technology has been used in several industries, including banking, supply chains, healthcare, and voting systems, to improve security, dependability, and efficiency. On the other hand, wireless network security focuses on protecting data while it is being sent through wireless links [5]. Wireless networks are becoming prevalent, making them vulnerable to cybersecurity risks, including illegal access, surveillance, and data modification.

This article thoroughly analyzes blockchain and wireless network security, including their salient features, significance, core tactics, leading studies, open problems, and potential research routes. It explores the access control mechanisms, consensus algorithms, cryptographic techniques, and encryption procedures used in blockchain security. In the same way, it examines the authentication methods, firewalls, and intrusion detection systems used in wireless network security. The paper also compares the security of wireless networks to blockchain, highlighting their distinct characteristics, challenges, and solutions. It emphasizes the significance of ongoing research and development in these fields to address new dangers, technical advancements, and the evolving digital environment.

By grasping the importance of blockchain and wireless network security, and the methods and mechanisms used to ensure their protection and reliability, stakeholders can make educated decisions about these technologies' deployment and create adequate security measures [10]. Cross-disciplinary collaborative research efforts, encompassing cryptography, Artificial Intelligence (AI), and quantum computing, will be pivotal in enhancing the security of both blockchain and wireless networks, guaranteeing a secure and trustworthy digital environment for individuals and organizations.

The convergence of blockchain, wireless network security, and AI represents a significant leap forward in addressing modern cybersecurity challenges. This integration enhances the resilience of networks, especially in highly dynamic environments like IoT, 5G, and emerging 6G networks [24 - 27].

BLOCKCHAIN SECURITY

A blockchain is a decentralized database that stores records or provides a general guideline of all digital transactions or events carried out amongst all the parties participating in the network [8]. Blockchain technology allows for the authorization of transactions with brokers through the Internet.

The primary blockchain access mechanism is a peer-to-peer network that adheres to a protocol for verifying original pieces. Once data has been recorded, it cannot be retroactively changed in any particular chunk without modifying all the blocks and understanding most of the network. Bitcoins are a cryptocurrency that may also be used as digital payment [8]. Bitcoins are only accessible via online services such as PayPal, Citrus, or Paytm. When exchanged from one person to another through the Internet, virtual currencies are treated much like cash, even though they are not actual. Blockchain technology and cryptocurrency bitcoin have evolved into a platform analogous to the one on which civilizations have been conducting their daily business.

Key Features of Blockchain Security

The most crucial components of blockchain security are covered in this section, including its decentralization, transparency, immutability, data integrity, and algorithms.

Decentralization: Blockchain runs on a peer-to-peer network; therefore, a central authority is unnecessary [8]. This decentralized design assures that no one party has total control over the data.

Transparency and Immutability: Data is consistent once stored on the blockchain. An unbroken chain of records is created by cryptographically connecting every transaction or data input to the one before. Transparency is attained by the Blockchain's open visibility, which makes it possible for anybody to check and audit a transaction and establishes trust and accountability [11, 12].

Algorithms: Blockchain uses powerful cryptography algorithms to safeguard data and transaction data. Encryption methods, digital signatures, and hashing techniques safeguard information confidentiality and integrity. These cryptographic techniques guarantee that data is impenetrable to outsiders and that only those with the proper permissions may access or change it [11, 12].

Importance of Blockchain Security

One of the most significant benefits of using blockchain is that it enables control to be distributed among several nodes. No centralized authority may be compromised or brought down by malicious actors. Instead, the network comprises nodes, each responsible for storing its unique copy of the blockchain. To corrupt the blockchain, a hacker would need to compromise every node in the network, which is a task that is incredibly difficult to accomplish [11].

Data Integrity: Blockchain offers high data integrity, guaranteeing that information stored once cannot be changed or changed. This capability is essential in industries where data integrity and trust are critical, like banking, supply chains, healthcare, and voting systems [11].

Enhanced Privacy: Blockchain protects the secrecy of data via encryption methods. It lowers the risk of data breaches and illegal access by allowing users to control their personal information and choose how and when it is shared [11, 12].

Fraud Prevention: The transparency and audibility of blockchain technology make it possible to identify and stop fraud. The fact that transactions are recorded on a distributed ledger makes it impossible for fraud to occur since doing so would need agreement from most users [11].

Resilience and Fault Tolerance Blockchain: The decentralized design of blockchain improves resilience and fault tolerance. The network can endure assaults or node failures without jeopardizing the integrity of the whole system since there is no single point of failure. Applications in critical industries, like banking or healthcare, where continuous service is essential, need this resilience [11].

Trust and Disintermediation: Blockchain provides a trustless environment, eliminating the need for intermediaries like banks or outside auditors. Blockchain guarantees participant

confidence by relying on cryptographic methods and consensus procedures, lowering intermediaries' costs and complexity [8, 11].

Blockchain Security's Significance

This section outlines the necessity of blockchain security in rapidly developing industries.

Transformation of the Financial Industry: Blockchain technology has the potential to alter the financial industry by enabling safe and effective peer-to-peer transactions, lowering fraud, and doing away with the need for intermediaries.

Supply Chain Management: By enabling end-to-end visibility and traceability of items, blockchain has the potential to transform supply chain management. Companies can trace and verify each stage of the supply chain securely using blockchain security, from the procurement of raw materials through manufacture, distribution, and sale [2]. Transparency enhances product quality, boosts customer confidence, and helps in the fight against counterfeiting.

Healthcare and Medical information: Blockchain security may help with the difficulties of storing and exchanging private medical information. Healthcare providers may increase data accuracy, safeguard patient privacy, and simplify information exchange amongst various healthcare groups by securely storing and exchanging patient data on the blockchain [8]. Blockchain may also make the safe transmission of prescriptions, clinical studies, and medical research possible.

Voting Systems: Blockchain security can potentially improve the integrity and transparency of voting systems. Votes are recorded on an immutable blockchain, making it difficult for hostile parties to change or rig election outcomes [8]. Voting systems built on blockchain technology may facilitate distant voting, boost voter participation, and reestablish faith in the democratic system.

Intellectual Property Protection: Blockchain has the potential to contribute to the protection of intellectual property rights significantly. Creators may securely date their work and prove ownership by storing digital assets like patents, copyrights, and trademarks on the blockchain. This may aid in preventing unlawful use of intellectual property, counterfeiting, and plagiarism.

Internet of Things (IoT) Security: As IoT devices increase, substantial security issues must be addressed. Blockchain can provide a safe, decentralized framework for IoT devices to connect and share data without jeopardizing privacy or integrity [2]. IoT networks may authenticate devices, confirm data integrity, and reduce the danger of illegal access or control by employing blockchain security.

Fundamental Approaches and Mechanisms

Data integrity, confidentiality, and immutability are all ensured by the rigorous security methods used by blockchain technology. This section will examine blockchain security's

fundamental methods and tools, including access control systems, consensus algorithms, and cryptographic techniques [8, 11].

Hash Functions: transform input data into a fixed-length character string known as a hash, which is essential to blockchain security. A hash value differs noticeably when the input data is even slightly altered. Hash functions guarantee the integrity of data recorded on the blockchain. It is computationally impossible to tamper with the data since even a slight change would necessitate recalculating the hash for the affected and all succeeding blocks [11. 12].

Digital Signatures: In blockchain transactions, digital signatures provide authenticity and non-repudiation. They are produced using public-key cryptography, in which the signer generates a signature using their private key, and anybody with access to their public key may validate the signature's validity. Digital signatures guarantee that transactions cannot be changed or falsified and are signed by the appropriate parties [8, 11].

Encryption Algorithms: Sensitive data saved on the blockchain is encrypted to maintain secrecy. As a result, the encrypted data can only be accessed by persons granted access and the decryption key.

Consensus Algorithms: Consensus algorithms allow network members to agree on the legitimacy of transactions and the sequence in which they are added to the blockchain. Consensus methods that are often utilized include:

Proof-of-Work (PoW): The initial consensus method for blockchain, most famously utilized in Bitcoin, PoW, is still in use today. Much computer power is needed when miners compete to solve challenging mathematical riddles [12]. The blockchain's next block is added by the miner who completes the puzzle first, and they are rewarded with bitcoin. It is exceedingly complex for malevolent actors to maintain control of the blockchain because PoW ensures that the bulk of the network's processing power is honest.

Proof-of-Stake (PoS), a different consensus mechanism, chooses block validators based on their ownership or stake in the cryptocurrency. Based on the quantity of bitcoin they own and are prepared to "stake" as collateral, validators are selected to produce new blocks and verify transactions [12]. PoS lowers the energy requirements associated with PoW and strengthens the blockchain’s defense against 51% attacks [4].

Delegated Proof-of-Stake (DPoS): is a version of Proof-of-Stake (PoS) in which token holders elect a small number of "delegates" to be in charge of verifying transactions and building blocks. By enabling token holders to participate in the consensus process while lowering the processing needs, DPoS combines the advantages of decentralization and efficiency.

Practical Byzantine Fault Tolerance (PBFT): is a consensus mechanism developed specifically for blockchains with permissions. To agree on the legitimacy of transactions, a

certain number of copies, or nodes, are needed. When it comes to maintaining the integrity and liveness of the blockchain, PBFT can accept a certain number of unreliable or malicious nodes.

Access Control Techniques: Access control techniques are essential for the security and privacy of data kept on the Blockchain. They specify who can use, alter, and operate on the blockchain. Access control techniques often employed in blockchain security include:

- Public and private key cryptography: Access to blockchain transactions and data is restricted using public and private key pairs. Each participant is given their own set of keys. The participant's data may be encrypted; others can verify signatures thanks to the public key's open sharing [14]. Transactions are signed using the private key, which is also used to decode data that has been encrypted. This asymmetric cryptography guarantees private communication and secure authentication.
- Role-Based Access Control (RBAC): RBAC is a popular access control technique in blockchain systems. Based on preset roles, it distributes permissions and privileges. Access to blockchain resources is dependent on participant roles, which are allocated. Thanks to RBAC, which may carry out specific operations inside the blockchain network is precisely within your control.
- Smart contracts have their terms and conditions expressed in code and are self-executing. They make automation possible, enact preset guidelines, and regulate access. Only those given permission may interact with certain blockchain features or data, thanks to the ability of intelligent contracts to specify access rights and permissions.
- Multi-signature (Multisig) wallets: A transaction in a Multisig wallet requires several signatures from various parties [14]. This technique improves security by lowering the possibility of single points of failure and requiring the consent of numerous parties before a transaction is carried out. Enterprise blockchain applications and Bitcoin exchanges often use multiset wallets.

Immutable Ledger: An essential technique for guaranteeing data security and integrity is the blockchain ledger's immutability. Once information is stored on the blockchain, it is tough to change or remove it. A cryptographic connection between blocks is created because each block includes a hash of the one before. The hash of a block and all succeeding blocks must be changed to change any data in a block, which is computationally impossible. The integrity and auditability of transactions recorded on the blockchain are guaranteed by immutability [11, 12].

The architecture of blockchain technology consists of multiple layers, as depicted in Figure 1.

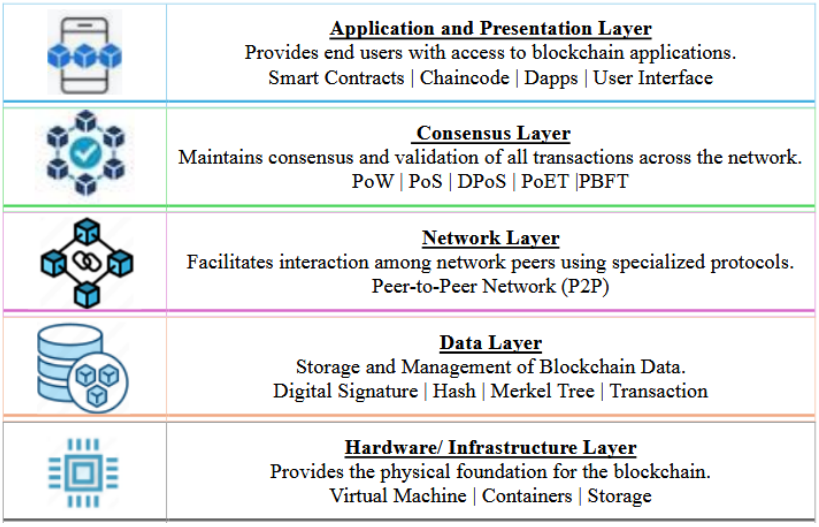

Figure 1: Layered Architecture of Blockchain

Challenges Facing Blockchain Security

Several obstacles remain despite the already available solutions. A 51% attack, in which an evil actor gets control over most of the network's hash power, can cause the blockchain as a whole to become corrupted. Other notable problems include flaws in smart contracts, risks posed by quantum computing to cryptographic concepts, and worries over protecting users' privacy in public blockchains.

Research in the future should focus on post-quantum cryptography, privacy-preserving mechanisms, and legislative frameworks to govern the usage of blockchain systems and ensure their safety. With the proliferation of decentralized finance (DeFi), ensuring the security of smart contracts also merits particular attention.

WIRELESS NETWORK SECURITY

Wireless networks have become widespread due to the proliferation of smartphones, tablets, laptops, and IoT devices. They provide people worldwide with seamless connections and enhanced mobility [9]. The security of wireless networks is crucial considering the expanding cyber threats. It guarantees data availability, confidentiality, and integrity while protecting users and businesses from violent assaults.

Relevance and Importance

Wireless network security is primarily concerned with protecting information during its transmission over a wireless network. This involves safeguarding data from unauthorized access and potential misuse. Given that any device can access that wireless signal within its range, the risk of unauthorized intrusion is higher than in wired networks, making robust security measures crucial.

Personal privacy is related to wireless network security's first layer of relevance. Data that, in the wrong hands, might result in identity theft, financial loss, or personal injury include private

emails, online banking information, and health records. Therefore, appropriate wireless network security measures prevent prospective hackers from accessing this sensitive information and provide consumers peace of mind while using digital platforms [5]. Businesses often handle delicate information, including trade secrets, employee information, and consumer data. A flaw in a wireless network may violate trust, harm their reputation, and result in sizable financial losses. Additionally, organizations must comply with regulatory requirements to secure certain kinds of information in industries like banking and healthcare, so network security is more than simply a question of best practices.

The complexity and capacity of wireless networks are growing tremendously along with the quick spread of IoT devices [24, 25]. Network security is essential since every connected device offers a possible access point for hackers. We can use the advantages of networked smart devices while reducing the hazards by protecting these networks. The ongoing remote work trend further emphasizes the need for robust wireless network security. Employees accessing corporate networks from potentially insecure home networks can inadvertently expose sensitive data. Thus, ensuring secure data transmission over such networks is necessary in today's work environment.

Fundamental Methods and Mechanisms

A variety of strategies have been developed for wireless security.

1) Encryption: Data must be transformed into an unreadable format for unauthorized users. The most recent standard, WPA3 (Wi-Fi Protected Access 3), employs 192-bit cryptographic strength to provide industrial, government, and military networks strong protection. It was developed specifically to enhance the safety of wireless networks [6]. It superseded the earlier WPA2 protocol and was made available by the Wi-Fi Alliance in 2018.

WPA3 has many characteristics including:

- WPA3 protects corporate networks using encryption that is 192 bits long, offering increased safety [3].
- Strong authentication based on passwords WPA3 employs the Simultaneous Authentication of Equals (SAE) protocol, a secure critical establishment method between devices. This approach is secure against offline dictionary attacks, which occur when an adversary tries to figure out a network password by testing many potential passwords.
- WPA3 adds customized data encryption to open networks, which means that the data of each user is secured from eavesdropping by other users on the same network [3]. This provides an increased level of security for public networks.

2) Authentication: Verifying the identity of people or devices entering the network. PEAP (Protected Extensible Authentication Protocol) and EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) are standard protocols that provide robust authentication. Protected Extensible Authentication Protocol (PEAP): This is a technique for sending authentication data, including passwords, across a network in a safe manner. The authentication data is sent inside this secure tunnel after establishing an encrypted link

between the client and the authentication server (usually TLS). PEAP is often used with a secondary authentication technique like MS-CHAP v2 or EAP-MSCHAP v2 to connect the client to the network [7].

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) is a secure, certificate-based authentication protocol that provides mutual authentication, thus mitigating risks like phishing and Man-in-the-Middle (MITM) attacks. It establishes an encrypted channel for transferring authentication messages and data using Transport Layer Security (TLS), improving overall security [7]. EAP-TLS is generally utilized in wireless network settings, although it may also be used in wired networks and VPNs because of its flexibility. It is widely supported across many different devices and systems since it is an open standard that the IETF published in RFC 5216. However, since it relies on certificates, managing it may be challenging. 3) Firewalls: These software systems mitigate possible threats by monitoring and regulating incoming and outgoing network traffic following pre-established security rules.

Leading Products and Research

A wide range of studies and cutting-edge solutions are boosting wireless network security. Quantum cryptography is being investigated for wireless networks in a landmark study from Stanford University to attain excellent security [1]. They suggest Quantum Key Distribution (QKD), which guarantees randomness and security of shared keys [18].

The emergence of AI and machine learning has produced ground-breaking products, such as Darktrace's Antigen Network, which uses AI to identify and react to active cyber threats. Another fantastic product from CISCO is the Identity Services Engine [17], which offers secure access and enforces security regulations across wireless networks.

Challenges with Wireless Networks Security

The security of wireless networks continues to have difficulty overcoming various obstacles, despite the significant strides made in the sector in recent years. The vulnerabilities within the WPA3 protocols are a primary source of worry [13]. Even if it improves security beyond a shadow of a doubt, it does not in every way remove the possibility of weaknesses. Specific devices use insecure protocols, such as Wired Equivalent Privacy (WEP), which provides an ideal environment for cybercriminals to exploit vulnerabilities.

In addition, the of IoT devices has dramatically increased networks' complexity, making monitoring and securing these networks more complex. Threats presented by individuals working inside the organization are also a serious concern. Since they already have the authorization to access the network, dishonest workers or partners can harm the organization significantly. Scalability is another significant obstacle since existing security solutions may become ineffective in the face of the expanding complexity and scale of the network, which may result in possible security flaws [13]. Scalability presents a challenge because it may lead to potential security vulnerabilities.

Against this backdrop, future studies in wireless network security are anticipated to address existing challenges and foster innovative solutions, keeping researchers ahead of burgeoning cyber threats. Among the most promising avenues for exploration is quantum computing. While it promises to secure wireless networks, it also carries potential threats, as it can circumvent traditional encryption. Exploring quantum-resistant algorithms and post-quantum cryptography holds the promise of a seismic shift in computing.

In addition to this, AI and machine learning also provide excellent opportunities. Research of a more advanced kind in these fields could one day make it possible to conduct predictive analysis for threat detection, enabling the transformation of network security systems from reactive to proactive modes. Another vital area of research is making strong AI models as robust as possible and ensuring they resist being manipulated. Because many IoT devices are now in use, maintaining the safety of their connectivity with wireless networks is of the utmost significance. Analysis of the behavior of devices for anomaly detection or the development of lightweight encryption solutions might be the focus of research in this field [1]. Methods enabling data processing while ensuring privacy, such as differential privacy or homomorphic encryption, are ripe for investigation as the importance of protecting data privacy increases.

These are crucial research directions that, if pursued, could provide significant advancements in wireless network security. By harnessing such strategies, the integrity of data transferred between multiple parties in a wireless network could be preserved, even if certain parties become compromised.

COMPARATIVE ANALYSIS

The comparison between blockchain security and wireless network security reveals unique attributes, challenges, and potential mitigation strategies associated with each. While blockchain security focuses on maintaining the integrity and authenticity of decentralized data chains, wireless network security aims to protect data during transmission over wireless connections. Below we delve into the details of these two areas of security.

Nature of Technology

Blockchain is a distributed, decentralized digital ledger system that uses cryptography to guarantee the accuracy and openness of transactions. Each participant (node) in the peer-to-peer networks it uses has access to the entire Blockchain. On the other hand, wireless networks are communication networks that rely on wireless data links among network nodes. The main security goal in these networks is to protect data transfer from harmful assaults.

Security Measures

In blockchain security, many cryptography methods are used. Hash functions, digital signatures, and consensus procedures are important elements. These controls guarantee user and data integrity and defense against majority and double-spending attacks. Security measures for wireless networks include firewalls, intrusion detection systems, and encryption protocols like WPA3. These precautions guard the network against unwanted access, data eavesdropping, and other cyberattacks.

Major Challenges

51% of attacks in which one party seizes most of the network's hash power are significant threats to blockchain security. Other problems include the weak points in smart contracts, privacy difficulties, and the potential danger quantum computing poses to cryptographic concepts. Man-in-the-middle (MitM) attacks, network spoofing, denial-of-service (DoS) assaults, and security lapses in IoT devices are the main threats to wireless network security.

Techniques for Enhancing Security

Blockchain security is improved by post-quantum cryptography developments, better smart contract auditing tools, privacy-preserving methods, and refined consensus algorithms. Stringent security standards for wireless network protocols, sophisticated intrusion detection systems, and better security protocols for IoT devices are some of the enhancement strategies for wireless network security.

Blockchain security research will focus on constructing solid regulatory frameworks for blockchain systems, developing quantum-resistant cryptographic approaches, boosting smart contract security, and improving user privacy [2]. Future research of wireless technologies focuses on IoT device security, improving intrusion detection systems, enhancing security standards for wireless network protocols, and tackling security issues brought on by 5G/6G. While blockchain security focuses on preserving the validity and integrity of the decentralized ledger, wireless network security is concerned with safeguarding data while it is being sent wirelessly. Both are essential components of the contemporary digital environment and need ongoing study and development to address new threats and weaknesses.

STATISTICS

The global blockchain security market is forecasted to climb from $3.0 billion in 2024 to reach $37.4 billion by 2029, marking a CAGR of 65.5%. This growth is driven by the increasing frequency of cybersecurity threats, the adoption of decentralized finance (DeFi), and the integration of blockchain with emerging technologies like IoT, AI, and quantum computing [15]. The wireless network security market, worth $23.45 billion in 2022, is expected to increase at a CAGR of 12.5% between 2023 and 2030. This growth is fueled by the rising adoption of cybersecurity solutions, the demand for professional and managed security services, and technological advancements such as the integration of AI and big data analytics [16].

Blockchain technology is increasingly being integrated into wireless networks to enhance security. Its decentralized and immutable nature helps in mitigating various security threats inherent in wireless communications. For instance, blockchain can address issues like eavesdropping, man-in-the-middle attacks, and session hijacking by providing secure authentication and data integrity mechanisms [10].

The convergence of blockchain and wireless network security is becoming more prominent. The decentralized, immutable, and transparent nature of blockchain provides powerful solutions to the security issues encountered by today’s wireless networks. This integration is particularly relevant in the context of 5G and 6G networks, where the complexity and scale of operations demand advanced security frameworks [10].

THE CONVERGENCE OF BLOCKCHAIN, WIRELESS NETWORK SECURITY, AND AI

Another interesting area is the integration of AI, blockchain, and wireless networks. The convergence of blockchain, wireless network security, and AI marks a transformative shift in the realm of cybersecurity, particularly for emerging technologies like IoT and 5G/6G networks. This convergence empowers modern security frameworks to resolve traditional issues like centralized weaknesses, inadequate data protection, and the growing threat of advanced cyberattacks [20, 21]. In the IoT ecosystem, the combination of blockchain and AI enables secure communication between devices over wireless networks by validating data and proactively detecting anomalies or potential threats [19]. Similarly, the deployment of 5G and emerging 6G networks demands highly secure, low-latency infrastructures capable of managing vast data volumes and billions of connected devices [26, 27]. By merging blockchain's decentralized architecture with AI's predictive capabilities, these advanced networks benefit from enhanced security through real-time threat detection, secure identity management, and comprehensive data encryption [10].

The table below outlines how blockchain and AI can work together to enhance wireless network security, along with their key benefits and challenges:

Table 1: Synergy of Blockchain and AI for Wireless Network Enhancement

Role	Explanation
Blockchain	Blockchain provides the backbone of secure data handling and transparency, offering features like decentralization, immutability, and smart contracts.
Artificial Intelligence	AI offers advanced capabilities for real-time threat detection, pattern recognition, anomaly detection, and automated defense.
Integration	Integration ensures that the decentralized trust model of blockchain works seamlessly with the adaptive, predictive power of AI, creating a robust security framework for wireless networks.

AI Methods in Wi-Fi, IoT, and 5G/6G Security

AI methods are increasingly integrated into Wi-Fi, IoT, and 5G/6G networks to enhance performance, optimize resources, and improve security. Here's an overview of how AI is applied across these technologies:

Wi-Fi: AI enhances Wi-Fi network security by enabling intelligent, adaptive, and real-time threat detection. Traditional defenses like encryption and firewalls are inadequate against advanced threats such as DoS attacks, rogue access points, and MAC spoofing. AI leverages machine learning (ML) and deep learning (DL) to identify traffic anomalies and respond instantly. Unsupervised methods, such as clustering and autoencoders, detect abnormal patterns that may signal intrusions [22], while behavioral profiling uncovers insider threats. Reinforcement learning (RL) is also being applied to optimize network configurations in response to evolving threats [23].

IoT: IoT devices are vulnerable to cyber threats due to limited resources and weak security. AI boosts IoT security through real-time anomaly detection, intrusion detection systems, and

threat intelligence. Supervised and unsupervised learning help identify known and unknown attacks [24]. Federated learning enables secure, collaborative model training without sharing raw data. Deep learning models like CNNs and LSTMs detect complex patterns in time-series data, supporting context-aware security decisions based on sensor inputs [25].

5G/6G: 5G and 6G networks face new security challenges due to increased complexity and a broader attack surface. AI enhances cyber resilience by enabling self-protecting networks and dynamic threat response. In 5G, deep reinforcement learning supports resource allocation and anomaly detection [26], while AI secures network slicing by ensuring isolation. For 6G, AI-native architecture will enable proactive defenses and strengthen zero-trust models through continuous, AI-driven risk assessments [27].

Below is a concise table summarizing the use of blockchain and AI in enhancing security for Wi-Fi, IoT, and 5G/6G networks:

Table 2: Blockchain and AI in Enhancing Security for Wi-Fi, IoT and 5G/6G Networks

Category	Wi-Fi	IoT	5G/6G
Problem	Weak passwords, rogue devices, MITM attacks	Insecure endpoints, lack of updates, data breaches	Massive connectivity, dynamic threats, central vulnerabilities
AI Role	Anomaly detection, behavior analysis, IDS	Predictive analytics, anomaly detection, threat automation	Real-time threat detection, adaptive security, intelligent slicing
Blockchain Role	Immutable logs, decentralized auth, smart contract-based access	Device identity, data integrity, secure updates	Secure roaming, decentralized trust, smart contract enforcement
Benefits	No central point of failure, transparent, responsive	Resilient, secure, transparent, scalable	Secure, scalable, audit-ready, adaptive
Challenges	Latency, device limits, privacy issues	Energy constraints, scalability, device heterogeneity	High throughput, blockchain latency, training overhead

CONCLUSION

The nature of blockchain and wireless network security technologies, their specific security mechanisms, the key issues they face, and approaches for improving security were discussed in this article. The integration of blockchain and AI was also explored, highlighting its significant potential in enhancing the security of Wi-Fi, 5G/6G, and IoT networks.

Given their crucial roles in the digital environment, the significance of protecting wireless networks and blockchain cannot be emphasized. Even if much progress has been made, future studies should consider new dangers, technological developments, and ongoing growth. Building the next generation of secure systems requires collaborative, multidisciplinary research that incorporates fields such as machine learning and quantum computing.

References

[1]. J. Ahmed, A. K. Garg, M. Singh, S. Bansal, M. Amir. (2014). Quantum cryptography implementation in wireless networks. International Journal of Science and Research, academia.edu.

[2]. G. Habib, et al. (2022). Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. Future Internet, mdpi.com.

[3]. A. Halbouni, L.Y. Ong, M.C. Leow. (2023). Wireless security protocols wpa3: A systematic literature review, IEEE Access.

[4]. IBM (2021). What is blockchain security? Retrieved from https://www.ibm.com/topics/blockchain-security

[5]. H. Azam, et al. (2023). Wireless Technology Security and Privacy: A Comprehensive Study. Preprints.org. https://doi.org/10.20944/preprints202311.0664.v1

[6]. A. Irei. (2022). Differences Among WEP, WPA, WPA2, and WPA3 Wireless Security Protocols. SearchNetworking. Retrieved from https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2

[7]. K Wang, et al. (2022). Assessing certificate validation user interfaces of WPA supplicants. ACM, MobiCom '22: Proceedings of the 28th Annual International Conference on Mobile Computing and Networking, acm.org.

[8]. K. Rangan. (2021). What Is Blockchain? Here is Everything You Need to Know. G2.com. Retrieved from https://www.g2.com/articles/what-is-blockchain

[9]. R. Nazir, et al. (2021). Survey on Wireless Network Security. Archives of Computational Methods in Engineering, Springer Nature.

[10]. T. Rathod, et al. (2022). Blockchain for Future Wireless Networks: A Decade Survey. Sensors, mdpi.com.

[11]. V. Wylde, et al. (2022). Cybersecurity, Data Privacy, and Blockchain: A Review. SN Computer Science, Springer Nature.

[12]. S. Ruoti, B. Kaiser, A. Yerukhimovich, J. Clark, R. Cunningham. (2019). Blockchain technology: what is it good for? Communications of the ACM, Volume 63, Issue 1.

[13]. A. N. Kadhim, S. B. Sadkhan. (2021). Security Threats in Wireless Network Communication-Status, Challenges, and Future Trends. IEEE, 2021 International Conference on Advanced Computer Applications (ACA).

[14]. W. Jiang, et al. (2023). IoT Access Control Model Based on Blockchain and Trusted Execution Environment. Processes, mdpi.com.

[15]. MarketsandMarkets. (2024). Blockchain Security Market. Retrieved from https://www.marketsandmarkets.com/Market-Reports/blockchain-security-market-197708696.html

[16]. Grand View Research. Wireless Network Security Market Size & Share Report. Retrieved from https://www.grandviewresearch.com/industry-analysis/wireless-network-security-market

[17]. Cisco Identity Services Engine (ISE) Solution Overview. (2024). Retrieved from https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/identity-ser-engine-so.html

[18]. O. Amer, V. Garg, W. O. Krawec. (2021). An Introduction to Practical Quantum Key Distribution. IEEE Aerospace and Electronic Systems Magazine.

[19]. A. M. Ruzbahani. (2024). AI-Protected Blockchain-based IoT environments: Harnessing the Future of Network Security and Privacy. arXiv preprint arXiv:2405.13847.

[20]. D. Zhang, C. Kuang, X. Yang, H. Li. (2024). Blockchain for Knowledge-Driven Wireless Network Security. In Proceedings of the Fourth International Conference on Sensors and Information Technology (ICSI 2024). https://doi.org/10.1117/12.3029210

[21]. Y. Zuo, J. Guo, N. Gao, Y. Zhu, S. Jin, X. Li. (2023). "A Survey of Blockchain and Artificial Intelligence for 6G Wireless Communications." IEEE Communications Surveys & Tutorials, DOI: 10.1109/COMST.2023.3315374.

[22]. Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, D. Breitenbacher, A. Shabtai, Y. Elovici. (2018). N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Computing, 17(3), 12–22. https://doi.org/10.1109/MPRV.2018.03367731

[23]. T. T. Nguyen and V. J. Reddi. (2023). Deep Reinforcement Learning for Cyber Security. IEEE Transactions on Neural Networks and Learning Systems.

[24]. M. Ammar, G. Russello, B. Crispo. (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38, 8–27. https://doi.org/10.1016/j.jisa.2017.11.002

[25]. H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, K. R. Choo. (2021). A survey on Internet of Things security: Requirements, challenges, and solutions. Internet of Things, 2021 – Elsevier.

[26]. D. C. Nguyen, et al. (2020). Blockchain for 5G and beyond networks: A state of the art survey. Journal of Network and Computer Applications. 2020 – Elsevier.

[27]. W. Saad, M. Bennis, M. Debbah, M. (2020). A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. IEEE Network, 34(3).