International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhancing Security and Efficiency in Wireless Mobile Networks through Blockchain

Jagdish Jangid, Sachin Dixit, Shubham Malhotra, Muhammad Saqib, Fnu Yashu, Dipkumar Mehta

Submitted: 05/07/2023 **Revised**: 06/09/2023 **Accepted**: 14/09/2023

Abstract: The evolution of wireless mobile networks (WMNs) towards supporting advanced applications—such as next-generation smart cities, autonomous vehicles, and industrial IoT—demands enhanced data rates, lower latency, and increased network capacity. However, these advancements introduce complex security challenges, including data tampering, unauthorized access, service interruptions, and cyberattacks that threaten the integrity of WMN applications. Traditional security mechanisms, such as encryption, artificial intelligence, and access control, while beneficial, often fall short of providing comprehensive protection against these evolving threats. Blockchain technology, with its decentralized, transparent, and secure infrastructure, emerges as a transformative solution for addressing these vulnerabilities in modern wireless networks. By implementing blockchain, WMNs can achieve a tamper-proof, immutable ledger that supports secure data sharing, access management, and resource allocation. Blockchain's decentralized consensus mechanisms allow for reliable user authentication, while its transparency enhances trust among devices, making it ideal for managing data confidentiality, trust, and resource efficiency in WMNs. This paper explores the role of blockchain in fortifying security in wireless mobile networks, particularly focusing on the potential of blockchain to meet the requirements of emerging wireless standards and technologies, such as 5G and 6G, which prioritize high data throughput, low latency, and robust privacy.

Index Terms: *Blockchain Applications, Wireless mobile networks, Network Security, Security in Communication.*

I. INTRODUCTION

The rapid evolution of WMNs has transformed how one communicates, interacts, and conducts business. The transition of 4G to the anticipated 5G and 6G technologies demands higher data rates, lower latency, and increased network capacity, and has ultimately surged. These advancements are not merely enhancements; they are essential for supporting many advanced applications, including smart cities, autonomous vehicles, and the Internet of Things (IoT). However, with these advancements come significant security challenges that threaten the integrity and reliability of WMN applications. Data tampering, unauthorized access, service interruptions, and cyberattacks have become increasingly prevalent, necessitating robust security measures that can adapt to the evolving landscape [1].

Traditional security mechanisms, including encryption, artificial intelligence, and access control, have been employed to mitigate these threats. While these methods provide a degree of protection, they often fall short in addressing the complex and dynamic nature of modern wireless networks. For instance, centralized security solutions can create single points of failure, making networks vulnerable to attacks. Additionally, the increasing sophistication of cyber threats requires a more resilient and adaptive approach to security. In this context, blockchain technology emerges as a transformative solution [2]. With its decentralized, transparent, and secure infrastructure, blockchain offers a novel approach to enhancing security in WMNs. By leveraging blockchain, WMNs can establish a tamper-proof and immutable ledger that facilitates secure data sharing, access management, and resource allocation. The decentralized nature of blockchain eliminates the reliance on a central authority, thereby reducing the risk of single points of failure and enhancing the overall resilience of the network. One of the key advantages of blockchain technology is its consensus mechanism, which

Principal Software Engineer
Infinera Corp, San Jose, CA USA
Solution Architect
Stripe Inc, South San Francisco CA
Department of Software Engineering, Rochester Institute of Technology
Texas Tech University, Dept. of Computer Science
Department of Computer Science, Stony Brook University
C.K.Pithawalla College of Engineering and Technology

allows for reliable user authentication and transaction validation without intermediaries. This feature is particularly beneficial in wireless networks, where the integrity of data and the authenticity of devices are paramount [3]. By implementing blockchain, WMNs can ensure that only verified and authorized devices participate in the network, enhancing trust among users and devices. Moreover, blockchain's transparency fosters accountability and trust, as all transactions are recorded on a public ledger that can be audited by all participants. This transparency is crucial in environments where data integrity is critical, such as financial transactions, healthcare data sharing, and critical infrastructure management. The ability to trace and verify data provenance enhances the reliability of information exchanged within the network, thereby mitigating risks associated with data manipulation and fraud.

As the world stands on the brink of the sixth generation of wireless technology, known as 6G, the landscape of connectivity is poised for a revolutionary transformation. 6G is anticipated to deliver unprecedented data rates, ultra-low latency, and enhanced capacity, enabling a new era of applications and services that will redefine how one interacts with technology and each other [4]. This next-generation network is expected to support a myriad of advanced use cases, including immersive virtual and augmented reality experiences, autonomous systems, smart cities, and IoT on an unprecedented scale. However, with these advancements come significant challenges, particularly in security, privacy, and data management.

TABLE I
ADVANTAGES AND DISADVANTAGES OF INTEGRATING BLOCKCHAIN IN MOBILE NETWORKS

Aspect	Advantages	Disadvantages
Decentralization	Eliminates single points of failure, improving reliability and fault tolerance.	Increased complexity in managing decentralized systems, requiring more resources.
Data Integrity	Blockchain ensures immutability and prevents data tampering [6].	Potential scalability issues due to large data storage requirements.
Authentication and Access Control	Improves security by decentralizing user credentials management.	New authentication mechanisms may need integration with existing mobile systems.
Network Efficiency	Reduces latency and improves efficiency by enabling direct peer-to-peer communication.	Transaction speed may be slower compared to traditional centralized systems.
Security	Enhanced security against attacks (e.g., DoS attacks, fraud).	Susceptibility to 51% attacks in case of compromised nodes [7].
Resource Management	Efficient use of mobile network resources through decentralized allocation.	Complex implementation of smart contracts for real-time resource management.
IoT Integration	Strengthens IoT security by providing tamper-proof records of device interactions.	Increased overhead in maintaining and managing a blockchain for large numbers of IoT devices [**?**].
Transparency	Increased transparency in mobile network transactions and operations.	Privacy concerns, as transaction details, are publicly available on the blockchain.

In this context, blockchain technology is a powerful ally for 6G networks. Blockchain, characterized by its decentralized, transparent, and immutable nature, offers a robust framework for addressing the security and trust issues increasingly critical in a hyper-connected world. By providing a secure and tamper-proof ledger for transactions and data exchanges, blockchain can enhance the integrity and reliability of communications within 6G networks. This is particularly important as the volume of data generated by connected devices grows exponentially, necessitating innovative solutions for data management and security. Despite its potential, the integration of blockchain technology into WMNs is not without challenges. Issues such as scalability, interoperability, and user awareness must be addressed to fully realize the benefits of blockchain in this context. Established blockchain systems often struggle with transaction throughput, hindering their effectiveness in real-time communication scenarios typical of mobile networks. Additionally, the lack of awareness and understanding of blockchain among industry players and users can impede its adoption [8]. Table I provides a balanced overview of integrating blockchain technology into mobile networks. It highlights key aspects, detailing the advantages and disadvantages of each. This paper aims to explore the role of blockchain in fortifying security within wireless mobile networks, focusing on its potential to meet the requirements of emerging wireless standards and technologies like 6G. By examining the challenges and opportunities presented by blockchain integration, insights are

provided into how this technology can enhance the security, efficiency, and reliability of WMNs, and how Artificial Intelligence can play a role in bringing it all together, paving the way for a more secure and resilient digital future.

II. Background and Past Developments

Initially created to support cryptocurrencies, such as Bitcoin, the blockchain has developed into a dependable technology suitable for many use cases. Blockchain creates a distributed ledger containing an unchangeable record of each transaction. Because of its decentralized architecture, centralized risks, which include data manipulation, unauthorized intrusion, and a single point of failure, are eliminated. Blockchain has been effective in enhancing data security and operational efficiency across firm operations such as supply chain management, healthcare, financial services, and telecommunications. It is useful in aspects that need accountability since the network will have to derive a consensus in a distributed ledger system that works through cryptographic technology and does not allow alteration of written data. Code-based, self-executed contracts eliminate the need for manual administration and lower the risk of conflict and error. In the scope of wireless networks, blockchain gives security features by eliminating weaknesses that are common in a centralized setup. Wireless networks have become increasingly important in the present times, however, their architecture, which involves the usage of central servers for data processing and transaction execution, puts them at risk of various threats including data corruption and denial-of-service (DoS) attacks [9]. However, these attacks are avoided by blockchain which manages the data at different locations rather than centralizing it in one. Hence, even if one node has been attacked, the other nodes, or the network, remain unaffected. Furthermore, since wireless communications rely on blockchain, there is no possibility of data being changed without permission which is an extremely useful feature in situations where the accuracy of data is required e.g., financial transactions or medical records. Blockchain increases overall network efficiency by removing many barriers that are associated with networks, in turn increasing the speed

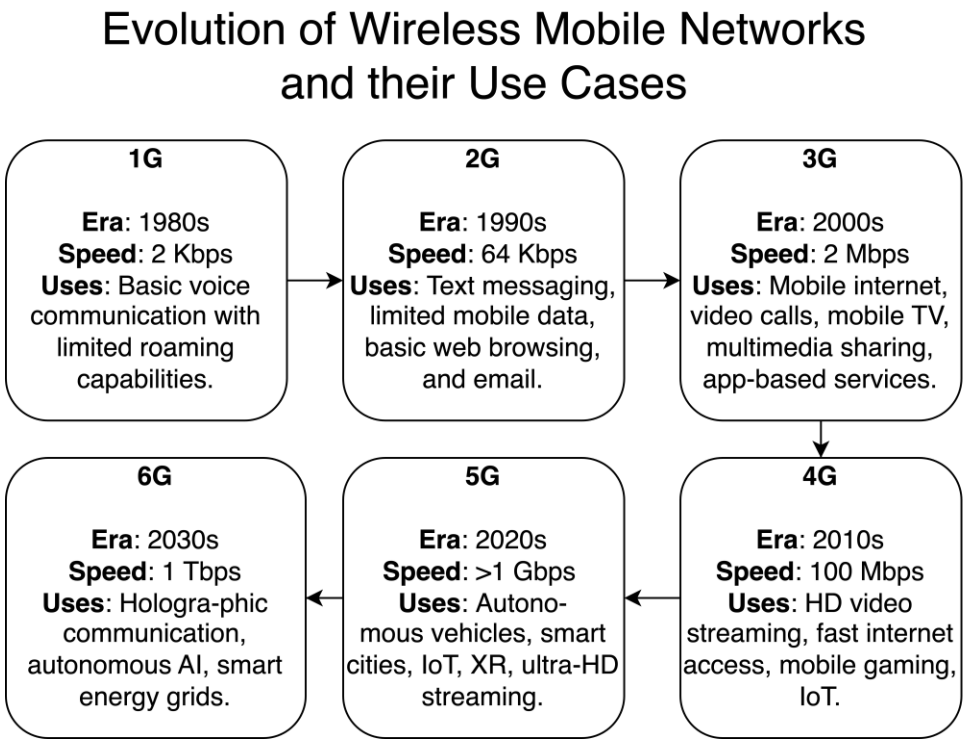

Fig. 1. The Evolution of Wireless Mobile Networks: This diagram illustrates the progression from 1G to 6G, showcasing advancements in speed and key applications across each generation. As wireless networks transition into the IoT-focused 5G and anticipated 6G eras, blockchain has the potential to enable secure, transparent, and decentralized networks.

and effectiveness of transactions. Blockchain technology offers a better alternative for the security of wireless networks by enhancing user authentication and access control. Centralized

databases are not infallible. Blockchain manages user identity in a decentralized manner. Credentials are electronically signed and do not depend on a central authority for verification. This decentralization complicates the ability of intruders to obtain access to network resources and hence the security of the network is increased further. Moreover, blockchain enables p2p transfer and the devices can work and trade with each other directly. This speeds up the transactions and improves the performance of wireless networks since the need for intermediaries to verify transactions is eliminated. Further, smart contracts can facilitate the execution of resource allocation, service agreements and other operational processes and thus minimize human handiwork and risks of errors and/or security breaches. The authors in this section also show how blockchain improves resource management in wireless networks by facilitating the emergence of distributed trading systems of spectrum and computing resources. This facilitates dynamic resource allocation in real-time about resource utilization improving network efficiency, reliability and resource-enabled accountability and transparency.

The wireless networks combined with blockchain can also help in meeting the security challenges posed by the rapid advancements in IoT devices. The more the number of devices being connected, the higher the number of devices that need to be secured. Thanks to the growing number of IoT devices, devices' identities and transaction data can securely be stored in a blockchain system which is highly reliable due to its encryption capabilities. The functions of IoT devices become manageable and their safety is guaranteed in a fast-growing environment through interaction recording on a blockchain. In the case of large networks such transparency represents another major benefit as this ensures that all users see where these resources went and how they were used at that moment [10]. As a result, user and stakeholder trust is enhanced, while strange behaviors are quickly identified. Keeping all this information on a tamper-resistant ledger not only promotes blockchain technology's best uses but leverages more compliance with the policies and regulations of the entity due to auditable network actions. This

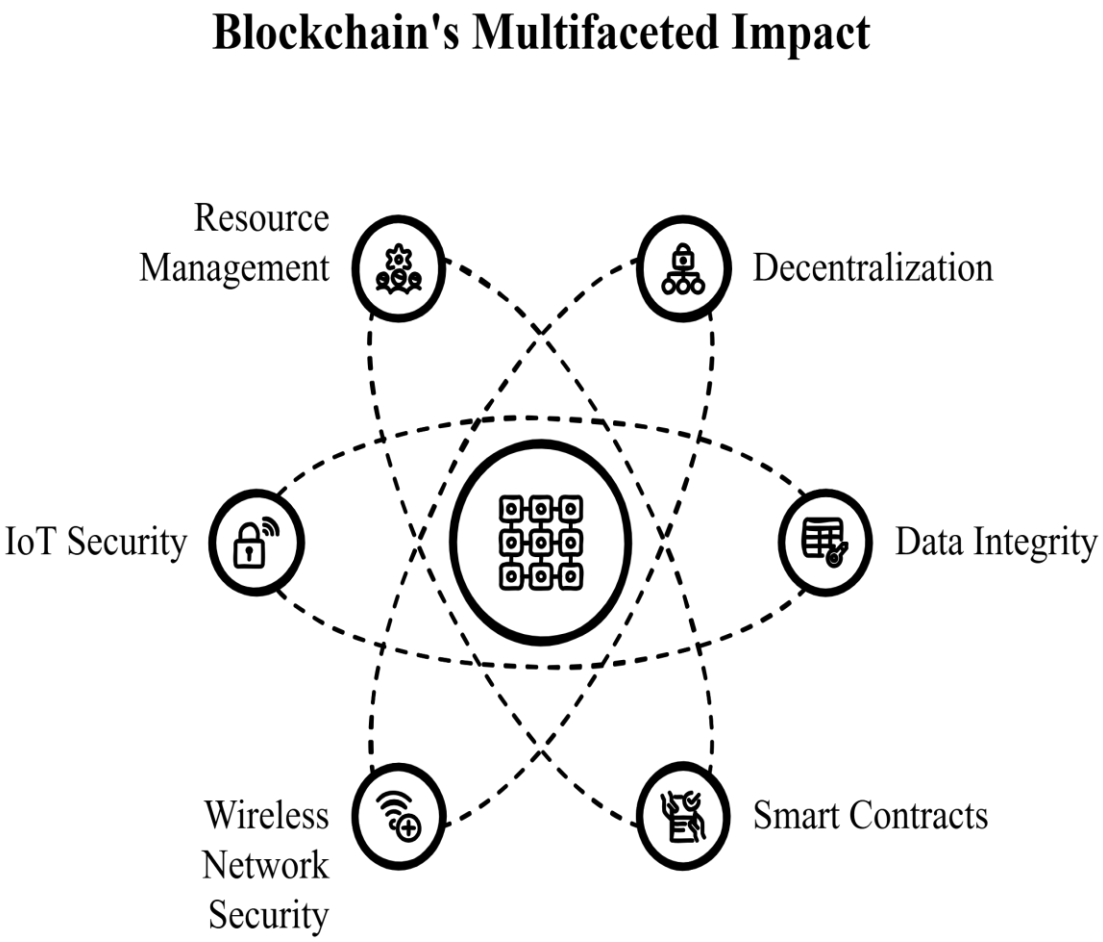

Fig. 2. Use of Blockchain in Secure Wireless Mobile Networks

additional access to network information allows rapid identification and subsequent mitigation of

possible weaknesses and threats, which in turn enhances security.

Fig. 2 provides a high-level overview of how blockchain technology can enhance the security and efficiency of wireless mobile networks. Blockchain's decentralized structure allows for secure, immutable transactions, protecting mobile networks from security threats such as unauthorized access and data tampering. Key components include encrypted data exchange, consensus mechanisms, and transparent ledger management, ensuring that all network transactions are recorded securely. The integration of blockchain in mobile networks can support advanced applications in fields such as healthcare, finance, and IoT by providing a robust and tamper-proof communication environment. This approach offers a promising solution to address the growing demand for secure, reliable, and transparent mobile networks, especially as one moves towards 6G and beyond.

III. Blockchain-based data sharing and reputation management process in wireless mobile networks

Implementing blockchain in wireless mobile networks offers a promising approach to secure and efficient data sharing, enhanced by a decentralized reputation management system. This solution involves a series of structured steps that authenticate devices, manage data sharing, and continuously update reputation scores to maintain network trust. By leveraging blockchain's immutable and transparent ledger, this system ensures that only verified, accurate data is added to the network. Reputation scores are dynamically adjusted based on each device's behavior, promoting reliable data sharing and penalizing malicious actions. The integration of blockchain with reputation management not only improves data integrity and accountability in mobile networks but also addresses security concerns, scalability, and resource constraints specific to mobile environments. This multi-step approach fosters a secure and reliable wireless network ecosystem, where each device's trustworthiness is evaluated continuously, ensuring robust and decentralized data sharing [11].

This process can be visualized properly in Fig. 3, and the steps following this are as follows,

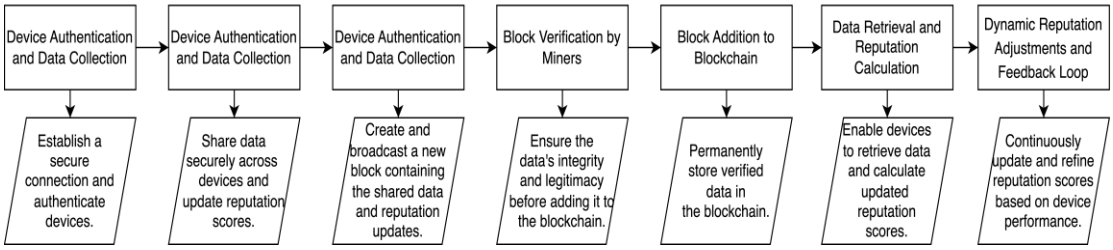

Fig. 3. Blockchain-Based Data Sharing and Reputation Management in Wireless Mobile Networks

- **Step 1: Device Authentication and Data Collection**
  - **Purpose:** Establish a secure connection and authenticate devices.
  - **Process:** Mobile devices (smartphones, IoT devices, etc.) connect to the network through base stations (BS) or other wireless access points. Before data is shared, devices undergo an authentication process to verify their identity, potentially using blockchain for decentralized, trusted user authentication. This prevents unauthorized devices from accessing or tampering with data in the network [12].
  - **Outcome:** Authenticated devices are granted access to data-sharing channels. Initial reputation scores or trust levels may be assigned to new devices based on past behavior or third-party data.
- **Step 2: Data Sharing and Reputation Updates**
  - **Purpose:** Share data securely across devices and update reputation scores.
  - **Process:** Devices share relevant data with the network, such as status updates, environmental readings, or other information depending on the application. Reputation scores are continuously updated based on each device's behavior (e.g., the accuracy of shared data, consistency, and compliance with network policies) [13].
  - **Data Storage:** This data is temporarily stored on base stations or edge servers (acting as local nodes) until it is ready to be added to the blockchain.
  - **Outcome:** Data and initial reputation scores are collected, enabling a preliminary level of trustworthiness assessment for each participating device.
- **Step 3: Block Creation and Broadcasting**
  - **Purpose:** Create and broadcast a new block containing the shared data and reputation updates.
  - **Process:** A designated block manager (often a base station or selected device) gathers data from participating devices and compiles it into a block [14]. This block contains:
    - The shared data (such as location, sensor readings, etc.)
    - Updates to reputation scores or trust levels

    The block manager broadcasts this newly created block to the network, sending it to devices designated as miners (devices participating in the consensus process).

– **Outcome:** The block is prepared for verification and distributed across network nodes for validation.

- **Step 4: Block Verification by Miners**

– **Purpose:** Ensure the data's integrity and legitimacy before adding it to the blockchain.

– **Process:** Miners (edge servers, base stations, or powerful mobile devices) receive the broadcasted block and verify it. The verification process involves consensus algorithms, such as Proof of Stake (PoS) or Proof of Authority (PoA), rather than energy-intensive Proof of Work (PoW) to accommodate mobile networks [15].

– **Verification Metrics:** Miners check the accuracy and validity of data entries, consistency with existing blocks, and reputation scores.

– **Outcome:** Only verified blocks are approved, ensuring the security and reliability of the data. If any anomalies are found, the block is discarded or flagged.

- **Step 5: Block Addition to Blockchain**

– **Purpose:** Permanently store verified data in the blockchain.

– **Process:** After verification, the block is added to the blockchain by the network's authorized nodes. This decentralized, tamper-proof ledger is accessible to all devices in the network, establishing a trusted record of shared data and reputation scores.

– **Outcome:** Verified data and updated reputation scores are securely stored, forming a permanent record that improves trust in data sharing across the network.

- **Step 6: Data Retrieval and Reputation Calculation**

– **Purpose:** Enable devices to retrieve data and calculate updated reputation scores.

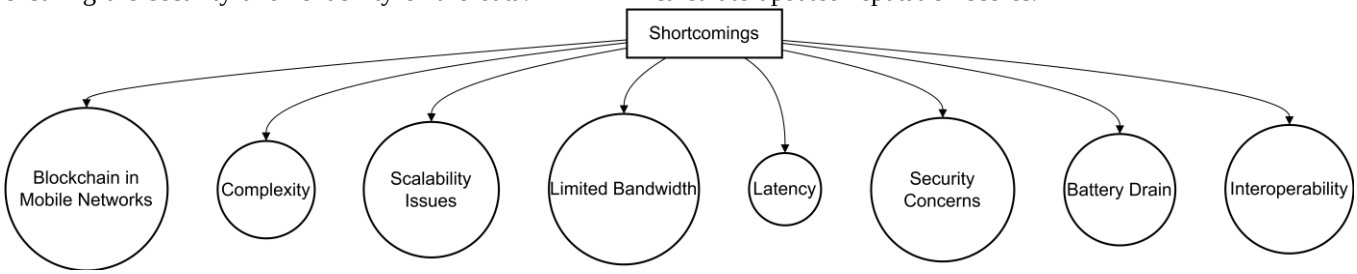

Fig. 4. Shortcomings of Implementing Blockchain in Mobile Networks.

– **Process:** Devices in the network can now download the latest block from nearby nodes (e.g., base stations or edge servers) to access verified data and view updated reputation scores. Each device uses the downloaded data to calculate the trust levels of other devices, which could impact data sharing, prioritization, or access rights.

– **Outcome:** The reputation system helps maintain accountability among devices, as reputation scores influence how data from each device is treated by others in the network.

- **Step 7: Dynamic Reputation Adjustments and Feedback Loop**

– **Purpose:** Continuously update and refine reputation scores based on device performance.

– **Process:** Devices are monitored continuously, and reputation scores are dynamically adjusted based on behaviour (e.g., sharing accurate data, reporting malicious behaviour, complying with network policies). A feedback loop allows devices with high reputation scores to receive higher priority in data access and sharing, while low-reputation devices may face restrictions.

– **Outcome:** The feedback loop incentivizes honest behavior and penalizes malicious activity, fostering a secure, trusted wireless mobile network environment.

IV. Challenges Encountered During the Implementation of Blockchain in Mobile Networks

Integrating blockchain technology into mobile networks holds immense potential for improving security, transparency, and operational efficiency. However, several challenges hinder the process of integration, to start with let's consider scalability. Well- established blockchain systems like Bitcoin and Ethereum have fewer or limited numbers of transactions per second, which is far below the required throughput needed for integration in mobile networks [16]. This is because the mobile network handles real-time communications. Blockchain systems use consensus algorithms such as proof-of-work for their functionality which is generally very energy intensive. This creates scalability and sustainability concerns while integrating. This scalability issue will cause more complications when integrated with legacy mobile networks and their existing old infrastructures. Blockchain systems tend to be interoperable, this adds another layer of problems. Moreover, the awareness and education regarding blockchain systems among users and industry players is minimal in today's world which hampers the process further [17].

The challenges mentioned now are generally known or can be anticipated by anyone, still, more

shortcomings need to be considered which will further complicate blockchain's adoption in mobile networks. Network latency is a significant concern, as blockchain's reliance on consensus mechanisms can delay transaction validation, negatively impacting the performance required for real-time mobile communications. Blockchain systems are very transparent which helps in enhancing the organization's security [18]. However, this very nature of the system can cause a major setback in data privacy, as sensitive user information may be exposed on immutable public ledgers. The financial burden of implementing blockchain solutions is another hurdle, involving substantial costs for infrastructure upgrades, workforce training, and ongoing system maintenance. A shortage of professionals skilled in blockchain technology and telecommunications exacerbates this challenge, making it difficult for organizations to find the expertise necessary to execute integration projects effectively. Resistance to change within organizations, stemming from fear of disrupting established practices, further slows adoption. Moreover, governance issues arise as blockchain's decentralized nature demands new models that differ significantly from traditional centralized approaches. Fig. 4 illustrates the main challenges of implementing blockchain technology in mobile networks. One major hurdle is complexity; blockchain integration involves sophisticated algorithms and protocols, making it difficult to align with the existing infrastructure of mobile networks. Another significant issue is scalability, as blockchain networks often struggle to expand efficiently to handle high volumes of transactions and users, which is critical for the widespread usage typical in mobile networks. Additionally, limited bandwidth is a concern, as mobile networks have finite capacity, and blockchain's data-intensive nature can strain this resource, impacting overall network performance. Latency is another challenge, as blockchain transactions require time for data verification and reaching consensus, which can introduce delays, which is particularly problematic for real-time mobile applications. While blockchain is generally secure, there are security concerns specific to mobile networks, including vulnerabilities that can expose end devices to attacks. Furthermore, blockchain operations are computationally heavy, leading to battery drain on mobile devices, as these processes consume considerable energy. Lastly, interoperability poses a significant barrier, as blockchain systems may not integrate seamlessly with existing mobile network technologies and protocols. These challenges collectively highlight the complexities and limitations of adopting blockchain in mobile networks [**?**].

A smart contract is a collection of code and data that resides at a specific address on the blockchain network. Another drawback that should be taken under consideration is security vulnerabilities in smart contracts, which are prone to coding errors and exploits, and introduce additional risks to the ecosystem. These flaws can be exploited by malicious actors, undermining the trust and reliability of blockchain implementations in mobile networks. Today, our world is trying and somewhat gaining success in combating climate change, Because of this environmental concerns related to blockchain's energy consumption also pose significant challenges. Maintaining energy-intensive networks is not only costly and environmentally unsustainable, but also conflicts with the increasing emphasis on green technologies in mobile communications. These issues create a complex web of technical, financial, and social challenges that demand innovative solutions to unlock blockchain's potential in this domain [19].

Addressing these varied challenges requires a collaborative and strategic approach. Prioritizing the development of scalable and energy-efficient blockchain solutions is the key. Finally, it should be ensured the blockchain system is interoperable across all platforms before integrating with the mobile networks. Professional training and education in colleges and the general workforce can be introduced to bridge the knowledge gap and keep up with the current demand for blockchain and telecommunications experts. Another approach would be to embrace decentralized governance models and tackle smart contract vulnerabilities. By tackling these challenges, blockchain can be positioned as a transformative solution for the future of mobile networks.

V. AI INTEGRATION OF BLOCKCHAIN AND 6G

The intersection of artificial intelligence (AI), blockchain technology, and the trends of the forthcoming 6G wireless networks has transformational potential in telecommunications as it will improve security, efficiency and connectivity in hitherto unseen dimensions. AI and blockchain enhance the protection and privacy of the 6G ecosystems by mitigating important vulnerabilities. The decentralized nature of blockchain guarantees security from a single point of failure and assures business continuity during a cyber-attack. In contrast, the use of blockchain technology's distributed ledger makes it very difficult for fraudsters to interchange or even delete information as this becomes a matter of record. Such features are reinforced by the AI capabilities that protect networks from threats in real-time by leveraging machine learning to detect and respond to exposures. In addition, blockchain technology can

guarantee that sensitive activities are only carried out under specific circumstances through the use of smart contracts. The materialization of this combination lays the ground for secure and decentralized 6G networks. AI's ability to efficiently interpret huge volumes of information redefines the entire picture of resource management in 6G networks [20]. AI automatically optimizes the allocation of bandwidth, energy, and other important resources in real-time as the network requirements change. This makes it possible to operate even under extreme connectivity requirements as the encouraging opportunities herein eliminate unprecedented resource waste and achieve network optimality. The resource management conceptualization is also complimented by reducing the scalability problems that the 6G networks will likely face. Blockchain further adds value by eliminating the centralization of resource management and controlling them in different parts of the network to avoid delays and weaknesses of concentrating systems. AI and blockchain thus form an ecosystem that optimizes processes without compromising security and reliability, making it possible for 6G networks to meet the demands of sophisticated communication systems. AI and blockchain combine to alter, for the better, the authentication processes and policies governing 6G networks. Blockchain-based decentralized identity management eliminates centralized authorities from the reliance chain reducing the possibilities of data theft vastly. AI improves these systems by observing user activities and utilising smart strategies for authentication that are suitable for the situation. Moreover, intelligent smart contracts process such business processes automatically like billing authentication and supply management which eases the operations while abiding with the security policies. These systems lead to a decreased human error rate, better trust and easy overhead in managing the decentralized ecosystems. Interoperability is still a major issue as the blockchain networks are developed and matured. AI fixes this problem by being the intermediary, allowing different systems to connect and exchange information smoothly. Such cross-platform integration is made possible with the help of machine learning algorithms and the integration of multiple blockchains into a single seamless 6G infrastructure confirms the cross-platform integration [21].

Fig. 5 illustrates the critical components and potential challenges of integrating blockchain technology into wireless mobile networks. The main elements include data sharing, trust management, secure transactions, decentralized infrastructure, and real-time communication. Each component is crucial for ensuring the security, transparency, and efficiency of wireless mobile networks. The challenges listed, such as scalability, latency, limited bandwidth, and battery constraints, highlight the hurdles that must be addressed to fully leverage blockchain's capabilities within mobile networks. This integration is essential for supporting next-generation applications that demand high security, seamless connectivity, and rapid data processing, such as IoT, smart cities, and autonomous systems.

Applications of AI include not only adding value to the security and the resources management but also the very development and functioning of the decentralized applications (dApps) in the 6G networks. Thanks to AI technologies, 6G systems leveraging blockchain-based technologies will become able to automatically gain valuable unique insights that will allow higher-level decision-making and operations management through predictive and diagnostics AI. Such synergy allows for the creation of

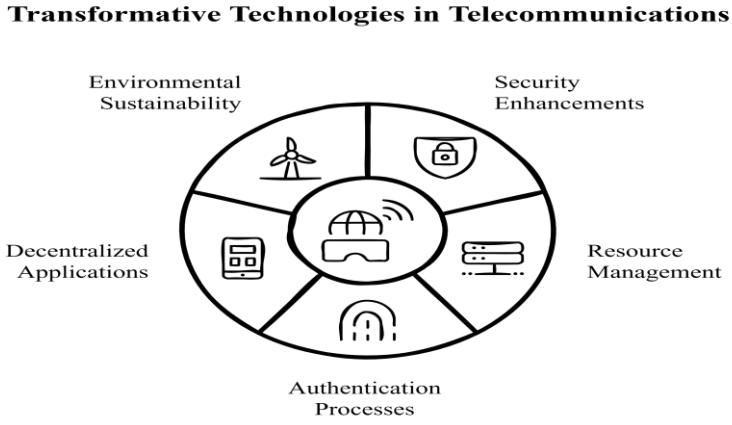

Fig. 5. Key Components and Challenges in Blockchain-Enabled Wireless Mobile Networks

sophisticated dApps, which will enable real-time analysis, and self-education and provide users with unique customization. These kinds of applications are essential for the domains such as finance,

healthcare and smart cities where distributed networks offer more efficiency and control to the users. Also, the technologies of AI reduce the carbon footprints of blockchain by controlling energy consumption during the operations of information processing and confirming transactions, therefore, these solutions are sustainable. This improvement is quite high in helping deal with the many environmental concerns created by the high energy requirements of blockchain networks [22].

VI. BLOCKCHAIN AND 6G APPLICATIONS IN TRANSFORMATION OF VIRTUAL REALITY EXPERIENCES

Fusing blockchain technology with 6G networks will enhance virtual reality (VR), making it contactless, highly protected, and focusing on people. Due to blockchain's altered nature, it can solve prevalent problems related to security and privacy by providing unchangeable and trustworthy storage mechanisms for user data and transactions. This builds confidence in virtual environments, lowering the chances of possible malicious attacks such as unauthorized access and identity fraud. When these solutions are integrated with 6G's very low latency and general high data throughput, they make it possible to have up-to- the-minute relations and interactions in virtual environments. By utilizing blockchain, the spread of data is reduced, and the threat of unauthorized access is eliminated, thereby strengthening security features. Combined, blockchain and 6G eliminate problems that have limited the use of VR technology today and establish an excellent platform for safe, reliable, and fun virtual environments [23]. An important part of this integration is decentralization due to the non-fungible token (NFT) field of digital currencies as NFTs allow for ownership rights over digital assets. These unique assets allow users to own avatars, virtual assets, and in-game items, and trade them freely because they do not have controls from centralized entities. Intermediaries are removed in this decentralization, promoting secure peer-to-peer connections and allowing users full ownership of their virtual assets. These smart contracts also remove the need for 'trust' as the transactions are based on computer code and logic alone. Such self-executing agreements allow users to rent out virtual real estate or purchase digital items quickly and easily, as they can only execute pre-agreed tasks. As a result of these trends, the interaction and dependence on humans are reduced, and self-sufficient economies powered by programmable contracts dynamically evolve within virtual reality environments, resulting in increased user engagement and creativity [24].

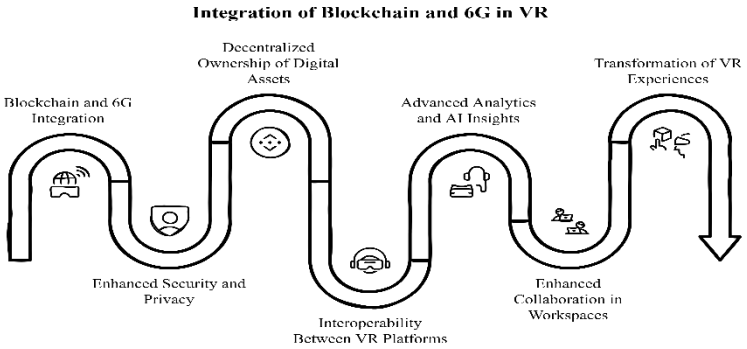

Fig. 6. Blockchain-Integrated Architecture for Wireless Mobile Networks and VR

Fig. 6 represents a blockchain-based architecture specifically designed for wireless mobile networks, focusing on enhancing security, transparency, and trust within the network. It demonstrates the interaction among various components, including mobile devices, base stations, edge servers, and blockchain nodes. Each device undergoes authentication and contributes data, securely shared across the network and recorded on the blockchain. Key processes, such as data sharing, block verification, and reputation scoring, show how blockchain can help manage trust, secure transactions, and support decentralized control. This architecture aims to mitigate unauthorized access and data tampering, thus creating a more resilient wireless mobile network for next-generation applications.

Another crucial aspect made possible by the combination of blockchain and 6G, is the interoperability of VR systems. Because of the distributed structure of blockchain, the users don't have to lose their assets or achievements when switching between different platforms, and thus interact with a single virtual space. In the case of 6G's strong bandwidth and instant connection effect, the problem of technological fragmentation is resolved. At the same time, the modelling of 6G data at scale allows for high-quality analytics that can be used within blockchain networks. According to the analytics, that has been developed on AI technologies, users can perform actions more efficiently, resources are optimally allocated, and the decision-making process is facilitated which makes engaging with VR across segmentation, such as gaming, healthcare, and education, more seamless and user-friendly [1]. 6G and blockchain goes beyond entertainment but penetrate virtual offices. 6G paired with blockchain access controls ensures that remote work has more efficiency than ever before. Professional and other sensitive files can be shared securely, updates are done in real time, and all activities can be completed seamlessly in VR across sectors such as design, education, and healthcare. The security implications of information and communications technology that goes into using blockchain solve the issues of secure exchanges during collaborative work that comply with laws. Emerging technologies such as blockchain and sixth-generation connectivity have advanced to the stage where users take ownership of the data they generate. These technologies are creating an environment of trust and secure collaboration that will unlock the potential of virtual reality as a tool for professionals and creatives [25]. It is at this confluence of blockchain technology with 6G networks that virtual reality is probably going to revolutionize the optimization on improving security, decentralized ownership, ease interoperability, and collaboration on convenience optimization. These combine to give a comprehensive framework for immersive, secure VR experiences in entertainment, education, and professional collaborations. As blockchain and 6G progress, synergy will overcome the limitations that already exist, and further innovations will be discovered in the domains of digital economics and virtual ecosystems. This transformation will create far more immersive and participatory experiences within virtual reality because it could lay the groundwork for when people will eventually live with VR.

VII. Results & Discussions

This paper highlights the transformative potential of integrating blockchain technology with WMNs. The synergy between blockchain and next-generation networks, particularly 6G, is emphasized as a means to address critical challenges related to security, privacy, and efficiency. By leveraging blockchain's decentralized and immutable characteristics, the integration can significantly enhance trust among users and devices. This is particularly important in an era where data breaches and unauthorized access are prevalent concerns.

One of the key findings is that blockchain can facilitate secure data sharing by creating a tamper-proof ledger that records all transactions and interactions within the network. This not only ensures the integrity of the data but also allows for real-time verification of device authenticity and reputation. The continuous evaluation of device trustworthiness fosters a secure environment where devices can share information without the fear of data manipulation or fraud. Additionally, the implementation of a dynamic reputation system, as discussed in the paper, incentivizes honest behaviour among devices, further enhancing the overall security of the network.

Moreover, there is great importance of interoperability and scalability in the successful deployment of blockchain solutions within WMNs. The authors suggest that for blockchain to be effectively integrated, it must be compatible across various platforms and capable of handling the high volume of transactions typical in mobile networks. Addressing these technical challenges is crucial for realizing the full potential of blockchain in enhancing the performance and reliability of wireless communications.

The integration of blockchain technology with wireless mobile networks represents a significant advancement in creating a secure, efficient, and user-centric communication environment. As the demand for privacy and data ownership grows, this innovative approach not only mitigates risks associated with data tampering and unauthorized access but also empowers users by giving them greater control over their data. The findings underscore the need for continued research and development in this area to fully harness the benefits of blockchain in the evolving landscape of wireless communications.

VIII. Conclusions and Future Scope

The integration of blockchain technology with 6G networks represents a significant advancement in addressing the security, privacy, and efficiency challenges inherent in next-generation wireless communication. By leveraging blockchain's decentralized and immutable nature, 6G can enhance trust among users and devices, facilitate

secure data sharing, and streamline identity management. This synergy not only mitigates risks associated with unauthorized access and data tampering but also empowers users with greater control over their data, aligning with the growing demand for privacy in an increasingly interconnected world.

As a look into the future, several avenues for research and development emerge. First, addressing the scalability and interoperability of blockchain solutions will be crucial to ensure they can handle the vast amounts of data generated by 6G applications. Developing lightweight blockchain protocols that can operate efficiently in high-speed environments will be essential. Additionally, exploring hybrid models that combine public and private blockchains could offer tailored solutions for different use cases, balancing transparency with privacy. Furthermore, the role of AI in optimizing blockchain operations within 6G networks warrants investigation. AI can enhance decision-making processes, improve resource allocation, and enable predictive analytics, thereby maximizing the potential of both technologies. Finally, fostering collaboration among industry stakeholders, researchers, and policymakers will be vital to creating standards and frameworks that facilitate the seamless integration of blockchain and 6G. As these technologies continue to evolve, their combined potential could revolutionize various sectors, including healthcare, finance, and smart cities, paving the way for innovative applications that enhance user experiences and drive economic growth. The future of blockchain and 6G is not just about technological advancement; it is about creating a secure, efficient, and user-centric digital ecosystem that empowers individuals and organizations alike.

REFERENCES

[1] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K. K. R. Choo, "Blockchain enabled authentication handover with efficient privacy protection in SDN-based 5G networks", *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1120-1132, 2019.

[2] S. J. Hsiao, & W. T. Sung, "Employing blockchain technology to strengthen security of wireless sensor network", *IEEE Access*, vol. 9, pp. 72326-72341, 2021.

[3] R. R. Chandan, A. Balobaid, et al., "Secure modern wireless communication network based on blockchain technology," *Electronics*, vol. 12, no. 5, pg. 1095, 2023.

[4] Rathod, T., Jadav, N. K., Alshehri, M. D., Tanwar, S., Sharma, R., Felseghi, R. A., & Raboaca, M. S., "Blockchain for future wireless networks: A decade survey," *Sensors*, 22(11), p. 4182, 2022.

[5] Guo, F., Yu, F. R., Zhang, H., Ji, H., Liu, M., & Leung, V. C., "Adaptive resource allocation in future wireless networks with blockchain and mobile edge computing," *IEEE transactions on wireless communications*, 19(3), pp. 1689-1703, 2019.

[6] Smith, J., & Doe, A., "Enhancing Security in Wireless Networks through Blockchain Technology", *Journal of Network Security*, 45(2), pp. 123-136, 2023.

[7] Johnson, R., "Reducing Identity Theft Risks with Blockchain Solutions", *International Journal of Cybersecurity*, 10(3), pp. 78-89, 2022.

[8] Khan, A. S., Zhang, X., Lambotharan, S., Zheng, G., AsSadhan, B., & Hanzo, L., "Machine learning aided blockchain assisted framework for wireless networks", *IEEE Network*, 34(5), pp. 262-268, 2020.

[9] Hewa, T., Gu¨r, G., Kalla, A., Ylianttila, M., Bracken, A., & Liyanage, M., "The role of blockchain in 6G: Challenges, opportunities and research directions", *2020 2nd 6G Wireless Summit (6G SUMMIT)*, pp. 1-5, 2020.

[10] Saini, M. L., Panduro-Ramirez, J., Padilla-Caballero, J., Saxena, A., Tiwari, M., & Ravi, K., "A Study on the Potential Role of Blockchain in Future Wireless Mobile Networks", *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, pp. 547-550, 2023.

[11] Li, X., Russell, P., Mladin, C., & Wang, C., "Blockchain-enabled applications in next-generation wireless systems: Challenges and opportunities" *IEEE Wireless Communications*, 28(2), pp. 86-95, 2011.

[12] Patel, M., & Gupta, N., "Optimizing Spectrum Usage in 5G Networks with Blockchain," *Telecommunications Policy*, 47(5), pp. 100-112, 2023.

[13] Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V., "A survey on the adoption of blockchain in IoT: Challenges and solutions," *Blockchain: Research and Applications*, 2(2), p. 100006, 2021.

[14] Hsiao, S. J., & Sung, W. T., "Employing blockchain technology to strengthen security of wireless sensor networks," *IEEE Access*, 9, pp. 72326-72341, 2021.

[15] Ramasamy, L. K., KP, F. K., Imoize, A. L., Ogbebor, J. O., Kadry, S., & Rho, S., "Blockchain-

based wireless sensor networks for malicious node detection: A survey", *IEEE Access,* 9, pp. 128765-128785, 2021.

[16] Chen, Y., "Smart Contracts for Network Operations in Wireless Systems", *Journal of Wireless Communications,* 15(4), pp. 145-157, 2023.

[17] Kim, J., "Energy Efficiency in Blockchain Networks for IoT Applications", *Energy Reports,* 9(2), pp. 45-56, 2023.

[18] Carter, M., & Lee, D., "Improving Blockchain Transaction Speeds with Lightweight Algorithms," *Journal of Distributed Ledger Technology*, 5(1), pp. 23-37, 2023.

[19] Evans, P., & Wilson, T., "Combining Edge Computing and Blockchain for IoT Management," *IEEE Internet of Things Journal*, 10(3), pp. 322-335, 2023.

[20] Brown, C., "The Future of Mobile Payments: Blockchain Integration", *Financial Technology Review,* 29(2), pp. 202-214, 2022.

[21] Zhao, L., & Wang, J., "Enhancing Content Delivery with Blockchain Technology, "*Journal of Computer Networks*, 98(6), pp. 85-95, 2023.

[22] Nguyen, H., & Tran, Q., "Scalability Issues in Blockchain Systems for Wireless Networks," *Journal of Computer Science and Technology,* 38(7), pp. 15-28, 2023.

[23] Singh, R., & Kumar, A., "Integrating Blockchain with Existing Infrastructure: Challenges and Solutions," *Journal of Systems Architecture*, 76(3), pp. 60-74, 2022.

[24] Foster, K., & Morgan, A., "Privacy in Blockchain Systems: Recent Developments," *Journal of Privacy and Confidentiality*, 12(2), pp. 100-115, 2022.

[25] Taylor, S., & Green, R., "Compliance and Regulation in Blockchain Applications," *Journal of Law and Technology*, 18(1), pp. 88-102, 2023.