Blockchain for Future Wireless Networks

Subjects: Biology

Contributor: Tejal Rathod, Nilesh Kumar Jadav, Mohammad Dahman Alshehri, Sudeep Tanwar, Ravi Sharma, Raluca-Andreea Felseghi, Maria Simona Raboaca, Marcello Cherchi

The emerging need for high data rate, low latency, and high network capacity encourages wireless networks (WNs) to build intelligent and dynamic services, such as intelligent transportation systems, smart homes, smart cities, industrial automation, etc. The WN is impeded by several security threats, such as data manipulation, denial-of-service, injection, man-in-the-middle, session hijacking attacks, etc., that deteriorate the security performance of the aforementioned WN-based intelligent services. Toward this goal, various security solutions, such as cryptography, artificial intelligence (AI), access control, authentication, etc., are proposed by the scientific community around the world.

Keywords: wireless networks ; security ; privacy ; blockchain

1. Introduction

The landscape of wireless networks (WNs) is continuously expanding as a fast-growing technology with innovative features, such as flexibility, mobility, lack of wiring, etc. Their usage is increasing in diverse smart applications, such as smart cities, e-healthcare, intelligent traffic management, smart agriculture, autonomous vehicle, smart retail, and smart grid [1]. It is becoming an integrated part of people's everyday life for day-to-day activities where a sender can transmit essential data to the receiver without using any physical medium (cables) [2]. Recent technological inclination in the WNs provides several benefits, such as ubiquitous high data rates, low latency, and high bandwidth, along with various limitations, such as security, privacy, reliability, authenticity, integrity, and scalability that can hinder the performance of WNs-based applications. To overcome the aforementioned issues, the scientific community has adopted effective radio resource management and modern technology, such as artificial intelligence, blockchain, quantum communication, etc., that offers better network performance in every next-generation wireless network. **Figure 1** shows the evolution of wireless communication technologies that started in the late 1970s. It took almost 50 years for WNs to evolve from the 1st generation to the 5th generation to deliver a progressive quality of services (QoS) to an individual and the nation's capital economy [3][4].

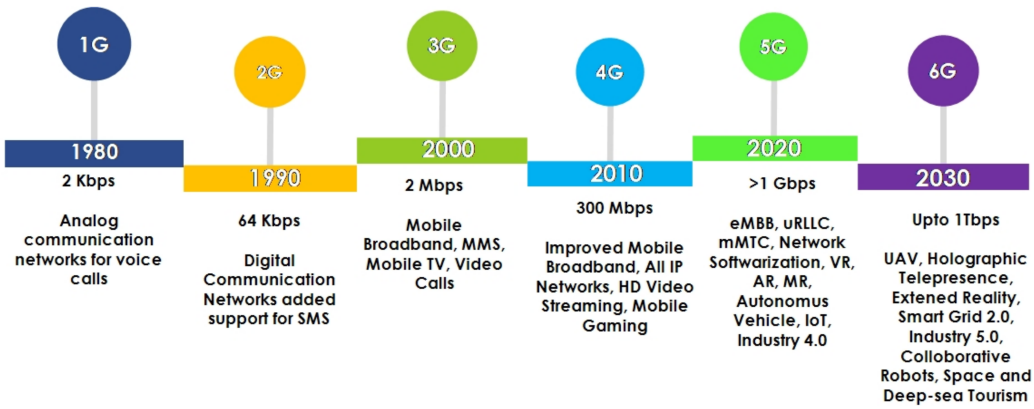

Figure 1. Evolution of wireless networks.

The first generation (1G) WN introduced in 1979 was meant to initiate voice communication between individuals using analog signals. Unfortunately, the success of 1G was quelled due to its several limitations, i.e., poor voice quality, high battery consumption, prone to security attacks, and limited capacity. Moreover, an adversary can perform clone and masquerade attacks and easily intercept the communications between two parties [5]. To mitigate the aforementioned problems in 1G, second generation (2G) introduced digital communication, such as a global system for mobile communication (GSM) and general packet radio services (GPRS). It offers features such as text and multimedia messages and data services with a transfer rate of 40 kbits/s. Additionally, it enhances the reliability of the 2G systems by providing error detection, and correction mechanisms [6]. However, with the internet services and multimedia platform, 2G

does not facilitate satisfactory data transmission rates. Additionally, there are several security issues in 2G, such as illegal interception, message spamming, and false information injection. Hence, it is recommended by many technology makers and innovators to stop using 2G systems.

To overcome the limitations of the 2G system, the third generation partnership project (3GPP) has deployed third generation (3G) networks that came up with asymmetric and symmetric traffic, global roaming, and packet-circuit switching to enhance the performance of WNs. In addition, the 3G network offers technologies, such as enhanced data rates for global evolution (EDGE), code division multiple access (CDMA), and early development of long-term evolution (LTE) that offer high data rates (14 Mbps), which raises the connectivity of mobile devices and improves the existing cellular systems. Furthermore, with the availability of IP-based communication, many users worldwide are getting connected by 3G networks to use semantic web services. However, it also raises different security vulnerabilities, such as denial-of-service (DoS), overbilling, and signaling-level attacks [7]. To overcome these issues, the international telecommunication union (ITU) has fostered the development of the fourth generation (4G) network that makes efficient use of the radio spectrum and increases the capacity, data rates, and bandwidth to deliver low latency multimedia services [8].

Similar to other legacy systems (1G–3G), the 4G network is also leveraged by several security threats and vulnerabilities, such as manipulation of access points, distributed denial of service (DDoS), data integrity, and replay attacks that deteriorate the QoS of 4G-based applications. To tackle such security hindrances, the previous generation WNs (2G to 4G) offer several security solutions, such as configuring the first line of defense by installing firewalls and intrusion detection systems, secure data by encapsulating, encryption and authentication, and incorporating demilitarized zones to protect sensitive data and critical infrastructure from the adversaries [9][10]. However, there is an increase in privacy concerns as user demands are increasing. When a user uses wireless communication to connect to the Internet, it leaves many footprints that an adversary can collect from different WNs-based applications to perform user tracking and social engineering attacks. The development of the internet-of-things (IoT) technology enables portability and more openness to the wireless network. Since a portable device is easy to attack and track instead of an entire infrastructure of the organization, it increases the privacy leakage issues in various technology, such as Bluetooth, Wi-Fi-based laptops, and smartphones [11][12].

5G has added another dimension to the WN by satisfying the user’s demands of high data rates, reliability, scalability, and low latency communication [13]. The primary objective of a 5G network is to transform a standard cellular network into an intelligent network by incorporating AI, blockchain, edge computing, and IoT technologies. It also brings effective radio access techniques, such as massive multiple-input multiple-output (MIMO), device-to-device (D2D), millimeter-wave (mmWave), and ultra-densification connectivity, which prolongs the user scalability in WN [14][15]. However, the 5G network has abstracted design principles and is not appropriately documented; as a result, there is a high risk that malicious adversaries can maneuver the standards and regulations of a 5G network [5][16]. Additionally, integrating modern technologies with WN creates a different horizon of challenges, such as lower network resiliency, data integrity, downtime, single-point failure, coordinated attacks, and unauthenticated access control [17].

One of the plausible solutions to overcome a few of the above-mentioned security issues from WN is to adopt cryptographic techniques, where most of the WN-based applications and devices use end-to-end encryption by incorporating asymmetric and symmetric key encryption, message digest, and hashing [18]. However, to fully secure WN from attackers, researchers need a stronger and considerable size key length, which is computationally expensive and not feasible. Though with modern computing capabilities, one can generate such keys and secure the WNs. However, the problem lies in sharing the keys with communicating parties, which formally use a public channel, i.e., the internet, to share the keys. The attackers can manipulate those public channels, where they can access the private keys and intercept the ongoing communication between the sender and receiver [19]. This affects the security of the WNs and imperils the privacy of the end-users. Hence, there is a requirement for a robust technology, i.e., the blockchain, which can integrate with the WNs to relieve the security and privacy constraints [20][21].

Blockchain technology has an immutable decentralized ledger that can securely store the sensitive information of WN applications in such a way that it complicates the process of manipulation by the attackers [22]. Currently, it is embraced by various WN-enabled smart applications, such as financial, smart homes, smart grids, smart supply-chain management, and smart cities, to ensure secure communication while sharing the data between different participating entities of WN [23][24]. Further, the decentralized nature of blockchain makes the technology transparent and more reliable. This is because a member of the blockchain can see transactions made by the other blockchain member. Additionally, it is inclined toward concrete cryptographic public and private keys to secure each blockchain transaction. Therefore, it is resistant to various security and privacy issues, such as data injection and data tampering attacks, and overcomes the issue of single-point

failure [25]. The integration of WN and blockchain has great potential, especially for mission-critical applications, such as e-healthcare, smart factories, public safety, and military services that require constant supervision against security threats. In addition, it also offers security to ensure interoperability and trust between complex sub-systems of smart applications.

To facilitate the integration of blockchain and WN, many researchers have proposed several state-of-the-art advances in blockchain-enabled WN. For example, Nguyen et al. [10] presented an extensive discussion on different opportunities that blockchain has brought to the world of 5G and future generation wireless networks. However, they have not discussed the critical shortcomings of blockchain in WN, such as security vulnerabilities and privacy concerns. Further, Wang et al. [26] introduced a comprehensive study of blockchain radio access network (B-RAN) based framework for 6G. They further elaborated on the necessity of a consensus mechanism, digital contracts, inter-network data sharing, and a trust model in WN to preserve the privacy of the authenticated users. Unfortunately, most of the integration between blockchain and WN specifies the partial aspects of security and privacy issues in WN. Many researchers have proposed blockchain-based solutions for secure wireless communication. However, very few of them discussed security issues and their countermeasures in depth. Thus, there is a requirement to follow a proactive way and consolidate emergent research works toward privacy and security issues of WNs. Hence, researchers highlight the security and privacy aspect and its effect on future WNs with possible solutions by resorting to blockchain technology.

2. Wireless Networks

The WNs evolved in a short span of time, witnessing explosive growth in the sector of industry, healthcare, science, and technology by pervasively connecting them. Since the 1970s, newer generations of WN have been introduced, which adroitly improve people's quality of life by providing productive services, such as voice calls, multimedia services, remote connections, on-demand, intelligent services, and many more. In 1979, the first cellular WN 1G was introduced, but it had low voice quality, higher interference, and no encryption mechanism was applied for secure communication. Then, with primary progressions, other generations (2G, 3G, 4G, and 5G) of cellular WNs were developed to add value to telecommunication and network service [3]. 2G provides a few imperative mobile call advancements, with encryption mechanisms, such as improving voice quality and reducing cross-talk [4]. On the contrary, 3G networks are faster and capable of transmitting data at a higher rate (maximum download speed 7 Mbps). They facilitated end-users to record video calls, watch TV online, surf the internet, and play online mobile games for the very first time [27]. Moreover, IoT-enabled devices become the center of social connectivity in 3G by using IP-based communication, but it also raises concern for security vulnerabilities [28].

4G has become the first generation to use long-term evolution (LTE) technology that improves the data rate and QoS of WNs. Moreover, 5G has replaced 4G with various changes, such as enhanced data rates (1 Gbps), low latency (100 ns), mobility range (100–500 km/h), etc., for better network coverage and reliability [29][30]. The communication latency in 5G has decreased substantially, resulting in fast download and upload speeds. Although 5G networks are becoming a reality, technologists have already started to be engaged with future WNs, i.e., 6G, which anticipates putting greater prominence on wearable technologies, unmanned aerial vehicles (UAVs), 3D networking, and wireless power transfer to amplify people's quality of life [31]. However, the radio resources used by the WNs operators are entirely open to security attacks, and therefore there is a need to explore and examine such attacks to stop them before they jeopardize the WN systems.

3. Security in Wireless Networks (From 4G to 6G)

Researchers highlight network security issues associated with different generations of WN, such as 4G, 5G, and 6G. In WN, a sender can share information via the Internet with the receiver. The Internet has an intricate design principle using network devices such as routers, switches, hubs, and cables, connected with simple topologies without a stronger security mechanism. This entices the attackers to scan the network devices and interfaces to find potential vulnerabilities which can further be exploited for their own benefit [32][33]. Thus, security and privacy play an essential role in protecting user data in the wireless medium [34]. To overcome that, security specialists have proposed several design factors that pave the way in thwarting the malicious attempts of the attackers. **Figure 2** shows the design factors, such as authorization, authentication, encryption, intercept probability, and channel characteristics, that confront the security attacks and improve the reliability of the WN communication. A summarized explanation of each design factor is given as follows.

- Authentication—A standard example of WN is the internet, where tons of internet services serve the end users. A sender sends confidential information from these services to the receiver, which in return, the sender expects that the information reaches the correct receiver. Thus, before sending the data, both users have to authenticate themselves for reliable communication. Formally, authentication states that a user has to validate who he/she claims to be with the help of authentication factors, such as a strong password, personal identification number (PIN), one-time password

(OTP), and biometrics. However, the attackers can attack the single layer authentication; for example, a password can be cracked using dictionary attacks, OTP can be brute-forced, and biometrics can be manipulated using masterprints or techniques, such as image processing, which generates similar finger prints of the authentic user. Therefore, multi-layer authentication systems are adopted by several organizations to secure their sensitive resources and provide seamless services to the users without any security hindrances.

- Authorization—Once the user in the public internet is authenticated, he/she can utilize various internet applications. However, from the security perspective, an attacker can impersonate the authentic user to maliciously read and write confidential information of the validated user or may use the services that are not meant for him. Therefore, there is a need to regulate access control mechanisms after authenticating the user, permitting only authorized users to access the system's services and resources. For that, the administrator has to assign roles and permission to the legitimate user in the access control list. For example, a person can authenticate himself by inserting a username and password into the website; once authenticated, based on the roles and permission assigned, he can access or deny the further services in the website. This helps in poising the security and privacy of the WN-based application.

- Encryption—Authentication and authorization help in preserving the privacy of the system. For instance, a web application utilizes the WN to transmit messages from one user to another. One can guarantee that the users who are enrolled with the application are authenticated and authorized to use this service. This is because they are validated and verified by the authentication scheme and authorization mechanism prior to using this application. Nevertheless, the security is violated when the message is in transit; an adversary can access the transit message and try to manipulate it, disobeying the data integrity principles. Therefore, there is a need for incorporating proper encryption standards that obfuscate the message in a way that is not readable by the attackers. There are various encryption methods available, such as public and private cryptosystems comprising advanced encryption standards (AES), Rivest–Shamir–Adleman (RSA), blowfish, triple data encryption standard (DES), and many more. Further, to augment the user's security and privacy, encryption algorithms can employ hashing algorithms, such as secure hash algorithm (SHA) and message digest, that strengths the WN security.

- Characteristic of channel—The aforementioned design factors are for higher-layer WN applications, but with the current exploration of radio frequencies, the attackers dwell in the physical layer security, wherein they exploit radio waves to intercept the ongoing communication. Thus, it is indispensable to understand the wireless channel and secure it by analyzing characteristics, such as bandwidth, data rates, channel quality indicators, i.e., signal-to-noise ratio (SNR), the reference signal received power and received signal strength indicators of the channel. Furthermore, a message generated at the sender machine has to pass through the dynamic wireless channel, which is time variant and has a lot of obstructions, such as interference, multipath propagation, delay, attenuation, path loss, and fading, which deteriorates the data rates of the WN. Therefore, an attacker tries to investigate such indicators to proliferate their physical attacks that dampen the performance of the wireless communication. Hence, it is essential to reinforce the wireless channel with effective channel coding, equalization techniques, and embracing physical layer security.

- Secrecy capacity—The notion of security and privacy in WN is not limited to studying the application and middle layer security, but also needs to investigate different malicious intent propagated at the physical layer. One such mechanism is the secrecy capacity, which is intrinsically associated with the channel capacity, where the channel is the broadcasting or transmitting the message from the legitimate user. Here the intended receiver is treated as an illegitimate user or an eavesdropper who is trying to intercept and decode the message from the legitimate user. An eavesdropper can decode the message if the channel gain between the transmitter and an eavesdropper is higher than the channel gain between the transmitter and receiver. This also means that the eavesdropper has a higher channel capacity resulting in decoding the messages of the users in close proximity. Therefore, as a network analyst, it is imperative to analyze channel gains and data rates to eliminate the eavesdropper from future communication.

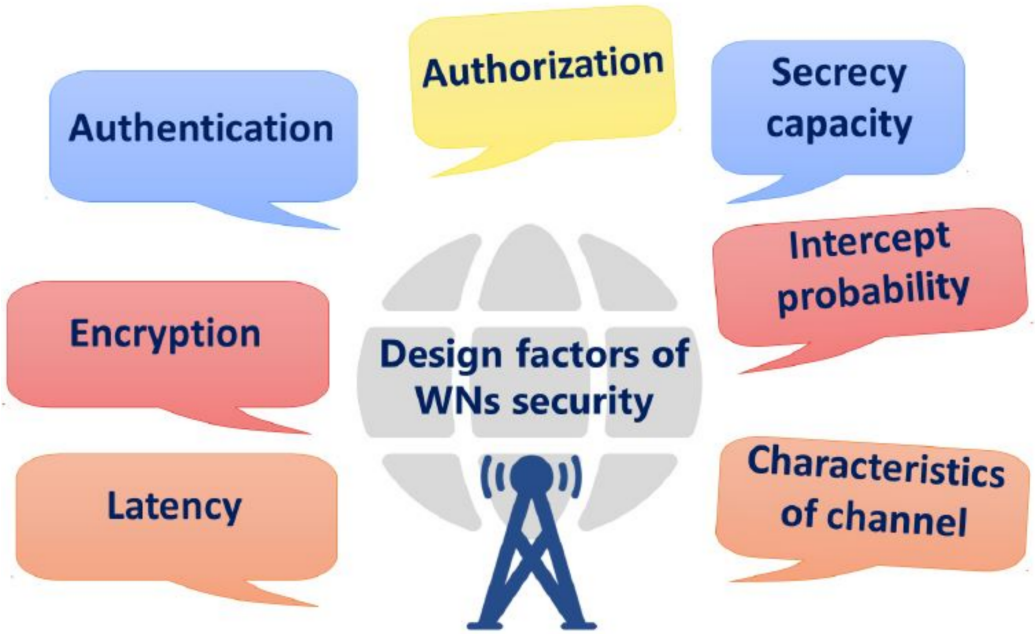

Figure 2. Design factors of wireless networks security.

4. Blockchain Technology

Blockchain is a peer-to-peer (P2P) architecture that weakens the dominance of third-party intermediaries by utilizing decentralization with essential features, such as immutability, reliability, transparency, and security. The blockchain blocks are connected with each other to form a distributed ledger, where each block stores/maintains the hash of the previous block. Any minuscule change in one block reflects the difference in the hash of the other blocks. Therefore, blockchain technology is transparent and reliable against data integrity attacks. Moreover, the distributed ledger is secured by cryptographic techniques, such as digital signatures, hash, and public–private key pairs that validate each transaction whenever a new transaction is added to the blockchain [35][36]. **Figure 3** shows a workflow of a blockchain transaction; wherein a transaction request is broadcast to all the nodes of the blockchain. In addition, digital signatures are used for user identity (a node can sign the document and broadcast it to all other nodes). Then, the private and public keys are used to verify the signature. Then, each block records this transaction to validate it by verifying the hash of the blocks. Moreover, all users connected to the blockchain contain the same updated copy of data which shows transparency within the network. After the successful verification, it is permanently added to the chain of blocks.

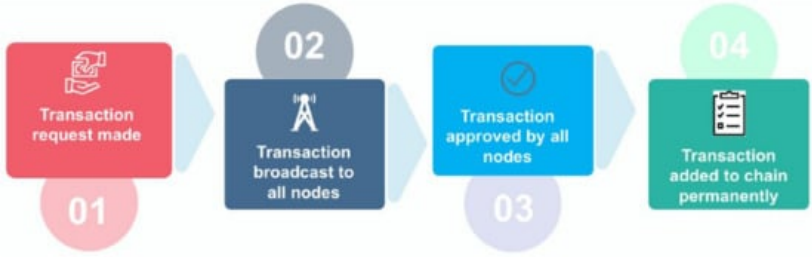

Figure 3. A workflow of the blockchain process.

The distributed nature of the blockchain benefits the WNs in various ways, such as handling the single-point failure issues, incorporating trust mechanisms, secure access control, and preserving the user privacy [37]. It enforces the new security advances to protect the WN from modern security threats, such as cryptojacking and ransomware. Toward this goal, when the WN user publishes (store) the data on the blockchain, it is difficult for an adversary to modify them because of the immutability feature of the blockchain technology. In addition, blockchain immutability can find internal and external attackers by analyzing the change in the hash of the blocks [38][39]. **Figure 4** illustrates unique features of blockchain that strengthen WNs.

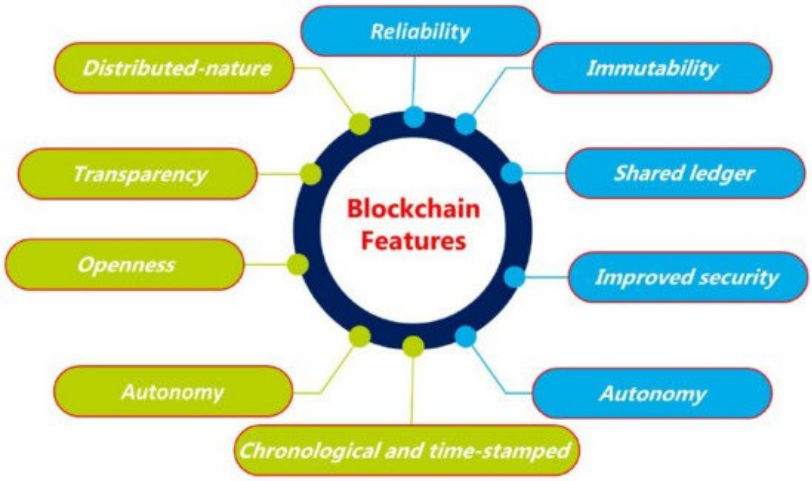

Figure 4. Blockchain features.

5. Blockchain: A Solution for Security and Privacy in WNs

Blockchain records information in the decentralized database (i.e., in a P2P manner) and supports immutability, becoming the critical pillar of future WN's security and privacy. Furthermore, blockchain facilitates secure communication in sophisticated WN technologies such as virtualization, edge, open-source application programming interface (API), network slicing, cloud radio access network (RAN), etc. Toward this goal, researchers proposed an architecture that integrates the blockchain technology to tackle the security issues in different WN applications.

Figure 5 illustrates the proposed architecture of WNs enabled blockchain technology. The entire architecture is divided into three different layers: (i) application layer, (ii) blockchain layer, and (iii) wireless network layer.

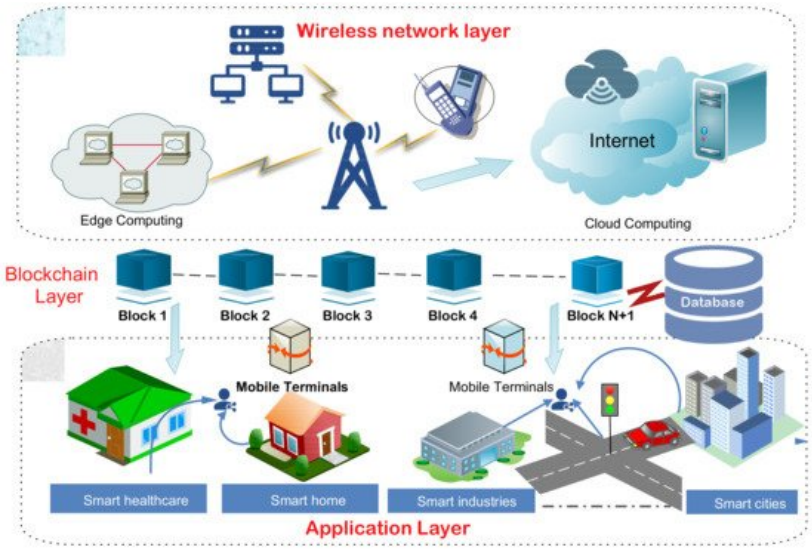

Figure 5. The proposed architecture: enabling blockchain technology for wireless networks.

5.1. Application Layer

This layer comprises various smart applications, such as smart healthcare, smart cities, smart industries, etc. The smart application components are linked via a wired or wireless connection. In the case of wireless connection, communication happens between two users using a mobile terminal. For example, the energy bill is generated through smart meters in the smart home. The energy bill is shared with the consumer (who is consuming energy) and the smart grid administrator via WNs (e.g., 4G or 5G). During data transfer, communication is established from a user device, such as a computer or smartphone to the nearest access point of the WN layer. Then it is transferred further to the intended destination. In the proposed architecture, communication between the application and WN layers through the blockchain layer is discussed in detail in the next section.

5.2. Blockchain Layer

This is the middle layer in the proposed architecture, which establishes secure communication between the WNs layer and the application. First, data generated at the application layer are captured using the blockchain layer over the blocks.

Once it is captured, one cannot alter it due to the immutability feature of blockchain. Then, the data are transferred from the source to the destination node securely using the WN layer. In WNs, blockchain technology offers numerous security services like access control, data integrity, and authentication, which are as follows [10]:

- Access Control: It is a physical layer security that restricts unauthorized users from accessing authorized services running on WN. The conventional access control is centralized and utilizes the standard encryption techniques that lack in providing trust in the WN application. Such a centralized system has a risk of single-point failures and privacy leakages from the key generator schemes. Therefore, as an alternative to centralized access control, trusted blockchain-based access control can help in resolving the above-mentioned issues in WN. To do that, access control permission, i.e., read and write permissions, are only granted to an authorized user, device, and machine. In addition, blockchain uses a smart contract (a set of codes to establish contracts within two parties) to secure the system against any malevolent threat [40].

- Data integrity: Data integrity is another such issue where the attackers tamper with the data of the smart application. As a consequence, the falsified data can mislead the behavior of the smart application. Therefore, storing the data inside the blockchain can ensure that the data are not manipulated. Furthermore, it performs data integrity verification of both the communicating parties by auditing all the transactions that occurred between them [41].

- Authentication: blockchain incorporates authentication capabilities to increase the robustness of the network, which detects and prevents malicious activity in the network resources. Smart contracts perform request authentication to avoid unauthorized access from malicious users [41]. Moreover, it offers a secure and authenticated environment to create virtual WNs (VWNs). Using this network, wireless resource owners can rent their resources, such as infrastructure and a slice of the RF spectrum, to the mobile virtual network operator [10].

5.3. Wireless Network Layer

This layer comprises various 6G services across several vertical sectors, such as vehicle-to-vehicle (V2V), D2D, virtual reality (VR), augmented reality (AR), video streaming, and collaborative gaming to the users residing in the application layer. In addition, it also consists of breakthrough technologies, for instance, SDN, NFV, cloud computing, and many more, that assist in meeting the significant specification of future WNs. The aforementioned services use the precarious wireless networks that hinder the performance of the 6G-based WN applications. This layer plays an important role in establishing a secure connection between sender and receiver using the blockchain layer. Enabling blockchain in WNs can ensure security and reliability in the network by securely storing the data in a distributed manner, i.e., no single stakeholder controls the data; the data are distributed to all the authenticated members of the blockchain. Then, the stakeholder requires a smart contract to establish a service level agreement (SLA) with communicating parties to place the 6G services on lease or share it. The smart contract also automates the resource allocation process (resources such as channel, spectrum, and power) and network orchestration that involve several stakeholders across the entire WNs to provide smooth and transparent service to end-users. Blockchain as the whole process is secure, reliable, and auditable. This integration of blockchain and WNs deliver services that create several other challenges, such as network resiliency, robustness, and data integrity.

References

1. Moya Osorio, D.P.; Ahmad, I.; Sánchez, J.D.V.; Gurtov, A.; Scholliers, J.; Kutila, M.; Porambage, P. Towards 6G-Enabled Internet of Vehicles: Security and Privacy. IEEE Open J. Commun. Soc. 2022, 3, 82–105.
2. Chen, L.; Ji, Z.Z. Wireless Network Security: Theories and Applications; Higher Education Press: Beijing, China, 2013.
3. Porambage, P.; Gür, G.; Osorio, D.P.M.; Liyanage, M.; Gurtov, A.; Ylianttila, M. The Roadmap to 6G Security and Privacy. IEEE Open J. Commun. Soc. 2021, 2, 1094–1122.
4. Timeline from 1G to 5G: A Brief History on Cell Phones. Available online: https://www.cengn.ca/timeline-from-1g-to-5g-a-brief-history-on-cell-phones/ (accessed on 12 May 2021).
5. Ahmad, I.; Shahabuddin, S.; Kumar, T.; Okwuibe, J.; Gurtov, A.; Ylianttila, M. Security for 5G and Beyond. IEEE Commun. Surv. Tutorials 2019, 21, 3682–3722.
6. 4G-LTE/LTE-A Coursework for Computer Networks II. Available online: https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2014_2/rafaelreis/background.html (accessed on 2 March 2022).

7. Tanwar, S.; Vora, J.; Tyagi, S.; Kumar, N.; Obaidat, M. A systematic review on security issues in vehicular ad hoc network. Secur. Priv. 2018, 1, e39.
8. Seddigh, N.; Nandy, B.; Makkar, R.; Beaumont, J.F. Security advances and challenges in 4G wireless networks. In Proceedings of the 2010 Eighth International Conference on Privacy, Security and Trust, Ottawa, ON, Canada, 17–19 August 2010; pp. 62–71.
9. Kundu, S.; Pados, D.A.; Batalama, S.N. Hybrid-ARQ as a communications security measure. In Proceedings of the 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Florence, Italy, 4–9 May 2014; pp. 5681–5685.
10. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for 5G and beyond networks: A state of the art survey. J. Netw. Comput. Appl. 2020, 166, 102693.
11. Makki, S.K.; Reiher, P.; Makki, K.; Pissinou, N.; Makki, S. Mobile and Wireless Network Security and Privacy; Springer US: Berlin/Heidelberg, Germany, 2007.
12. Hakak, S.; Khan, W.Z.; Gilkar, G.A.; Imran, M.; Guizani, N. Securing Smart Cities through Blockchain Technology: Architecture, Requirements, and Challenges. IEEE Netw. 2020, 34, 8–14.
13. Everything You Need to Know about 5G. Available online: https://www.qualcomm.com/5g/what-is-5g (accessed on 3 March 2022).
14. Tahir, M.; Habaebi, M.H.; Dabbagh, M.; Mughees, A.; Ahad, A.; Ahmed, K.I. A Review on Application of Blockchain in 5G and Beyond Networks: Taxonomy, Field-Trials, Challenges and Opportunities. IEEE Access 2020, 8, 115876–115904.
15. Tanwar, S.; Vora, J.; Kaneriya, S.; Tyagi, S.; Kumar, N.; Sharma, V.; You, I. Human Arthritis Analysis in Fog Computing Environment Using Bayesian Network Classifier and Thread Protocol. IEEE Consum. Electron. Mag. 2020, 9, 88–94.
16. 6G Wireless: What It Is and When It's Coming. Available online: https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/6g-wireless-what-it-is-and-when-it-s-coming-networks/ (accessed on 13 May 2021).
17. Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; Gurtov, A. 5G security: Analysis of threats and solutions. In Proceedings of the 2017 IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, Finland, 18–20 September 2017; pp. 193–199.
18. The Role of Cryptography in Information Security. Available online: https://www.triskelelabs.com/blog/the-role-of-cryptography-in-information-security (accessed on 4 March 2022).
19. Cryptography Benefits & Drawbacks. Available online: https://www.tutorialspoint.com/cryptography/benefits_and_drawbacks.htm (accessed on 4 March 2022).
20. Liu, X.; Huang, H.; Xiao, F.; Ma, Z. A Blockchain-Based Trust Management With Conditional Privacy-Preserving Announcement Scheme for VANETs. IEEE Internet Things J. 2020, 7, 4101–4112.
21. Yaqoob, I.; Salah, K.; Uddin, M.; Jayaraman, R.; Omar, M.; Imran, M. Blockchain for Digital Twins: Recent Advances and Future Research Challenges. IEEE Netw. 2020, 34, 290–298.
22. Cryptography in Blockchain: Types & Applications . Available online: https://www.upgrad.com/blog/cryptography-in-blockchain/ (accessed on 4 March 2022).
23. Bodkhe, U.; Mehta, D.; Tanwar, S.; Bhattacharya, P.; Singh, P.K.; Hong, W.C. A Survey on Decentralized Consensus Mechanisms for Cyber Physical Systems. IEEE Access 2020, 8, 54371–54401.
24. Gupta, R.; Tanwar, S.; Tyagi, S.; Kumar, N.; Obaidat, M.S.; Sadoun, B. HaBiTs: Blockchain-based Telesurgery Framework for Healthcare 4.0. In Proceedings of the 2019 International Conference on Computer, Information and Telecommunication Systems (CITS), Beijing, China, 28–31 August 2019; pp. 1–5.
25. Hathaliya, J.; Sharma, P.; Tanwar, S.; Gupta, R. Blockchain-Based Remote Patient Monitoring in Healthcare 4.0. In Proceedings of the 2019 IEEE 9th International Conference on Advanced Computing (IACC), Tiruchirappalli, India, 13–14 December 2019; pp. 87–91.
26. Wang, J.; Ling, X.; Le, Y.; Huang, Y.; You, X. Blockchain-enabled wireless communications: A new paradigm towards 6G. Natl. Sci. Rev. 2021, 8, nwab069.
27. Vora, J.; Tanwar, S.; Tyagi, S.; Kumar, N.; Rodrigues, J.J.P.C. Home-based exercise system for patients using IoT enabled smart speaker. In Proceedings of the 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), Dalian, China, 12–15 October 2017; pp. 1–6.
28. Generations of Mobile Networks: Explained. Available online: https://justaskthales.com/us/generations-mobile-networks-explained/ (accessed on 12 May 2021).

29. Gupta, R.; Tanwar, S.; Tyagi, S.; Kumar, N. Tactile Internet and its Applications in 5G Era: A Comprehensive Review. Int. J. Commun. Syst. 2019, 32, e3981.
30. Gupta, R.; Reebadiya, D.; Tanwar, S. 6G-enabled Edge Intelligence for Ultra -Reliable Low Latency Applications: Vision and Mission. Comput. Stand. Interfaces 2021, 77, 103521.
31. Kakkar, R.; Gupta, R.; Tanwar, S.; Rodrigues, J.J.P.C. Coalition Game and Blockchain-Based Optimal Data Pricing Scheme for Ride Sharing Beyond 5G. IEEE Syst. J. 2021, 1–10.
32. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A survey on wireless security: Technical challenges, recent advances, and future trends. Proc. IEEE 2016, 104, 1727–1765.
33. Tanwar, S.; Tyagi, S.; Kumar, N.; Obaidat, M.S. LA-MHR: Learning Automata Based Multilevel Heterogeneous Routing for Opportunistic Shared Spectrum Access to Enhance Lifetime of WSN. IEEE Syst. J. 2019, 13, 313–323.
34. Check Point Software Technology Limited: What is Network Security? Available online: https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/ (accessed on 17 May 2021).
35. Siyal, A.A.; Junejo, A.Z.; Zawish, M.; Ahmed, K.; Khalil, A.; Soursou, G. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography 2019, 3, 3.
36. Kumari, A.; Gupta, R.; Tanwar, S.; Kumar, N. Blockchain and AI Amalgamation for Energy Cloud Management: Challenges, Solutions, and Future Directions. J. Parallel Distrib. Comput. 2020, 143, 148–166.
37. Gupta, R.; Tanwar, S.; Kumar, N.; Tyagi, S. Blockchain-based Security Attack Resilience Schemes for Autonomous Vehicles in Industry 4.0: A Systematic Review. Comput. Electr. Eng. 2019, 86, 106717.
38. Dwivedi, S.K.; Amin, R.; Vollala, S.; Chaudhry, R. Blockchain-based secured event-information sharing protocol in internet of vehicles for smart cities. Comput. Electr. Eng. 2020, 86, 106719.
39. Gupta, R.; Kumari, A.; Tanwar, S.; Kumar, N. Blockchain-Envisioned Softwarized Multi-Swarming UAVs to Tackle COVID-I9 Situations. IEEE Netw. 2021, 35, 160–167.
40. Zhang, Y.; Kasahara, S.; Shen, Y.; Jiang, X.; Wan, J. Smart Contract-Based Access Control for the Internet of Things. IEEE Internet Things J. 2019, 6, 1594–1605.
41. Liu, B.; Yu, X.L.; Chen, S.; Xu, X.; Zhu, L. Blockchain Based Data Integrity Service Framework for IoT Data. In Proceedings of the 2017 IEEE International Conference on Web Services (ICWS), Honolulu, HI, USA, 25–30 June 2017; pp. 468–475.
