Wireless Blockchain Meets 6G: The Future Trustworthy and Ubiquitous Connectivity

Haoxiang Luo, *Graduated Student Member, IEEE*, Gang Sun, *Senior Member, IEEE*, Jiacheng Wang, Hongfang Yu, *Senior Member, IEEE*, Dusit Niyato, *Fellow, IEEE*, Schahram Dustdar, *Fellow, IEEE*, Zhu Han, *Fellow, IEEE*

***Abstract*—Blockchain has emerged as a foundational element in establishing trust relationships within networks, demonstrating its reliability and efficacy across diverse applications. It can coordinate all nodes within the network independently of third-party entities for unified decision-making and consistency, and is traceable and immutable, making blockchain particularly attractive for communication networks. Wireless networks are an important part of network and communication systems, their flexibility significantly enhances the coverage of communication systems, making their integration with blockchain undeniably promising. This synergy between wireless communication and blockchain has culminated in the development of Wireless Blockchain Network (WBN). It offers a more trustworthy communication paradigm for the forthcoming sixth-generation (6G) wireless networks. This paper serves as a comprehensive tutorial on the integration of WBN and 6G, to establish trustworthy wireless networks. We begin by defining the WBN and exploring its advantages, underscoring its broad applicability in various 6G scenarios. Furthermore, we present the key technologies underpinning WBN and its critical performance metrics. Subsequently, we provide a series of case studies that illustrate the integration of WBN with 6G use cases, which underscore the utility and effectiveness of WBN in practical communication settings, indicating potential benefits for future networks. Finally, we summarize the current practical blockchain cases deployed by network operators and discuss the future direction of WBN. This tutorial is expected to provide an in-depth exploration of the fundamental principles, technological architectures, and practical applications on the integration of blockchain with 6G.**

***Index Terms*—Blockchain, wireless blockchain networks, blockchain performance optimization, 6G wireless networks, trustworthy networks.**

I. Introduction

A. Background

With the ongoing advancements in communication technology, the development of the sixth-generation (6G) communication systems is progressing rapidly, with expectations for formal commercial deployment in the 2030s [1]. In comparison to the fifth-generation (5G) communication systems, 6G presents a more ambitious vision, aiming to support transmission speeds exceeding 1 Tbps and achieving latency levels between 10 and 100 microseconds [2]. This would represent an efficiency improvement of 10 to 100 times relative to 5G [3]. The enhanced transmission rates associated with 6G enable the provision of a broader and more diverse array of communication services in the future. In particular, wireless communication facilitates a more flexible and ubiquitous networking paradigm for 6G. Consequently, this advancement has led to the emergence of various new communication application scenarios, including autonomous driving [4], implantable medical devices [5], satellite internet [6], and others. With the substantial increase in coverage and the heterogeneity of networks, there is growing concern regarding the security and privacy of 6G, which may be worse than previous generations. For instance, implantable devices that monitor various health metrics pose a significant risk of personal information leakage [7]. Furthermore, the potential repercussions of malicious attacks can be catastrophic, resulting not only in immediate financial losses or damage to personal reputations, but also in the loss of human lives, as evidenced by fatal incidents resulting from attacks on autonomous vehicles [8]. Additionally, the integration of Artificial Intelligence (AI) within 6G networks may facilitate the surveillance of network information, further exacerbating these security and privacy concerns [9].

Fortunately, blockchain, as a novel chain-based distributed ledger technology, possesses features such as decentralization, immutability and traceability. These characteristics offer a robust framework for safeguarding data security and privacy in 6G, positioning blockchain as a necessary enabling technology for establishing trustworthy 6G networks [10], [11], [12]. The security characteristics of 6G networks can be attributed to six key components of blockchain technology [13].

- **Cryptography:** In blockchain technology, cryptography plays a crucial role in data encryption and privacy protection. It emploies the asymmetric encryption algorithm, hash algorithm, homomorphic encryption, Zero-Knowledge Proof (ZKP), Secure Multi-Party Computation (SMPC), etc., to attempt to ensure data security, integrity, and immutability [14], thus enhancing the blockchain privacy [15]. This cryptographic method will provide a strong guarantee of information security for 6G.

H. Luo, G. Sun, and H. Yu are with the Key Laboratory of Optical Fiber Sensing and Communications (Ministry of Education), University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: lhx991115@163.com; {gangsun, yuhf} @uestc.edu.cn).

J. Wang and D. Niyato are with the College of Computing and Data Science, Nanyang Technological University, Singapore 639798 (e-mail: {jiacheng.wang, dniyato} @ntu.edu.sg).

S. Dustdar is with the Distributed Systems Group, TU Wien, Vienna 1040, Austria, and also with the ICREA, Universitat Pompeu Fabra, Barcelona 08002, Spain (e-mail: dustdar@dsg.tuwien.ac.at).

Z. Han is with the Department of Electrical and Computer Engineering at the University of Houston, Houston, TX 77004, USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul 446-701, South Korea (e-mail: hanzhu22@gmail.com).

The corresponding author: Gang Sun.

- **Peer-to-Peer (P2P) Network:** The P2P network serves not only as the foundational infrastructure for implementing the blockchain, but also facilitates direct data exchange between blockchain nodes [16]. This capability is essential to achieve decentralization in a blockchain system, thus avoiding a single-point failure (SPF). As a result, its P2P characteristics will also build a robust elastic network for 6G.
- **Consensus Mechanism:** The consensus mechanism facilitates consistency among all blockchain nodes without needing a third-party trusted entity, thereby mitigating the risk of compromised sensitive information by centralized nodes [17]. Furthermore, it can establish security thresholds for the network to resist faculty or Byzantine nodes. This benefit means a consensus-based 6G network can fully automate management and decision making. In general, the common consensus includes Proof of Work (PoW) [18], Practical Byzantine Fault Tolerance (PBFT) [19], Raft [20], corresponding to the public chain, consortium chain, and private chain.
- **Smart Contracts:** Smart contracts are computer programs operating on the blockchain that function as automated agents, designed to facilitate the execution of blockchain tasks by enabling mutual collaboration between users when predefined conditions are satisfied [21]. The execution of smart contracts is independent of any third party, ensuring that no entity can alter the terms of the contract. This characteristic enhances the reliability and trustworthiness of the transaction process and its outcomes, and also provides 6G with an intelligent resource trading environment.
- **Distributed Database:** In addition to decentralized P2P networks, the distributed nature of blockchain is further attributed to its data storage methodologies. Each transaction is redundantly backed up across all nodes, which enhances the disaster resilience of the system. Even if a local node fails, the data can still be recovered from other nodes, ensuring the continuity of services [22], [23]. When the blockchain enables 6G, the network will also have such characteristics.
- **Incentive Mechanism:** It can be categorized into monetary and non-monetary incentives aimed at encouraging participant engagement [24]. Monetary incentives increase the costs associated with aggressive or selfish behavior by promoting economic balance within the system. Conversely, non-monetary incentives foster cooperation among participants by leveraging the reputation of nodes, thereby encouraging honest interactions. This approach will effectively mitigate the potential malicious activities of nodes within the 6G network.

Due to the components mentioned above, blockchain possesses robust security features, extending to the security of the 6G wireless networks facilitated by blockchain. As illustrated in Fig. 1, blockchain plays a significant role across wireless networks, particularly in 6G. This also highlights the emerging research trends surrounding the application of blockchain, including the Internet of Things (IoTs) [25], Internet of Vehicles (IoVs) [26], Internet of Drones (IoDs) [27], Space-Air-Ground Integrated Networks (SAGINs) [28], and Web 3.0 [29].

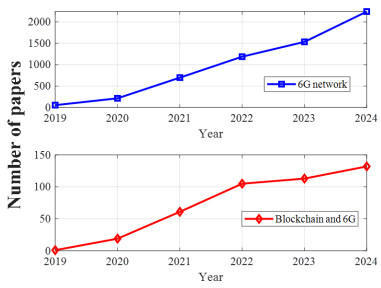


Fig. 1. The number of published papers by searching "6G Network" [30] and "Blockchain and 6G" [31] in Web of Science (Access date: May-10-2025).

B. Motivations and Related Works

Blockchain has garnered significant success across a variety of networking scenarios, showcasing its potential utility in facilitating the development of 6G. Research at the intersection of blockchain and 6G can be categorized into two primary areas: *one focuses on how blockchain can enhance 6G wireless networks* [32], while the *other addresses the performance modeling and optimization of blockchain systems within the context of 6G* [33]. Since 6G networks is created and maintained by specific organizations such as operators, certain licenses are required to join this network. Therefore, the blockchain oriented towards 6G should be a permissioned chain.

In the first category, blockchain offers a comprehensive suite of solutions for 6G, encompassing identity authentication, data sharing, spectrum management, circumvention of adversaries, and others, all of which are designed to provide a secure and reliable network environment for 6G [11]. In the second category, it is important to note that the original design of blockchain was primarily intended for wired networks, specifically to facilitate digital currency transactions [18]. Therefore, when applied to wireless network scenarios such as 5G and 6G, its existing communication modes are susceptible to challenges posed by channel fading, path loss, and other factors, particularly impacting consensus performance [34], [35]. The above enable functions and the unique requirements of 6G present significant challenges for the blockchain will be described in detail in Section II.

While blockchain offers several advantages for 6G networks, it also presents a distinct set of challenges. Notably, the inherent complexity of blockchain technology can lead to suboptimal performance, which may prove insufficient for supporting 6G in delivering high-quality and efficient communication services. These performance limitations primarily pertain to scalability, efficiency, consensus success rate, and related factors [36], [37]. Additionally, the deployment cost of blockchain in 6G networks poses a significant challenge, particularly in light of the complex geographical distribution and dynamic wireless communication environments that characterize the real world [38], [39], [40]. However, these challenges should not overshadow the potential of blockchain within the

TABLE I
SUMMARY OF RELEVANT WORKS WITH OUR TUTORIAL

Type	Year	Ref.	Contributions	Blockchain	WBN for 6G	WBN in 6G
Survey	2019	[35]	Review the performance of different consensus in IoT	✓	✗	✗
	2020	[41]	Discuss the process, classification, performance, and application of blockchain consensus	✓	✗	✗
	2021	[32]	Introduce the work on blockchain-based 6G and propose a unified blockchain-based radio access network	✓	✓	✗
	2021	[42]	Review the work on blockchain and IoT-based smart cities and propose a decentralized IoT architecture	✓	✗	✗
	2021	[43]	Review blockchain networks from topology and neighbor discovery, over block and transaction propagation, to sharding and off-chain networks	✓	✗	✗
	2022	[44]	Introduce the secure, transparent, decentralized services that blockchain provides for 6G, and discuss future challenges and research directions	✓	✓	✗
	2022	[45]	Discuss the privacy protection scheme provided by blockchain for 6G-powered IoV, and future challenges	✓	✗	✗
	2022	[46]	Discuss the resources required for different blockchain consensus to operate in a wireless network	✓	✗	✗
	2022	[47]	Discuss the system architecture, features, and security threats of blockchain-enabled SAGIN	✓	✓	✗
	2023	[13]	Discuss blockchain systems, technologies, and applications from a methodological perspective	✓	✗	✗
	2023	[17]	Focus on the theoretical foundations, models, classifications, and challenges of the blockchain consensus	✓	✗	✗
	2023	[27]	Review the privacy and security integrated drone communication with the assistance of blockchain	✓	✓	✗
	2023	[48]	Discuss applications and challenges of the integration of blockchain and AI for 6G wireless networks	✓	✓	✗
	2023	[49]	Introduce the definition, architecture, design, and comparison of different blockchains	✓	✗	✗
	2024	[50]	Investigate basic principles, communication models, failure models, and applications of consensus in wireless networks	✓	✗	✓
	2024	[51]	Introduces how the convergence of blockchain and AI can optimize future wireless networks, as well as limitations	✓	✓	✗
	2024	[52]	Describe blockchain-assisted 6G services, deployment, and their benefits and limitations	✓	✓	✗
	2024	[53]	Explore the components of blockchain at the micro level, and propose a vision for its scalability	✓	✗	✗
	2024	[54]	Investigate the related work on the integration of blockchain and AI, and introduce its impacts and benefits	✓	✗	✗
Tutorial	2020	[55]	Discuss the concepts, challenges, and future directions of blockchain, and discuss the usability and data integrity of the blockchain, as well as its limitations	✓	✗	✗
	2021	[25]	Discuss blockchain-based security IoT	✓	✗	✗
	2022	[56]	Discuss the definition, motivation, and method of the integration of blockchain and edge intelligence	✓	✗	✗
	2023	[57]	Introduce the ledger structure, key technologies, and applications of blockchain	✓	✗	✗
	—-	Our work	Discuss the key technologies of wireless blockchain networks, performance optimization, and present their integration with 6G, applications, and future challenges	✓	✓	✓

6G. Rather, they should be viewed as novel areas for further research and development. Enhancements and modifications of traditional blockchain to address these issues effectively could facilitate substantial advancements in the establishment of trustworthy 6G networks.

In light of the growing interest in the convergence of blockchain and 6G networks, this tutorial has outlined a comprehensive survey and tutorials related to blockchain and blockchain for various wireless network scenarios. Table I provides a comparative analysis of these papers in relation to our tutorial. These works include surveys and tutorials.

The surveys can be categorized into two areas of focus. The first area centers on the blockchain itself. For instance, [17], [35], and [41] primarily explore key functional modules of blockchain, namely the consensus mechanism, and provide an analysis of its performance and working process. Additionally, [13], [43], [49], and [53] offer comprehensive examinations of blockchain technology, discussing its concepts, architecture, component modules, design frameworks, and optimization methodologies, while also contemplating future development

trends, particularly concerning scalability. Notably, the authors in [43] concentrate specifically on the networking modes of blockchain. Building upon this foundation, the authors in [46] and [50] introduce the concept of Wireless Blockchain Networks (WBNs), which considers the deployment of blockchain within wireless environments and analyzes the resource consumption associated with consensus operations in these networks, including communication cost and transmission power. This concept serves as the basis for the more detailed analyses presented in Sections II-IV. The second category of surveys focuses on blockchain applications across various domains, such as IoD [27], smart cities [42], IoV [45], SAGIN [47], wireless networks [51], and 6G communications [32], [44], [48], [52]. In particular, the discussions surrounding 6G demonstrate the capability of blockchain to establish a secure framework for these advanced communication systems. Furthermore, the works cited in references [48], and [51] highlight additional possibilities for integrating blockchain with AI for 6G. However, these works involving blockchain and 6G only focus on the enabling effect of blockchain on 6G, lacking discussion and optimization of the blockchain.

At present, there are not many comprehensive tutorials on blockchain. For instance, [55] and [57] give us a comprehensive understanding of the concepts, technologies, and challenges of the blockchain. In [25], the authors discuss the security and privacy protection solutions that blockchain provides for IoT. Meanwhile, [56] highlights the motivations, solutions, and potential benefits of integrating blockchain with AI. As an important application scenario of blockchain, the wireless blockchain network is about to usher in large-scale deployment in the 6G era. Thus, a systematic and comprehensive tutorial is necessary for researchers and engineers.

Building upon the aforementioned works, we identify several gaps in the current comprehensive surveys or tutorials on the integration of blockchain with 6G communications:

- **Q1.** The existing works predominantly center on the advantages that blockchain offers to 6G and the associated design schemes, often overlooking the considerations and discussions regarding the deployment of blockchain within 6G wireless environments.Especially the terahertz (THz) and millimeter-Wave (mmWave) high-frequency signals that are about to be deployed in 6G are affected by the environment to a much different extent than wired networks and early wireless networks. Their signal strength is more prone to attenuation. Therefore, a thorough performance analysis of WBN in this high-frequency signal environment is an indispensable key for it to provide high-quality security guarantees for 6G.
- **Q2.** The application scenarios involved in this type of work also lack the consideration of new communication requirements and blockchain performances in the 6G era. For example, in 5G, there is a demand for Ultra-Reliable and Low-Latency Communication (URRLC), enhanced Mobile BroadBand (eMBB), and massive Machine Type Communication (mMTC). The three demands in 5G all require performance improvements in the 6G era. 6G has also expanded into three additional new scenarios, namely, ubiquitous connectivity, Integrated Sensing and Communication (ISAC), and Integrated AI and Communication (IAAC). Compared with the scalability and latency performance that traditional blockchains focus on, these improved demands and new scenarios pose different challenges to WBN, such as energy consumption, high mobility, and integration with AI. Consequently, to facilitate the effective integration of blockchain with 6G, it is imperative to develop application cases that specifically address the unique demands of 6G.
- **Q3.** Due to the lack of a comprehensive tutorial on the integration of blockchain and 6G, there is a gap in understanding the role and application of blockchain in the 6G framework. Meanwhile, the case for the actual deployment of blockchain in wireless networks managed by network operators has not yet been summarized.

C. Contributions

In contrast to existing surveys and tutorials, our tutorial places a particular emphasis on the deep integration of blockchain technology with 6G communications to facilitate the establishment of trustworthy wireless networks. This focus encompasses not only the mechanisms by which blockchain enhances 6G but also an analysis of the blockchain performance within 6G environments. Consequently, potential readers of this tutorial are regarded as scientists, researchers, engineers, students, network operators, etc., interested in blockchain and wireless communication, especially the blockchain network layer. Our contributions to this tutorial can be summarized as follows:

- We initially cover how 6G networks are being shaped by blockchain, including the definition of WBN, and 6G communication requirements. Consequently, we present the motivation for using WBN in 6G, supplemented by two illustrative examples that highlight both the challenges and implications associated with WBN for 6G and WBN in 6G respectively.
- We provide a comprehensive tutorial on WBN key techniques and performance optimization in 6G networks. The former includes Wireless Blockchain Consensus (WBC), sharding for WBN, node deployment, and message propagation. For the latter, we improve the performance of WBN from consensus success rate, consensus efficiency, and consensus cost.
- We present several applications as case studies on the convergence of blockchain and 6G, namely IoV, symbiotic communication, SAGIN, Web 3.0, and SAGIN. Based on trustworthiness, these applications can correspond to Hyper-Reliable and Low-Latency Communication (HRLLC), massive communication, immersive communication, and ubiquitous connectivity.
- We summarize the instances of network operators who have deployed blockchain to service wireless networks in recent years. Then, we discuss potential directions for blockchain and 6G fusion research regarding heterogeneous dynamic networks, ISAC, and IAAC, providing insights into how blockchain will evolve and continue to influence future 6G network design.

This article has been accepted for publication in IEEE Communications Surveys & Tutorials. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/COMST.2025.3593918

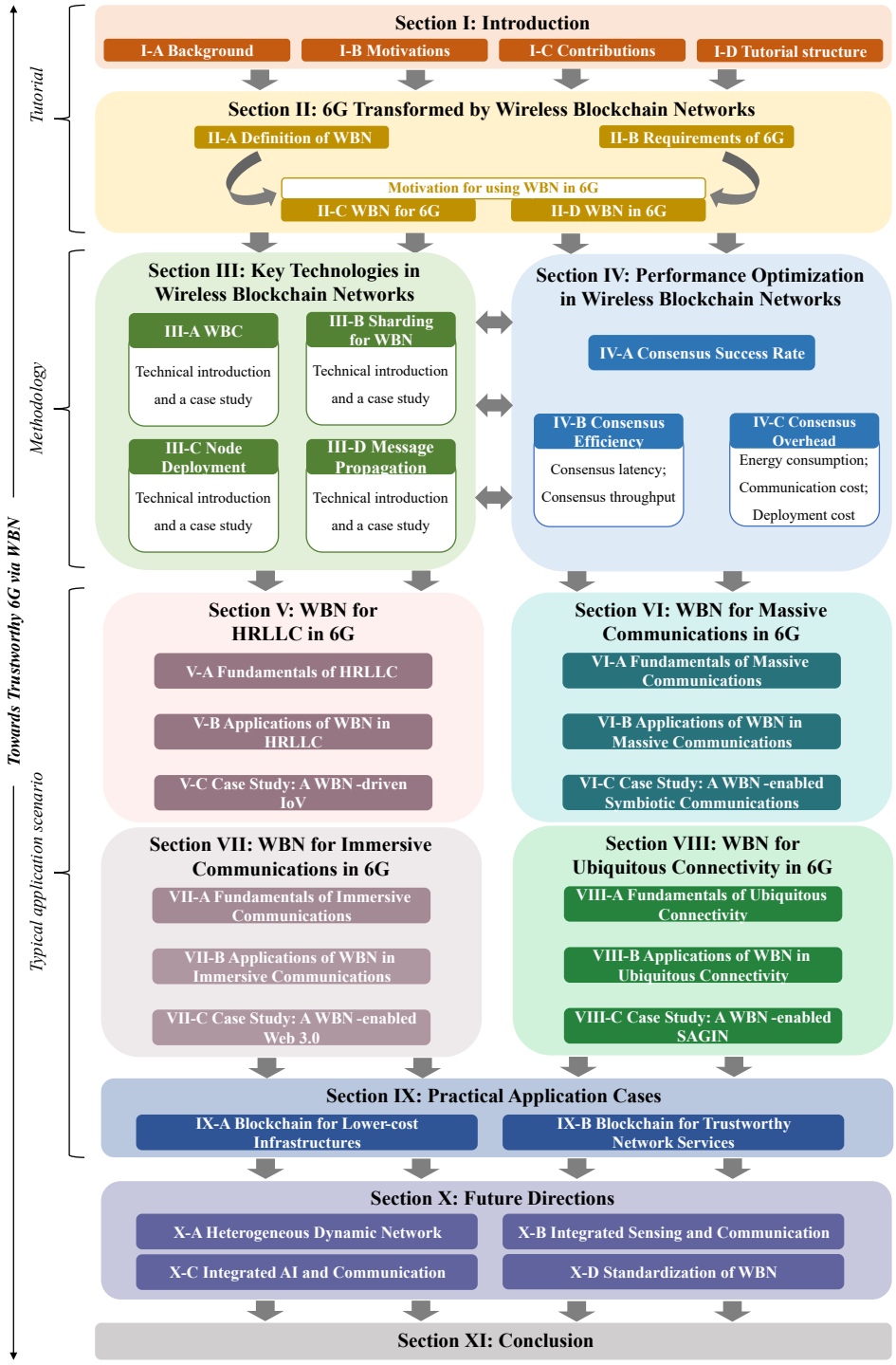


Fig. 2. Structure of our tutorial.

D. Tutorial structure

As shown in Fig. 2, the rest contents are structured as follows: We first look at how WBN can transform 6G networks in Section II. Then in Sections III and IV, the key technologies and performance optimization of WBNs are discussed. In Sections V-VIII, we show several application scenarios for WBN to enable 6G, namely HRLLC, massive communication, immersive communication, and ubiquitous connectivity. Then, in Section IX, we sum up the cases of network operators deploying blockchain-served wireless networks in recent years. In addition, we outline potential research directions in Section X. Finally, Section XI summarizes this tutorial.

II. 6G Transformed by Wireless Blockchain Networks

This section introduces the background and basic principle of WBN-enabled 6G. Specifically, we present the definition of

This article has been accepted for publication in IEEE Communications Surveys & Tutorials. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/COMST.2025.3593918

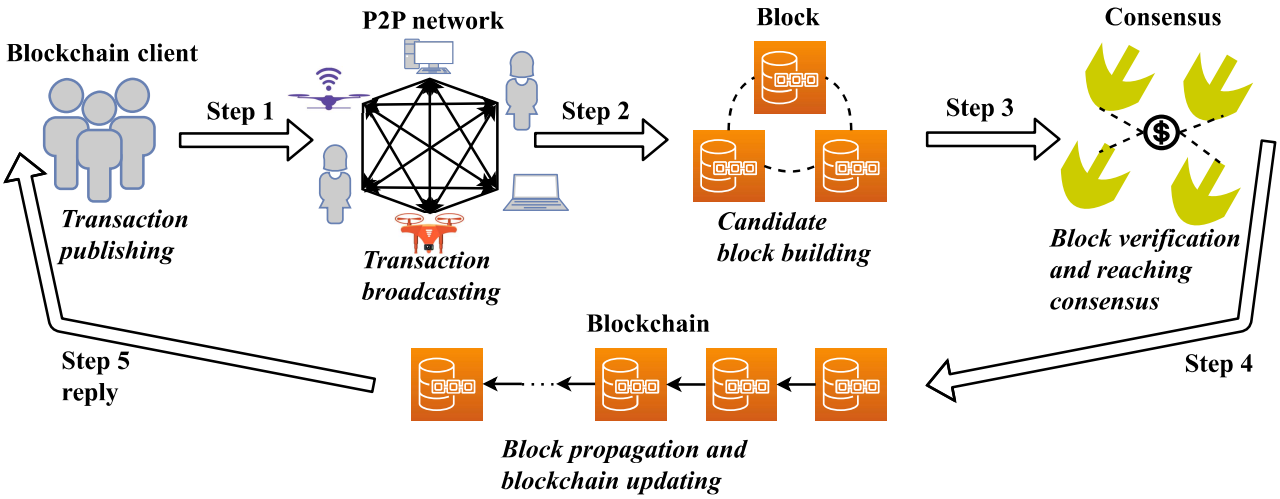


Fig. 3. Blockchain workflow. 1) The client publishes the transaction. 2) Through the P2P network, the transaction is broadcast to the whole network. 3) Multiple transactions are packaged into one block. 4) Determine the legitimacy of the block through the consensus mechanism. 5) The legitimate block is linked to the chain and the blockchain is updated. 6) The result is replied to the client.

WBN and discuss the requirements for 6G communications. Finally, we illustrate the motivation for using and improving WBNs in 6G from two aspects of WBN in 6G and WBN for 6G combined with case studies.

A. Definition of WBN

Before discussing how WBNs can transform 6G, it is necessary to introduce the concept of WBN, and its differences from traditional blockchain networks to carry out targeted performance research and optimization.

The initial purpose of blockchain is to facilitate the decentralized financial industry, leading to the emergence of several prominent digital currencies, including Bitcoin [18] and Ethereum [58]. Communication models within this sector typically rely on stable wired networks, consequently, the original design of blockchain did not account for unstable wireless networks. Nevertheless, due to its advantages in distribution and security, blockchain has progressively expanded its applicability to include wireless networks. Therefore, the concept of WBN arises naturally when the nodes within a blockchain system utilize wireless communication to establish the blockchain network [46].

Next, we will focus on the operational differences between WBNs and traditional blockchain systems brought about by wireless networking. Although various blockchain systems show some differences due to their deployment scenarios, their working principles are consistent [13], [59]. That is, the common operational steps of the blockchain shown in Fig. 3, namely transaction publishing, transaction broadcasting, transactions packaging into blocks, block consensus, and block on-chain. Through these processes, transactions are propagated in the P2P network, and multiple transactions are packaged into blocks, which are then attached to the chain based on the decision of the consensus mechanism [60]. Notably, each block incorporates the preceding block's hash, thereby rendering both the linked blocks and transaction data immutable. This decentralized architecture facilitates robust and secure operations within the blockchain, providing significant advantages such as resistance to tampering and the elimination of SPF [61], [62].

From this, we can find that the steps pertinent to the network environment and performance encompass the broadcasting of transaction and block information, as well as block consensus. Given that the former operations all involve spreading messages across a blockchain network, we can combine them as "message propagation". The subsequent process is designated as WBC within the WBN [63]. Moreover, sharding has the potential to significantly enhance the consensus performance of the blockchain, particularly in terms of scalability [64], and is closely associated with various network parameters [65]. Thus, it warrants consideration within the WBN. Additionally, the deployment of blockchain in a wireless environment must take into account factors such as node geographical distribution and transmission power, as these elements are influenced by wireless channels [48], [51]. Consequently, node deployment is also a critical consideration in the design of WBNs. The four major differences between WBNs and traditional blockchains summarized above, provide important ideas for our discussion in Section III. That is to say, other technologies that are not related to the communication environment or network parameters but may also have an impact on the blockchain operation are out of the scope of this tutorial. Since we pay more attention to the opportunities and challenges at the network level when WBN and 6G are integrated.

B. Requirements of 6G

Previous generations of communication security have relied on supplementary mechanisms, such as cryptography. This "patch" design approach has resulted in the underlying network being susceptible to various security threats, particularly in identity authentication, access control, and network communication, while also incurring additional costs. Consequently, the initial design objectives of the 6G network aimed to

This article has been accepted for publication in IEEE Communications Surveys & Tutorials. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/COMST.2025.3593918

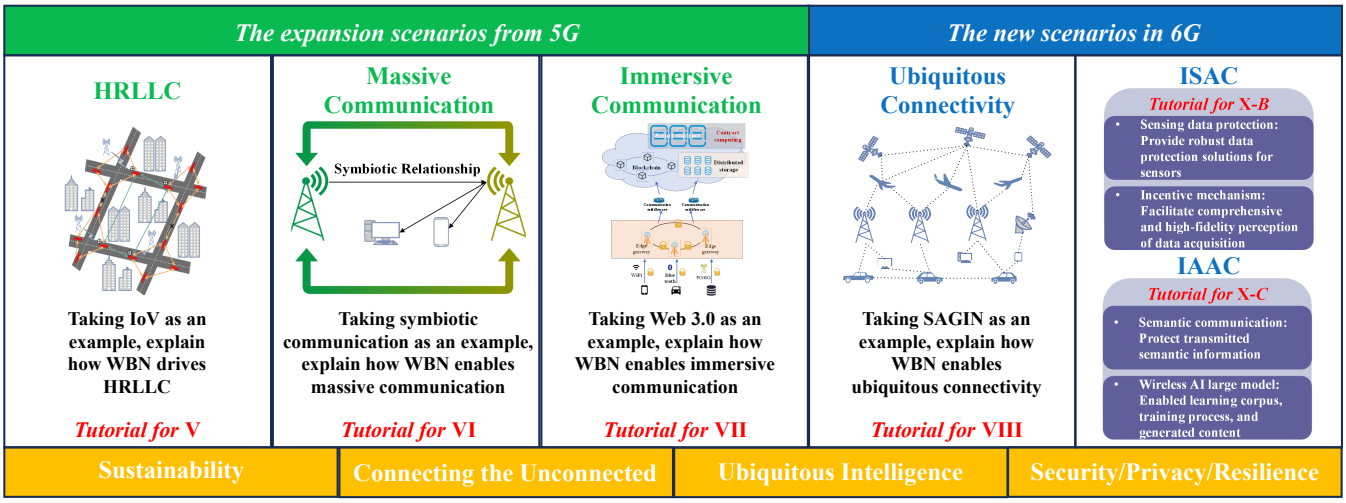


Fig. 4. Scenarios for 6G in IMT-2030. HRLLC, massive Communications, and immersive communications come from the expansion of 5G. We use IoV, symbiotic communication, and Web 3.0 as examples to demonstrate the empowerment of WBN in Sections V-VII. Ubiquitous connectivity, ISAC, and IAAC are new scenarios in 6G. We use SAGIN as an example to show the enabling role of WBN in Section VIII, and the latter two are discussed in Section X.

achieve the ambitious goal of native security [10], [66], [67], with the intent of establishing a trustworthy wireless network. The security features inherent to blockchain are regarded as a fundamental core technology that can enable the establishment of an native security network within the 6G communication [11], [32], [68], [69], [70], [71].

Moreover, building upon the foundation of native security, 6G must also address a broader array of communication requirements and anticipated communication scenarios. As shown in Fig. 4, according to the IMT-2030 proposed by the International Telecommunication Union-Radiocommunication (ITU-R), 6G has six usage scenarios and four overarching aspects [72]. Among them, three usage scenarios are derived from the advancements of the 5G communication era, including immersive communication, massive communication, and HRLLC, which correspond to the eMBB, mMTC, and URLLC, respectively. The expansion of these three scenarios means that 6G requires faster data transfer rates, more device connection density, lower latency, and greater reliability. In addition, IMT-2030 envisages three new scenarios for 6G, which are ubiquitous connectivity, IAAC, and ISAC. Ubiquitous connectivity falls under the category of massive communication, however, it exhibits significant variations in terms of coverage and mobility. It is emphasized that, in addition to terrestrial networks, 6G should also incorporate non-terrestrial networks to facilitate cost-effective communication in rural, remote, and sparsely populated areas [6]. IAAC emphasizes the deep integration of AI and 6G communication, so that wireless networks have native intelligence capabilities and efficiency advantages in data transmission and resource interaction [73]. ISAC aims to enable communication and sensing to complement each other. On the one hand, the entire communication network can act as a giant sensor that can better perceive and understand the physical world [74]. On the other hand, the high-precision positioning, imaging, and environmental reconstruction capabilities provided by sensing can help improve communication performance [75].

To successfully facilitate the widespread application of 6G across the above six scenarios, it is essential to adhere to four principles: sustainability, connectivity for the unconnected, security/privacy/resilience, and ubiquitous intelligence. Consequently, when deploying blockchain to support 6G networks, it is imperative to consider these scenarios and meet these principles. Building upon these considerations, we examine the applications and roles of WBN in HRLLC, massive communication, immersive communication, and ubiquitous connectivity in Sections V to VIII. Given that the convergence of blockchain and IAAC, ISAC has not been thoroughly investigated, we address this topic in Section X: Future Directions. It is expected that through such discussions, it can be proved that blockchain can not only shape a trustworthy 6G network, but also apply to different 6G scenarios and needs.

C. Wireless Blockchain Networks for 6G

In this part, we focus on the enabling effect of WBNs on 6G. The WBN is attractive for 6G networks to achieve native security. Specifically, its role can be divided into trusted resource sharing, secure data interaction, and privacy protection. Table II summarizes the blockchain components corresponding to these functions.

Trusted Resource Sharing: The rapid proliferation of diverse mobile services necessitates substantial network resources, such as spectrum and infrastructure, which are often limited and need to be shared to enhance utilization and improve efficiency [76]. However, in practice, the separation among resource hosts frequently impedes effective resource sharing. Additionally, resource hosts may lack the necessary incentives or may face cost and security considerations that render coordination and cooperation among network entities impractical. Conversely, the advent of new functionalities, such as Mobile Edge Computing (MEC), [77], Software-Defined Networking (SDN) [78], and Network Function Virtualization

TABLE II
ROLES OF WBN AND ITS CORRESPONDING COMPONENTS FOR 6G

Roles		Blockchain components
Trusted resource sharing		Smart contract, consensus mechanism, incentive mechanism, distributed database
Secure data interaction	Authentication and access control	Cryptography, consensus mechanism, smart contract, P2P network
	Interactive data verification	
Privacy Protection	User privacy protection	Cryptography, consensus mechanism
	Data privacy protection	

(NFV) [79] in the 5G and 6G networks has resulted in an increase in the variety and quantity of network resources, including computing and storage resources. This presents significant challenges for resource management and sharing. Fortunately, WBN sets the conditions, rights, and responsibilities of participants for resource sharing through smart contracts and automatically executes sharing operations. Furthermore, the consensus is utilized to enable network nodes to reach consistency on resource sharing, verifying and confirming the authenticity and legality of the sharing behavior. Meanwhile, an appropriate incentive mechanism will also encourage the participants to share idle resources. Finally, detailed information such as the type, quantity, owner and usage rights of resources is recorded through a distributed ledger and updated in real time to ensure information transparency and traceability. With these processes, blockchain can effectively facilitate collaboration while addressing trust and reliability concerns between disparate network entities, thereby fostering more efficient resource sharing. For example, Maksymyuk et al. [80] design a blockchain-enabled decentralized spectrum resource management framework for 6G. It facilitates the tokenization of spectrum resources and infrastructure, allowing them to be transacted efficiently and credibly within a blockchain ledger.

Secure Data Interaction: As wireless traffic and connection densities continue to surge in 6G, data from diverse sources must interact and collaborate to provide services [81]. However, the absence of trust among data holders participating in wireless networks complicates the security of the data interaction process, as well as the authenticity of the data [82]. Recently, researchers have begun exploring the application of blockchain to establish mutual trust among different devices, thereby creating secure channels for data interactions [83]. Efforts to leverage blockchain to facilitate secure data interactions in wireless networks mainly focus on two key areas: ensuring the trustworthiness of each network participant's identity and enhancing the authenticity of transmitted data. For the former, authentication [84], [85] and access control [86], [87], [88] can be used to ensure the legitimacy of each user equipment (UE)'s identity and prevent attackers from entering the network and spreading false information. For the latter, the combined use of asymmetric encryption and hash algorithms can confirm the data source, and ensure the uniqueness and integrity of data, to prevent it from being tampered with or forged. Then, the consensus mechanism can verify the transaction data to prevent false data entry. In addition, smart contracts can also automate the above-mentioned process, similar to resource sharing. These data are also securely transmitted over the blockchain P2P network. Their cooperation provides a powerful solution for data authenticity [89]. For example, Yang et al. [90] propose a Proof of Event (PoE) consensus for IoV that uses passing vehicles to verify the authenticity of traffic data. Li et al. [91] are looking forward to the data security of AI in 6G networks enabled by blockchain.

Privacy Protection: When different devices communicate over wireless links, the openness of wireless transmission combined with the mobility of these devices raises numerous privacy concerns [92], [93]. For instance, malicious actors may intercept, forward, or manipulate transmitted messages, which frequently contain private identities or confidential data. Consequently, there is an increasing focus on privacy protection within wireless networks. Relying on the powerful cryptographic tools in the blockchain, privacy protection can be effectively achieved. ZKP can prove relevant facts without disclosing private information. Homomorphic encryption can achieve direct calculation of encrypted data, avoiding privacy leakage during the decryption process. For specific examples, we can describe them separately from two aspects: identity and transaction privacy. For the former, blockchains typically utilize pseudonymous strategies to conceal UEs' true identities [94]. In [95], the authors introduce a verifiable and lightweight three-party Replicated Secret Sharing (RSS) protocol into the blockchain for cross-summing of features between overlapping UEs. The integration of this protocol with blockchain not only supports anonymous interactions between participants, but also protects their real identities. For the latter, some blockchain implementation is based on the Hyperledger architecture and construct data storage systems utilizing the Interplanetary File System (IPFS) [96], [97]. Furthermore, the data stored in IPFS is encrypted using public key encryption algorithms, thereby establishing a robust blockchain solution for the private data protection [98]. The above methods provide a reliable security tool for frequent resource and data sharing and trading in 6G networks.

Tutorial with an Example: In this part, we will introduce a typical scenario of WBNs enabling 6G networks as a case study for this tutorial. The False Base Station (FBS) attack has posed significant challenges to 5G and its predecessor communication systems [99]. This attack typically involves FBS positioning themselves near legitimate base stations (BS) to capture System Information (SI) and subsequently replay or broadcast falsified SI to UE at elevated transmission power. This strategy compels the UE to initiate a Radio Resource Control (RRC) setup request, inadvertently establishing a

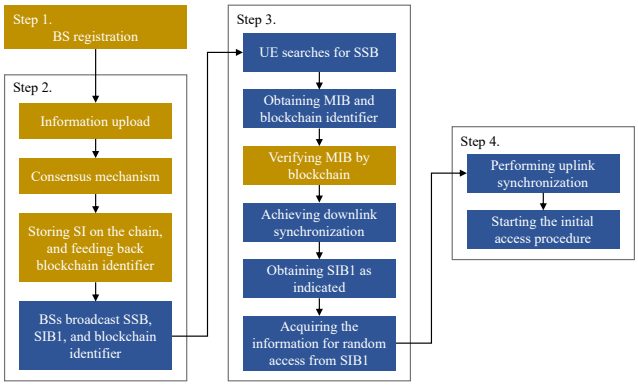


Fig. 5. The Blockchain-enabled SI protection (BeSI) workflow.

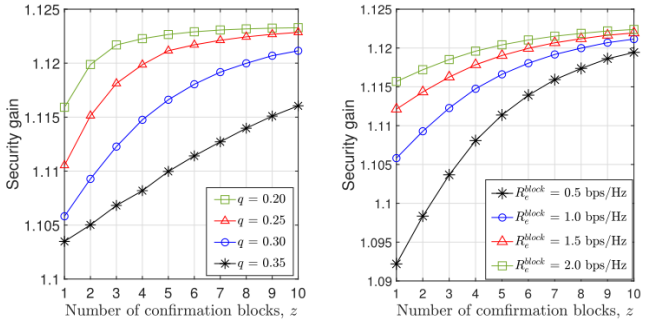
connection with the attacker [100]. Once associated with an FBS, the UE becomes vulnerable to various security threats, including eavesdropping, identity theft, and location tracking [101]. To prevent such attacks, there will be a huge economic cost to society. According to statistics, in January 2023, China used a total of 923 radio monitoring vehicles, 2,457 monitoring and positioning devices, and dispatched 2,459 monitoring personnel for 37,575 hours to combat FBS attacks [102]. Currently, several cryptography-based solutions have been discussed in the Third Generation Partnership Program (3GPP) standardization, including digital signatures, and identity authentication [103]. While these solutions can somewhat mitigate the threat of FBS attacks, there are still some challenges. For example, terminals must trust third parties to generate and manage their keys, which has a high SPF risk. Meanwhile, the complex trust relationship between multiple entities brings difficulties to the unified management of keys, especially in the trend of wireless networks to autonomous and decentralized development. Due to this attack being difficult to root out, it is considered a potential security threat in the 6G era [104].

Fortunately, Wang et al. [105] proposed with blockchain-based solutions to defend against FBS attacks. The authors propose that within a distinct cellular network, the UE acquires essential information about the BS by receiving SI. At the same time, the BS collaboratively maintains a blockchain network to verify and store accurate SI. In light of the potential presence of unknown FBS in proximity, even legitimate BS are regarded as potentially malicious, necessitating the maintenance of trust relationships among the various BS through a consensus mechanism. Building on this framework, the authors have further developed the Blockchain-enabled SI protection (BeSI) scheme, which serves as a mechanism to enhance SI security and prevent UE from inadvertently connecting to FBS.

On the basis of 3GPP [106], [107], the authors proposed the BeSI scheme shown in Fig. 5. The blue box indicates the access process specified in 3GPP, and the yellow box indicates the additional steps specially introduced in BeSI. Furthermore, they summarized BeSI into four steps: BS registration, information upload, cell selection, and random access, as follows.

The **BS registration** means that BS uploads its public key and public key certificate to the blockchain network for registration. The public and private key pairs are configured by the operator, and the public key certificate is also signed by the operator [108]. Subsequently, the BS uploads its public key and certificate to the blockchain network for registration. The blockchain network processes the BS registration request by utilizing the root certificate for verification. Upon successful verification, a registration certificate is issued to the BS. Finally, the pre-registration certificate is replaced with the newly issued one to complete the registration process. Then, is the **information upload** phase, according to the specifications established by the 3GPP, except for certain parameters, such as the system frame number [103], [109], most information elements in cellular communication remain the same, including the Master Information Block (MIB) and System Information Block Type 1 (SIB1). Consequently, pre-validation of the MIB and SIB1 can expedite the consensus process of BeSI. Each authentication request should encompass essential parameters, namely the MIB, cell ID, downlink frequency, and time counter. Once the blockchain network achieves consistency, new blocks containing SI are appended to the chain. Then, a blockchain identifier corresponding to the SI is generated and returned to the BS. Subsequently, the BS broadcasts the blockchain identifier alongside the MIB. Additionally, considering the limitations imposed by physical channel coding [109] and drawing inspiration from [103], blockchain identifiers may be incorporated into the new SIB1. Next for the **cell selection** phase, the combination of a Synchronization Signal (SS) and a Physical Broadcast CHannel (PBCH) is referred to as a SS/PBCH Block (SSB) [110], which is necessary for the UE to establish an initial connection with the cell. Then, the UE detects the SSB based on the frequency band (FB) by the operator, enabling it to achieve downlink synchronization in both the time and frequency domains, and obtaining the corresponding MIB and Physical Cell Identity (PCI), which assigns a distinct identifier to each cell [111]. Consequently, the UE is able to obtain SIB1 by utilizing the information contained in the MIB to detect the physical downlink shared channel. Finally, the UE selects the appropriate cell according to TS 38.133 [112], TS 38.304 [113], and the blockchain verification procedure in [105]. Finally, for the **random access** phase, once the UE verifies the BS to be accessed through the blockchain validation procedure, it can extract information related to the random access procedure, including uplink frequency and the configuration of the Physical Random Access CHannel (PRACH) from SIB1. Following this, the initial access procedure is initiated.

BeSI offers a blockchain-based cell verification mechanism enabling UE to securely access BS. This innovative mechanism enhances the existing schemes outlined by the 3GPP, mitigating the likelihood of vulnerabilities associated with FBS attacks. The specific security analysis is as follows. The authors model the spatial distribution of BS and FBS as a Poisson Point Process (PPP) with densities λ_b and λ_f, assuming that the UE is situated at a geographically central location [114]. BeSI framework subsequently seeks to derive the probabilities of access failure for itself and conventional networks. These probabilities are used as security indicators to evaluate the system. For BeSI, UE access to FBS can be divided into three steps. The first is that the signal sent by BS



(a) z and q (b) z and R_e^{block}

Fig. 6. The impact of z on security gain. (a) z and q. (b) z and R_e^{block}.

to UE is eavesdropped, that is, the security outage [115]. The probability can be denoted as P_{SO}^{block}, which is closely related to R_e^{block}, the redundancy rate that provides security against eavesdropping. It can be obtained by the well-known Wyner eavesdropping channel [116].

Upon successful interception, then, the FBS transmits a deceptive signal to the UE. Within the BeSI, the FBS must undertake an additional step to manipulate the associated UE. Specifically, it is required to initiate a Double Spending Attack (DSA) against the UE [117]. A successful DSA necessitates that the FBS generates a parasite chain that exceeds the length of the main chain of the BS after a specified threshold of z confirmation blocks. From a rational perspective, should the FBS lag by M blocks, it will cease efforts to advance the parasite chain. Where M stands for the maximum number of blocks it can afford to catch up with the main chain. Therefore, similar to [118], the probability of FBS successfully completing a DSA is

$$P_{DSA} = 1 - \sum_{n=0}^{z} \binom{n+z-1}{z-1} (1-q)^z q^n \times \begin{cases} \frac{(\frac{q}{1-q})^{z-n+1}-1}{(\frac{q}{1-q})^M-1} & \text{if } q \neq 0.5, \\ \frac{z-n+1}{M} & \text{if } q = 0.5, \end{cases} \quad (1)$$

where q is the probability that FBS generates the latest block. The value is based on characteristics of the consensus, such as the proportion of the computing power controlled by attackers in PoW or the number of Byzantine nodes in PBFT. Furthermore, it is essential to ensure that the signal quality of the FBS surpasses that of the BS and the probability is P_H^{block}. Therefore, for the BeSI framework, the probability of a successful FBS attack is $P_{FBS}^{block} = P_{DSA} P_{SO}^{block} P_H^{block}$, where P_{SO} denotes the security outage probability and P_H is the probability that the signal quality of FBS is higher than that of BS.

A successful FBS has only two steps for the traditional 3GPP scheme without blockchain, as it does not involve a DSA on the blockchain. Thus, the probability is $P_{FBS} = P_{SO} P_H$.

To quantitatively measure the effectiveness of BeSI against FBS attacks, the authors further define security gain S, which reflects the performance improvements by blockchain, namely

$$S = \frac{1 - P_{FBS}^{block}}{1 - P_{FBS}}. \quad (2)$$

In Fig. 6, the authors set FBS and BS densities of λ_f = 10 $nodes/km^2$ and λ_b = 30 $nodes/km^2$, respectively, the path loss exponent τ = 2.5, bandwidth B = 20 MHz, and block size L = 3616 bits to investigate changes in security gain by varying the values of z, q, and R_e^{block}, where the R_e^{block} = R_e. As illustrated in Fig. 6 (a), the security gain exhibits an increasing trend with the augmentation of z. Additionally, it is evident that the security gain also rises as q decreases. Moreover, Fig. 6 (b) indicates that security gains can be further amplified by increasing the redundancy rate threshold R_e^{block}, associated with FBS eavesdropping in the blockchain.

The BeSI scheme and its simulation results highlight the significant advantages of blockchain in enhancing wireless networks and mitigating potential security threats. This promising efficacy has consequently motivated us to explore the application of blockchain in 6G, intending to establish native secure and trustworthy networks.

D. Wireless Blockchain Networks in 6G

This part focuses on the modeling and optimization of the performance of WBNs in 6G

Considering the security and privacy benefits that blockchain offers in wireless networks, it is anticipated to play a pivotal role in 6G. To effectively facilitate the integration of blockchain within 6G networks, it is imperative to further investigate the performance of blockchain in this context upon its deployment. That is the WBN performance, due to 6G being an extensive wireless network. This part will provide a discussion on WBNs within 6G, addressing key concerns related to its implementation for optimizing its performance, supported by a relevant case study.

In Section II-A, we briefly introduce the four key technologies in WBNs: WBC, sharding, node deployment, and message propagation. We further find that the latter three are essential for WBC to work better. Specifically, sharding allows transactions to be processed in parallel within each shard, thereby avoiding global consensus for more efficient transaction processing [119], [120]. On the basis of meeting the normal operation of the blockchain, node deployment also needs to consider the consensus security threshold to design a low-cost deployment scheme [121], [122]. Message propagation focuses on more efficient dissemination of transactions and block messages, ensuring synchronization of consensus results across the WBN [123], [124], [125]. Therefore, it can be said that the main performance of WBNs is focused on WBC, so that some researchers directly refer to WBNs by wireless consensus networks [46], [126].

Furthermore, WBC working in 6G first needs to comply with the communication standards of 6G, such as native security, sustainability, ubiquitous connection, etc., to apply in various scenarios. Current WBC performance mainly focuses on consensus security (or consensus success rate), consensus latency and throughput, scalability, and required communication resources. Among them, consensus security represents the

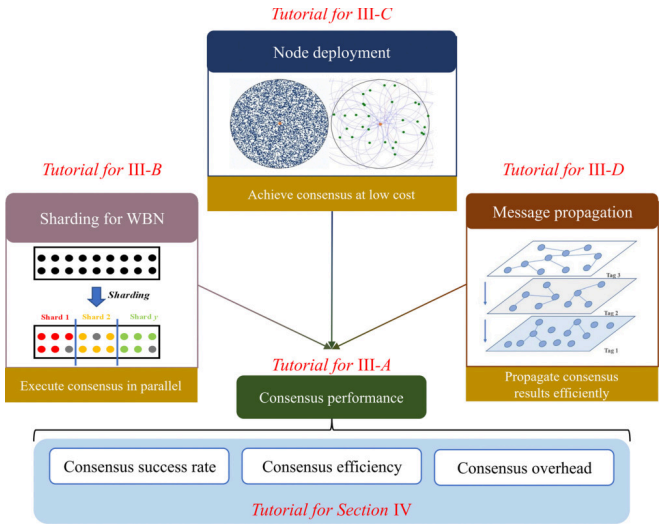


Fig. 7. Key WBN technologies, including WBC, sharding, node deployment, and message propagation, are covered separately in Section III A-D. They all focus on WBN performance, namely consensus success rate, consensus efficiency, and consensus overhead, which are discussed in Section IV.

robustness of the blockchain network, and a higher consensus success rate will maintain a more resilient 6G network when facing Byzantine and faulty nodes [127]. Scalability is often related to communication overhead [36], latency and throughput [128], [129], so it can be combined with the latter into consensus efficiency to promote the efficient operation of 6G. In addition, the communication resources required by WBC in 6G often involve communication costs, communication power or energy consumption, deployment costs, etc. To summarize, this tutorial will concentrate on the consensus performance of WBNs within 6G, as shown in Fig. 7. It will provide a detailed examination of how techniques such as sharding, node deployment, and message propagation can enhance consensus performance, including the consensus success rate, consensus efficiency, and consensus overhead. The above content provides the basis and groundwork for Sections III-IV.

Tutorial with an Example: In this part, we present a thorough analysis of the performance of a classic consensus, PBFT within a 6G environment as a case study for this tutorial. Because it has been widely used in many network fields [130], and is favored by 6G [83], [131].

PBFT allows a maximum of Byzantine or faulty nodes f that exist in WBNs, as long as the relationship $f \leq \lfloor \frac{n-1}{3} \rfloor$ is satisfied, where n is the total number of nodes in the WBN [19]. Upon receiving a consensus request from the client, the consensus process of PBFT is structured into four distinct stages: *pre-prepare*, *prepare*, *commit*, and *reply*. Among them, the *pre-prepare* stage is the primary node that broadcasts a pre-prepare message to each replica. Additionally, the *prepare* and *commit* stages involve n-1 and n nodes making global broadcasting, respectively. Finally, each node feeds back to the client the judgment result of the transaction. In accordance with the fault tolerance threshold of PBFT, the consensus messages received by nodes at each stage must exceed $2f$.

According to the derivation in [132] and [133], the probability of reaching PBFT consensus can be expressed as the probability product of the smooth progress of the four stages, i.e (3). The P_s denotes the probability of successful transmission between two nodes, and its value is related to the wireless environment and geographical distribution. In order to accurately characterize the performance of PBFT in 6G wireless networks, the wireless environment involved will consider high-frequency signals such as THz or mmWave signals deployed in 6G [134], [135].

Furthermore, the authors assume that the consensus nodes of PBFT also conform to PPP, with a node density λ. Subsequently, they randomly select a node to serve as the sending node, establishing it as the center of a circular area with a radius R_a within which the other receiving nodes are distributed. Based on the two-dimensional Poisson distribution, the probability density function that describes the distance r between the sending node and a receiving node can be formulated as follows

$$f(r) = \frac{d(r^2/R_a^2)}{dr} = \frac{2r}{Ra^2}. \tag{4}$$

If the communication between any two nodes satisfies Rayleigh fading, its Signal-to-Interference-plus-Noise Ratio (SINR) can be represented as $\gamma = \frac{p_{PBFT} h r^{-\tau}}{\sigma^2 + I}$, where p_{PBFT} is the node's transmission power. Moreover, to create a 6G environment, the value of path loss exponent τ are adopted as 2.229 [136] and 1.7 [137], corresponding to the 0.22 THz signal and 28 GHz mmWave signal, respectively.

Next, the authors define the sensitivity of receivers for the SINR as η. Accordingly, the average transmission success rate between the two nodes can be expressed as follows

$$\begin{aligned} P_s &= \int_0^{R_a} P\{\gamma > \eta\} f(r) dr \\ &= \frac{2\pi\lambda}{n} \int_0^{\sqrt{n/(\pi\lambda)}} \exp\{\frac{-(\sigma^2 + I) r^\tau z}{p_{PBFT}}\} r dr. \end{aligned} \tag{5}$$

On the basis of obtaining P_s, not only the consensus success rate of wireless PBFT can be derived, namely (3), but also the consensus latency can be obtained according to the following equation [138], [139].

$$1 - P_s = f_Q \left(\frac{NTBC - NTBR + \frac{\log NTB}{2}}{(\log e)\sqrt{NTB}} \right), \tag{6}$$

where f_Q represents the Q function. R and C are the transmission rate and channel capacity, respectively. T denotes latency for a channel and N is the number of subcarriers, which are closely related to the number of channels connected by nodes. Therefore, the first three stages of the PBFT can be denoted as t_1, since these stages involve broadcasting messages to $n-1$ nodes. Conversely, the *reply* latency can be represented by t_2, which is just P2P communication. As a result, the consensus latency is $t_{PBFT} = 3t_1 + t_2 = (3n-2)T$.

Moreover, to assess the extent to which consensus on WBN aligns with the requirements for sustainable and low-energy consumption in 6G, the authors evaluate the transmission energy consumption with wireless PBFT. Specifically,

This article has been accepted for publication in IEEE Communications Surveys & Tutorials. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/COMST.2025.3593918

$$P_{PBFT} = \sum_{i=0}^{f} \left(\binom{n-1}{i} (1-P_s)^i P_s^{(n-1-i)} \sum_{j=0}^{f-i} \left(\binom{n-1-i}{j} (1-P_s)^j P_s^{(n-1-j-i)} \right. \right.$$
$$\left. \left. \sum_{k=0}^{f-i-j} \left(\binom{n-i-j}{k} (1-P_s)^k P_s^{(n-i-j-k)} \sum_{l=0}^{f-i-j-k} \binom{n-i-j-k}{l} (1-P_s)^l P_s^{(n-i-j-k-l)} \right) \right) \right), \quad (3)$$

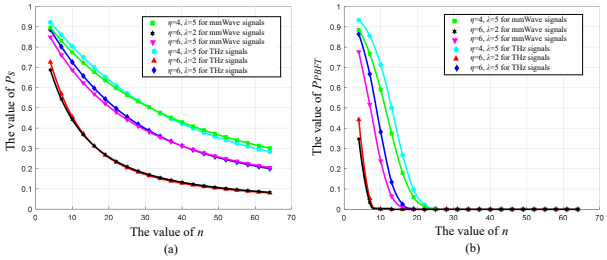


Fig. 8. The success rate of Wireless PBFT in 6G. (a) The value of P_s. (b) PBFT consensus success rate.

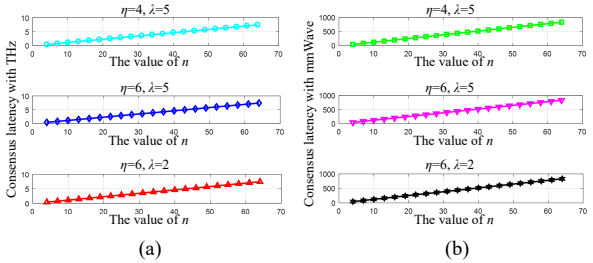


Fig. 9. PBFT consensus latency in 6G. (a) THz signals. (b) mmWave signals.

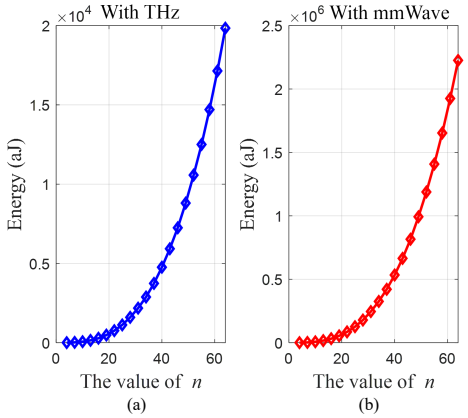


Fig. 10. PBFT consensus energy consumption in 6G. (a) THz signals. (b) mmWave signals.

the four stages of the PBFT consensus process necessitate communications involving $n-1$, $(n-1)^2$, $n(n-1)$, and n nodes, respectively, resulting in a total energy consumption as $E_{PBFT} = (2n^2t_1 - 2nt_1 + nt_2)p_{PBFT}$.

Building upon the preceding theoretical analysis, the authors subsequently conduct simulations to further validate the performance of PBFT within a 6G wireless network. The specific scenarios involved are divided into THz and mmWave signals. Specifically, for the THz scenario, $\tau = 2.229$, $\sigma^2 + I = 0.2$ W, $p_{PBFT} = 1$ W, $B = 10$ GHz, $C = 80$ Gbps, $R = 40$ Gbps; for the mmWave scenario, $\tau = 1.7$, $\sigma^2 + I = 0.2$ W, $p_{PBFT} = 1$ W, $B = 800$ MHz, $C = 8$ Gbps, $R = 4$ Gbps. In addition, to explore the influence of node density and receiver sensitivity on consensus performance, three sets of parameters are designed for comparison in both signal scenes, namely $\eta =$ 6 dB, $\lambda = 2$ $nodes/m^2$; $\eta = 6$ dB, $\lambda = 5$ $nodes/m^2$; $\eta = 4$ dB, $\lambda = 5$ $nodes/m^2$.

Fig. 8 (a) illustrates the success rate P_s. It is observed that as the number of nodes increases, the value of P_s decreases. This trend can be explained by the principles of the PPP, which indicate that a proliferation of nodes within a wireless network leads to increased distances among certain nodes. Concurrently, as these distances grow, the effects of channel fading become more pronounced, resulting in a diminished P_s. Additionally, a smaller η enhances the signal recovery capability of the receiving node, thus contributing to an increased transmission success rate. Conversely, a smaller λ signifies a greater distance between nodes, correlating with a reduced P_s. Moreover, under conditions where η and λ are held constant, the performance of mmWave signals is inferior to that of THz signals when the number of nodes is low. However, as the number of nodes increases, the performance of mmWave surpasses that of THz. Fig. 8 (b) shows the consensus success rate of PBFT in 6G networks. The observed decrease in the P_{PBFT} value with n indicates that mmWave and THz signals are not well-suited for communication in long-distance wireless PBFT networks. Importantly, the results reveal that THz signals exhibit a higher consensus success rate in wireless PBFT networks compared to their mmWave counterparts. This suggests that, in scenarios where the value of n is insufficiently large, a τ within the PPP corresponds to an enhanced consensus success rate.

Figs. 9 (a) and (b) illustrate the PBFT consensus latency experienced at each stage under THz and mmWave signals, respectively. The unit of results is as ($1as = 10^{-18}s$). Both figures exhibit similar fluctuation patterns as the values of n change. However, in the case of mmWave signals, the PBFT latency is two orders of magnitude greater than that observed with THz signals. This disparity suggests that THz signals offer greater bandwidth than mmWave signals, resulting in higher communication rates. Furthermore, the parameters η and λ appear to have minimal impact on latency variations. These results suggest that the influences of receiver sensitivity and node density can be excluded from further evaluations of consensus energy consumption.

Figs. 10 (a) and (b) demonstrate the consensus energy con-

sumption of PBFT under THz and mmWave signals, respectively. In both cases, the consensus energy consumption shows a cubic increase trend concerning the number of nodes n. This trend indicates that, within WBNs, energy consumption may emerge as a critical limiting factor impacting scalability, potentially more so than communication overhead and storage overhead, which exhibit only a square increase concerning n [23], [36]. Such significant growth in energy consumption directly contradicts the sustainability objectives outlined for 6G. Moreover, in a wireless environment, blockchain devices often face challenges in obtaining timely energy supplies, increasing the likelihood of disconnection due to power depletion, which adversely affects the normal operation of the WBN. Therefore, designing a low-energy consensus mechanism for WBNs is necessary to cope with 6G requirements.

III. Key Technologies in Wireless Blockchain Networks

In this section, we will introduce the key technologies underpinning WBN from WBC, sharding, node deployment, and message propagation. These elements play a crucial role in facilitating the efficient execution, dissemination, and practical implementation of transactions within WBN. A further understanding of these technologies can provide us with potential directions for the further optimization of WBN in 6G.

A. Wireless Blockchain Consensus

The consensus mechanism is fundamental to the blockchain system, as it enables participating nodes to add blocks in a synchronized and unique order [17], [41], [140]. This mechanism is critical for maintaining consistency within the network, thereby eliminating the necessity for intervention by a trusted third party [141].

Based on the classification of blockchains, various types of blockchains employ distinct consensus mechanisms. In **public chains**, PoW is one of the most well-known early consensus protocols, initially applied in Bitcoin, which was proposed by Nakamoto [18]. This consensus incentivizes participating nodes to compete in solving complex cryptographic puzzles, with the first node resolving the puzzle assuming the role of the leader successfully. The leader is granted the authority to generate a new block and append it to the blockchain. However, this mechanism has faced significant criticism due to its substantial computational power requirements and high electricity consumption [142], [143]. Proof of Stake (PoS) consensus is currently being implemented in Ethereum as a viable alternative to PoW, primarily due to its energy-efficient properties [144], [145]. In this mechanism, the leader responsible for generating a new block is selected through a cryptographic random algorithm. The likelihood of a node being chosen as the leader is proportional to the amount of cryptocurrency it has staked. Consequently, this system introduces certain drawbacks, such as the potential concentration of resources among nodes with greater financial interests, a phenomenon often referred to as the Matthew effect [146]. Proof of Solution (PoSo) is another prominent consensus mechanism utilized within public chains, specifically developed to address mathematical optimization problems [147]. This approach simulates the principles of PoW by substituting the arbitrary mathematical puzzles characteristic of PoW with meaningful optimization challenges. Building upon the public chains, **consortium chains** enhance the identity verification process for participating nodes. In this model, authority is distributed among multiple governing entities, thereby there is no trust relationship between nodes [148], [149]. Unlike public chains, the consensus mechanisms employed in consortium chains predominantly utilize Byzantine Fault Tolerance (BFT), which aims to achieve consistency among nodes through the regulation and allocation of voting rights. An example is the PBFT consensus, which features a fault tolerance threshold of $1/3$ and exhibits a communication overhead of $O(n^2)$ [19]. To address the high communication overhead issue, various strategies have been proposed, including two-layer PBFT [36] and novel consensus such as HotStuff [150] and Vote-as-a-Proof (VaaP) [151]. The two-layer PBFT reorganizes nodes to achieve a communication overhead of $O(n^{4/3})$. Additionally, both HotStuff and VaaP utilize threshold signatures to disseminate transaction information, significantly reducing communication overhead to $O(n)$. For the **private chains**, characterized by a more stringent access control mechanism, restrict participation to members of the organization operating the blockchain, resulting in a higher degree of exclusivity [152]. This restricted access facilitates increased transaction processing efficiency, as these systems are less susceptible to Byzantine attacks [128]. Consequently, the consensus mechanism employed in private blockchains typically relies on Crash Fault Tolerance (CFT), such as Paxos [153]. It is recognized as the first consensus to achieve strong consistency within an asynchronous network, enabling a distributed system to function logically as a standalone entity. Building upon this work, Raft consensus addresses the notable disparity between consensus theory and practical system implementation that is evident in Paxos [20]. By decoupling the consensus phase and ensuring consistency through stringent constraints, Raft minimizes uncertainty in consensus processes. Consequently, Raft has emerged as a predominant choice for consensus mechanisms in private chains [154].

The blockchain types mentioned above can also be classified into the permissioned chain and permissionless chain. Public chains allow nodes to freely join or exit and represent permissionless chains. Both consortium chains and private chains have certain requirements for the identities of nodes intended to join the network, and thus can be summarized as permissioned chains. In 6G networks, which are operated by specific organizations and have identity management for UEs within them, the permission-chain WBC is often used. Additionally, the consensus mechanisms used across various types of blockchain are predominantly designed for wired environments. In WBNs, the propagation of both transactions and blocks is inherently reliant on wireless channels. As evidenced by the modeling of PBFT in a 6G environment discussed above, factors such as path loss in wireless scenarios pose significant challenges to the effective operation of these consensus mechanisms. This challenge is particularly

pronounced for consortium and private chain consensus mechanisms, which depend on multiple rounds of voting facilitated through communication. In contrast, the impact on public chain consensus is comparatively minimal, as consensus is achieved through problem-solving processes, affecting only the propagation of blocks after consensus attainment [155]. This is why most research efforts on WBC performance have focused on consortium and private chains [132], [133]. To further clarify the role of WBC in WBN, we also use PBFT as an example to demonstrate its performance when implemented with the IEEE 802.11 protocol [156], [157]. This protocol is one of the standards of the wireless local area network, and is an important basis for constructing wireless networks [158].

The consensus success rate of wireless PBFT under the IEEE 802.11 protocol can also be evaluated according to the derivation in (3). The sole distinction lies in the success rate of the consensus messages transmitted within the channel. To quantify this metric more accurately, the authors further investigate the actual PBFT traffic by evaluating the performance of the IEEE 802.11 protocol under unsaturated traffic conditions. Then, the probability of a node broadcasting a message in a random time slot can be obtained by [159]. It can be represented by P_r, which also indicates that this time slot is not occupied by other types of messages (including but not limited to consensus, as non-consensus nodes have been considered), and is closely related to the backspace window size W. Furthermore, the probability of successful transmission of the consensus message in the channel can be deduced by

$$P_s = \frac{(n-1)P_r(1-P_r)^{(n-2)}}{1-(1-P_r)^{(n-1)}}. \tag{7}$$

Consensus latency represents another critical metric warranting evaluation. Unlike the latency assessment of PBFT in 6G discussed previously, the authors incorporate the general medium access latency associated with the IEEE 802.11 protocol involving n competing nodes. According to [160], if the transfer is successful i times, the latency can be expressed as follows

$$t(i) = iT + \frac{1-(1-P_r)^i - iP_r(1-P_r)^{i-1}}{P_r(1-P_r)^{i-1}}T + \frac{1-P_r}{P_r}t_s, \tag{8}$$

where t_s is the idle time slot. Based on this, the latency of *pre-prepare*, *prepare*, *commit*, and the consensus latency of PBFT consensus can be obtained successively.

Furthermore, this study also points out that consensus latency is related to view change, which is neglected in the modeling of PBFT in 6G. A view change may occur when a node receives multiple *pre-prepare* messages that contain the same view and serial number, or when it receives a prepare message from the primary node, even in instances where the primary has not sent the corresponding prepare message [161].

Subsequently, the authors set the sizes of the Medium Access Control (MAC) and Physical (PHY) headers to 24 bytes and 16 bytes, with a payload size of 1023 bytes. The channel capacity C and transmission rate R are established at

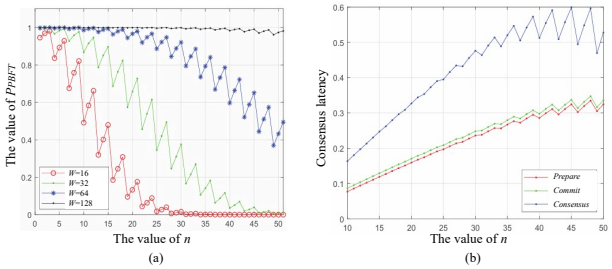


Fig. 11. Wireless PBFT consensus performance with IEEE 802.11. (a) Consensus rate. (b) Consensus latency.

1 Mbps. The time slot and idle time slot are defined as 20 μs and 1 μs. Additionally, the Short InterFrame Space (SIFS) and Distributed InterFrame Space (DIFS) durations are established at 10 μs and 50 μs. The following simulation results are derived based on these parameters.

Fig. 11 (a) illustrates the variation in the PBFT consensus success rate as the number of nodes increases within this protocol. The decline in success rate can be attributed to the heightened probability of message collisions that occur with an increasing number of nodes. Moreover, the figure demonstrates the impact of the backoff window size on the consensus success rate. As the value of the backoff window W increases, there is a corresponding decrease in the consensus success rate. Fig. 11 (b) depicts the relationship between the wireless PBFT consensus latency (unit: s) and the number of nodes n. Specifically, it illustrates the latency associated with the *prepare* and *commit* phases, as well as the overall consensus process. The results indicate that, as the number of nodes increases, the latency escalates rapidly.

These findings serve as a valuable reference for optimizing the latency in the design of wireless PBFT consensus mechanisms utilizing the IEEE 802.11 protocol. In addition, there are many modeling works on the performance of blockchain consensus in wireless networks, such as the fork probability analysis of WBC [162], the performance analysis of wireless Raft consensus [154], [163], and the comparison of the consensus performance of Raft and HotStuff in wireless networks [164]. These works, in conjunction with the previously discussed modeling of PBFT in 6G, not only facilitate a comparative analysis of WBC performance across various wireless environments but also establish a practical foundation for optimizing WBC performance in Section IV.

B. Sharding for WBN

The intricate blockchain operations, particularly those associated with complex consensus processes, contribute to its reduced efficiency in transaction processing. Notably, as the number of nodes increases, the efficiency of processing transactions declines significantly, thereby imposing constraints on the scalability of the blockchain system [129], [165]. This limitation poses a substantial challenge to the seamless integration of blockchain with 6G, which aspires to facilitate massive communication and ubiquitous connectivity.

To enhance the scalability of blockchain, various solutions have been proposed, including side chains [166], child chains

[167], multi-chains [85], [168], payment channels [169], [170], and Directed Acyclic Graph (DAG) structures [171], [172]. However, the design of these chain structures is not closely related to the characteristics of wireless network environments. Consequently, this part will concentrate on sharding schemes to improve the performance of the WBN and WBC, because its performance is related to the communication and location distribution between nodes. The sharding scheme is regarded as a significant approach to enhancing the scalability of blockchain [64], [173]. This mechanism involves partitioning the nodes within the blockchain network into multiple groups, referred to as shards [174], based on specific criteria. Transactions are subsequently divided and processed in parallel across these shards, with consensus achieved concurrently within each group [119]. This parallelization significantly improves the efficiency of the blockchain's transaction processing capabilities.

Elastico [175] represents one of the earliest sharding methodologies and offers novel approaches for enhancing consensus performance. This framework efficiently manages network messages and is capable of tolerating up to one-quarter of Byzantine nodes. Following this, OmniLedger [176] augmented Elastico by integrating Atomix, which is based on lock validation, along with Byzcoin [177] to bolster node validation security. Additionally, RapidChain [119] advanced the OmniLedger model from a cross-shard perspective. In the cross-shard PBFT and PoW shard model, [178] and [179] have analyzed security performance, comparing it to the non-cross-shard model. Furthermore, several hierarchical sharding schemes have been proposed to clarify the consensus process of sharding to facilitate node management. Notably, [36] introduces a two-layer PBFT sharding scheme designed to minimize communication overhead and extend its application to scenarios involving multiple layers. Subsequently, Hong et al. [120], [180] have explored cross-shard transactions within hierarchical sharding frameworks, culminating in the design of a Pyramid structure that achieves 3.2 times the throughput of other works. Liu et al. [181] have provided a scalable decentralized identity (DID) management architecture for Web 3.0 by using a multi-layer sharding structure. Given that the number of nodes within a shard is typically smaller than the total number of nodes in the network, there exists a heightened risk of control by colluding Byzantine nodes. Therefore, in addition to enhancing performance, several sharding schemes have been developed to bolster consensus security following the implementation of sharding [182]. For example, [183] has proposed a monitoring sharding architecture termed CoChain, which ensures the correctness of shard consistency outcomes through monitored shards. In addition, Zhang et al. [184] have designed the node allocation scheme based on node trust to avoid excessive aggregation of malicious nodes in a certain shard. While, Zhai et al [185] work to anonymize the nodes of the election committee in the shard, thereby reducing Distributed Denial of Service (DDoS) attacks.

However, the application of these sharding schemes, originally designed for wired network scenarios, presents significant challenges in 6G wireless networks due to several issues. First, these schemes often randomly assign nodes to each shard or focus solely on cross-shard transactions or node trust factors, without accounting for the geographical location, distance, and communication environment that significantly influence node interactions in a wireless network. Second, 6G aims to achieve the goal of ubiquitous connectivity within the SAGIN, yet existing sharding schemes struggle to accommodate high-speed mobile entities such as vehicles, drones, and satellites. Third, blockchain nodes in wireless scenarios frequently face difficulties in securing a reliable power supply, making energy consumption a critical factor that limits blockchain scalability. There are a few current sharding schemes to improve the scalability and sustainability of blockchain in wireless networks from the perspective of energy consumption.

With respect to the first two issues, [26], [186], in [187] offers partial solutions. In [26], the authors integrated vehicular fog computing to develop an efficient and stable sharding scheme that takes into account factors such as vehicle driving direction, speed, and geographical location. Then, on this basis, the work presented in [186] further enriches the dimensions of vehicle behavior and introduces a sharding dynamic adjustment strategy based on Deep Reinforcement Learning (DRL). Moreover, sharding based on the nodes stability will be another promising method. For example, in [187], the authors designed a robust sharding model based on node stability for IoV, aiming to balance the stability of each shard as much as possible, thereby achieving superior throughput performance when handling cross-slice transactions. For the third problem, Chen et al. [188] have designed an energy-efficient sharding scheme for mobile IoDs from the perspective of sustainable work. Meanwhile, Luo et al. [189] have presented a low-energy consumption sharding for 6G wireless networks for PBFT on the basis of [133]. Below we will use this work as an example to introduce the WBN sharding work in 6G networks.

According to the simulation results of PBFT performance in 6G, the sensitivity γ of the receiver is closely related to SINR η. As long as γ is not greater than SINR η, then the receiving node must be able to receive the consensus message to ensure the smooth progress of the wireless consensus [133], the following formula can be obtained

$$r \leq \left(\frac{p_{PBFT} h}{\gamma(\sigma^2 + I)} \right)^{-\tau}. \tag{9}$$

The authors further postulate that the nodes are situated within a rectangular region characterized by a length d_1 and a width w, with a uniform distribution of nodes throughout this area. The authors then propose a low-energy consumption sharding design, known as Green Sharding (GS). As shown in Fig. 12, the rectangle is evenly divided into y subregions based on length. Each subregion corresponds to a shard, and each shard has x nodes executing PBFT in parallel. Then y, y, and n satisfy $xy = n$. Then, each shard elects a leader as a committee node (CN). Therefore, y CNs were selected for PBFT again to achieve global consistency.

Assume that the maximum distance for intra-shard communication after sharding is d_2. This is the result of assuming that the diagonal distance of the rectangle is approximately

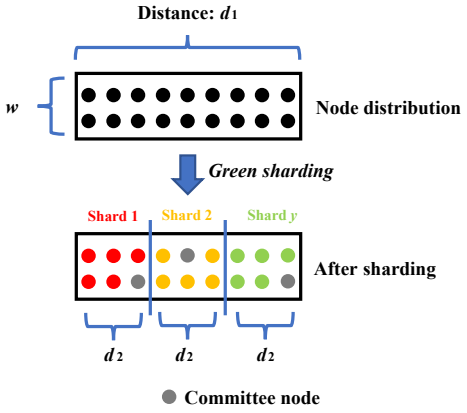


Fig. 12. Green sharding scheme.

the length of the rectangle. Then, the relationship between d_1 and d_2 can be expressed by $d_2 = \frac{d_1}{y}$.

Furthermore, to ensure the smooth progress of wireless consensus, d_1 and d_2 should also satisfy 9. Among them, for d_2, its transmission power after sharding is p_{GS}. Then, to eliminate interference resulting from simultaneous operations of different shards within the same frequency band (FB), frequency division multiplexing is employed within the WBN. Subsequently, based on the relationship of d_1, d_2, p_{PBFT}, and p_{GS}, the transmission power after sharding can be articulated as $p_{GS} = p_{PBFT} y^{-\tau}$.

Next, according to the energy consumption model in Section II-D, the authors obtain the consensus energy consumption after wireless PBFT sharding, i.e

$$E_{GS} = (2x^2 t_3 - 2xt_3 + xt_2)p_{GS} + 2y^2 t_4 - 2yt_4 + yt_2)p_{PBFT}, \quad (10)$$

where t_3 and t_4 denote the average latency associated with the first three phases of the PBFT consensus execution for each shard and the overarching network, respectively. t_2 remains unchanged, as the latency incurred during the *reply* phase is independent of the number of nodes [132] and [133]. Additionally, the authors ascertain from the performance simulation of PBFT in 6G that the latency corresponding to the first three phases of PBFT can be approximated as a linear function that crosses zero concerning n. Consequently, they further express t_4 in terms of $t_3 \frac{y^2}{n}$. Then, x and p_{GS} can be substituted with n/y and $p_{PBFT} y^{-\tau}$. The consensus energy consumption for the wireless PBFT sharding can be further simplified. The simplified equation can be regarded as a function of y, and its second derivative is always greater than 0. As a result, when its first derivative equals zero, it allows for the determination of the value of y that minimizes E_{GS}.

Drawing upon the simulation parameters for PBFT in 6G, the authors have conducted simulations to compare the performance of the GS scheme with that of both the two-layer [36] and Pyramid [120] sharding schemes, specifically under THz and mmWave signals. Figs. 13 and 14 respectively show the energy consumption comparison between GS and the other schemes, where Pyramid schemes 1 and 2 represent two and

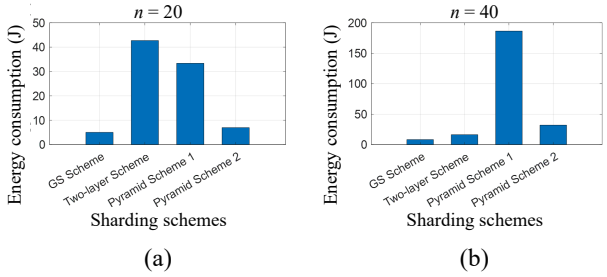


Fig. 13. Energy consumption comparison under THz signals. (a) n = 20. (b) n = 40.

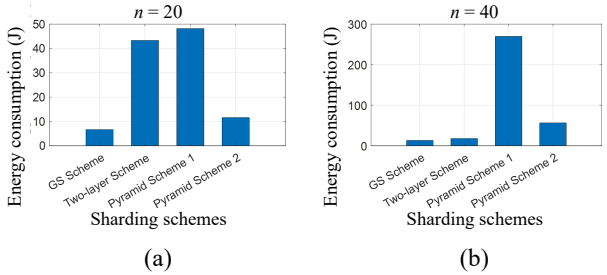


Fig. 14. Energy consumption comparison under mmWave signals. (a) n = 20. (b) n = 40.

three shards in WBN. Meanwhile, the simulation results are quantified in consensus energy consumption per second for statistical standardization purposes. Irrespective of the signal environment and node number, the GS scheme consistently demonstrates the lowest consensus energy consumption. This outcome underscores its potential to support the sustainable operation of WBN within 6G, thereby overcoming the energy consumption limitations that impact the WBN scalability. In addition, sharding can also alleviate the storage burden of the blockchain. The transaction data that nodes need to back up has been narrowed down from the entire network to the local shard where they are located [23]. Meanwhile, combined with erasure coding, the storage overhead can be optimized without affecting the data availability [190].

C. Node Deployment

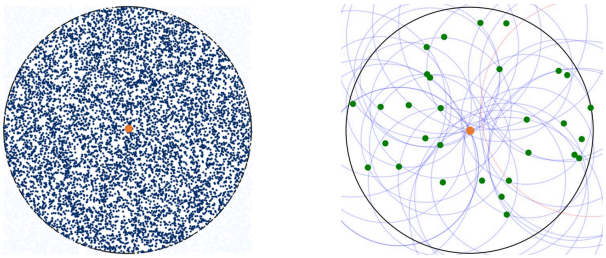
When blockchain is required to effectively support wireless network operations, such as 6G, the deployment of blockchain becomes a critical subject. This encompasses not only the functionality and capabilities of WBN but also incorporates considerations regarding the associated deployment costs.

Currently, several initiatives have commenced initial efforts toward the practical deployment of blockchain. For instance, in [191], the authors have implemented blockchain within smart meters to facilitate the distributed management of local energy markets, conducting a pilot project in 18 residential buildings in Switzerland. They have concluded that memory requirements present a limitation to blockchain deployment. Furthermore, Luo et al. [40] have investigated the Vehicle-to-Grid (V2G) enabled by blockchain and developed a deployment scheme for charging nodes that minimizes communication costs. Additionally, research conducted in Malaysia

regarding the use of blockchain in small building management identified obstacles to blockchain deployment, including technical, operational, regulatory, and economic challenges [38]. In [192], the authors have implemented the deployment of blockchain at the United Arab Emirates University and evaluated network latency and bandwidth. Moreover, Tran et al. [39] have proposed the adoption of a software framework designed to automate the deployment and evaluation of blockchain networks, thereby reducing both the threshold and costs associated with blockchain implementation.

However, these efforts exhibit limitations in wireless networks, as they do not adequately account for the communication resources necessary for the operation of blockchain nodes, nor do they consider the unique characteristics of wireless communication scenarios. [121] represents an early wave of research focused on the deployment of WBN nodes. In these works, blockchain and its PoW consensus mechanism are implemented within wireless IoT environments. The authors have employed a spatiotemporal Poisson distribution model to analyze node and transaction arrival rates, subsequently deriving the distribution of SINR, consensus success rate, and throughput. Meanwhile, they have proposed an optimal deployment scheme for blockchain nodes aimed at maximizing transaction throughput, with the term "optimal" referring to the utilization of the minimum number of consensus nodes possible in order to reduce the costs associated with blockchain deployment. Additionally, Onireti et al. [193] have investigated the effective coverage of wireless PBFT in practical deployment scenarios, identifying what is termed the "viable area." Building upon this analysis, they optimized both the number of nodes and the transmission power of these nodes, thereby establishing a foundational framework for the low-cost deployment of wireless PBFT consensus mechanisms. Additionally, numerous researchers have directed their attention toward the practical deployment of the Raft consensus mechanism. For instance, in [194], the authors examine the consensus range and security performance of Raft in the presence of malicious node interference. Concurrently, Yu et al. [139] integrate Raft consensus within industrial IoT (IIoT) scenarios and analyze its deployment's effects on the number of nodes and the reliability of wireless channels. Furthermore, [195] facilitates the adoption of blockchain at the hardware level. This research employs the Micro Controller Units (MCU) to manage the operation of a network of 3-7 vehicles that runs Raft consensus. It not only ensures the consistency and security of the data transmitted among the vehicles but also enables distributed synchronization of vehicle actions.

Here, we once again utilize PBFT consensus as a case study to present a cost-effective deployment strategy for blockchain in the IoT [122]. This approach aims to facilitate a successful consensus while simultaneously minimizing both the number of blockchain nodes and the transmission power of the nodes. In this deployment scenario, the system comprises IoT nodes (IoTNs) and blockchain nodes (BNs), as illustrated in Fig. 15 (a). The blue nodes in the figure represent IoTNs. When valuable information is exchanged among IoTNs, it is treated as a transaction that is transmitted via wireless communication to the BNs, where it is confirmed and subsequently recorded



(a) (b)

Fig. 15. The low-cost blockchain node deployment. (a) IoTNs. (b) BNs.

on the blockchain. To prevent communication interference between BNs and IoTNs, which could negatively impact consensus performance, each BN is interconnected through a high data rate link utilizing a dedicated interface. The BNs are organized such that there is one primary node and $n-1$ replica nodes. To maximize consensus coverage, the primary node is always positioned at the center of the circle, represented by the orange node in Fig. 15 (b), while the remaining green nodes serve as replicas, and the curve is the node's coverage area. In addition, these BNs are also subject to PPP.

First, the authors determine the minimum number of BNs to meet IoTNs throughput requirements. They define the maximum throughput T_{TPS} required by the user. According to [121], it can be expressed as $T_{TPS} = N\alpha t_{PBFT} L P_{BN}$, where N is the number of IoTNs, α denotes the transaction arrival rate, L and P_{BN} represent the packet length and the successful rate of BNs receiving the message. Then, the authors give an expression for P_{BN},

$$P_{BN} = 2\pi(n-1)d_{I,B}\iint_{\Omega}\frac{1}{\Omega}\exp\left(-\frac{k}{\Omega}\pi d_{I,B}^2\right)d\Omega, \quad (11)$$

where $d_{I,B}$ is the mean distance between IoTN and the nearest BN. Ω is the communication area of the primary node.

However, owing to the complexity of the (11), deriving the value of n through it and T_{TPS} proves to be challenging. Consequently, the authors initially define the search region for the value of n and subsequently seek its optimal value within this defined region. The process for determining n can be organized into the following three steps.

(1) Begin by setting the initial value of n as n_0. If $N\alpha t_{PBFT} L P_{BN} < T_{TPS}$, then update n_0 to $2n_0$ and reevaluate the relationship between $N\alpha t_{PBFT} L P_{BN}$ and T_{TPS}.

(2) Define $a = \frac{n_0}{2}$, $b = n_0$, and express $n_0 = \frac{(a+b)}{2}$. If $N\alpha t_{PBFT} L P_{BN} < T_{TPS}$, set $a = n$, and conversely, if the condition is not met, assign $b = n$.

(3) Iterate through Step (2) until the $|b-a| < \varepsilon$ is satisfied, where ε denotes an infinitesimally small value. The final value of n obtained at this stage represents the minimum number of blockchain nodes required to meet the throughput condition.

Furthermore, the authors optimize the transmission power of these nodes. By the $1/3$ fault tolerance threshold of PBFT, the communication range of the primary node needs to encompass $2f$ replicas. Consequently, referencing the findings presented in [193], the transmission power of the BN can be articulated

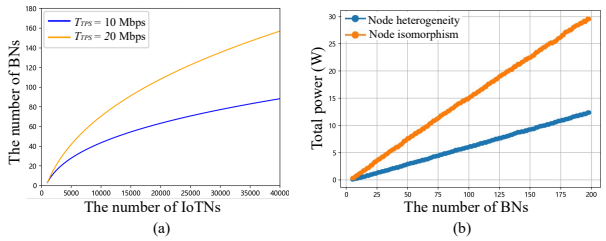


Fig. 16. The deployment cost of Wireless PBFT consensus. (a) Number of IoTNs *vs* number of BNs. (b) Number of BNs *vs* total power of the entire WBN.

as $p_{BN} = \frac{\eta}{K} {R_r}^{\tau}$, where R_r is the communication radius between replicas, and K represents a constant associated with antenna characteristics and channel attenuation.

Then, the authors simulate the proposed low-cost BNs deployment scheme with $L = 256$ bits, $\alpha = 1800$ per second, $\eta = -84.5$ dBm, $K = 1$, $\tau = 4$, $R_r = 1000m$, $\varepsilon = 0.01$. Initially, the authors have investigated the relationship between the number of IoTNs and BNs, setting the upper throughput limits T_{TPS} for IoT at 10 Mbps and 20 Mbps, respectively, as depicted in Fig. 16 (a). In the scenario where $T_{TPS} = 10$ Mbps, it is observed that as the number of IoTNs gradually approaches approximately 15,000, the growth rate of BNs begins to decline. This phenomenon occurs because, as the IoT throughput approaches the established upper limit, there is diminished reliance on increasing the number of BNs to enhance overall throughput. A similar trend is noted for the case of $T_{TPS} = 10$ Mbps. Collectively, these simulation results demonstrate that it is possible to achieve a minimum number of BNs sufficient to meet the throughput requirements of the IoT. Additionally, the total power consumption (unit: W) of the entire WBN is analyzed, and the deployment strategy is compared with the traditional approach. In the proposed scheme, each BN is heterogeneous; that is, each BN can operate at different transmission power levels while only needing to satisfy the node coverage requirements. In contrast, the traditional method employs uniform power levels for all BNs, resulting in significant energy waste. The simulation results, illustrated in Fig 16 (b), demonstrate the advantages of the proposed scheme in terms of power efficiency.

D. Message Propagation

Message propagation within blockchain networks comprises two types of messages: transactions and block data. The propagation rates of transactions reflect the operational efficiency of the blockchain system [196], while the timely dissemination of block data is critical for ensuring information synchronization across networks. This widespread and rapid diffusion of information establishes the decentralized foundation of blockchain.

Efficient propagation, also referred to as broadcast protocols, fulfills two additional functions in blockchains. First, it facilitates the implementation of consensus mechanisms, as many consensus processes depend on broadcasting for vote aggregation. Consequently, efficient broadcast protocols accelerate the consensus process [197]. Second, these broadcast protocols assist in addressing the network splitting problem that can arise in blockchain environments [41]. In instances where nodes diverge, effective broadcast protocols can intervene to maintain the consistency and integrity of the network.

Furthermore, propagation protocols can be categorized into structured and unstructured protocols based on the underlying network architecture. A quintessential example of an unstructured broadcast overlay protocol is Gossip [198], which is utilized in the Bitcoin network. This protocol employs flooding that compels each node within the network to relay transactions to a greater number of peers. While this approach enhances message dissemination, it simultaneously increases network load and diminishes overall throughput. To address this limitation, Erlay [199] integrates a low fan-out flooding strategy with a harmonic approach, achieving an 84% reduction in bandwidth consumption compared to the traditional Gossip protocol employed by Bitcoin. However, in highly dynamic environments, Erlay may encounter challenges. Additionally, building upon the Gossip, Saldamli et al. [200] take into account the existence of faulty nodes and propose an improved Gossip protocol for blockchain networks. This protocol incorporates a fault detection system and a self-healing method that the authors have developed. In comparison to unstructured broadcast protocols that offer extensive coverage, structured broadcast protocols demonstrate enhanced efficiency. Kadcast [125], [201] organizes nodes within a blockchain network into a Kademlia distributed hash table (DHT) [202], facilitating efficient message propagation with a remarkable success rate of 99%. Additionally, Urocissa [203] addresses the issue of latency heterogeneity by maintaining Multiple Minimum Latency Broadcast Trees (MLBTs), which effectively reduces block relay times and acknowledgment latency. Today, there are semi-structured broadcast protocols that combine the best of both. For example, Wang et al. [204] introduce Swift, a dynamic topology adjustment method that employs unsupervised learning and greedy algorithms. This approach enables nodes to select optimal neighbors for data transmission, thereby minimizing propagation hops.

In addition to optimizing network topology, compressing the size of propagating information constitutes a critical strategy for enhancing the efficiency of message propagation in blockchain networks. Zhao et al. [205] focus on transaction data within the Ethereum network and developed a hybrid compact block (HCB) framework to minimize the transmitted data volume. This approach has been shown to reduce propagation latency by more than fifty percent in comparison to the block propagation scheme in Ethereum. Furthermore, this research team proposes that the block body can be transmitted without prior verification during the propagation phase [206], thereby enhancing network throughput without compromising security. This approach effectively eliminates the dependency of propagation time on the number of transactions contained within the block, thereby facilitating greater scalability.

Building upon the principles of low latency and high throughput, the researchers optimized various performance metrics of message propagation in different network environments, including high fault tolerance, high consistency, and energy efficiency [124]. To achieve high fault tolerance, the MERCURY protocol [207] employs a secure virtual co-

ordinate system (VCS) that ensures robust coordinate assignment for each node, thereby resisting potential attacks. Simulation results indicate that this protocol achieves lower latency and demonstrates superior propagation efficiency even in the presence of 49% malicious nodes. Regarding high consistency, the NefSBFT protocol [208] capitalizes on the intermittent connectivity of nodes and the social characteristics associated with frequent network partitioning to facilitate message multicast. It enables effective transaction ordering and block validation, thereby contributing to efficient consensus achievement. For energy efficiency, Luo et al. [59] built a broadcast energy consumption model, thereby building a minimum-energy broadcast tree for blockchain networks. This method has superior energy efficiency advantages over traditional structured or unstructured broadcasting.

However, in 6G wireless networks, the above propagation protocols encounter new challenges. The instability of wireless channels can disrupt the message propagation process, thereby adversely affecting the broadcast performance of the network. Furthermore, the ubiquitous connectivity and high-speed mobile environments of 6G involve many new communication devices, such as vehicles, satellites, and drones. They exhibit greater dynamism and uncertainty compared to the static base stations of traditional networks. Consequently, these nodes will frequently join or leave the WBN, interrupting the normal propagation process within the network. This is particularly problematic for structured propagation protocols that rely on broadcast trees. When a node goes offline, its connected counterparts become unable to receive new transactions and block data [209].

In this regard, we introduce an efficient propagation protocol, designated as DHBN [210], tailored for highly dynamic and heterogeneous wireless networks. The authors provide a preliminary discussion on the challenges associated with nodes joining and exiting the WBN at high frequencies.

This protocol categorizes nodes into three distinct types: the full node (FN), coordinated node (CN), and dynamic node (DN). The FN typically corresponds to the base stations operated by network service providers, possessing abundant resources in terms of bandwidth, storage, and computational capacity. CNs include roadside units and access routers, which exhibit relative stability in network connectivity. Such nodes have the dual capability of both requesting services from other nodes and acting as service providers themselves. DNs encompass mobile vehicles and smartphones, characterized by high levels of dynamism as they may join or exit the network at any time. Although dynamic nodes possess certain computational and storage capabilities, they primarily rely on advanced nodes for service provision.

These three types of nodes collectively establish a three-tier model for the network. To facilitate the identification of the appropriate layer for each node, the corresponding label information is assigned at the time of the node's initial connection to the network. This assignment process can be executed within a Trusted Execution Environment (TEE) [211], ensuring the accuracy of the node's identity. Nodes are intended to form MLBT exclusively with other nodes within their respective layers, while message propagation between different layers occurs through random connections. When a new message ascends to the next layer, it disseminates rapidly through the tree network established within that layer. This hierarchical structure minimizes the necessity for frequent reconfiguration within a structured network topology, accommodating the presence of highly dynamic nodes.

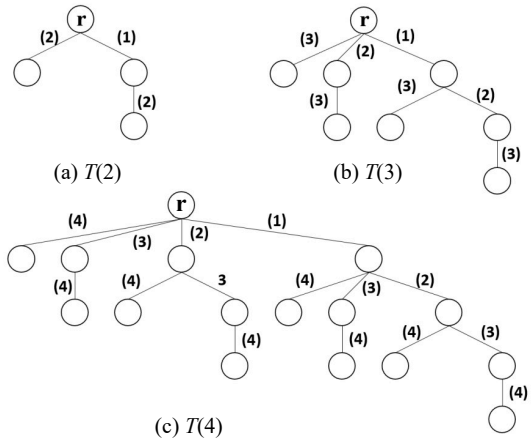


Fig. 17. The different orders for MLBFTs.

Following the construction of a hierarchical network model, the authors define the order of the MLBT as the number of children directly connected to the root node. Each time an additional node is integrated into the tree, the order increases by one. As a consequence, they designate this configuration as the Minimum Latency Broadcast Full Tree (MLBFT), as shown in Fig 17. Subsequently, the authors designate the MLBFT of order i as $T(i)$, and the total number of nodes is 2^i. Within such an MLBFT, any node and its corresponding subtree are capable of forming a new MLBFT. Then, in $T(i)$, there are 2^{i-j-1} existing sub-MLBFTs designated as $T(j)$. Therefore, the probability that an arbitrary node in $T(i)$ is the root node of $T(j)$ is

$$P_j = \frac{2^{i-j-1}}{2^i}. \tag{12}$$

If the root of a sub-MLBFT goes offline unexpectedly, it results in the formation of j independent MLBFTs, denoted as $T(0), T(1), T(2), \ldots, T(j-1)$. Upon the reconnection of these independent subtrees to the original MLBFT, a random node within the tree is selected to establish a connection.

Next, the authors have conducted simulations to evaluate the performance of the DHBN protocol and compare it with the Gossip and Urocissa protocols. The maximum capacity for MLBFT is set to 50, 30, and 10 nodes for the FN, CN, and DN layers, respectively, and the total number of nodes is 300, with the block size configured at 1 MB. Fig. 18 (a) illustrates the relationship between the propagation latency and the number of nodes that successfully received blocks. The simulation assumed a dynamic environment where 10% of the nodes in the WBN change every second, either exiting or joining the network. The measurement results demonstrate the superior latency performance of the DHBN protocol in dynamic heterogeneous networks, resulting in 12% and 14% more

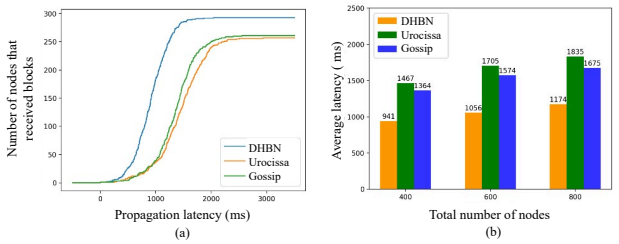


Fig. 18. Propagation latency comparison. (a) Number of nodes that successfully received blocks. (b) Scalability.

signatures compared to the Urocissa and Gossip protocols, respectively. Fig. 18 (b) illustrates the variations in scalability among the three protocols as the number of DNs increases. As the proportion of dynamic nodes rises, the average latency experienced by all three protocols also increases. However, the performance advantage of the DHBN protocol continues to expand.

IV. Performance Optimization in Wireless Blockchain Networks

This section concentrates on performance optimization for WBNs. As discussed in Section II-C, several key technologies within WBN are primarily designed to enhance the functionality of WBC, thereby improving the overall performance of the WBN [212], [213]. Based on the findings presented in Section III and a comprehensive summary of WBN performance optimization provided in Tables III and IV, we categorize the optimization of WBN performance into three distinct aspects: consensus success rate, consensus efficiency, and consensus overhead, to guide the subsequent tutorial.

A. Consensus Success Rate

The consensus success rate, often referred to as consensus security [36], [189] reflects the resilience of consensus mechanisms within WBN against Byzantine and faulty nodes. The technical approach to enhancing the consensus success rate in WBN primarily encompasses two dimensions: first, improving the adaptability of consensus mechanisms to wireless channels to mitigate the impact of wireless network instability on the consensus success rate. Second, refining the consensus process of WBC, including integrating cryptographic techniques to bolster fault tolerance against Byzantine and faulty nodes.

Next, we present several typical optimization schemes categorized by consensus types. The first category is voting-based consensus, commonly utilized in consortium and private chains, with notable examples including PBFT and Raft. Second, some studies have discussed the block propagation success rate of public chain consensus represented by Proof of X in wireless networks.

For the PBFT, in the study by [226], the authors introduce a novel three-stage consensus for PBFT, specifically tailored for less reliable communication channels within the IoV. This mechanism addresses challenges posed by potential inaccuracies in local sensor readings. The proposed framework comprises veto collection and gossip stages, meticulously designed to accommodate the stringent and multifaceted demands associated with vehicle mobility. Simulation outcomes indicate that this enhanced consensus remains effective even under suboptimal wireless communication conditions and scenarios involving faulty vehicles. While the SCBC represents a committee-based consensus mechanism specifically engineered for Byzantine fault-tolerant protocols [234]. This mechanism encompasses three core components: a robust committee selection algorithm, a highly scalable consensus algorithm, and an efficient consensus-supporting threshold signature scheme. These elements collectively enhance the security and scalability. A security analysis demonstrates that SCBC is resilient against many attacks and exhibits a commendably high consensus success rate. In [237], Zhou et al. have proposed an innovative framework for implementing the PBFT consensus mechanism within wireless cellular networks. They have assumed a scenario where the network infrastructure is predicated on BSs, with nodes relying exclusively on these base stations for communication. Consequently, the effective coverage area of each base station plays a pivotal role in determining the likelihood of a random node accurately decoding received signals, which directly impacts the success rate of achieving PBFT. The authors employed the PPP on a two-dimensional plane to model the spatial distribution of both base stations and nodes. By conducting a thorough coverage probability analysis, they were able to derive the success probabilities for both uplink (from nodes to base stations) and downlink (from base stations to nodes) communication channels. Simulation results collectively demonstrated that the integration of base stations into the PBFT significantly enhances the consensus success rate, thereby underscoring the potential benefits of leveraging cellular network infrastructure for improving Byzantine fault tolerance mechanisms. For this consensus, it is particularly important to resist FBS attacks.

For the Raft, in [218], Cao et al. have introduced a two-hop Raft consensus, to enhance its applicability in distributed systems with geographically dispersed nodes. Specifically, it addresses the challenge of distant nodes communicating with the leader by incorporating intermediary one-hop nodes, thereby facilitating efficient information exchange across larger distances. This modified Raft consensus mechanism holds particular relevance for IoV applications, where it can facilitate autonomous decision-making processes among vehicles by ensuring timely and accurate consensus. Simulation-based evaluations presented in the work reveal that the proposed two-hop Raft outperforms the traditional Raft consensus in consensus success rate. In [222], the authors posit that the consensus performance within WBN is predominantly influenced by the reliability of wireless channels, which are stochastic and constrained by limited communication resources. Consequently, to augment the consensus performance of wireless Raft, they emphasize the necessity for a judicious communication resource allocation strategy. The authors delve into an investigation aimed at identifying the optimal number of nodes of consensus success rate performance under these constraints. Through rigorous derivation and subsequent simulation-based validation, their findings substantiate the assertion that strategic allocation of communication resources significantly enhances the consensus success rate within WBN environments, thereby

TABLE III
SUMMARY OF WBN PERFORMANCE OPTIMIZATION

Year	Ref.	Contributions	Consensus success rate	Consensus efficiency	Consensus overhead
2019	[193]	Study the coverage of wireless PBFT, and save the consensus overhead by optimizing node numbers	✗	✗	✓
2019	[121]	Optimize the number of consensus nodes and transmit power in wireless IoT supported by PoW consensus	✗	✗	✓
2020	[34]	Design a Proof of Communication (PoC) for single-hop wireless networks with low time complexity	✗	✓	✗
2020	[214]	Optimize the mining energy consumption when wireless mobile nodes work in PoW	✗	✗	✓
2021	[215]	Based on [34], present Fault-Tolerant PoC (FTPoC) for wireless networks with time complexity $O((f+1)\log n)$	✓	✓	✗
2021	[216]	Propose wChain by archical spanner to achieve efficient fault-tolerant consensus for multihop wireless networks	✓	✓	✗
2022	[217]	Present an energy-efficient and efficient consensus mechanism for multi-hop wireless IoT	✓	✓	✓
2022	[218]	Design a fast and efficient two-hop Raft consensus for IoV by consensus and communication jointly optimization	✓	✓	✗
2022	[219]	Present a fault-tolerant consensus for mobile wireless networks optimized by NOMA	✗	✓	✗
2023	[155]	Model the energy consumption and block confirmation probability of PoW consensus in wireless networks	✓	✗	✓
2023	[220]	Propose a double auction mechanism of transaction costs for mobile WBN nodes	✗	✗	✓
2023	[221]	Based on broadcast and channel competition, propose a Proof of CHannel (PoCH) for single-hop wireless networks under an adversarial SINR model	✓	✓	✓
2023	[222]	Design an optimal allocation scheme of communication resources for wireless Raft consensus	✓	✓	✓
2023	[223]	Use the path loss of the sending node as a fingerprint to improve the security of wireless Raft	✓	✗	✗
2023	[224]	Present an efficient Byzantine fault-tolerant consensus for the majority problem in edge wireless networks	✓	✓	✗
2023	[225]	Based on [34], use multi-agent reinforcement learning to improve the consensus success rate of PoC consensus	✓	✗	✗
2023	[226]	Combine veto collection and Gossip to design an improved three-stage reliable PBFT consensus for IoV	✓	✗	✗
2023	[227]	Propose a Symbiotic PBFT (S-PBFT) consensus based on cognitive backscatter communication and symbiotic communication for wireless PBFT	✓	✗	✓
2024	[122]	Provide a low-cost node deployment solution for IoT supported by wireless PBFT consensus	✗	✗	✓
2024	[157]	Optimize the transaction arrival rate and contention window size in wireless PBFT consensus	✓	✓	✗
2024	[188]	Design a sustainable and low energy consumption sharding scheme for PBFT-based IoD	✗	✓	✓

contributing to more robust and reliable distributed consensus operations. Moreover, Buttar et al. [223] examine the implications of interference and impersonation attacks within wireless Raft networks. Employing stochastic geometry, they derive closed-form expressions for the coverage probabilities associated with both uplink and downlink transmissions. These probabilities are correlated with the consensus success rate of Raft. Then, in response to the above attack scenarios, the authors propose an innovative countermeasure whereby the receiving node utilizes the path loss characteristics of the transmitting node as a unique fingerprint. This approach facilitates the implementation of a binary hypothesis testing mechanism to mitigate the effects of attacks. Simulation outcomes corroborate the efficacy of this method, demonstrating a notable improvement in the consensus success rate for wireless Raft networks under adversarial conditions.

For these voting-based consensus mechanisms, Luo et al. [227], [236] have conducted an analysis highlighting the critical reliance on multi-round communication processes, which exposes such mechanisms to the unstable channels prevalent in wireless network environments. To address this challenge, the authors cleverly combined WBN with symbiotic communication, using backscattering technology to design a new paradigm called SBC Within this symbiotic communication, a secondary transmitter (STx) is empowered to convey messages with minimal energy expenditure by harnessing the radio

TABLE IV
SUMMARY OF WBN PERFORMANCE OPTIMIZATION

Year	Ref.	Contributions	Consensus success rate	Consensus efficiency	Consensus overhead
2024	[189]	Optimize the energy consumption of PBFT consensus by sharding in 6G wireless networks	✗	✓	✓
2024	[228]	Design a low-latency and reliable Byzantine fault-tolerant consensus for single-hop wireless networks	✓	✓	✗
2024	[229]	Considering node entry and exit, propose an adaptive Raft consensus to enhance its robustness in wireless networks	✓	✗	✗
2024	[230]	Design a Byzantine fault-tolerant over-the-Air Consensus (AirCon) for WBN	✓	✗	✓
2024	[231]	Use the distributed randomized multi-channel communication algorithm to achieve BFT consensus	✗	✓	✗
2024	[232]	Based on digital twins propose a virtual static consensus Proof of Network Coding (PoNC) for IoD	✓	✓	✗
2024	[233]	Optimize the leadership election process of wireless Raft and design a robust consensus named RoUBC	✓	✓	✗
2024	[234]	Design a scalable credible-committee-based consensus (SCBC) to suppress broadcast redundancy and improve consensus efficiency	✓	✓	✗
2024	[235]	Present a consortium blockchain based on Quorum for 6G wireless networks and optimize its scalability	✓	✗	✗
2024	[236]	Based on [227], propose the Symbiotic Blockchain Consensus (SBC) by further extending the method to almost consensus that relies on broad voting	✓	✓	✓
2024	[237]	Use a novel timeout mechanism and combine with the base station to improve wireless PBFT consensus	✓	✓	✓
2025	[238]	In the interference environment, design a jamming-resilient distributed four-stage consensus	✓	✗	✗

frequency (RF) signals broadcast by a primary transmitter (PTx). Reciprocally, the STx enhances the communication reliability of the PTx through the provision of multipath gain, thereby establishing a mutually beneficial exchange that optimizes resource utilization. The authors have demonstrated its universal applicability by enabling 6 PBFT-like and 4 RAFT-like consensus. Simulation results show that SBC can increase the consensus success rate of PBFT-like and RAFT-like by 54.1% and 5.8%, respectively.

For consensus mechanisms akin to Proof of X, which eschew reliance on iterative communication rounds in favor of deterministic puzzle-solving to ascertain block legitimacy, such as PoW [18] and PoSo [147]. As a result, researchers have redirected their optimization efforts towards enhancing the block propagation success rate as a means to bolster the consensus success rate within WBN [155]. A case in point is the wChain framework devised by Xu et al. [216], which addresses the issue of block propagation within multi-hop wireless networks. This architecture ingeniously employs a spanner as its communication backbone, thereby ensuring robust block propagation performance. This design enables WBN to maintain consistency despite the failure of up to half of the nodes. Furthermore, the research team extended their innovation to single-hop wireless networks by introducing a novel consensus termed PoCH [221]. It adeptly adapts the adversarial SINR environment, selecting the most advantageous propagation channel for block transmission based on real-time assessments. Such channel selection significantly enhances the resilience and efficacy of block propagation, thereby contributing to an elevated consensus success rate in potentially unstable wireless environments.

B. Consensus Efficiency

Consensus efficiency includes consensus latency and throughput, the former represents the time required to reach consensus, and the latter represents the ability of WBN to process transactions.

In the pursuit of this performance enhancement, the construction of an efficient block propagation framework emerges as a pivotal strategy, exemplified by contributions such as the wChain protocol and PoCH consensus. In [219], the authors integrate Non-Orthogonal Multiple Access (NOMA) to streamline the consensus process and mitigate latency. This approach bears resemblance to the integration of symbiotic communication techniques outlined in [227] and [236], underscoring a shared trend towards harnessing advanced communication technologies to augment consensus efficiency.

In [229], Yu et al. address the dynamism of nodes within wireless networks, that nodes may dynamically join or depart, thereby potentially compromising the efficacy of communication protocols tailored to the original protocol. To counteract these challenges, the authors leverage the Raft consensus algorithm as a case study, incorporating a node-counting module managed by clients. This innovation ensures that candidates possess accurate knowledge of the total node count prior to initiating the leader election phase. Moreover, they achieve state synchronization via the implementation of a log synchronization phase. In tandem with this, they devise a

sophisticated node joining and exiting mechanism grounded in a routing protocol akin to Ad-hoc On-demand Distance Vector (AODV) [239]. This design facilitates the maintenance of consensus consistency even amidst dynamic changes in node states, thereby enhancing the resilience and adaptability of the network to topological shifts. Finally, simulation results show that the adaptive Raft consensus has a lower consensus latency than the original design.

It is also a technical path to improve consensus efficiency to realize batch forwarding of blocks based on network coding. This approach is exemplified in [228], where the authors introduce the LRBP consensus. It leverages the bulk forwarding capabilities of stochastic linear network coding to ensure reliable and efficient block transmission across the network. This integration not only optimizes bandwidth utilization but also enhances resilience against packet losses and network congestion. The simulation results presented substantiate the rationality and effectiveness of the proposed scheme, demonstrating significant improvements in both throughput and under varying network conditions. In a parallel endeavor, Luo et al. [232] have developed the PoNC consensus, which capitalizes on the intrinsic network coding capabilities of nodes within the IoD. This consensus is adept at identifying the optimal routing node, termed the ”coder”, thereby enhancing path transmission and data dissemination efficacy. Through simulations, it has been demonstrated that PoNC significantly outperforms conventional mechanisms in network throughput and consensus latency, underscoring its potential as a transformative solution for next-generation wireless networks.

In addition, the leader node in the blockchain consensus plays the role of opening the consensus and collecting the opinions of other nodes. Once it does not work properly, the steps to re-elect the leader, such as view change [157], will be initiated. Therefore, a stable and robust leader is essential for consensus efficiency. In [34], [215] the authors introduce a PoC consensus tailored for wireless networks, which incorporates crucial leadership selection procedures. This protocol employs robust listening signals to identify the most active node as the leader, thereby ensuring consensus consistency with relatively low time complexity. Building upon this foundation, the research team further devises an anti-interference consensus framework encompassing stages such as leader election, leader broadcast, leader aggregation, and leader announcement [238]. By determining the leader through a competitive process, the proposed mechanism achieves asymptotically optimal time complexity for reaching consensus. Meanwhile, Wang et al. [233] have devised an efficacious and robust leader election mechanism tailored for the Raft consensus within Flying Ad Hoc Networks (FANET), specifically addressing the challenges posed by substantial packet loss prevalent in such networks. This leader election strategy ingeniously integrates multi-criteria decision-making processes with a link prediction algorithm to enhance reliability. Empirical evaluations indicate that their proposed scheme markedly outperforms the conventional Raft approach, achieving a noteworthy improvement in consensus efficiency by approximately 25%.

C. Consensus Overhead

Consensus overhead represents the cost of the actual deployment of the WBN, and typically includes consensus energy consumption, communication cost, and node deployment cost.

A tailored sharding scheme for WBN emerges as a potent solution to mitigate consensus energy consumption and reduce communication overhead [26], [36]. For instance, in [189], Luo et al. have proposed GS scheme for wireless PBFT consensus demonstrating its efficacy in minimizing energy expenditure during the consensus process while concurrently optimizing communication cost. Building upon this groundwork, Chen et al. [188] have advanced the concept by developing SusChain, a sustainable sharding scheme specifically for a mobile wireless network, IoD. This innovation not only excels in promoting energy sustainability but also boasts an exceptionally low storage overhead, thereby enhancing the overall network environmentally friendly.

Moreover, the SBC framework delineated herein leverages the unique attributes of symbiotic communication, employing the passive backscatter communication modality to supplant active communication modes that consume [240]. This strategic substitution substantially mitigates both communication overhead and consensus-related energy expenditure. Simulation evidence presented in [236] corroborates this assertion, revealing that the proposed methodology effectively diminishes the consensus energy consumption for PBFT-like and Raft-like consensus by 9.2% and 23.7%, respectively.

After understanding the key technologies of WBN and its optimization directions, we will further combine the application needs of 6G in the subsequent content to analyze how WBN supports 6G.

V. Wireless Blockchain Networks for HRLLC in 6G

A. Fundamentals of HRLLC

HRLLC in 6G represents an extension of the URLLC within 5G [241]. This evolution underscores a stringent mandate for both elevated levels of communication reliability and minimized latency thresholds. Within the intricate architecture of wireless networks, latency is a multifaceted phenomenon influenced by several pivotal components. They are the network management strategy, signal processing schemes such as the modulation and coding of the end-to-end part, and the propagation latency of the signals in the network [242].

In alignment with the IMT-2030, hyper-low latency requirements necessitate adherence to a stringent range of 0.1 to 1 ms [72]. This benchmark is instrumental in facilitating the realization of 6G use cases. Meanwhile, 6G essentially requires a hyper-reliable network foundation. In particular, for mission-critical applications such as autonomous vehicles and industrial automation, the network must concurrently satisfy stringent reliability standards from 10^{-5} to 10^{-7} [72], while concurrently achieving the aforementioned hyper-low latency objectives. It is this synergistic fulfillment of hyper reliability and low latency that constitutes the cornerstone of HRLLC.

B. Applications of WBN in HRLLC

While addressing the hyper-low latency requirements of the 6G, blockchain technology assumes a three-faceted role. First, it ensures an elevated communication success rate within the network, thereby mitigating the likelihood of message transmission failures and consequent re-transmissions that would otherwise exacerbate communication duration. Additionally, as delineated in Section IV, performance optimizations for consensus mechanisms contribute to a reduction in the operational latency associated with consensus processes, thereby aligning more closely with the stringent latency demands of 6G wireless networks. Concurrently, within the realm of wireless networks, the integration of NFV [243], MEC [244], AI [245], [246], and others underpinned by a WBN, facilitates not only the secure deployment of these technologies, but also enhances their robustness. This augmentation accelerates the communication processes to 6G wireless networks. According to the conclusion of many works, the deployment of WBNs in wireless environments is instrumental in realizing and supporting the hyper-low latency communication essential for 6G advancements [247], [248].

It is expected that WBN will support HRLLC needs in various wireless scenarios, especially Connected and Autonomous Vehicle (CAV), industrial automation, telemedicine, and more. Such scenarios have extremely strict requirements on communication reliability and latency. For CAV, consensus between vehicles will break through the performance bottleneck of traditional centralized management, and rely on self-decision-making to determine the next driving route efficiently and reliably. Zhang [249] has proposed Wireless Distributed Local Consensus (WDLC), which enables driving decisions to require notification and consent from other nearby vehicles to avoid conflicts and collisions between vehicles. For industrial automation, the reliable decision-making blockchain provides is essential for industrial production. In addition, smart contracts can also be used to automate product production, thereby improving production efficiency. In [250], the authors look forward to the benefits of WBN combined with 6G for industrial automation. For telemedicine, it aims to provide patients with the most convenient and lowest-cost medical services across space constraints. Since medical privacy data and even surgical decisions are involved, the data and processes involved in telemedicine have raised various concerns in real-time and reliability. Ahmed et al. [251] have designed a blockchain-based telemedicine service for COVID-19 to improve patients' medical experience by providing a transparent and secure platform for storing patient data.

C. A Case Study: A WBN-driven IoV

In this part, we take IoV as an example to introduce how CAVs work independently based on blockchain to show the supporting role of WBN for HRLLC communication in 6G.

Currently, many of the emerging AI-based CAVs are considered far less reliable than real-world requirements and hardly considered usable. Meanwhile, in recent years, traffic accidents caused by automatic driving false alarms have caused multiple catastrophic consequences for road users [252]. Therefore, a more comprehensive solution is needed to improve the reliability of CAVs to enable L4 and above levels of automated driving. At these levels, human intervention and processing time need to be minimized. WBC can solve the above problems, which can not only make the autonomous decision-making between CAVs to avoid human interference, but also prevent the conflict between intelligent sensors from leading to unreliable decision-making through fault tolerance [253].

In [254], the authors have proposed the Perception-Initiative-Consensus-Action (PICA) protocol based on the WBC to construct driving decisions for CAVs. In this protocol, the initial Perception is based on local sensor acquisition, such as Lidar, mmWave radar and cameras. Following that, the CAV makes a request based on Perception, the Initiative, which is then sent to the IoV for a joint decision, that is Consensus. Finally, the CAV executes the result of the WBC, namely the Action. Obviously, under this scheme, the driving strategy of the CAV is no longer determined by itself, but involves the adjacent CAVs in the IoV.

Fig. 19 illustrates a scenario wherein an autonomous truck initially perceives its surroundings and subsequently proposes a lane-change maneuver to the right, seeking validation through a WBN comprised of proximate vehicles to ensure maximal safety. While the truck itself deems the action as safe to initiate, neighboring vehicles may perceive the situation differently and convey dissenting opinions or negative feedback within the WBN. The definitive authorization for the truck's intended movement is contingent upon corroborative verification from these adjacent vehicles, which have collectively established their own WBN, thereby reinforcing the decision-making process. Consequently, this validation mechanism significantly enhances the robustness and dependability of the ultimate maneuver approval. Furthermore, within the proposed PICA framework, a synchronization procedure is integrated atop the WBC. Specifically, this enhancement mandates that CAVs which are not engaging in the consensus receive the consolidated consensus outcome disseminated by the CAV that initiated the consensus. This measure guarantees a uniform comprehension across the entire IoV regarding the precise geolocation of the CAV in question, thereby reinforcing data consistency and system coherence.

Taking into account both node failure and communication link interruption, the authors derive the consensus success rates of PBFT and Raft consensus with the synchronization step respectively. Here, we take Raft consensus, which has not been shown before, as an example to analyze its reliability and latency. The consensus process is relatively simple, consisting of only two steps: *downlink* and *uplink* transmission [154], [255]. The node that initiates the consensus is called the leader, and it sends the consensus message to other nodes, called followers, via *downlink*. Then, the followers send consensus feedback to the leader by *uplink*. This consensus has a fault tolerance threshold of $\frac{n-1}{2}$ [20].

In this consensus, only the leader knows the consensus result at the end, so the authors add a synchronization phase after *uplink*. The communication process is similar to the *downlink* phase to let all other CAVs know about the driving decision for that CAV. Its consensus success rate with the synchronization

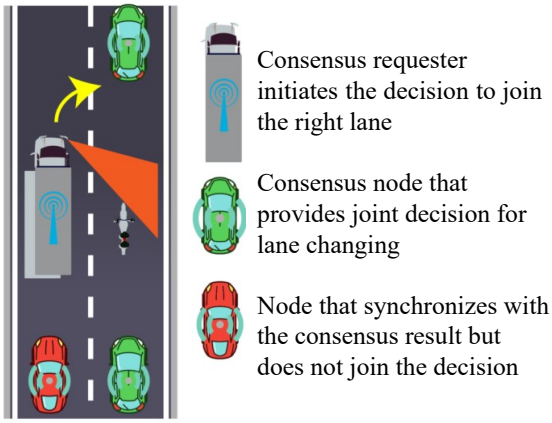


Fig. 19. WBC for the traffic decision with PICA protocol.

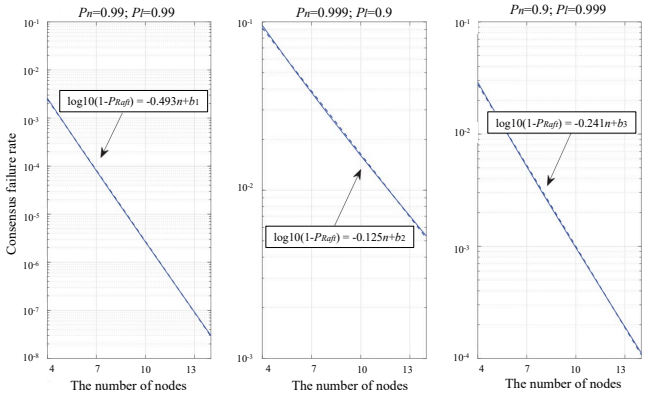


Fig. 20. Raft consensus failure rate.

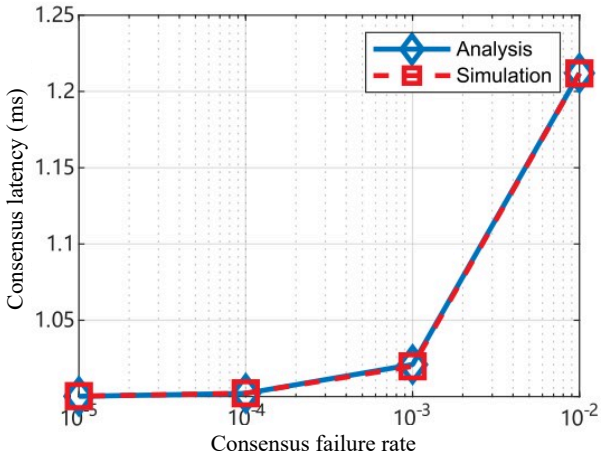


Fig. 21. Raft consensus latency.

phase is shown below,

$$P_{Raft} = \sum_{i=\lceil \frac{n-1}{2} \rceil}^{n-1} \left(\binom{n-1}{i} P_l^i (1-P_l)^{n-1-i} \right. \sum_{j=\lceil \frac{n-1}{2} \rceil}^{i} \left(\binom{i}{j} P_n^j (1-P_n)^{i-j} \right. \left. \sum_{k=\lceil \frac{n-1}{2} \rceil}^{j} \binom{j}{k} P_l^k (1-P_l)^{j-k} \right) \left. \right) P_l^{n-1-i-j+k}, \quad (13)$$

where P_n represents the reliability of the node (i.e., CAV), and P_l is the transmission success rate of the communication link. The first two summation symbols in this equation represent the *downlink* and *uplink* success rates, respectively. And the last summation symbol represents the success rate of the synchronization phase. Together, they have formed a wireless Raft consensus success rate within the PICA framework.

Then, the authors give the consensus latency of this wireless Raft, considering that the consensus leader fails and needs to be re-elected, as follows

$$t_{Raft} = \sum_{n_f=1}^{\infty} \left[(1-P_{Raft})^{n_f} P_{Raft} (n_f t_e + 2t_n) \right] + P_{Raft} t_n, \quad (14)$$

where n_f denotes the number of leader re-elections that take place, which is related to the consensus failure rate. t_n and t_e represent the normal operation required for wireless Raft and the extra time required for leader re-election, respectively. Specifically, the $n_f t_e + 2t_n$ illustrates the latency for each leader re-election.

To verify that the scheme meets the vision of 6G in IMT-2030, the authors have conducted simulations for the consensus success rate and latency of the derivation. Fig. 20 shows the consensus success rate under the three groups of node reliability and communication link interruption probability, which is expressed as the logarithm value of the consensus failure rate. The results illustrate that we can adjust the number of nodes according to the reliability of nodes and the probability of communication link interruption to achieve hyper-reliable CAVs driving. In addition, when the number of CAVs on the road is determined, to achieve hyper-reliable driving decisions, the results also provide a reference range of node reliability and communication link interruption probability. For example, when $P_n = P_l = 0.99$ and the number of CAVs on the road is greater than 10, the PICA framework with wireless Raft consensus can be made to meet the range specified in IMT-2030 for hyper-reliable communication, that is, 10^{-5} to 10^{-7}. Fig. 21 illustrates the consensus latency of wireless Raft, which takes consensus reliability as the horizontal coordinate. This curve intuitively shows that consensus latency is strongly correlated with consensus reliability. When the WBN-driven IoV is hyper-reliable (i.e., the failure rate is less than 10^{-5}), its communication latency is much lower than the description of hyper-low latency in IMT-2030, namely less than 1 ms.

The above findings collectively illuminate the latent capabilities of WBN in facilitating IoVs, while also underscoring the profound synergy between WBN and the forthcoming 6G communication. This integration is poised to significantly enhance the communication system's proficiency in accomplishing the stringent requirements of URLLC, thereby advancing toward the realization of HRLLC objectives.

VI. Wireless Blockchain Networks for Massive Communications in 6G

A. Fundamentals of Massive Communications

Massive communication in 6G is an enhanced version of mMTC compared to 5G and aims to exceed the connection density of 5G by 10-100 times, to reach 100 per square meter or 100 million per square kilometers [256]. More and richer device access in the communication network will strongly support intelligent applications, such as smart cities, intelligent transportation, etc., which involve a large number of terminals.

Within this vision, it is essential to ensure an adequate provision of spectrum, computational power, storage capacity, and other critical resources for the extensive communication terminals. Nonetheless, the finite nature of these resources in the physical realm necessitates the exploration of novel technologies aimed at enhancing resource utilization efficiency or facilitating resource-sharing mechanisms. Furthermore, the integration of large-scale communication devices in a network introduces concomitant security challenges that require meticulous attention and innovative solutions [257].

B. Applications of WBN in Massive Communications

When WBN is assigned to 6G, the trusted transaction environment it provides can help the sharing and exchange of various network resources, helping to achieve massive communications. Xu et al. [258] have pioneered the use of blockchain to effectively manage the utilization of resources in 6G. They also have discussed multiple 6G scenarios for resource sharing, such as device-to-device communication, network slicing, etc. Then, Sun et al. [259] emphasized that smart contracts can ensure the intelligence and automation of spectrum resource exchange, and proposed a highly efficient spectrum-sharing method. In [260], the authors propose the concept of SpectrumChain, focusing on the potential of blockchain in 6G spectrum sharing, and propose a dynamic sharing framework. In addition, for innovations in WBN, [261] and [262] have designed a DAG chain-based and hierarchical blockchain architecture, both providing sufficient scalability for the spectrum exchange of 6G large-scale devices.

The data privacy management of these massive devices is similar to the application of WBN in ubiquitous connectivity, discussed in Section VIII. The only distinction lies in the emphasis placed by ubiquitous connectivity on accommodating the heterogeneity of communication apparatus, including mobile platforms. Thus, we should optimize WBN architectures for mobile node participation. Conversely, in scenarios involving mass-scale communications, the WBN implementation is geared towards enhancing scalability to support an extensive network of devices, such as [26], [189].

C. A Case Study: A WBN-enabled Symbiotic Communications

Based on the exchange of network resources, Liang et al. [263] have introduced symbiotic communication, a new paradigm for resource and service reciprocity. The concept compares radio systems to nature. Living things in nature consume resources such as food, water, and light, and communication systems also require spectrum, computing, and storage resources. Furthermore, they expect to build reciprocal resource exchange relationships in the communication system, namely, symbiotic communication. In this paradigm, all Symbiotic Devices (SDs) are expected to gain performance through the exchange of resources and services. As a result, SDs can make full use of network resources and break through the resource constraints caused by massive communication [264].

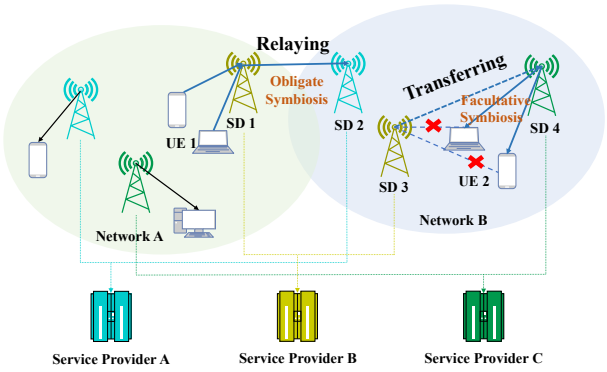


Fig. 22. Throughput with removing a new domain.

Specifically, symbiotic relationships can be divided into obligate and facultative relationships [263]. An obligate relationship is when an SD relies heavily on the collaborative efforts of other SDs to provide communication services to the UE because it cannot achieve its communication goals independently. For example, cognitive backscatter communication [240]. As shown in Fig. 22, SD 2 cannot provide network access services to UE 1 without intermediate support from SD 1, illustrating this inherent dependency. This relationship is very similar to that between plants and bees, where plants provide the bees with essential pollen for food and, in turn, the bees help pollinate. Neither of these entities can grow autonomously in their natural habitat. In addition, a facultative relationship means that each SD can perform communication tasks as an independent server, but together they can provide higher-quality communication services to the UE. As shown in Fig. 22, both SD 3 and SD 4 can independently provide network access services for UE. Through resource sharing, they can provide better communication services for end users. The relationship is similar to the one between sharks and remora. The remora gets extra nutrients by cleaning food debris and parasites from the shark's teeth.

The limited network resource bottleneck can be obtained through symbiotic relationships, but unreliable information sharing between heterogeneous SDs poses a serious challenge to trusted transactions. Especially when there is a Byzantium SD, initiating malicious resources to exchange information to fool other SDs or UEs will harm symbiotic relationships. Cheng et al. [265], [266] have proposed that blockchain can provide a trusted environment for exchanging resources and services and promote the construction of symbiotic relationships. Their simulation results show that the proposed DAG-based blockchain scheme can enable auxiliary symbiotic communication to accelerate the transmission of services in both non-attack scenarios and malicious attack scenarios.

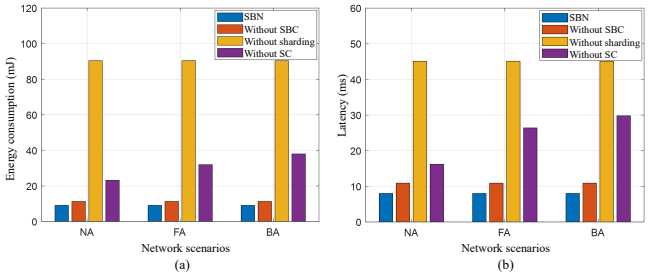


Fig. 23. Network performance for WBN-enabled SC. (a) Energy consumption. (b) Latency.

Furthermore, symbiotic communication can be divided into host (UE) and network (SD) initiation. For the **host initiation**, the UE actively requests data services or transmissions based on its own needs. However, if a large number of hosts initiate requests simultaneously, it may cause network congestion and lead to an increase in network latency. Furthermore, there may be cases where the host maliciously initiates false service requests. If there is a lack of an effective verification mechanism, it may lead to the unreasonable utilization of resources, such as some hosts excessively occupying network bandwidth. As for the **network initiation**, it is started by a specific SD in the network to allocate and trade network resources to improve the transaction processing efficiency. SD can systematically arrange the transaction verification sequence based on the network load to reduce congestion. However, this scenario is prone to the occurrence of SPF due to the SD malice or failure, thereby preventing the entire symbiotic network from rationally utilizing network resources and services. According to this, it is urgent to use WBN-based symbiotic communication to enable massive communications.

Here, we introduce a scheme that designs a low-energy consumption sharding for S-PBFT consensus serving symbiotic communications [267]. This method considers the malicious or faulty situations of both UE and SD simultaneously, covering the symbiotic communication types initiated by the host and the network. It provides a sustainable and trustworthy networking function for 6G. In this work, the authors summarized symbiotic services into four categories: relaying, transferring, computing, and charging. The relaying service is when an SD uses its spectrum resources to relay radio signals for the UE so that it can connect to a network provided by another SD that would otherwise be difficult to connect directly. Transferring service indicates that when an SD cannot provide necessary network services for a UE, the responsibility for network access is transferred to another SD. The computing and charging services are that when the computing power or energy of one SD is insufficient, the other SD can perform computing or power support through task unloading or wireless charging.

In addition, they also point out how WBN provides an efficient and trustworthy environment for symbiotic communications. First, consensus, as a key evaluation tool for network decision-making, enables all SDs to independently evaluate the legality of transactions based on factors such as account balance, transaction amount, and timestamp, without third-party intervention. When all SDs reach consistency, transactions are securely recorded on the blockchain in the form of hashes, ensuring reliability, security, and traceability. Then, in order to improve the transaction processing efficiency of WBN, the authors also design a scalable, energy-efficient sharding scheme for the possible implementation of S-PBFT consensus. The idea is similar to the GS scheme we introduced in Section III-B [189], so the details are not given here.

Figs. 23 (a) and (b) respectively show the energy consumption and latency required when the scheme is integrated into symbiotic communication employing ablation experiments. Where NA, FA, and BA represent that there are no attackers in SD, 10% of SDs are faulty nodes that do not participate in the symbiotic service and WBN consensus, and 10% of SDs are Byzantine nodes that generate false transactions in the symbiotic service and WBN consensus. To get closer to the 6G network requirements and scenarios, they adopted SAGIN in the simulation, and the parameters were from [268]. Collectively, they exhibited the efficacy of the sharded WBN in facilitating symbiotic communication. The ablation study indicates that the integration of sharding, SBC, and symbiotic communication collectively enhances energy efficiency and minimizes latency in 6G network communications. Notably, when amalgamated with WBN, this approach demonstrates robust resilience against both attacks.

Consequently, the synergy between WBN and symbiotic communication emerges as a potent technological strategy for realizing massive communication for 6G networks.

VII. Wireless Blockchain Networks for Immersive Communications in 6G

A. Fundamentals of Immersive Communications

Immersive communication will become one of the key service categories for 6G and is a further iteration of eMBB in 5G [242]. It will introduce interactive services such as Augmented Reality (AR) and Virtual Reality (VR), holographic communications, and others over cellular networks. A case in point is a live VR concert, which, when simultaneously accessed by thousands of participants, imposes stringent requirements on the wireless network infrastructure to sustain high data rates without compromising the Quality of Experience (QoE) for end-users. In alignment with the IMT-2030 vision for immersive communication, the projected peak throughput is poised to reach an extraordinary threshold of 1 Tbps [72].

Metaverse and Web 3.0 are the most typical application cases [29]. As the successor to the mobile Internet, they are gaining popularity. Web 3.0 is the poster child for the shift of the Internet to decentralization. Metaverse is expected to be a virtual world populated by User Generated Contents (UGCs) [269]. These provide users with ubiquitous immersive services, allowing them to interact with digital avatars in the virtual world in real time, expanding people's living, entertainment, office, and learning space.

B. Applications of WBN in Immersive Communications

In juxtaposition with the content-centric "read" paradigm of Web 1.0 and the "read-write" paradigm of Web 2.0, Web 3.0 adopts a user-centric "read-write-own" model [270]. This

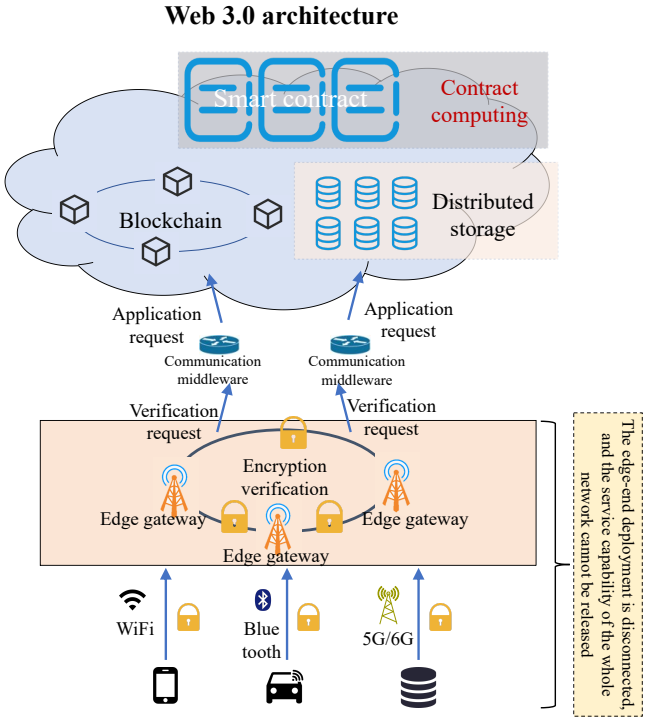


Fig. 24. Web 3.0 architecture.

paradigm shift signifies a platform where data sovereignty is vested in users, eschewing centralized control mechanisms. The deployment of Web 3.0 applications operates on decentralized and transparent principles, which inherently mitigate risks associated with malicious program installations. Nevertheless, this paradigm may inadvertently facilitate unwarranted data utilization, uneven value distribution, and privacy breaches. Furthermore, in identity management, Web 3.0 empowers local users to generate verifiable identities across decentralized applications, serving as proof of ownership for their data. These user identities and associated data are securely stored via blockchain's distributed ledger technology, enabling seamless transferability across various applications with user consent, thereby addressing the issue of data siloing.

Complementing these advancements, the emergent concept of the Metaverse has garnered significant interest from both industry and academic sectors due to its potential to craft a fully immersive and self-sustaining virtual reality ecosystem. Technologies such as VR and AR offer users an immersive experience. Notably, blockchain plays a pivotal role within the virtual world ecosystem by ensuring fairness, transparency, and genuine entitlement to digital assets [271]. These sophisticated technologies facilitate the creation of digital replicas of the physical world, generating unique virtual content and paving the way for a hyper-realistic digital universe [272].

However, none of these blockchain technologies and applications are related to wireless networks, as the traditional Metaverse and Web 3.0 architectures rely on wired networks. It is foreseeable that with the further expansion of Metaverse and Web 3.0 deployment and service scope, the wireless network scenario will be included in them [273], [274], which will

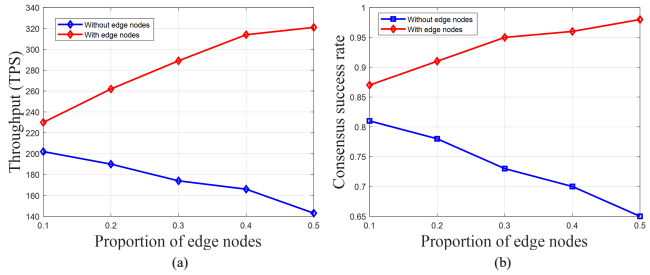


Fig. 25. Web 3.0 performance. (a) Throughput. (b) Consensus success rate.

significantly free up the service capabilities.

C. A Case Study: A WBN-enabled Web 3.0

According to the Web 3.0 technology and industry ecological development report released by the China Academy of Information and Communications Technology (CAICT) [275], a potential Web 3.0 architecture is shown in Fig. 24. It includes terminal devices, edge gateways, communication middleware, blockchain, etc., embodying the P2P and distributed characteristics of Web 3.0. Based on this, the subsequent discussions are carried out relying on this architecture. From this architecture, we find that the deployment of blockchain in Web 3.0 is hosted on the cloud platform. It means that there is a disconnection between edge-end deployment, which makes it difficult to release the service capacity of the whole network, since the participation of edge nodes and terminal devices is missing. This setting is due to the unstable channel environment and limited node resources of the edge wireless network, it is difficult to manage and schedule the resources of the blockchain deployed on the edge side.

Due to real-world constraints, the blockchain deployment scenario requires users to host code and data to a cloud service. This deviates from the original intention of Web 3.0's design of "autonomous management and distributed interconnection". With the continuous upgrading of hardware devices, a large number of servers and terminals deployed at the edge of the network can store and trade crypto assets locally. As a result, deploying blockchains in a distributed manner or locally at the end is bound to become the future trend of Web 3.0.

Unlike the data center networks where cloud servers reside, most devices on the edge side communicate over wireless networks with greater flexibility and coverage. However, as we have described for WBNs before, the channel is less stable than the wired connection in the data center, which will seriously affect the performance of WBNs.

Based on the evaluation of WBN performance in [132], [133], [157], and optimization methods in Tables II and III, we have preliminary schemes for the deployment and operation of blockchain network in a wireless environment on the side. This can not only further expand the scale of Web 3.0 application and deployment scope, but also the only way for Web 3.0 to achieve "user co-construction, co-governance, and sharing".

Fig. 25 shows the throughput and consensus success rates of Web 3.0 with and without edge nodes over wireless connections. This result is performed when the total number of

nodes is 30 and PBFT consensus is used. As the proportion of edge nodes increases, both features of Web 3.0 that cover edge nodes are optimized. Conversely, Web 3.0 performance without covering edge nodes deteriorates further. The reason is that edge nodes can also provide users with reliable services such as digital asset transactions, contributing to the popularization and improvement of 6G immersive communications.

VIII. Wireless Blockchain Networks for Ubiquitous Connectivity in 6G

A. Fundamentals of Ubiquitous Connectivity

With the continuous exploration of the natural world, the communication needs of satellites, spacecraft in space, unmanned probes in the deep sea, and other equipment cannot be ignored. To meet a wider range of "anytime, anywhere" connectivity needs, 6G proposes ubiquitous connectivity. It is a new communication requirement of 6G compared with 5G [72], [276], which aims to connect all communication equipment from space, sky, sea, etc., in addition to the ground network, to build a three-dimensional SAGIN [277], [278]. This metric and its unprecedented communication coverage express the vision of connecting unconnected users and providing them with low-cost, ubiquitous communication services.

Nevertheless, the augmentation of connectivity and the omnipresence of communication are poised to introduce multifaceted challenges in network administration. These include the authentication of numerous device identities and concerns regarding the disclosure of users' communication privacy [11]. As network coverage extends, it inadvertently furnishes malicious actors with enhanced opportunities for cyber-attacks.

B. Applications of WBN in Ubiquitous Connectivity

The security guarantee provided by WBN for the 6G network can make it realize ubiquitous connectivity without worry. Its decentralized identity authentication, privacy protection, covert communication, etc., can provide 6G with a powerful and secure toolbox [279].

Furthermore, the proliferation of communication devices within the 6G, governed by distinct administrative entities, necessitates the establishment of a multi-domain communication paradigm. This scenario introduces complexities in device identity verification and privacy preservation, given the potential for disparate communication protocols across domains. Concurrently, the huge number of terminals presents scalability issues for WBNs, thereby significantly impinging upon blockchain's operational efficiency and hindering the attainment of HRLLC objectives. Therefore, the design of the cross-domain security protection mechanism for ubiquitous connectivity based on WBN is put forward to ensure information security on the basis of taking into account 6G communication efficiency, for example, the blockchain-assisted cross-domain data sharing [82], and the cross-domain identity authentication based on the split chain [85].

In addition to identity management, the ubiquitous network also accesses large-scale communication, computing, and storage resources. How these resources work together to serve the 6G network to achieve efficient communication also needs to be solved [280]. The processes involved in resource management, sharing, and trading will also concern attackers, leading to security issues. This is similar to the massive communication need for WBN described in Section VI. A typical example is the layered multi-chain architecture [262], which not only can optimize blockchain communication and storage cost, but also can resist the wireless spectrum resource deals in the period of interferences and attacks.

C. A Case Study: A WBN-enabled SAGIN

In this part, we use blockchain-enabled cross-domain authentication for SAGIN to demonstrate how WBN can help 6G achieve ubiquitous connectivity. As previously discussed, security and privacy concerns significantly restrict communication and data exchange among the multitude of devices within the SAGIN framework, confining interactions to their designated administrative domains. This limitation severely impedes the potential for inter-domain data sharing. To facilitate seamless data sharing and resource exchange across disparate domains, robust identity authentication mechanisms are imperative. Traditional authentication approaches, particularly those reliant on Public Key Infrastructure (PKI), have been foundational in securing electronic communications [281]. However, these centralized systems exhibit several vulnerabilities, with the most critical being the SPF [282]. In a PKI system, the compromise of a central authority or key distribution center can have far-reaching consequences, compromising the overall system security.

For cross-domain authentication, blockchain constructs a distributed network that eliminates the above disadvantages. Nonetheless, despite the plethora of studies investigating blockchain-based cross-domain authentication frameworks [47], [84], [85], a notable gap exists in addressing the dynamic nature of managing domain interactions. This is particularly important in dynamic networks such as SAGIN, where drones, satellites, and vehicles are mobile and often join, exit, or transition between domains. A prevailing issue with most existing blockchain solutions is their static configuration, which does not accommodate fluid and evolving relationships between domains. This shortcoming may precipitate operational challenges and diminish flexibility in practical applications, compromising both the blockchain performance and the authentication efficacy.

Therefore, to better serve SAGINs, Luo et al. rely on WBN to design a novel cross-domain authentication that supports dynamic node changes [283]. At its core, it allows node join and exit processes to be perfectly merged into the normal consensus flow, thereby optimizing the consensus efficiency.

This scheme leverages an Identity-Based Signature (IBS) approach to administer device identities within SAGIN, to mitigate storage costs [284]. Each SAGIN device is assigned a unique identifier that functions as its public key. While the corresponding private key is generated by the Management Server (MS) located within the same administrative domain. In cross-domain authentication, the initiating SAGIN device is required to incorporate a valid signature within its request to substantiate its legitimate identity. The authenticating device

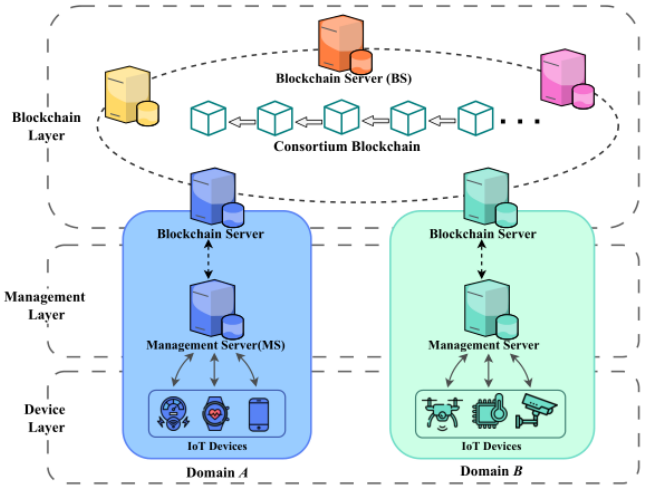


Fig. 26. The cross-domain authentication architecture.

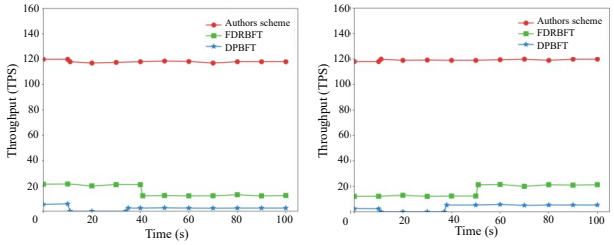


Fig. 27. Throughput. (a) Removing a domain. (b) Adding a domain.

subsequently verifies the request by scrutinizing the requester's public key and accompanying signature.

Furthermore, the authentication architecture, as depicted in Fig. 26, comprises three layers: a blockchain layer, a management layer, and a device layer. The **device layer** encompasses a myriad of SAGIN devices, including satellites, drones, vehicles, and sensors. Given their constrained computational and storage capacities, these devices are ill-suited for executing the computationally intensive algorithms. Consequently, they delegate these responsibilities to the MS. The **management layer** possesses significantly augmented computing power relative to SAGIN devices. The primary remit of these servers is to generate and disseminate private keys for the devices. Additionally, MS registers the identifiers of SAGIN devices on the blockchain, thereby facilitating subsequent cross-domain authentication procedures. The **blockahin layer** comprises BlockChain Servers (BCSs) that maintain the immutable blockchain ledger. During the system initialization phase, BCS inscribes the public parameters pertaining to each domain and the public key information of registered SAGIN devices onto the blockchain.

Then, for the consensus, as the core of WBN supporting SAGIN dynamic device authentication, the authors employ a strategy analogous to the piggybacking mechanism in the Transmission Control Protocol (TCP) protocol [285]. The central tenet of this approach involves integrating dynamic participation events into the conventional consensus process, thereby mitigating the efficiency loss associated with the frequent joining and exiting of SAGIN devices. When adding a new domain to the blockchain is necessitated, its corresponding BCS, herein referred to as the applicant, submits a formal application to the nearest BCS within the existing WBN. The receiving BCS then proceeds to verify the legitimacy of the applicant's identity, which may involve the authentication of digital certificates. Should the domain exhibit a history of misconduct, for instance, repeated failure to engage in the consensus process, the request to join the network is duly rejected. Conversely, if no such record exists, the $JOIN$ request is broadcast to other BCSs for further consideration and validation, i.e. $\langle JOIN, DC, TS\rangle E_i$, where DC denotes the applicant's digital certificate, TS is timestamp the request initiated, and E_i represents an endorsement provided by BCS_i. After receiving the application, once the other BCSs confirm that the DC of the applicant is legitimate, its public key information will be included in the next round of consensus voting. In addition, legitimate applicants need to regularly participate in consensus.

Domains are not allowed to exit the blockchain prematurely before consistency is reached. Otherwise, the leader reserves the right to add the public key of the exiting BCS to the blacklist. After the consensus ends, the domain can initiate an $EXIT$ request, namely, $\langle EXIT, DC, TS\rangle E_i$.

To empirically assess the cross-domain authentication efficacy of the proposed consensus under dynamic SAGIN device participation, the authors have configured the simulation with 4 domains, the 20 MB block size, and set the authentication request arrival rate at 120 per second. For the comparison purpose, two dynamic blockchain consensus mechanisms are selected: Dynamic PBFT (DPBFT) [286] and Fast, Dynamic and Robust Byzantine Fault Tolerance (FDRBFT) [287]. Figs. 27 (a) and (b) illustrate the throughput of a WBN during the domain joining and exiting, at the 10th second. In both, the proposed scheme demonstrates a significant advantage. Consequently, the simulation reflects a quicker response time to domain connection or interruption requests of this scheme and has little impact on performance. Conversely, FDRBFT exhibits a longer consensus cycle, with approximately 25 seconds required for a domain to successfully join the network. Furthermore, DPBFT temporarily halts the normal consensus process to exclusively manage the domain join or exit event upon receiving a domain join or exit request, resulting in a complete cessation of authentication request processing and a consequent drop in throughput to zero.

These outcomes substantiate the WBN capability to support 6G in achieving ubiquitous connectivity while effectively managing dynamic node participation and departure. Furthermore, when WBN is combined with interoperability operations, cryptographic algorithms, and other advanced technologies in cross-domain identity authentication, it will provide more powerful and comprehensive services for ubiquitous connectivity requirements.

IX. Practical Application Cases

It is difficult to fully grasp the importance of WBN to wireless communication systems only from the above theoretical analysis. Combined with the practical application cases

of WBN in network operators, it will establish a more comprehensive knowledge structure for us. At this stage, telecom operators are adopting blockchain mainly as a way to build a lower-cost infrastructure and provide trustworthy network services to users on this basis.

A. Blockchain for Lower-cost Infrastructures

China Mobile: As the largest operator in China, it led the launch of the construction of blockchain interconnection infrastructure for telecom operators in 2023 [288]. This infrastructure is designed to enable the sharing of trusted data between different operators to meet the needs of users across operators.

PCCW Global: Based in Hong Kong, China, partnering with Syntropy in 2022 to monetize unused bandwidth based on blockchain and make it available on demand to Web 3.0 application developers or network infrastructure engineers [289]. This move allows network operators to benefit from underutilized links in the networks they operate. This network infrastructure will significantly reduce bandwidth costs.

AT&T: As one of the largest operators in the United States, it released a blockchain-enabling network infrastructure scheme together with Microsoft and IBM as early as 2018 [290]. It combines IoT technology to automate low-cost deployment of network facilities and achieve traceability in the deployment process.

Telefónica: It is a large multinational telecommunications operator based in Spain. In 2024, this company and Nova Labs adopted blockchain technology to reduce the operating cost of network infrastructure, thereby expanding their communications coverage in Mexico [291]. The basic principle is that Telefonica can safely offload peak data traffic to the Helium network operated by Nova Labs, thereby easing congestion in the cellular network.

SK Planet: As the largest information and communications technology company in South Korea, it announced in 2024 that it will jointly build Web 3.0 applications for South Korea with the flagship platform of Web 3.0, Mocaverse [292]. The app will offer various Web 3.0 experiences, including immersive games, sports, and IP-based products.

Lesson Learned: Telecom operators worldwide are leveraging blockchain technology to drive innovation and cost savings in network infrastructure. Through partnerships, as seen with PCGW Global and Syntropy, and SK Planet and Mocaverse, they are adapting to Web 3.0 trends. Blockchain helps cut costs, as demonstrated by China Mobile, AT&T, and Telefónica, which use it for data sharing, automated deployments, and traffic management. Early adopters like AT&T, starting in 2018, gain a competitive edge by having more time to refine their use of this technology.

B. Blockchain for Trustworthy Network Services

China Mobile: In 2022, it released the China Mobile Blockchain-as-a-Service (CMBaaS) [293]. This technology can coordinate the trust between multiple users, and is suitable for various scenarios such as trusted data flow and trusted data asset storage between multiple users, such as data security sharing between different medical institutions.

China Telecom: As another well-known operator in China, it released a blockchain Subscriber Identity Module (BSIM) card in 2023 [294]. Each BSIM card serves as a blockchain node. Compared with the traditional card, this card can generate and store the user's public and private keys, and has portability, high security, and high performance characteristics, which will promote Web 3.0 Innovation and development.

PCCW Global: It is one of the first companies to incorporate blockchain into telecom networks. As early as 2018, it jointly designed the Proof of Concept consensus with Colt Technology Services and used it in the settlement of cross-border roaming services [295]. By using blockchain, they were able to reduce this labor-intensive process from hours to minutes. This practical case shows that blockchain can enable roaming to be automatically verified and settled between operators, and provide users with efficient and trusted cross-border roaming services. In 2022, PCCW Global also partnered with Sandbox to develop the world's first blockchain-based virtual mobile network and a Metaverse modeled on Hong Kong [296].

Vodafone: As one of the world's largest network operators in the United Kingdom, it has launched the Digital Asset Broker (DAB) blockchain network, which aims to enable secure resources and financial transactions. In 2023, this company further combined the Cross-Chain Interoperability Protocol (CCIP) from Chainlink Labs with DAB to provide security and interoperability for IoT devices at the network edge [297].

Telefónica: It has developed a Blockchain-as-a-Service (BaaS), TrustOS, based on blockchain, which was showcased at Mobile World Congress (MWC) 2024 [298]. This service can easily provide users with traceability information on telecom products and also support the trustworthy certification service of data workflows and documents in the network.

Lesson Learned: Telecom operators are using blockchain to boost trust in services. China Mobile's CMBaaS and China Telecom's BSIM card use it for user-related trust and identity protection. PCGW Global's early blockchain-based cross-border roaming settlement with Colt speeds up verification. Vodafone's Digital Asset Broker and Telefónica's BaaS apply it to asset and IoT security, plus info traceability. The key lesson is that blockchain can transform telecom with trust, security, and efficiency, and early adoption helps operators innovate in the digital era.

X. Future Directions

A. Heterogeneous Dynamic Networks

Heterogeneous Dynamic Networks (HDNs) are the inevitable form of networking caused by ubiquitous connectivity.

- **Considering underwater node:** The presently contemplated SAGIN framework does not encompass the communication prerequisites for submerged submersibles. In an underwater context, radio signal attenuation is significantly more pronounced, with high-frequency transmissions, as envisaged in 6G, experiencing particularly severe degradation. The exploration of alternative communication modalities such as underwater acoustic systems

[299], visible light communication [300], and infrared transmission [301] is underway. However, these methods exhibit incomplete compatibility and integration capabilities with the prospective 6G network. Consequently, a critical need arises to investigate the development of a WBN that can seamlessly interface with diverse underwater communication apparatus, thereby facilitating the establishment of a holistic and trustworthy 6G network.

- **More flexible data storage:** To safeguard the integrity and security of system data storage, each node within the WBN maintains a comprehensive backup of transactional information about the entire network. Within the HDNs, the heterogeneity and dynamic nature manifest in nodes' propensity for mobility, including arbitrary entry into and departure from the network at any time. Consequently, this fluidity poses challenges for newly integrated nodes, as they grapple with making informed judgments on novel transactions due to their lack of historical transactional context. Concurrently, nodes in the process of exiting the network must implement robust measures to mitigate the risk of inadvertent transactional data disclosure. In addition, for sharding scenarios, when the mobile node changes shards, its transaction record needs to be updated in time to maintain synchronization. These problems need urgent attention to be solved in the HDN. Perhaps the storage method that combines on-chain and off-chain has the potential to alleviate the above-mentioned challenges.
- **Adaptive WBN topology:** While the above WBN consensus allows node entry and exit, it still impacts WBN performance. Since broadcasting and consensus are intimately tied to the geographical distribution of nodes and the network topology. Perturbations in these parameters can precipitate substantial detrimental effects on both broadcast efficacy and consensus mechanisms. Especially for sharding, the dynamically changing nodes not only affect the network structure but also bring about many cross-shard transactions, imposing a burden on the blockchain system. Presently, digital twin-based strategies offer a means to construct virtual static environments for mobile nodes, contingent upon establishing timely and precise information interactive protocols between virtual and physical realms [232]. Nonetheless, the adaptive WBN topology to accommodate fluctuations in node positions remains an underexplored domain.

B. Integrated Sensing and Communications

ISAC is an important scenario of 6G, but also a link that is not fully combined with WBN at present. This part discusses the benefits and roles that WBNs can provide for ISAC.

- **Sensing data protection:** In the ISAC system, it is imperative that perceptual data not only maintains its authenticity but also adheres to robust privacy protection protocols, particularly for sensitive information such as human biometrics and geographical mappings. The incorporation of WBNs enhances the traceability of perceptual data, thereby mitigating the potential for data fabrication. Concurrently, blockchain offers reliable mechanisms for privacy preservation, capable of withstanding diverse cyber threats [302]. Furthermore, in scenarios involving cross-domain sensing data sharing, there emerges a pressing requirement for WBN to implement decentralized identity management for inter-domain nodes, facilitating seamless sensing data flow and collaborative exchange [303].
- **Incentive mechanism:** Within the ISAC systems, WBNs have the potential to introduce an incentive-compatible governance paradigm. It involves implementing a gamified point system or adopting a token economy model, where ISAC nodes are rewarded for their active participation and contribution to sensing data-sharing endeavors. Such mechanisms not only incentivize user engagement but also promote the generation and dissemination of perceptual data. Complementarily, integrating a penalty system that penalizes the submission of inaccurate or fraudulent data ensures data integrity and quality, thereby facilitating the acquisition of comprehensive and high-fidelity perceptual datasets essential for ISAC systems.

C. Integrated Artificial Intelligence and Communications

Consistent with ISAC, IAAC is also one of the important scenarios in 6G, and its data collection, training, and transmission can use WBN to build secure and trustworthy solutions.

- **Semantic communication:** Semantic communication deeply integrates wireless communications with AI, enabling the extraction of semantic information from communication content. This innovation transcends the Shannon capacity limit in information theory, enhancing both the communication capacity and efficiency [304]. Currently, research efforts of WBN and semantic communication primarily concentrate on leveraging blockchain to facilitate semantic data sharing among disparate semantic knowledge bases [305], [306]. However, there is a lack of work in WBN to enable the semantic communication process, because attackers can send malicious semantic data with similar semantic information but expect different content to interfere with the receiving node [307].
- **Wireless AI large model:** Currently, Large Language Models (LLMs) serve people in the AI-Generated Content (AIGC) form, which is widely used in consulting and education [308]. Due to concerns about the privacy of user interaction data, LLM deployment is moving from the cloud to the edge side [309], giving birth to the concept of Wireless AI Large Model (WAILM) and gradually applied to wireless communications [310], [311]. WBN can provide them with the reliable learning corpus, secure training process, and traceable generated content [312]. However, the consensus adapted to WAILM needs to be studied urgently, and its consensus process and decision must consider the communication optimization gain provided by WAILM deployed on edge nodes.

D. Standardization of WBN

To promote and standardize the practical deployment of WBN in 6G, it is indispensable to discuss the standards of

WBN. Below, focusing on the six application scenarios in 6G, we have proposed the initial standardized norms of WBN:

- **WBN for HRLLC:** 6G requires an end-to-end latency of less than 1ms and a reliability of 10^{-5} to 10^{-7}. Typical scenarios include autonomous driving and industrial automation. This means that it is necessary to ensure that WBN has a consensus success rate greater than 99.999% and a consensus latency less than 100 μs from aspects such as consensus mechanism optimization and node resource collaboration.
- **Massive Communications:** 6G supports a connection density of 1 million/km^2, with typical scenarios including smart cities and IoT. To enable WBN to support the normal operation of devices of such a scale, its scalability and energy efficiency can be enhanced through sharding and blockchain-based spectrum sharing. For example, a single shard shold support more than 100,000 device consensus, and the cross-shard latency does not exceed 10 ms. Meanwhile, the energy consumption of each consensus node is less than 100 mW.
- **Immersive Communications:** 6G supports a peak rate of 1 Tbps, with typical scenarios including the Web 3.0, Metaverse, and VR/AR live streaming. Thus, more wireless edge nodes need to be incorporated into the WBN consensus so that it can meet such high throughput and reliability. A potential standard is to expect the processing capacity of a single node to be greater than 1 Gbps and the latency for immersive interaction requirements to be less than 20 ms. In addition, for Quality of Experience (QoE), the stuttering rate is less than 1% and the resolution supports greater than 8K@60fps.
- **Ubiquitous Connectivity:** 6G looks forward to an integrated coverage network of space, air, ground and sea, with typical scenarios being satellite communication and deep-sea exploration. Consequently, it is necessary to develop a cross-domain identity authentication based on WBN to build a trusted environment for this ubiquitous scenario. This means that WBN needs to support non-terrestrial network (NTN) access, and the connection interruption recovery time should be less than 1 s, and the synchronization latency of cross-domain data should be less than 100 ms.
- **ISAC:** The integration of communication and sensing in 6G can be applied to various detection scenarios, such as environmental monitoring and accident warning in autonomous driving. WBN can provide reliable guarantees for its perception data and achieve secure sharing. As a result, our expectation for WBN in this scenario is to assist in the perception positioning error being less than 1 m and the latency being less than 50 ms. Furthermore, for spectrum sensing, its detection bandwidth should cover 100 MHz to 10 GHz, and the detection sensitivity need to be increased by 10 dB.
- **IAAC:** 6G requires deep integration with AI, which cannot do without the collaborative training of wireless edge AI models. Typical scenarios are intelligent transportation and manufacturing. The intervention of WBN can ensure the credibility of model training and data security. Meanwhile, the incentive mechanism can enhance the participation of training nodes. We expect that with the participation of WBN, the convergence speed of the training of the wireless AI model can increase by more than 30%, and the training data involved will meet the compliance requirements of the General Data Protection Regulation (GDPR) [313].

Also, we need to note that the purpose of WBN standardization discussion is to make it better deployed in and serve 6G. However, it must be admitted that WBN cannot solve all the challenges and problems in 6G. For example, in privacy leakage cases, it is necessary to cooperate with cryptographic means such as ZKP and SMPC. Meanwhile, in addition to parallel processing methods such as sharding in blockchain, scalability challenges can also be addressed by leveraging new multiple access technologies to enhance the connection density of 6G networks. Moreover, the trade-off between 6G performance and blockchain cost needs to be taken into account. Not all 6G scenarios require the involvement of blockchain, such as local area networks in private institutions. Therefore, the integration of WBN with these auxiliary technologies to jointly provide high-quality services for 6G is an important part of the future WBN standardization process.

XI. Conclusion

In this tutorial, we delve into the potential of WBN in shaping trusted 6G networks. We take a WBN-assisted cellular network to defend against attacks as an example, introducing how WBN transforms the 6G network. Meanwhile, we highlight the key technologies in WBN, as well as main directions of performance optimization. In addition, case studies have been conducted on the enabling effects of WBN in various 6G applications, such as HRLLC, massive communications, immersive communications, and ubiquitous connectivity. These explorations prove the practicality and effectiveness of WBN in 6G. Finally, this tutorial predicts future research directions for WBN in building 6G networks, such as HDN, ISAC, IAAC, and WBN standardization. In general, it is expected that this tutorial will provide a valuable introduction to research in the field of WBN and 6G networking, encouraging further exploration in this promising area.

References

[1] C.-X. Wang *et al.*, "On the road to 6G: Visions, requirements, key technologies, and testbeds," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 905–974, 2023.

[2] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6G wireless communications: Vision and potential techniques," *IEEE Netw.*, vol. 33, no. 4, pp. 70–75, 2019.

[3] T. Nakamura, "5G evolution and 6G," in *Proc. IEEE Symp. VLSI Technol.*. IEEE, 2020, pp. 1–5.

[4] K. Zheng, J. Mei, H. Yang, L. Hou, and S. Ma, "Digital retina for IoV towards 6G: Architecture, opportunities, and challenges," *IEEE Netw.*, 2024.

[5] S. Abadal, C. Han, V. Petrov, L. Galluccio, I. F. Akyildiz, and J. M. Jornet, "Electromagnetic Nanonetworks beyond 6G: From wearable and Implantable networks to on-chip and quantum communication," *IEEE J. Sel. Areas Commun.*, 2024.

[6] S. Mahboob and L. Liu, "Revolutionizing future connectivity: A contemporary survey on AI-empowered satellite-based non-terrestrial networks in 6G," *IEEE Commun. Surveys Tuts.*, 2024.

[7] V. Vakhter, B. Soysal, P. Schaumont, and U. Guler, "Threat modeling and risk analysis for miniaturized wireless biomedical devices," *IEEE Internet Things J.*, vol. 9, no. 15, pp. 13338–13352, 2022.

[8] R. Song, M. O. Ozmen, H. Kim, R. Muller, Z. B. Celik, and A. Bianchi, "Discovering adversarial driving maneuvers against autonomous vehicles," in *32nd USENIX Security Symp. (USENIX Security 23)*, 2023, pp. 2957–2974.

[9] Y. Sun, J. Liu, J. Wang, Y. Cao, and N. Kato, "When machine learning meets privacy in 6G: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2694–2724, 2020.

[10] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2384–2428, 2021.

[11] A. H. Khan *et al.*, "Blockchain and 6G: The future of secure and ubiquitous communication," *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 194–201, 2021.

[12] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open J. of Commun. Soc.*, vol. 2, pp. 1094–1122, 2021.

[13] B. Cao *et al.*, "Blockchain systems, technologies, and applications: A methodology perspective," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 353–385, 2023.

[14] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain: Res. Appl.*, vol. 3, no. 2, p. 100067, 2022.

[15] X. Sun, F. R. Yu, P. Zhang, Z. Sun, W. Xie, and X. Peng, "A survey on zero-knowledge proof in blockchain," *IEEE Netw.*, vol. 35, no. 4, pp. 198–205, 2021.

[16] W. Hao *et al.*, "Towards a trust-enhanced blockchain P2P topology for enabling fast and reliable broadcast," *IEEE Trans. Netw. Service Manag.*, vol. 17, no. 2, pp. 904–917, 2020.

[17] J. Xu, C. Wang, and X. Jia, "A survey of blockchain consensus protocols," *ACM Comput. Surveys*, vol. 55, no. 13s, pp. 1–35, 2023.

[18] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," in *2008 Proc. of Decentralized Bus. Rev.*, 2008, p. 21260.

[19] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *OsDI*, vol. 99, no. 1999, 1999, pp. 173–186.

[20] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in *2014 USENIX Annu. Tech. Conf. (USENIX ATC 14)*, 2014, pp. 305–319.

[21] S. Datta and S. Namasudra, "Blockchain-based smart contract model for securing healthcare transactions by using consumer electronics and mobile edge computing," *IEEE Trans. Consum. Electron.*, 2024.

[22] J. Li, Y. Lu, Y. Zeng, and Z. Guo, "Segmented storage based on parallel execution for IoT Blockchains," *IEEE Internet Things J.*, 2024.

[23] H. Luo, "ULS-PBFT: An ultra-low storage overhead PBFT consensus for blockchain," *Blockchain: Res. Appl.*, vol. 4, no. 4, p. 100155, 2023.

[24] R. Han, Z. Yan, X. Liang, and L. T. Yang, "How can incentive mechanisms and blockchain benefit with each other? a survey," *ACM Comput. Surveys*, vol. 55, no. 7, pp. 1–38, 2022.

[25] M. A. Ferrag and L. Shu, "The performance evaluation of blockchain-based security and privacy systems for the internet of things: A tutorial," *IEEE Internet Things J.*, vol. 8, no. 24, pp. 17236–17260, 2021.

[26] H. Luo *et al.*, "ESIA: An efficient and stable identity authentication for internet of vehicles," *IEEE Trans. Veh. Technol.*, vol. 73, no. 4, pp. 5602–5615, 2024.

[27] S. Hafeez *et al.*, "Blockchain-assisted UAV communication systems: A comprehensive survey," *IEEE Open J. of Veh. Technol.*, vol. 4, pp. 558–580, 2023.

[28] Y. Zhang *et al.*, "Blockchain-based secure communication of internet of things in space–air–ground integrated network," *Future Gener. Comput. Syst.*, vol. 158, pp. 391–399, 2024.

[29] X. Zhang, G. Min, T. Li, Z. Ma, X. Cao, and S. Wang, "AI and blockchain empowered Metaverse for web 3.0: Vision, architecture, and future directions," *IEEE Commun. Mag.*, vol. 61, no. 8, pp. 60–66, 2023.

[30] "6G network," Jan. 2025. [Online]. Available: https://webofscience-clarivate-cn-s.vpn.uestc.edu.cn:8118/wos/alldb/summary/72f3722e-5fe3-4aa4-9773-0b349067a4dd-012850c204/relevance/1

[31] "Blockchain and 6G," Jan. 2025. [Online]. Available: https://webofscience-clarivate-cn-s.vpn.uestc.edu.cn:8118/wos/alldb/summary/5d09d577-f390-40bf-b11c-ea14530ea0b9-01285030e6/relevance/1

[32] J. Wang, X. Ling, Y. Le, Y. Huang, and X. You, "Blockchain-enabled wireless communications: A new paradigm towards 6G," *Nat. Sci. Rev.*, vol. 8, no. 9, p. nwab069, 2021.

[33] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6G: Challenges, opportunities and research directions," in *Proc. 2nd 6G Wireless Summit (6G SUMMIT)*. IEEE, 2020, pp. 1–5.

[34] Q. Xu, Y. Zou, D. Yu, M. Xu, S. Shen, and F. Li, "Consensus in wireless blockchain system," in *Int. Conf. Wireless Algorithms, Syst., Appl.*. Springer, 2020, pp. 568–579.

[35] B. Cao *et al.*, "When internet of things meets blockchain: Challenges in distributed consensus," *IEEE Netw.*, vol. 33, no. 6, pp. 133–139, 2019.

[36] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, "A scalable multi-layer PBFT consensus for blockchain," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 5, pp. 1146–1160, 2020.

[37] X. Xu, G. Sun, L. Luo, H. Cao, H. Yu, and A. V. Vasilakos, "Latency performance modeling and analysis for hyperledger fabric blockchain network," *Inf. Process. Manage.*, vol. 58, no. 1, p. 102436, 2021.

[38] A. Waqar, A. H. Qureshi, I. Othman, N. Saad, and M. Azab, "Exploration of challenges to deployment of blockchain in small construction projects," *Ain Shams Eng. J.*, vol. 15, no. 2, p. 102362, 2024.

[39] N. K. Tran, M. A. Babar, and A. Walters, "A framework for automating deployment and evaluation of blockchain networks," *J. Netw. Comput. Appl.*, vol. 206, p. 103460, 2022.

[40] H. Luo, H. Yu, and J. Luo, "PRAFT and RPBFT: A class of blockchain consensus algorithm and their applications in electric vehicles charging scenarios for V2G networks," *Internet of Things Cyber-Physical Syst.*, vol. 3, pp. 61–70, 2023.

[41] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1432–1465, 2020.

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

[43] M. Dotan, Y.-A. Pignolet, S. Schmid, S. Tochner, and A. Zohar, "Survey on blockchain networking: Context, state-of-the-art, challenges," *ACM Comput. Surveys*, vol. 54, no. 5, pp. 1–34, 2021.

[44] A. Kalla, C. De Alwis, P. Porambage, G. Gür, and M. Liyanage, "A survey on the use of blockchain for future 6G: Technical aspects, use cases, challenges and research directions," *J. of Ind. Inf. Integr.*, vol. 30, p. 100404, 2022.

[45] K. Shah, S. Chadotra, S. Tanwar, R. Gupta, and N. Kumar, "Blockchain for IoV in 6G environment: Review solutions and challenges," *Clust. Comput.*, vol. 25, no. 3, pp. 1927–1955, 2022.

[46] L. Zhang, H. Xu, O. Onireti, M. A. Imran, and B. Cao, "How much communication resource is needed to run a wireless blockchain network?" *IEEE Netw.*, vol. 36, no. 1, pp. 128–135, 2022.

[47] Y. Wang, Z. Su, J. Ni, N. Zhang, and X. Shen, "Blockchain-empowered space-air-ground integrated networks: Opportunities, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 160–209, 2022.

[48] Y. Zuo, J. Guo, N. Gao, Y. Zhu, S. Jin, and X. Li, "A survey of blockchain and artificial intelligence for 6G wireless communications," *IEEE Commun. Surveys Tuts.*, 2023.

[49] M. H. Tabatabaei, R. Vitenberg, and N. R. Veeraragavan, "Understanding blockchain: Definitions, architecture, design, and system comparison," *Comput. Sci. Rev.*, vol. 50, p. 100575, 2023.

[50] Y. Zou *et al.*, "A survey of fault tolerant consensus in wireless networks," *High-Confidence Comput.*, p. 100202, 2024.

[51] Z. Zhou, O. Onireti, H. Xu, L. Zhang, and M. Imran, "AI and blockchain enabled future wireless networks: A survey and outlook," *Distrib. Ledger Technol.: Res. Pract.*, 2024.

[52] K. M. B. Hasan, M. Sajid, M. A. Lapina, M. Shahid, and K. Kotecha, "Blockchain technology meets 6 G wireless networks: A systematic survey," *Alexandria Eng. J.*, vol. 92, pp. 199–220, 2024.

[53] M. Xu *et al.*, "Exploring blockchain technology through a modular lens: A survey," *ACM Comput. Surveys*, vol. 56, no. 9, pp. 1–39, 2024.

[54] D. Bhumichai, C. Smiliotopoulos, R. Benton, G. Kambourakis, and D. Damopoulos, "The convergence of artificial intelligence and blockchain: The state of play and the road ahead," *Information*, vol. 15, no. 5, p. 268, 2024.

[55] J. Kolb, M. AbdelBaky, R. H. Katz, and D. E. Culler, "Core concepts, challenges, and future directions in blockchain: A centralized tutorial," *ACM Comput. Surveys*, vol. 53, no. 1, pp. 1–39, 2020.

[56] X. Wang, X. Ren, C. Qiu, Z. Xiong, H. Yao, and V. C. Leung, "Integrating edge intelligence and blockchain: What, why, and how," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 4, pp. 2193–2229, 2022.

[57] A. Kalla, "Blockchain perspectives, mining, and types: An introductory tutorial," *IEEE Potentials*, vol. 42, no. 5, pp. 23–32, 2023.

[58] V. Buterin *et al.*, "Ethereum white paper," *GitHub repository*, vol. 1, pp. 22–23, 2013.

[59] H. Luo, S. Liu, S. Xu, and J. Luo, "LECast: A low-energy-consumption broadcast protocol for UAV blockchain networks," *Drones*, vol. 7, no. 2, p. 76, 2023.

[60] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. of Web Grid SServices*, vol. 14, no. 4, pp. 352–375, 2018.

[61] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in IoT: Challenges and solutions," *Blockchain: Res. Appl.*, vol. 2, no. 2, p. 100006, 2021.

[62] R. Agrawal *et al.*, "Continuous security in IoT using blockchain," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*. IEEE, 2018, pp. 6423–6427.

[63] L. Zhang, B. Zhang, and C. Li, "An efficient and reliable byzantine fault tolerant blockchain consensus protocol for single-hop wireless networks," *IEEE Trans. Wireless Commun.*, vol. 23, no. 3, pp. 1974–1987, 2024.

[64] Y. Liu *et al.*, "Building blocks of sharding blockchain systems: Concepts, approaches, and open problems," *Comput. Sci. Rev.*, vol. 46, p. 100513, 2022.

[65] J. Huang *et al.*, "Secure data sharing over vehicular networks based on multi-sharding blockchain," *ACM Trans. Sensor Netw.*, vol. 20, no. 2, pp. 1–23, 2024.

[66] G. Liu *et al.*, "Vision, requirements and network architecture of 6G mobile network beyond 2030," *China Commun.*, vol. 17, no. 9, pp. 92–104, 2020.

[67] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: Opening new horizons for integration of comfort, security, and intelligence," *IEEE Wireless Commun.*, vol. 27, no. 5, pp. 126–132, 2020.

[68] Y. Wang, X. Kang, T. Li, H. Wang, C. Cheng, and Z. Lei, "SIX-trust for 6G: Towards a secure and trustworthy future network," *IEEE Access*, 2023.

[69] S. Velliangiri, R. Manoharan, S. Ramachandran, and V. Rajasekar, "Blockchain based privacy preserving framework for emerging 6G wireless communications," *IEEE Trans. Ind. Informat.*, vol. 18, no. 7, pp. 4868–4874, 2021.

[70] P. Porambage, G. Gür, D. P. M. Osorio, M. Livanage, and M. Ylianttila, "6G security challenges and potential solutions," in *2021 Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*. IEEE, 2021, pp. 622–627.

[71] Y. Liu, S. Peng, M. Zhang, S. Shi, and J. Fu, "Towards secure and efficient integration of blockchain and 6G networks," *Plos One*, vol. 19, no. 4, p. e0302052, 2024.

[72] ITU Recommendation, "Framework and overall objectives of the future development of IMT for 2030 and beyond," *Int. Telecommunication Union (ITU) Recommendation (ITU-R)*, 2023.

[73] R. Singh *et al.*, "Towards 6G evolution: Three enhancements, three innovations, and three major challenges," *arXiv preprint arXiv:2402.10781*, 2024.

[74] Y. Cui, H. Ding, L. Zhao, and J. An, "Integrated sensing and communication: A network level perspective," *IEEE Wireless Commun.*, vol. 31, no. 1, pp. 103–109, 2024.

[75] X. Zhu *et al.*, "Enabling intelligent connectivity: A survey of secure ISAC in 6G networks," *IEEE Commun. Surveys Tuts.*, 2024.

[76] H. Guo, Y.-C. Liang, R. Long, and Q. Zhang, "Cooperative ambient backscatter system: A symbiotic radio paradigm for passive IoT," *IEEE Wireless Commun. Lett.*, vol. 8, no. 4, pp. 1191–1194, 2019.

[77] G. Sun, Z. Wang, H. Su, H. Yu, B. Lei, and M. Guizani, "Profit maximization of independent task offloading in MEC-enabled 5G internet of vehicles," *IEEE Trans. Intell. Transp. Syst.*, 2024.

[78] Z. Ye, G. Sun, and M. Guizani, "ILBPS: An integrated optimization approach based on adaptive load-balancing and heuristic path selection in SDN," *IEEE Internet Things J.*, vol. 11, no. 4, pp. 6144–6157, 2024.

[79] G. Sun, G. Zhu, D. Liao, H. Yu, X. Du, and M. Guizani, "Cost-efficient service function chain orchestration for low-latency applications in NFV networks," *IEEE Syst. J.*, vol. 13, no. 4, pp. 3877–3888, 2018.

[80] T. Maksymyuk *et al.*, "Blockchain-empowered framework for decentralized network management in 6G," *IEEE Commun. Mag.*, vol. 58, no. 9, pp. 86–92, 2020.

[81] X. S. Shen *et al.*, "Blockchain for transparent data management toward 6G," *Engineering*, vol. 8, pp. 74–85, 2022.

[82] S. Zeng, B. Cao, Y. Sun, C. Sun, Z. Wan, and M. Peng, "Blockchain-assisted cross-domain data sharing in industrial IoT," *IEEE Internet Things J.*, vol. 11, no. 16, pp. 26778–26792, 2024.

[83] Z. Guo, G. Wang, Y. Li, J. Ni, and G. Zhang, "Attribute-based data sharing scheme using blockchain for 6G-enabled vanets," *IEEE Trans. Mobile Comput.*, vol. 23, no. 4, pp. 3343–3360, 2023.

[84] D. Luo, Y. Zhang, G. Sun, H. Yu, and D. Niyato, "An efficient consensus algorithm for blockchain-based cross-domain authentication in bandwidth-constrained wide area IoT networks," *IEEE Internet Things J.*, vol. 11, no. 19, pp. 31917–31931, 2024.

[85] D. Luo, Q. Cai, G. Sun, H. Yu, and D. Niyato, "Split-chain based efficient blockchain-assisted cross-domain authentication for IoT," *IEEE Trans. Netw. Service Manag.*, vol. 21, no. 3, pp. 3209–3223, 2024.

[86] Y. Chen, H. Luo, Q. Huang, and J. Luo, "BCACP-IoE: A novel blockchain-based security access control protocol for internet of energy," in *Proc. 6th Int. Conf. Inf. Communication Signal Process. (ICICSP)*. IEEE, 2023, pp. 711–716.

[87] K. Gai, Y. She, L. Zhu, K.-K. R. Choo, and Z. Wan, "A blockchain-based access control scheme for zero trust cross-organizational data sharing," *ACM Trans. Internet Technol.*, vol. 23, no. 3, pp. 1–25, 2023.

[88] X. Ling, Y. Le, J. Wang, Z. Ding, and X. Gao, "Practical modeling and analysis of blockchain radio access network," *IEEE Trans. Commun.*, vol. 69, no. 2, pp. 1021–1037, 2020.

[89] L.-E. Wang, Y. Qi, Y. Bai, Z. Sun, D. Li, and X. Li, "MuKGB-CRS: Guarantee privacy and authenticity of cross-domain recommendation via multi-feature knowledge graph integrated blockchain," *Inf. Sciences*, vol. 638, p. 118915, 2023.

[90] Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, and C.-C. Liu, "Blockchain-based traffic event validation and trust verification for VANETs," *IEEE Access*, vol. 7, pp. 30868–30877, 2019.

[91] W. Li, Z. Su, R. Li, K. Zhang, and Y. Wang, "Blockchain-based data security for artificial intelligence applications in 6G networks," *IEEE Netw.*, vol. 34, no. 6, pp. 31–37, 2020.

[92] J. Wang, S. Wang, Q. Zhang, and Y. Deng, "A two-layer consortium blockchain with transaction privacy protection based on sharding technology," *J. of Inf. Security Appl.*, vol. 74, p. 103452, 2023.

[93] T. Nguyen, N. Tran, L. Loven, J. Partala, M.-T. Kechadi, and S. Pirttikangas, "Privacy-aware blockchain innovation for 6G: Challenges and opportunities," in *Proc. 2nd 6G Wireless Summit (6G SUMMIT)*. IEEE, 2020, pp. 1–5.

[94] M. Fan, Z. Zhang, Z. Li, G. Sun, H. Yu, and M. Guizani, "Blockchain-based decentralized and lightweight anonymous authentication for federated learning," *IEEE Trans. Veh. Technol.*, vol. 72, no. 9, pp. 12075–12086, 2023.

[95] M. Fan *et al.*, "SecureVFL: Privacy-preserving multi-party vertical federated learning based on blockchain and RSS," *Digit. Commun. Netw.*, 2024.

[96] E. Androulaki *et al.*, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. Thirteenth EuroSys Conf.*, 2018, pp. 1–15.

[97] S. K. Dwivedi, R. Amin, and S. Vollala, "Smart contract and IPFS-based trustworthy secure data storage and device authentication scheme in fog computing environment," *Peer-to-Peer Netw. Appl.*, vol. 16, no. 1, pp. 1–21, 2023.

[98] S. Chenthara, K. Ahmed, H. Wang, F. Whittaker, and Z. Chen, "Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology," *Plos One*, vol. 15, no. 12, p. e0243043, 2020.

[99] S. Wuthier, J. Kim, J. Kim, and S.-Y. Chang, "Fake base station detection and blacklisting," in *Proc. 33rd Int. Conf. Comput. Commun. Netw. (ICCCN)*. IEEE, 2024, pp. 1–9.

[100] A. Singla, R. Behnia, S. R. Hussain, A. Yavuz, and E. Bertino, "Look before you leap: Secure connection bootstrapping for 5G networks to defend against fake base-stations," in *Proc. 2021 ACM Asia Conf. Comput. Commun. Security*, 2021, pp. 501–515.

[101] T. Heijligenberg, D. Rupprecht, and K. Kohls, "The attacks aren't alright: Large-scale simulation of fake base station attacks and detections," in *Proc. 17th Cyber Security Experimentation Test Workshop*, 2024, pp. 54–64.

[102] CCTV News Clients, the ministry of industry and information technology announced the situation and typical cases of cracking down on black broadcasting and false base station in january. Mar. 2023. [Online]. Available: https://cbgc.scol.com.cn/news/4035087

[103] 3GPP TR 33.809, "Study on 5G security enhancements against false base stations (FBS)," Mar. 2020.

[104] Z. Wei *et al.*, "Integrated sensing and communication enabled multiple base stations cooperative sensing towards 6G," *IEEE Netw.*, vol. 38, no. 4, pp. 207–215, 2024.

[105] Z. Wang, B. Cao, Y. Sun, C. Liu, Z. Wan, and M. Peng, "Protecting system information from false base station attacks: A blockchain-based approach," *IEEE Trans. Wireless Commun.*, 2024.

[106] 3GPP TS 23.501, "Procedures for the 5G system," Sept. 2023.

[107] 3GPP TS 23.502, "System architecture for the 5G system," Sept. 2023.

[108] 3GPP TR 33.310, "Network domain security (NDS); authentication framework (AF)," Jun. 2022.

[109] 3GPP TS 38.331, "Radio resource control (RRC) protocol specification," Sep. 2020.

[110] X. Lin *et al.*, "5G new radio: Unveiling the essentials of the next generation wireless access technology," *IEEE Commun. Standards Mag.*, vol. 3, no. 3, pp. 30–37, 2019.

[111] C. E. Andrade, L. S. Pessoa, and S. Stawiarski, "The physical cell identity assignment problem: A practical optimization approach," *IEEE Trans. Evol. Comput.*, vol. 28, no. 2, pp. 282–292, 2022.

[112] 3GPP TS 38.133, "Requirements for support of radio resource management," Jan. 2020.

[113] 3GPP TS 38.304, "User equipment (UE) procedures in idle mode and in RRC inactive state," Jul. 2020.

[114] Y. Ma, H. Sun, S. Li, X. Wang, and T. Q. Quek, "Performance analysis of IoT networks with mobile data collectors," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*. IEEE, 2021, pp. 1–7.

[115] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347–4362, 2015.

[116] A. D. Wyner, "The wire-tap channel," *Bell System Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[117] S. Zhang and J.-H. Lee, "Double-spending with a sybil attack in the bitcoin decentralized network," *IEEE Trans. Ind. Informat.*, vol. 15, no. 10, pp. 5715–5722, 2019.

[118] Y. Li *et al.*, "Direct acyclic graph-based ledger for internet of things: Performance and security analysis," *IEEE/ACM Trans. Netw.*, vol. 28, no. 4, pp. 1643–1656, 2020.

[119] M. Zamani, M. Movahedi, and M. Raykova, "Rapidchain: Scaling blockchain via full sharding," in *Proc. 2018 ACM SIGSAC Conf. Comput. Commun. Security*, 2018, pp. 931–948.

[120] Z. Hong, S. Guo, and P. Li, "Scaling blockchain via layered sharding," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 12, pp. 3575–3588, 2022.

[121] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, and M. A. Imran, "Blockchain-enabled wireless internet of things: Performance analysis and optimal communication node deployment," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5791–5802, 2019.

[122] X. Lai, Y. Zhang, and H. Luo, "A low-cost blockchain node deployment algorithm for the internet of things," *Peer-to-Peer Netw. Appl.*, vol. 17, no. 2, pp. 756–766, 2024.

[123] J. Chen and Y. Qin, "Reducing block propagation delay in blockchain networks via guarantee verification," in *Proc. IEEE 29th Int. Conf. Netw. Protocols (ICNP)*. IEEE, 2021, pp. 1–6.

[124] Y. Lai *et al.*, "Accelerating block and transaction propagation: A survey on broadcast protocols in blockchain networks," *Techrxiv preprint techrxiv:172565468.81767780*, 2024.

[125] E. Rohrer and F. Tschorsch, "Kadcast: A structured approach to broadcast in blockchain networks," in *Proc. 1st ACM Conf. Adv. Financial Technol.*, 2019, pp. 199–213.

[126] Y. Li, B. Cao, L. Liang, D. Mao, and L. Zhang, "Block access control in wireless blockchain network: Design, modeling and analysis," *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 9258–9272, 2021.

[127] H. Yang, Y. Yu, Y. Zhu, X. Tao, and J. Yu, "Towards trustworthy 6G networks: A trust-based consensus scheme," *IEEE Netw.*, 2024.

[128] X. Chen, K. Nguyen, and H. Sekiya, "On the latency performance in private blockchain networks," *IEEE Internet Things J.*, vol. 9, no. 19, pp. 19246–19259, 2022.

[129] A. I. Sanka and R. C. Cheung, "A systematic review of blockchain scalability: Issues, solutions, analysis and future research," *J. Netw. Comput. Appl.*, vol. 195, p. 103232, 2021.

[130] F. Tang, T. Xu, J. Peng, and N. Gan, "TP-PBFT: A scalable PBFT based on threshold proxy signature for IoT-blockchain applications," *IEEE Internet Things J.*, vol. 11, no. 9, pp. 15434–15449, 2024.

[131] H. Xu, P. V. Klaine, O. Onireti, and C.-L. I, "6 G resource management and sharing: Blockchain and O-RAN," *Blockchains: Empowering Technol. Ind. Appl.*, pp. 253–285, 2023.

[132] H. Luo, X. Yang, H. Yu, G. Sun, S. Xu, and L. Luo, "Performance analysis of non-ideal wireless PBFT networks with mmWave and terahertz signals," in *Proc. IEEE Int. Conf. Metaverse Comput., Netw. Appl. (MetaCom)*. IEEE, 2023, pp. 104–108.

[133] H. Luo, X. Yang, H. Yu, G. Sun, B. Lei, and M. Guizani, "Performance analysis and comparison of non-ideal wireless PBFT and RAFT consensus networks in 6G communications," *IEEE Internet Things J.*, vol. 11, no. 6, pp. 9752–9765, 2024.

[134] Q. Xue *et al.*, "A survey of beam management for mmWave and THz communications towards 6G," *IEEE Commun. Surveys Tuts.*, 2024.

[135] D. Moltchanov, E. Sopin, V. Begishev, A. Samuylov, Y. Koucheryavy, and K. Samouylov, "A tutorial on mathematical modeling of 5G/6G millimeter wave and terahertz cellular systems," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 1072–1116, 2022.

[136] N. A. Abbasi, A. Hariharan, A. M. Nair, and A. F. Molisch, "Channel measurements and path loss modeling for indoor THz communication," in *Proc. 14th Eur. Conf. Antennas Propagat. (EuCAP)*. IEEE, 2020, pp. 1–5.

[137] Y. Guan, J. Zhang, L. Tian, P. Tang, and T. Jiang, "A comparative study for indoor factory environments at 4.9 and 28 GHz," in *Proc. 14th Eur. Conf. Antennas Propagat. (EuCAP)*. IEEE, 2020, pp. 1–5.

[138] B. Chang, L. Zhang, L. Li, G. Zhao, and Z. Chen, "Optimizing resource allocation in URLLC for real-time wireless control systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 8916–8927, 2019.

[139] D. Yu, W. Li, H. Xu, and L. Zhang, "Low reliable and low latency communications for mission critical distributed industrial internet of things," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 313–317, 2020.

[140] C. Cachin and M. Vukolić, "Blockchain consensus protocols in the wild," *arXiv preprint arXiv:1707.01873*, 2017.

[141] S. Li, Z. Liu, Q. Li, X. Du, J. Chen, and K. Xu, "Stable byzantine fault tolerance in wide area networks with unreliable links," *IEEE/ACM Trans. Netw.*, 2024.

[142] T. Jiang *et al.*, "Blockchain for energy market: A comprehensive survey," *Sustain. Energy, Grids Netw.*, vol. 41, p. 101614, 2025.

[143] B. Cao *et al.*, "Performance analysis and comparison of PoW, PoS and DAG based blockchains," *Digit. Commun. Netw.*, vol. 6, no. 4, pp. 480–485, 2020.

[144] P. Vasin, "Blackcoin's proof-of-stake protocol v2," *URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf*, vol. 71, p. 25, 2014.

[145] F. Saleh, "Blockchain without waste: Proof-of-stake," *Rev. of Financial Stud.*, vol. 34, no. 3, pp. 1156–1190, 2021.

[146] E. Deirmentzoglou, G. Papakyriakopoulos, and C. Patsakis, "A survey on long-range attacks for proof of stake protocols," *IEEE Access*, vol. 7, pp. 28712–28725, 2019.

[147] S. Chen *et al.*, "A blockchain consensus mechanism that uses proof of solution to optimize energy dispatch and trading," *Nature Energy*, vol. 7, no. 6, pp. 495–502, 2022.

[148] Y. Li, L. Qiao, and Z. Lv, "An optimized byzantine fault tolerance algorithm for consortium blockchain," *Peer-to-Peer Netw. Appl.*, vol. 14, pp. 2826–2839, 2021.

[149] G. Sun, M. Dai, J. Sun, and H. Yu, "Voting-based decentralized consensus design for improving the efficiency and security of consortium blockchain," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6257–6272, 2020.

[150] M. Yin, D. Malkhi, M. K. Reiter, G. G. Gueta, and I. Abraham, "HotStuff: BFT consensus with linearity and responsiveness," in *Proc. 2019 ACM Symp. Princ. of Distrib. Comput.*, 2019, pp. 347–356.

[151] X. Fu, H. Wang, and P. Shi, "votes-as-a-proof (VaaP): Permissioned blockchain consensus protocol made simple," *IEEE Trans. Parallel Distrib. Syst.*, vol. 33, no. 12, pp. 4964–4973, 2022.

[152] B. Cao, X. Wang, W. Zhang, H. Song, and Z. Lv, "A many-objective optimization model of industrial internet of things based on private blockchain," *IEEE Netw.*, vol. 34, no. 5, pp. 78–83, 2020.

[153] L. Lamport, "Paxos made simple," *ACM SIGACT News (Distrib. Comput. Column)*, vol. 32, no. 4, pp. 51–58, 2001.

[154] D. Huang, X. Ma, and S. Zhang, "Performance analysis of the raft consensus algorithm for private blockchains," *IEEE Trans. Syst., Man, Cybern.: Syst.*, vol. 50, no. 1, pp. 172–181, 2019.

[155] W. Wang, J. Chen, Y. Jiao, J. Kang, W. Dai, and Y. Xu, "Connectivity-aware contract for incentivizing IoT devices in complex wireless blockchain," *IEEE Internet Things J.*, vol. 10, no. 12, pp. 10413–10425, 2023.

[156] Z. Zhou, O. Onireti, L. Zhang, and M. A. Imran, "Performance analysis of wireless practical byzantine fault tolerance networks using IEEE 802.11," in *Proc. IEEE Globecom Workshops (GC WKSHPS)*. IEEE, 2021, pp. 1–6.

[157] Z. Zhou, O. Onireti, X. Lin, L. Zhang, and M. A. Imran, "On the performance of wireless PBFT-based blockchain network with IEEE 802.11," *IEEE Syst. J.*, 2024.

[158] B. P. Crow, I. Widjaja, J. G. Kim, and P. T. Sakai, "IEEE 802.11 wireless local area networks," *IEEE Commun. Mag.*, vol. 35, no. 9, pp. 116–126, 1997.

[159] F. Daneshgaran, M. Laddomada, F. Mesiti, and M. Mondin, "Unsaturated throughput analysis of IEEE 802.11 in presence of non ideal transmission channel and capture effects," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1276–1286, 2008.

[160] G. Wang, Y. Shu, L. Zhang, and O. W. Yang, "Delay analysis of the IEEE 802.11 DCF," in *Proc. IEEE 14th Proc. Pers., Indoor Mobile Radio Commun.*, vol. 2. IEEE, 2003, pp. 1737–1741.

[161] G. G. Gueta *et al.*, "SBFT: A scalable and decentralized trust infrastructure," in *Proc. 49th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*. IEEE, 2019, pp. 568–580.

[162] Q. Liu, Y. Xu, B. Cao, L. Zhang, and M. Peng, "Unintentional forking analysis in wireless blockchain networks," *Digit. Commun. Netw.*, vol. 7, no. 3, pp. 335–341, 2021.

[163] Y. Li, Y. Fan, L. Zhang, and J. Crowcroft, "RAFT consensus reliability in wireless networks: Probabilistic analysis," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 12839–12853, 2023.

[164] D. Yu and L. Zhang, "Centralized and distributed consensus in wireless network: An analytical comparison," in *Proc. IEEE 20th Int. Conf. Embedded Ubiquitous Comput. (EUC)*. IEEE, 2022, pp. 81–89.

[165] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu, "A survey on the scalability of blockchain systems," *IEEE Netw.*, vol. 33, no. 5, pp. 166–173, 2019.

[166] F. Gai, J. Niu, M. M. Jalalzai, S. A. Tabatabaee, and C. Feng, "A secure Sidechain for Decentralized trading in internet of things," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 4029–4046, 2024.

[167] L. Li, J. Wu, and W. Cui, "A review of blockchain cross-chain technology," *IET Blockchain*, vol. 3, no. 3, pp. 149–158, 2023.

[168] W. Liu, B. Cao, M. Peng, and B. Li, "Distributed and parallel blockchain: Towards a multi-chain system with enhanced security," *IEEE Trans. Dependable Secure Comput.*, 2024.

[169] J. Khamis, A. Kotzer, and O. Rottenstreich, "Topologies for blockchain payment channel networks: Models and constructions," *IEEE/ACM Trans. Netw.*, 2024.

[170] Q. Cai, J. Chen, D. Luo, G. Sun, H. Yu, and M. Guizani, "Deter-pay: A deterministic routing protocol in concurrent payment channel network," *IEEE Internet Things J.*, 2024.

[171] J. Ni, J. Xiao, S. Zhang, B. Li, B. Li, and H. Jin, "Fluid: Towards efficient continuous transaction processing in DAG-based blockchains," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 12, pp. 12679–12692, 2023.

[172] W. Yang, L. Shi, H. Liang, and W. Zhang, "Trusted mobile edge computing: DAG blockchain-aided trust management and resource allocation," *IEEE Trans. Wireless Commun.*, vol. 23, no. 5, pp. 5006–5018, 2024.

[173] R. Adhikari, C. Busch, and D. R. Kowalski, "Stable blockchain sharding under adversarial transaction generation," in *Proc. 36th ACM Symp. Parallelism Algorithms Archit.*, 2024, pp. 451–461.

[174] H. Dang, T. T. A. Dinh, D. Loghin, E.-C. Chang, Q. Lin, and B. C. Ooi, "Towards scaling blockchain systems via sharding," in *Proc. 2019 Int. Conf. Manage. of Data*, 2019, pp. 123–140.

[175] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proc. 2016 ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 17–30.

[176] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: A secure, scale-out, decentralized ledger via sharding," in *Proc. IEEE Symp. Security Privacy (SP)*. IEEE, 2018, pp. 583–598.

[177] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 2016.

[178] X. Li, H. Luo, and J. Duan, "Security analysis of sharding in blockchain with PBFT consensus," in *Proc. Proc. 4th Int. Conf. Blockchain Technol.*, 2022, pp. 9–14.

[179] D. Yu, H. Xu, L. Zhang, B. Cao, and M. A. Imran, "Security analysis of sharding in the blockchain system," in *Proc. IEEE 32nd Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*. IEEE, 2021, pp. 1030–1035.

[180] Z. Hong, S. Guo, P. Li, and W. Chen, "Pyramid: A layered sharding blockchain system," in *IEEE INFOCOM 2021-IEEE Conf. Comput. Commun.*. IEEE, 2021, pp. 1–10.

[181] Y. Liu *et al.*, "SS-DID: A secure and scalable Web3 decentralized identity utilizing multi-layer sharding blockchain," *IEEE Internet Things J.*, vol. 11, no. 15, pp. 25694—5705, 2024.

[182] M. Li, X. Luo, K. Xue, Y. Xue, W. Sun, and J. Li, "A secure and efficient blockchain Sharding scheme via hybrid consensus and dynamic management," *IEEE Trans. Inf. Forensics Security*, 2024.

[183] M. Li, Y. Lin, J. Zhang, and W. Wang, "CoChain: High concurrency blockchain sharding via consensus on consensus," in *IEEE INFOCOM 2023-IEEE Conf. Comput. Commun.*. IEEE, 2023, pp. 1–10.

[184] P. Zhang, W. Guo, Z. Liu, M. Zhou, B. Huang, and K. Sedraoui, "Optimized blockchain sharding model based on node trust and allocation," *IEEE Trans. Netw. Service Manag.*, vol. 20, no. 3, pp. 2804–2816, 2023.

[185] M. Zhai *et al.*, "Accountable secret committee election and anonymous Sharding blockchain consensus," *IEEE Trans. Inf. Forensics Security*, 2024.

[186] Y. Lin *et al.*, "DRL-based adaptive sharding for blockchain-based federated learning," *IEEE Trans. Commun.*, vol. 71, no. 10, pp. 5992–6004, 2023.

[187] R. Chen, H. Luo, G. Sun, H. Yu, D. Niyato, and S. Dustdar, "DRDST: Low-latency DAG consensus through robust dynamic Sharding and tree-broadcasting for IoV," *arXiv preprint arXiv:2412.04742*, 2024.

[188] J. Chen and H. Luo, "SusChain: A sustainable sharding scheme for UAV blockchain networks," *Peer-to-Peer Netw. Appl.*, vol. 17, no. 10, pp. 3603–3617, 2024.

[189] H. Luo, G. Sun, H. Yu, B. Lei, and M. Guizani, "An energy-efficient wireless blockchain Sharding scheme for PBFT consensus," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 3, pp. 3015–3027, 2024.

[190] C. Yang, K.-W. Chin, J. Wang, X. Wang, Y. Liu, and Z. Zheng, "Scaling blockchains with error correction codes: A survey on coded blockchains," *ACM Comput. Surveys*, vol. 56, no. 6, pp. 1–33, 2024.

[191] D. Strepparava, L. Nespoli, E. Kapassa, M. Touloupou, L. Katelaris, and V. Medici, "Deployment and analysis of a blockchain-based local energy market," *Energy Reports*, vol. 8, pp. 99–113, 2022.

[192] L. Ismail, H. Hameed, M. AlShamsi, M. AlHammadi, and N. AlDhanhani, "Towards a blockchain deployment at UAE university: Performance evaluation and blockchain taxonomy," in *Proc. 2019 Int. Conf. Blockchain Technol.*, 2019, pp. 30–38.

[193] O. Onireti, L. Zhang, and M. A. Imran, "On the viable area of wireless practical byzantine fault tolerance (PBFT) blockchain networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*. IEEE, 2019, pp. 1–6.

[194] H. Xu, L. Zhang, Y. Liu, and B. Cao, "RAFT based wireless blockchain networks in the presence of malicious jamming," *IEEE wireless Commun. Lett.*, vol. 9, no. 6, pp. 817–821, 2020.

[195] Z. Li, L. Zhang, X. Zhang, and M. Imran, "Design and implementation of a raft based wireless consensus system for autonomous driving," in *GLOBECOM 2022-Proc. IEEE Global Commun. Conf.*. IEEE, 2022, pp. 3736–3741.

[196] H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, "IoT information sharing security mechanism based on blockchain technology," *Future Gener. Comput. Syst.*, vol. 101, pp. 1028–1040, 2019.

[197] I. Kaklamanis, L. Yang, and M. Alizadeh, "Poster: Coded broadcast for scalable leader-based BFT consensus," in *Proc. 2022 ACM SIGSAC Conf. Comput. Commun. Security*, 2022, pp. 3375–3377.

[198] A. Demers *et al.*, "Epidemic algorithms for replicated database maintenance," in *Proc. sixth Annu. ACM Symp. Princ. of Distrib. Comput.*, 1987, pp. 1–12.

[199] G. Naumenko, G. Maxwell, P. Wuille, A. Fedorova, and I. Beschastnikh, "Erlay: Efficient transaction relay for bitcoin," in *Proc. 2019 ACM SIGSAC Conf. Comput. Commun. Security*, 2019, pp. 817–831.

[200] G. Saldamli, C. Upadhyay, D. Jadhav, R. Shrishrimal, B. Patil, and L. Tawalbeh, "Improved gossip protocol for blockchain applications," *Clust. Comput.*, vol. 25, no. 3, pp. 1915–1926, 2022.

[201] E. Rohrer and F. Tschorsch, "Kadcast-ng: A structured broadcast protocol for blockchain networks," *IEEE/ACM Trans. Netw.*, vol. 31, no. 6, pp. 3269–3283, 2023.

[202] P. Maymounkov and D. Mazieres, "Kademlia: A peer-to-peer information system based on the xor metric," in *Int. workshop peer-to-peer Syst.*. Springer, 2002, pp. 53–65.

[203] Y. Zhu, C. Hua, D. Zhong, and W. Xu, "Design of low-latency overlay protocol for blockchain delivery networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*. IEEE, 2022, pp. 1182–1187.

[204] X. Wang, X. Jiang, Y. Liu, J. Wang, and Y. Sun, "Data propagation for low latency blockchain systems," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 12, pp. 3631–3644, 2022.

[205] C. Zhao, T. Wang, S. Zhang, and S. C. Liew, "HCB: Enabling compact block in Ethereum network with secondary pool and transaction prediction," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 1, pp. 1077–1092, 2024.

[206] C. Zhao, S. Zhang, T. Wang, and S. C. Liew, "Bodyless block propagation: Tps fully scalable blockchain with pre-validation," *Future Gener. Comput. Syst.*, p. 107516, 2024.

[207] M. Zhou *et al.*, "Mercury: Fast transaction broadcast in high performance blockchain systems," in *IEEE INFOCOM 2023-IEEE Conf. Comput. Commun.*. IEEE, 2023, pp. 1–10.

[208] X. Feng, J. Ma, Y. Miao, X. Liu, and K.-K. R. Choo, "Social characteristic-based propagation-efficient PBFT protocol to broadcast in unstructured overlay networks," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 6, pp. 3621–3639, 2021.

[209] Y. Li, L. Liang, Y. Jia, and W. Wen, "PRESYNC: An efficient transaction Synchronization protocol to accelerate block propagation," *IEEE Trans. Netw. Service Manag.*, 2024.

[210] R. Zheng, H. Luo, G. Sun, and H. Yu, "DHBN: An efficient broadcast protocol for blockchain networks in highly dynamic heterogeneous environment," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*. IEEE, 2024, pp. 1–6.

[211] W. Peng, X. Li, J. Niu, X. Zhang, and Y. Zhang, "Ensuring state continuity for confidential computing: A blockchain-based approach," *IEEE Trans. Dependable Secure Comput.*, 2024.

[212] M. Xu, Y. Zou, and X. Cheng, *Wireless Consensus: Theory and Applications*. Springer Nature, 2024.

[213] B. Cao, L. Zhang, M. Peng, and M. A. Imran, *Wireless Blockchain: Principles, Technologies and Applications*. John Wiley & Sons, 2021.

[214] G. Lee, J. Park, W. Saad, and M. Bennis, "Performance analysis of blockchain systems with wireless mobile miners," *IEEE Netw.ing Lett.*, vol. 2, no. 3, pp. 111–115, 2020.

[215] Y. Zou, M. Xu, J. Yu, F. Zhao, and X. Cheng, "A fast consensus for permissioned wireless blockchains," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 12102–12111, 2021.

[216] M. Xu, C. Liu, Y. Zou, F. Zhao, J. Yu, and X. Cheng, "wChain: A fast fault-tolerant blockchain protocol for multihop wireless networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 10, pp. 6915–6926, 2021.

[217] L. Yang, Y. Zou, M. Xu, Y. Xu, D. Yu, and X. Cheng, "Distributed consensus for blockchains in internet-of-things networks," *Tsinghua Sci. Technol.*, vol. 27, no. 5, pp. 817–831, 2022.

[218] J. Cao, S. Leng, L. Zhang, M. Imran, and H. Chai, "A V2V empowered consensus framework for cooperative autonomous driving," in *GLOBECOM 2022-Proc. IEEE Global Commun. Conf.*. IEEE, 2022, pp. 5729–5734.

[219] Y. Zou, M. Xu, J. Yu, F. Zhao, and X. Cheng, "Fault-tolerant consensus with NOMA in mobile networks," *IEEE Wireless Commun.*, vol. 29, no. 3, pp. 80–86, 2022.

[220] W. Wang, Y. Jiao, J. Chen, W. Dai, J. Kang, and Y. Xu, "Dual auction mechanism for transaction forwarding and validation in complex wireless blockchain network," *arXiv preprint arXiv:2309.01920*, 2023.

[221] M. Xu, F. Zhao, Y. Zou, C. Liu, X. Cheng, and F. Dressler, "BLOWN: A blockchain protocol for single-hop wireless networks under adversarial SINR," *IEEE Trans. Mobile Comput.*, vol. 22, no. 8, pp. 4530–4547, 2022.

[222] D. Yu, Y. Sun, Y. Li, L. Zhang, and M. A. Imran, "Communication resource allocation of raft in wireless network," *IEEE Sensors J.*, vol. 23, no. 17, pp. 19398–19408, 2023.

[223] H. M. Buttar, W. Aman, M. M. U. Rahman, and Q. H. Abbasi, "Countering active attacks on RAFT-based IoT blockchain networks," *IEEE Sensors J.*, vol. 23, no. 13, pp. 14691–14699, 2023.

[224] G. Jing, Y. Zou, D. Yu, C. Luo, and X. Cheng, "Efficient fault-tolerant consensus for collaborative services in edge computing," *IEEE Trans. Comput.*, vol. 72, no. 8, pp. 2139–2150, 2023.

[225] Y. Zou, Z. Jin, Y. Zheng, D. Yu, and T. Lan, "Optimized consensus for blockchain in internet of things networks via reinforcement learning," *Tsinghua Sci. Technol.*, vol. 28, no. 6, pp. 1009–1022, 2023.

[226] C. Feng, Z. Xu, X. Zhu, P. V. Klaine, and L. Zhang, "Wireless distributed consensus in vehicle to vehicle networks for autonomous driving," *IEEE Trans. Veh. Technol.*, vol. 72, no. 6, pp. 8061–8073, 2023.

[227] H. Luo, Q. Zhang, H. Yu, G. Sun, and S. Xu, "Symbiotic PBFT consensus: Cognitive backscatter communications-enabled wireless PBFT consensus," in *GLOBECOM 2023-Proc. IEEE Global Commun. Conf.*. IEEE, 2023, pp. 910–915.

[228] J. Zhang, W. Chen, Z. Hong, G. Xiao, L. Du, and Z. Zheng, "Efficient execution of arbitrarily complex cross-shard contracts for blockchain Sharding," *IEEE Trans. Comput.*, vol. 73, no. 5, pp. 1190–1205, 2024.

[229] D. Yu, H. Wu, Y. Sun, L. Zhang, and M. Imran, "Adaptive protocol of raft in wireless network," *Ad Hoc Netw.*, vol. 154, p. 103377, 2024.

[230] X. Xie, C. Hua, J. Hong, P. Gu, and W. Xu, "AirCon: Over-the-air consensus for wireless blockchain networks," *IEEE Trans. Mobile Comput.*, vol. 23, no. 5, pp. 4566–4582, 2024.

[231] G. Jing, Y. Zou, Z. Zhang, D. Yu, F. Dressler, and X. Cheng, "Byzantine fault tolerant consensus in open wireless networks via an abstract MAC layer," *IEEE Trans. Commun.*, 2024.

[232] H. Luo, Y. Wu, G. Sun, H. Yu, and M. Guizani, "ESCM: An efficient and secure communication mechanism for UAV networks," *IEEE Trans. Netw. Service Manag.*, vol. 21, no. 3, pp. 3124–3139, 2024.

[233] Z. Wang *et al.*, "Robust Permissioned blockchain consensus for unstable communication in FANET," *IEEE/ACM Trans. Netw.*, vol. 32, no. 1, pp. 699–712, 2024.

[234] L. Zhang, Z. Yao, B. Zhang, and C. Li, "Scalable creditable-committee-based blockchain consensus protocol for multi-hop wireless networks," *IEEE Internet Things J.*, vol. 11, no. 18, pp. 29628–29642, 2024.

[235] B. Li, G. Cheng, H. Gao, X. Yan, and S. Deng, "Scenarios analysis and performance assessment of blockchain integrated in 6G scenarios," *Sci. China Inf. Sciences*, vol. 67, no. 7, p. 170301, 2024.

[236] H. Luo, Q. Zhang, G. Sun, H. Yu, and D. Niyato, "Symbiotic blockchain consensus: Cognitive backscatter communications-enabled wireless blockchain consensus," *IEEE/ACM Trans. Netw.*, 2024.

[237] Z. Zhou, O. Onireti, L. Zhang, and M. A. Imran, "Implementing practical byzantine fault tolerance over cellular networks," *IEEE Open J. of Commun. Soc.*, 2024.

[238] Y. Zou *et al.*, "Jamming-resilient consensus for wireless blockchain networks," *Tsinghua Sci. Technol.*, vol. 30, no. 1, pp. 262–278, 2025.

[239] I. D. Chakeres and E. M. Belding-Royer, "AODV routing protocol implementation design," in *24th Int. Conf. Distrib. Comput. Syst. Workshops, 2004. Proc.* IEEE, 2004, pp. 698–703.

[240] Q. Zhang, Y.-C. Liang, H.-C. Yang, and H. V. Poor, "Mutualistic mechanism in symbiotic radios: When can the primary and secondary transmissions be mutually beneficial?" *IEEE Trans. Wireless Commun.*, vol. 21, no. 10, pp. 8036–8050, 2022.

[241] T. Tao, Y. Wang, D. Li, Y. Wan, P. Baracca, and A. Wang, "6G hyper reliable and low-latency communication–requirement analysis and proof of concept," in *Proc. IEEE 98th Veh. Technol. Conf. (VTC2023-Fall)*. IEEE, 2023, pp. 1–5.

[242] A. A. Shamsabadi, A. Yadav, Y. Gadallah, and H. Yanikomeroglu, "Exploring the 6G potentials: Immersive, hyper reliable, and low-latency communication," *arXiv preprint arXiv:2407.11051*, 2024.

[243] H. Huang, W. Miao, G. Min, J. Tian, and A. Alamri, "NFV and blockchain enabled 5G for ultra-reliable and low-latency communications in industry: Architecture and performance evaluation," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5595–5604, 2020.

[244] A. Vladyko, V. Elagin, A. Spirkina, A. Muthanna, and A. A. Ateya, "Distributed edge computing with blockchain technology to enable ultra-reliable low-latency V2X communications," *Electronics*, vol. 11, no. 2, p. 173, 2022.

[245] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Low-latency federated learning and blockchain for edge association in digital twin empowered 6G networks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 7, pp. 5098–5107, 2020.

[246] C. Chaccour and W. Saad, "Edge intelligence in 6G systems," in *6G Mobile Wireless Networks*. Springer, 2021, pp. 233–249.

[247] S. M. Alrubei, E. A. Ball, J. M. Rigelsford, and C. A. Willis, "Latency and performance analyses of real-world wireless IoT-blockchain application," *IEEE Sensors J.*, vol. 20, no. 13, pp. 7372–7383, 2020.

[248] M. Alaslani, F. Nawab, and B. Shihada, "Blockchain in IoT systems: End-to-end delay evaluation," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8332–8344, 2019.

[249] L. Zhang, *How automated decision-making can increase the safety of connected and autonomous vehicles*, University of Glasgow, 2022.

[250] M. Yadav *et al.*, "Exploring synergy of blockchain and 6G network for industrial automation," *IEEE Access*, vol. 11, pp. 137163–137187, 2023.

[251] I. Ahmed, A. Chehri, and G. Jeon, "Artificial intelligence and blockchain enabled smart healthcare system for monitoring and detection of COVID-19 in biomedical images," *IEEE/ACM Trans. Comput. Biol. Bioinf.*, 2023.

[252] B. Paden, M. Čáp, S. Z. Yong, D. Yershov, and E. Frazzoli, "A survey of motion planning and control techniques for self-driving urban vehicles," *IEEE Trans. Intell. Vehicles*, vol. 1, no. 1, pp. 33–55, 2016.

[253] J. Kang *et al.*, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, 2018.

[254] H. Xu, Y. Fan, W. Li, and L. Zhang, "Wireless distributed consensus for connected autonomous systems," *IEEE Internet Things J.*, vol. 10, no. 9, pp. 7786–7799, 2022.

[255] L. Hou, X. Xu, K. Zheng, and X. Wang, "An intelligent transaction migration scheme for RAFT-based private blockchain in internet of things applications," *IEEE Commun. Lett.*, vol. 25, no. 8, pp. 2753–2757, 2021.

[256] X. You *et al.*, "Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts," *Sci. China Inf. Sciences*, vol. 64, pp. 1–74, 2021.

[257] F. Guo, F. R. Yu, H. Zhang, X. Li, H. Ji, and V. C. Leung, "Enabling massive IoT toward 6G: A comprehensive survey," *IEEE Internet Things J.*, vol. 8, no. 15, pp. 11891–11915, 2021.

[258] H. Xu, P. V. Klaine, O. Onireti, B. Cao, M. Imran, and L. Zhang, "Blockchain-enabled resource management and sharing for 6G communications," *Digit. Commun. Netw.*, vol. 6, no. 3, pp. 261–269, 2020.

[259] Z. Sun, F. Qi, L. Liu, Y. Xing, and W. Xie, "Energy-efficient spectrum sharing for 6G ubiquitous IoT networks through blockchain," *IEEE Internet Things J.*, vol. 10, no. 11, pp. 9342–9352, 2022.

[260] Q. Wu, W. Wang, Z. Li, B. Zhou, Y. Huang, and X. Wang, "SpectrumChain: A disruptive dynamic spectrum-sharing framework for 6G," *Sci. China Inf. Sciences*, vol. 66, no. 3, p. 130302, 2023.

[261] H. Zhang, S. Leng, H. Yin, and S. Yu, "Intelligent consensus enhanced spectrum sharing in heterogeneous wireless networks," *IEEE Internet Things J.*, vol. 11, no. 19, pp. 30939–30952, 2024.

[262] W. Wang and Y. Zhao, "Blockchain-based spectrum management architecture and trading mechanism design for space-air-ground integrated network," *IEEE Commun. Lett.*, 2023.

[263] Y.-C. Liang, Q. Zhang, E. G. Larsson, and G. Y. Li, "Symbiotic radio: Cognitive backscattering communications for future wireless networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 6, no. 4, pp. 1242–1255, 2020.

[264] R. Long, Y.-C. Liang, H. Guo, G. Yang, and R. Zhang, "Symbiotic radio: A new communication paradigm for passive internet of things," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 1350–1363, 2019.

[265] R. Cheng, Y. Sun, L. Mohjazi, Y.-C. Liang, and M. Imran, "Blockchain-assisted intelligent symbiotic radio in space-air-ground integrated networks," *IEEE Netw.*, vol. 37, no. 2, pp. 94–101, 2023.

[266] R. Cheng, Y. Sun, Y. Liu, Y.-C. Liang, and M. Imran, "BIO-SD: A blockchain-empowered intelligent resource management for symbiotic devices," *IEEE Trans. Veh. Technol.*, vol. 73, no. 5, pp. 6517–6529, 2023.

[267] H. Luo, G. Sun, C. Chi, H. Yu, and M. Guizani, "Convergence of symbiotic communications and blockchain for sustainable and trustworthy 6g wireless networks," *IEEE Wireless Commun.*, vol. 32, no. 2, pp. 18–25, 2025.

[268] F. Tang, H. Hofner, N. Kato, K. Kaneko, Y. Yamashita, and M. Hangai, "A deep reinforcement learning-based dynamic traffic offloading in space-air-ground integrated networks (SAGIN)," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 1, pp. 276–289, 2021.

[269] X. Wang, M. Bennis, P. Wang, R. Yu, and W. Y. B. Lim, "Green technologies for the sustainable Metaverse and web 3.0," *IEEE Wireless Commun.*, vol. 30, no. 5, pp. 74–75, 2023.

[270] W. Liu, B. Cao, and M. Peng, "Web3 technologies: Challenges and opportunities," *IEEE Netw.*, vol. 38, no. 3, pp. 187–193, 2024.

[271] P. Xia *et al.*, "A reputation-aided lightweight consensus service framework for multi-chain Metaverse," *IEEE Netw.*, 2024.

[272] Y. Cheng, Y. Guo, M. Xu, Q. Hu, D. Yu, and X. Cheng, "An adaptive and modular blockchain enabled architecture for a decentralized Metaverse," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 4, pp. 893–904, 2024.

[273] Y. Jiang, J. Kang, X. Ge, D. Niyato, and Z. Xiong, "QoE analysis and resource allocation for wireless Metaverse services," *IEEE Trans. Commun.*, vol. 71, no. 8, pp. 4735–4750, 2023.

[274] Y. Lin *et al.*, "A unified blockchain-semantic framework for wireless edge intelligence enabled web 3.0," *IEEE Wireless Commun.*, vol. 31, no. 2, pp. 126–133, 2024.

[275] China Academy of Information and Communications Technology, "Web 3.0 technology and industry ecological development report," Dec. 2022. [Online]. Available: http://www.caict.ac.cn/kxyj/qwfb/bps/202212/P020230105569849787721.pdf

[276] H. Lee *et al.*, "Towards 6G hyper-connectivity: Vision, challenges, and key enabling technologies," *J. Commun. Netw.*, vol. 25, no. 3, pp. 344–354, 2023.

[277] G. Sun, Y. Wang, H. Yu, and M. Guizani, "Proportional fairness-aware task scheduling in space-air-ground integrated networks," *IEEE Trans. Services Comput.*, 2024.

[278] L. Luo, C. Zhang, H. Yu, Z. Li, G. Sun, and S. Luo, "Energy-efficient hierarchical collaborative learning over LEO satellite constellations," *IEEE J. Sel. Areas Commun.*, 2024.

[279] A. S. Khan *et al.*, "Blockchain-based lightweight multifactor authentication for cell-free in ultra-dense 6G-based (6-CMAS) cellular network," *IEEE Access*, vol. 11, pp. 20524–20541, 2023.

[280] M. Rasti, S. K. Taskou, H. Tabassum, and E. Hossain, "Evolution toward 6G multi-band wireless networks: A resource management perspective," *IEEE Wireless Commun.*, vol. 29, no. 4, pp. 118–125, 2022.

[281] S. Khan *et al.*, "A survey on X. 509 public-key infrastructure, certificate revocation, and their modern implementation on blockchain and ledger technologies," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 4, pp. 2529–2568, 2023.

[282] A. Panigrahi, A. K. Nayak, and R. Paul, "A blockchain based PKI system for peer to peer network," in *Adv. Distrib. Comput. Mach. Learn.: Proc. of ICADCML 2021*. Springer, 2022, pp. 81–88.

[283] D. Luo, G. Sun, H. Yu, and M. Guizani, "Blockchain-based cross-domain authentication with dynamic domain participation in IoT," *IEEE Internet Things J.*, 2024.

[284] E. Kiltz and G. Neven, "Identity-based signatures," in *Identity-based cryptography*. IOS Press, 2009, pp. 31–44.

[285] J. He, K. Yang, K. Guild, and H.-H. Chen, "On bandwidth request mechanism with piggyback in fixed IEEE 802.16 networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 5238–5243, 2008.

[286] X. Hao, L. Yu, L. Zhiqiang, L. Zhen, and G. Dawu, "Dynamic practical byzantine fault tolerance," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*. IEEE, 2018, pp. 1–8.

[287] A. Song, J. Wang, W. Yu, Y. Dai, and H. Zhu, "Fast, dynamic and robust byzantine fault tolerance protocol for consortium blockchain," in *Proc. IEEE Int. Conf. Parallel Distrib. Process. Appl., Big Data Cloud Comput., Sustain. Comput. Commun., Social Comput. Netw. (ISPA/BDCloud/SocialCom/SustainCom)*. IEEE, 2019, pp. 419–426.

[288] "The blockchain interconnection infrastructure for telecom operators led by china mobile research institute is officially launched," Dec. 2023. [Online]. Available: https://finance.sina.com.cn/tech/roll/2023-12-05/doc-imzwxuyt6530565.shtml

[289] "PCCW global collaborates with syntropy to deliver network on demand through Web3 open bandwidth exchange," Sep. 2022. [Online]. Available: https://www.pccwglobal.com/company/news-and-events/news/pccw-global-collaborates-with-syntropy-to-deliver-network-on-demand-through-web3-open-bandwidth-exchange/

[290] "ATT announces suite of blockchain solutions," Sep. 2018. [Online]. Available: https://about.att.com/story/2018/att$_b lockchain.html$

[291] A. P. Pereira, "Telefónica, nova labs roll out blockchain-based mobile infrastructure in mexico," Jan. 2024. [Online]. Available: https://cointelegraph.com/news/telefonica-nova-labs-roll-out-blockchain-based-mobile-infrastructure-in-mexico

[292] "Mocaverse partners with SK planet to co-develop Web3-enabled experiences with realm SDK and MOCA coin," Dec. 2024. [Online]. Available: https://www.crypto-reporter.com/press-releases/mocaverse-partners-with-sk-planet-to-co-develop-web3-enabled-experiences-with-realm-sdk-and-moca-coin-83450/

[293] "BSN and china mobile officially launch the open consortium chain CMBaaS," Mar. 2022. [Online]. Available: https://cn.cointelegraph.com/news/bsn-works-with-cmcc

[294] C. Wang, "Blockchain SIM card for Web3.0 comes out," May. 2023. [Online]. Available: https://digitalpaper.stdaily.com/http$_w ww.kjrb.com/kjrb/html/2023-05/18/content_5$53342$.htm?div=-1$

[295] "PCCW global and colt expand their blockchain trial while more carriers join the initiative," May. 2018. [Online]. Available: https://www.hkt.com/staticfiles/PCCWCorpsite/Press

[296] "PCCW-HKT, first hong kong-based CMT partner of the sandbox, plans to launch world's first virtual 5G mobile network and brand-new Web3 multimedia experience in Metaverse," May. 2022. [Online]. Available: https://www.animocabrands.com/pccw-hkt-to-launch-virtual-5g-mobile-network-and-web3-multimedia-experience-in-the-sandbox

[297] "Vodafone links its blockchain SIM to tokenized deposits," Oct. 2023. [Online]. Available: https://www.ledgerinsights.com/vodafone-links-blockchain-sim-to-tokenized-deposits/

[298] "Telefónica tech at the MWC 2024, the edition of our centenary," Feb. 2024. [Online]. Available: https://telefonicatech.com/en/blog/telefonica-tech-mwc-2024

[299] W. Aman, S. Al-Kuwari, and M. Qaraqe, "A novel physical layer authentication mechanism for static and mobile 3D underwater acoustic communication networks," *Physical Communication*, vol. 66, p. 102430, 2024.
[300] A. Elfikky *et al.*, "Performance analysis of convolutional codes in dynamic underwater visible light communication systems," *Opt. Quantum Electron.*, vol. 56, no. 1, p. 55, 2024.
[301] Y. Wang *et al.*, "Research on infrared detection and image simulation of ships applied to underwater unmanned vehicles," in *Fifth Int. Conf. Image, Video Process., Artif. Intell. (IVPAI 2023)*, vol. 13074. SPIE, 2024, pp. 13–17.
[302] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3162–3173, 2018.
[303] H. Duan, A. El Saddik, and X. Hu, "Blockchain-based integrated sensing and communication services in 6G networks," *IEEE Netw.*, vol. 39, no. 2, pp. 158–165, 2025.
[304] C. Liang *et al.*, "Generative AI-driven semantic communication networks: Architecture, technologies and applications," *IEEE Trans. Cogn. Commun. Netw.*, 2024.
[305] Y. Lin *et al.*, "A blockchain-based semantic exchange framework for web 3.0 toward participatory economy," *IEEE Commun. Mag.*, vol. 61, no. 8, pp. 94–100, 2023.
[306] Y. Lin *et al.*, "Blockchain-based semantic information sharing and pricing for web 3.0," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 5, pp. 3918–3930, 2024.
[307] Y. Lin *et al.*, "Blockchain-aided secure semantic communication for AI-generated content in Metaverse," *IEEE Open J. of Comput. Soc.*, vol. 4, pp. 72–83, 2023.
[308] H. Du *et al.*, "Enhancing deep reinforcement learning: A tutorial on generative diffusion models in network optimization," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 4, pp. 2611–1170, 2024.
[309] Z. Li, W. Feng, M. Guizani, and H. Yu, "TPI-LLM: Serving 70B-scale LLMs efficiently on low-resource edge devices," *arXiv preprint arXiv:2410.00531*, 2024.
[310] Z. Chen, Z. Zhang, and Z. Yang, "Big AI models for 6G wireless networks: Opportunities, challenges, and research directions," *IEEE Wireless Commun.*, vol. 31, no. 5, pp. 164–172, 2024.
[311] H. Luo *et al.*, "A trustworthy multi-LLM network: Challenges, solutions, and a use case," *arXiv preprint arXiv:2505.03196*, 2025.
[312] H. Luo, J. Luo, and A. V. Vasilakos, "BC4LLM: A perspective of trusted artificial intelligence when blockchain meets large language models," *Neurocomputing*, vol. 599, p. 128089, 2024.
[313] EU GDPR, "General data protection regulation (gdpr)," 2018.

Haoxiang Luo (Graduate Student Member, IEEE) received the B.Eng. degree in communication engineering from the University of Electronic Science and Technology of China (UESTC), China, in 2021, where he is currently pursuing the Ph.D. degree with the Key Laboratory of Optical Fiber Sensing and Communications (Ministry of Education). His research interests include communication networks, the IoT technology, and blockchain. He was the Session Chair of the 2023 IEEE MetaCom and a TPC Member of 9 prestigious IEEE conferences, such as the 2025 IEEE ICC and 2025/2024 IEEE WCNC. He is a reviewer of 14 top IEEE/ACM Magazines, Transactions, and Journals. He was the recipient of the Chinese National Scholarship in 2024 and won the Student Travel Grant of IEEE Globecom in 2024 and the Best Paper Award of IEEE DLCV in 2025.

Gang Sun (Senior Member, IEEE) received his Ph.D. degree from the University of Electronic Science and Technology of China (UESTC), China, in 2012. He was a Visiting Scholar at The Australian National University in 2015. He is currently a Full Professor at the Key Laboratory of Optical Fiber Sensing and Communications (Ministry of Education), UESTC. His research interests include network virtualization, high-performance computing, parallel and distributed systems, and blockchain. As a (Lead) Guest Editor, he has edited many special issues in top journals, such as the *IEEE Internet of Things Magazine*, *IEEE Vehicular Technology Magazine*, *Future Generation Computer Systems*, and *Multimedia Tool and Applications*.

Jiacheng Wang is a Postdoctoral Research Fellow in the College of Computing and DataScience at Nanyang Technological University, Singapore. Prior to that, he received the Ph.D. degree in School of Communications and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China. His research interests include wireless sensing, semantic communications, and generative AI, Metaverse.

Hongfang Yu (Senior Member, IEEE) received the B.S. degree from the Xidian University in 1996, the M.S. and Ph.D. degrees from the University of Electronic Science and Technology of China (UESTC), China, in 1999 and 2006, respectively. She was a Visiting Scholar at the University at Buffalo SUNY, USA and the City University of Hong Kong, Hongkong, China, in 2010 and 2012, respectively. She is currently a Full Professor with the Key Laboratory of Optical Fiber Sensing and Communications (Ministry of Education), UESTC, and the Vice Dean of the School of Information and Communication Engineering, UESTC. Her research interests include data center networking, network function virtualization, software-defined networking, blockchain technology, and federated learning. She is an Area Editor of the *IEEE Internet of Things Journal*, a Technical Editor of the *IEEE Network*, an Associate Editor of the *IEEE Communications Surveys & Tutorials*, and *Digital Communications and Networks*.

Dusit Niyato (Fellow, IEEE) is a Professor in the College of Computing and Data Science, at Nanyang Technological University, Singapore. He received B.Eng. from King Mongkuts Institute of Technology Ladkrabang (KMITL), Thailand and Ph.D. in Electrical and Computer Engineering from the University of Manitoba, Canada. His research interests are in the areas of mobile generative AI, edge intelligence, decentralized machine learning, and incentive mechanism design.

Schahram Dustdar (Fellow, IEEE) is currently a Full Professor heading the Distributed Systems Group at the Technische Universität Wien (TU Wien), Vienna, Austria. He received the Ph. D. degree in business informatics from the University of Linz, Austria, in 1992. He was the founding Co-Editor-in-Chief of ACM Transactions on Internet of Things as well as Editor-in-Chief of Computing (Springer). He is an Associate Editor of IEEE Transactions on Services Computing, IEEE Transactions on Cloud Computing, ACM Computing Surveys, ACM Transactions on the Web, and ACM Transactions on Internet Technology, as well as on the editorial board of IEEE Internet Computing and IEEE Computer. He is an elected Member of the Academia Europaea: The Academy of Europe, where he is Chairman of the Informatics Section, as well as an IEEE Fellow (2016), an AAIA President (2021-2023) and Fellow (2021). He is an EAI Fellow (2021) and an I2CICC Fellow (2021). He is a Member of the 2022 IEEE Computer Society Fellow Evaluating Committee (2022).

Zhu Han (Fellow, IEEE) received the B.S. degree in electronic engineering from Tsinghua University, in 1997, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, in 1999 and 2003, respectively. From 2000 to 2002, he was an RD Engineer of JDSU, Germantown, Maryland. From 2003 to 2006, he was a Research Associate at the University of Maryland. From 2006 to 2008, he was an assistant professor at Boise State University, Idaho. Currently, he is a John and Rebecca Moores Professor in the Electrical and Computer Engineering Department as well as in the Computer Science Department at the University of Houston, Texas. Dr. Han's main research targets on the novel game-theory related concepts critical to enabling efficient and distributive use of wireless networks with limited resources. His other research interests include wireless resource llocation and management, wireless communications and networking, quantum computing, data science, smart grid, carbon neutralization, security and privacy. Dr. Han received an NSF Career Award in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society in 2011, the EURASIP Best Paper Award for the Journal on Advances in Signal Processing in 2015, IEEE Leonard G. Abraham Prize in the field of Communications Systems (best paper award in IEEE JSAC) in 2016, IEEE Vehicular Technology Society 2022 Best Land Transportation Paper Award, and several best paper awards in IEEE conferences. Dr. Han was an IEEE Communications Society Distinguished Lecturer from 2015 to 2018 and ACM Distinguished Speaker from 2022 to 2025, AAAS fellow since 2019, and ACM Fellow since 2024. Dr. Han is a 1% highly cited researcher since 2017 according to Web of Science. Dr. Han is also the winner of the 2021 IEEE Kiyo Tomiyasu Award (an IEEE Field Award), for outstanding early to mid-career contributions to technologies holding the promise of innovative applications, with the following citation: "for contributions to game theory and distributed management of autonomous communication networks."