SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

July 2024, Vol. 67, Iss. 7, 170301:1–170301:22
https://doi.org/10.1007/s11432-023-4054-5

Special Topic: XAI-Enabled Network Automation for 5G and Beyond: Move Closer to Zero-Touch

Scenarios analysis and performance assessment of blockchain integrated in 6G scenarios

Bo LI[1], Guanjie CHENG[1*], Honghao GAO[2], Xueqiang YAN[3] & Shuiguang DENG[1*]

[1]*College of Computer Science and Technology, Zhejiang University, Hangzhou* 310027*, China;*
[2]*College of Computer Science and Technology, Shanghai University, Shanghai* 200131*, China;*
[3]*2012 Lab, Huawei Technologies Co., Ltd., Shenzhen* 201206*, China*

Received 19 March 2023/Revised 25 January 2024/Accepted 31 May 2024/Published online 27 June 2024

Abstract Emerging applications such as smart city infrastructures and virtual reality landscapes are setting rigorous benchmarks for 6G mobile networks, requiring elevated levels of confidentiality, integrity, nonrepudiation, authentication, and stringent access controls. Blockchain technology is heralded as a transformative enabler for meeting 6G standards, owing to its intrinsic attributes. However, a gap exists in the holistic investigation of blockchain's applicability in 6G realms, particularly addressing the "whether", "when", and "how" of its deployment. Present research trails in developing robust methodologies to gauge blockchain's efficacy within 6G use cases. Addressing this, our study introduces a novel confluence of blockchain with 6G networks, where data resides in distributed Hash tables (DHTs) while their hashes are secured in distributed ledger technology (DLT), harnessing blockchain's core strengths-immutability, traceability, and fortified security. We delineate seven specific 6G use cases poised for enhancement through blockchain integration, and scrutinize the rationale, nature, and timing of this convergence. Furthermore, we devise a comprehensive methodology for assessing blockchain's performance metrics and scalability in 6G environments. Our extensive experimental analyses evaluate the synergistic performance of this integration, revealing that the Quorum blockchain satisfactorily supports 80% of 6G scenarios. The findings suggest that, with appropriate configurations, consortium blockchains are well-equipped to fulfill the demanding performance and scalability requisites of 6G networks.

Keywords blockchain, distributed ledger technology (DLT), 6G, performance assessment, 6G scenarios analysis, transaction arrival rate

1 Introduction

With the emergence of 5G networks, we have entered a new age of digital society in which various smart applications, including industrial automation, intelligent transportation, and remote healthcare, are thriving [1, 2]. The enormous rise of mobile traffic, which is projected to reach 607 Exabyte/month by 2025 and 5016 Exabyte/month by 2030 [3], renders 5G incapable of meeting the new needs of future significant applications. Moreover, the fast growth of data-centric intelligent systems reveals new latency constraints of 5G networks [4]. Thus, several research programs are transitioning towards the next generation of mobile networks, 6G, with the goal of satisfying increasingly severe requirements such as latency, connection, scalability, and reliability by combining diverse networks spanning space, air, and ground [5, 6].

At the heart of these cutting-edge communication systems lie antenna systems, which play a pivotal role in enabling seamless transmission and reception of signals across various network components [7]. Antenna systems serve as the interface between the electromagnetic spectrum and the physical world, converting electrical signals into electromagnetic waves for transmission and vice versa for reception. In 5G and forthcoming 6G systems, the significance of antenna systems is further amplified due to the unique challenges and requirements posed by these advanced networks [8]. The deployment of mmWave frequencies, massive MIMO (multiple input multiple output) techniques, beamforming technologies, and intelligent antenna arrays necessitates sophisticated antenna designs capable of supporting diverse use

* Corresponding author (email: chengguanjie@zju.edu.cn, dengsg@zju.edu.cn)

cases and meeting stringent performance metrics. Antenna systems in 5G and 6G networks must exhibit enhanced beamforming capabilities, wider bandwidths, improved efficiency, and compact form factors to accommodate the evolving demands of wireless connectivity [9].

Compared to its 5G predecessor, 6G is anticipated to be a ubiquitous integrated network with faster transmission speed, lower communication latency, improved dependability, and larger coverage. Despite the fact that the emergence of advanced technologies, such as edge intelligence, TeraHertz (THz) communication, wireless optical technology, and large-scale satellite constellation, promotes the implementation of 6G, there are still a number of obstacles to overcome prior to the actual landing [10–14]. Generally speaking, the issues encountered by 6G may be divided into two categories based on the application needs [5]. The first category includes scalability, latency, throughput, and synchronization, which are performance requirements resulting from future systems' vast interconnectedness [15]. For example, the THz band (0.1–10 THz) will be used in 6G wireless communication systems to support the demand for higher data rates and ultra-high-speed communication for many future applications [11]. The second category includes security-related requirements such as confidentiality, integrity, non-repudiation, authentication, and access control. The first group permits widespread communication, whilst the second group ensures the security of entities and data transferred.

Blockchain, a distributed ledger system, employs consensus algorithms for consistent chain-structured data storage and smart contracts for operational automation [16]. As a decentralized, immutable, and autonomous database, blockchain facilitates trust establishment among untrusted entities in distributed settings. Blockchain's numerous advantages, such as decentralization, traceability, anonymity, and immutability, render it an ideal choice for integrating into the security and data management aspects of 5G/6G systems [5]. Recently, there are many studies now on how blockchain is applied in 5G networks. For example, Chaer et al. [17] discussed the opportunities and challenges of blockchain in 5G. Nguyen et al. [18] investigated the motivations and possibilities for the integration of blockchain and 5G. Mistry and colleagues [19] explored how blockchain can enhance industrial automation of the Internet of Things (IoT) under 5G networks. Antennas form part of a wireless transmitting or receiving system designed to receive/ radiate electromagnetic waves. In considering the wireless link's balance for a typical wireless link, the antennas play a critical role [20]. An et al. [21] enhanced the manufacturing efficiency and reliability of 5G antennas by integrating blockchain and smart contract technologies, supported by in-depth analytic hierarchy process (AHP) analysis. However, these articles only focus on the integration of blockchain with certain scenarios in 5G networks. They do not consider the entire architecture of 5G networks to determine where and how blockchain should be integrated. Furthermore, since 6G networks have a different network architecture compared to 5G, such as the unique sensing network architecture of 6G [22], this requires in-depth consideration and research.

Similarly, in recent studies, the integration of blockchain with 6G networks is also gradually emerging. Xu et al. [23] have shown that by incorporating the trustless and automated capabilities of blockchain, resource management and sharing in 6G networks can be made more performance-effective. 6G IoT survey [4] also shows that blockchain is expected to empower future 6G IoT networks. Thus, blockchain offers a viable option for addressing the second group of challenges described above. In addition, blockchain is lauded for its intrinsic properties, such as decentralization, traceability, anonymity, immutability, and security [24]. It is not difficult to deduce that the second set of obstacles may also be addressed by establishing a communication network using blockchain as its underlying technology. Consequently, blockchain is generally regarded as one of the essential 6G enabling technologies.

Despite the above-mentioned capabilities, scalability is a significant hurdle to the widespread use of blockchain from the standpoint of storage and distribution [25]. The maintenance of network consistency necessitates that each blockchain node keep a copy of the whole ledger locally, and the blockchain's trustworthiness is maintained by verifying each transaction and block, at the sacrifice of transaction performance. Moreover, blockchain implementation must contend with the impossible trinity, i.e., security, decentralization, and scalability. Any two attributes that are realized must come at the price of the third. Therefore, if the blockchain is included in 6G in an irresponsible manner, not only will it not provide any advantages, but it may also pose certain problems. This concern makes it crucial to verify the requirement and efficacy of the integration architecture by conducting a comprehensive analysis of the performance and possible bottlenecks in the blockchain-enabled 6G network. Several studies are currently investigating blockchain integration for 6G, with the majority focusing on addressing specific issues, such as spectrum sharing, service-level agreement (SLA) management, and mobile user privacy protection [23, 26, 27]. We have conducted a comparative analysis of related literature in Table 1 [4, 19, 21, 23, 24, 27–29]. This table

Table 1 Summary of recent advances in the combination of blockchain and communication

Reference	Year	Contribution	Limitation	Category
Nguye et al. [4]	2012	It explores the emerging opportunities brought by 6G technologies in IoT networks and applications.	• There is no specific discussion on how blockchain is used in 6G scenarios. • There is no experimental evaluation proving that blockchain can be applied in 6G scenarios.	Survey
Mistry et al. [19]	2020	It discusses the potential applications of blockchain in industrial automation, such as smart city, smart home, healthcare 4.0, smart agriculture, autonomous vehicles, and supply chain management.	• The article is limited to IoT scenarios. • The article does not evaluate the performance and scalability of blockchain in IoT scenarios.	IoT
Cheng et al. [24]	2021	This document presents a blockchain-based mutual authentication scheme for collaborative edge computing (CEC) in the IoT.	The discussion and experiments are solely based on the authentication scenario, without placing the scenario within 6G to prove that blockchain-based authentication meets the requirements of 6G.	IoT
Xu et al. [23]	2020	The paper explores multiple application scenarios, including IoT, device-to-device communications, network slicing, and inter-domain blockchain ecosystems.	• The article is limited to scenarios of resource sharing. • The article does not provide relevant experiments or proof to demonstrate whether blockchain can meet the performance and scalability requirements of 6G.	Resource sharing
Velliangiri et al. [27]	2021	The paper focuses on integrating blockchain with 6G, addressing security, resource sharing, designing a privacy-secure framework, and suggesting areas for future research.	This framework is primarily designed for the scenario of privacy protection and does not address the rationale for integrating blockchain into 6G in terms of anticipated 6G scenarios.	Privacy preservation
An et al. [21]	2024	The integration of blockchain enhances record keeping and traceability, while smart contracts automate processes for issue resolution, leading to improved efficiency and reliability in antenna production.	• Only analyze a single scenario • No security certification considered	Antenna
Wang et al. [28]	2024	The document proposes a novel architectural system model that fuses wireless edge computing with blockchain consensus techniques to deliver decentralized 6G communication services tailored for consumer electronics.	Edge servers cannot directly observe device credentials, computing power, or energy budgets.	Communication
Wei et al. [29]	2024	The main contributions of the work are highlighted as the proposal of a blockchain-enabled access control approach for 6G-MEC and a multitier validation scheme for attribute matching.	Only consider edge environments	Acecss control

succinctly outlines the strengths and limitations of each referenced work.

Although these studies have confirmed the advantages blockchain may bring in, a problem-specific integration architecture cannot provide a general guideline for blockchain deployment as a fundamental component of the 6G network. To the best of our knowledge, there are currently few publications addressing the rationale for the integration of blockchain in 6G in terms of foreseen 6G scenarios. Detailed performance evaluations to forecast possible integration architectural constraints are also lacking. To fill this gap, we present a comprehensive perspective by studying and assessing the role of blockchain in seven plausible 6G scenarios. In addition, we propose a methodology for evaluating the performance and scalability of blockchain-based 6G scenarios. Finally, we implement it in a real-life environment to undertake a thorough assessment of its performance. This paper is intended to serve as an enlightening guideline to spur interest and further investigations for subsequent research on blockchain-empowered 6G systems. The main contributions are summarized as follows:

• We extract seven fine-grained scenarios from the foreseeable 6G application layer to analyze whether, when, and how to integrate blockchain into 6G network architecture. All additional application situations are one or more combinations of these seven fundamental application scenarios, which serve as the foundation for further scenarios.

• We propose a methodology for assessing the scalability and performance of blockchain in 6G scenarios.

This methodology can help evaluate whether new 6G application scenarios can use blockchain services.

• We conduct performance evaluations on a real network environment consisting of multi-site data centers, on which a consortium blockchain (Quorum) has been implemented. Several configurations, including the number of nodes, compute capacity, and consensus procedure, are used to evaluate the performance of Quorum. Besides, we conducted a more extensive performance experiment based on the Poisson distribution's transaction arrival model. The solid experimental results indicate that the methodology has strong usability, and blockchain can be integrated into 6G networks with the proper setups.

The remainder of this paper is organized in the following order. Section 2 presents a review of related works. Analyses of detailed 6G scenarios are presented in Section 3. The methodology is described in Section 4. In Section 5, we illustrate the extensive experimental evaluation. Finally, we conclude the work in Section 6.

2 Related work

Since massive data connectivity is essential for the ever-increasingly intelligent, automated, and ubiquitous digital world [8], 6G is gradually developing towards a marginal and distributed structure. However, the huge risks of attacks and threats occurring in a distributed system make it a tough challenge to achieve a high degree of security and privacy in 6G networks. Moreover, how to perform efficient and reliable data management in the 6G data systems such as vehicular data sharing, medical data storage, and access control is a critical but troublesome issue.

Blockchain technology offers some key opportunities in 5G networks, such as infrastructure for crowdsourcing, infrastructure sharing, international roaming, network slicing, management, and authentication [30]. But, 5G considers the issue of smooth interoperability between different blockchain platforms. These several limitations can be mitigated in 6G by using consensus algorithms, applying novel blockchain architecture and sharing techniques, and increasing the block size of the network [31].

Regarding security issues arising from heterogeneous standard integration and access delegations in 6G environments, Manogaran et al. [32] introduced a blockchain-based integrated security measure for providing secure access control and privacy preservation for resources and users. Although the performance of the proposed solution is verified by several metrics, the latency caused by block validation in the blockchain has not been studied, nor has the evaluation of the data leakage probability. Deb et al. [33] integrated blockchain into fog nodes and centralized servers to establish a secure model-sharing platform in a 6G-based industrial Internet of Things (IIoT). Zhao et al. [34] used blockchain to audit the correctness of privacy-preserving IOT data classification against malicious data processors/data centers. Besides, some studies dove deeper into the field of blockchain-enabled resource sharing and spectrum management in 6G and verified that the integration between wireless networks and the blockchain would allow the network to monitor and manage spectrum and resource utilization in a more efficient manner [23,35,36].

An et al. [21] integrated blockchain with antenna systems. The integration of blockchain enhances record-keeping and traceability, while smart contracts automate the issue resolution process, thereby improving the efficiency and reliability of antenna production. Wang et al. [28] proposed a novel architectural system model that integrates wireless edge computing with blockchain consensus technology, providing decentralized 6G communication services tailored for consumer electronic products. Wei et al. [29] proposed a blockchain-supported 6G-MEC access control method and a multi-layer verification scheme for attribute matching. These efforts envision blockchain-based resource management, spectrum sharing, and energy trading as drivers for future 6G use cases.

Although these studies have highlighted the integration of blockchain for 6G, most of them deal with specific issues such as data management [32, 37, 38], spectrum sharing [35, 36], and privacy protection [27, 39, 40]. The exact scope of requirements may vary in different 6G application scenarios due to the diverse nature of involved entities, such as wearable devices, edge servers, and base stations. Therefore, a comprehensive view of blockchain integration in foreseeable 6G scenarios is of great importance. Besides, the inherent scalability-related issues in blockchain, such as throughput and storage bottlenecks, may become potential threats that hinder the efficient operation of 6G systems [23]. Thus, deep performance evaluation is vital for further exploration of incorporating blockchain in 6G networks. To explicitly highlight the unique features and technical requirements of 6G, some surveys present representative applications and shed light on fundamental technologies that are expected to empower future

6G networks [4, 25, 31]. However, they focused on how blockchain can benefit these applications without delving into integration details such as whether to use blockchain, how to define a transaction, and when to generate a transaction. To the best of our knowledge, no work has been done to investigate in detail how to integrate blockchain into 6G networks from a general scenario perspective, and there are no methods to review the performance and scalability of blockchain-based 6G scenarios. This paper intends to fill this gap and serve as an enlightening guideline to spur deeper investigations for subsequent research on blockchain-empowered 6G networks.

3 Scenarios analysis on integrating blockchain in 6G network architecture

In this section, we extract seven fine-grained scenarios from emerging 6G applications to conduct a detailed analysis of why, what, and when to integrate blockchain technology into 6G network architecture. The scenario analysis reflects the actual requirements of 6G applications, based on which we judge the performance demands of the blockchain and adjust integration schemes.

3.1 Public key management

In the 6G era, a huge number of devices are connected for data interaction. Public key encryption schemes inherently need to prevent malicious attacks on devices and exchanged data, such as man-in-the-middle attacks and eavesdropping. Key management is the foundation of all security mechanisms. They do everything from data encryption and decryption to authentication, authorization, and access control (AAA) [41]. Any compromise of cryptographic keys can lead to compromise for the entire security infrastructure, allowing attackers to decrypt sensitive data, authenticating themselves as privileged users, or giving themselves access to unauthorized information. Therefore, proper management of public keys is an integral part of the 6G network. As a distributed platform, blockchain has been one of the most viable solutions for storing user keys. The tamper-proof nature of blocks can be leveraged to build a chain of trust for public keys. There are two use cases for public key management in 6G: public key management for users and public key management for network devices.

• The public key management of users is for individual users. For example, users need to add or delete public key information in the blockchain when they register or cancel their devices. When using a public key to encrypt personal information, not only prevents confidential information from being stolen but also well meets the requirements of GDPR. At the same time, user authentication and access control are of great significance to ensure a secure network cooperation environment.

• The public keys of network devices can be mutually authenticated in multiple network devices, not only to prevent pseudo base stations but also to establish a shared network by different operators.

The process of public key management is illustrated in Figure 1. Below, we introduce public key infrastructure (PKI), key management lifecycle, secure communication protocols, and the process of public key usage.

3.1.1 *PKI*

• Key generation. The illustrated public key management system, as depicted in Figure 1, relies on a robust PKI framework for generating cryptographic key pairs, consisting of a public key and its corresponding private key. These key pairs are created using secure algorithms such as RSA, ECC, or EdDSA.

• Certificate authority (CA). A crucial component of the PKI is the CA, responsible for issuing digital certificates that securely associate public keys with their respective owners. In the context of communication networks, CA entities typically function as network service providers.

• Certificate revocation. To uphold PKI security, mechanisms for certificate revocation are implemented, enabling the invalidation of certificates in cases of compromise or loss of trust. This process often involves maintaining certificate revocation lists (CRLs) or employing online certificate status protocol (OCSP) services.

3.1.2 *Key management lifecycle*

• Key generation and distribution. Public and private key pairs are securely generated by the operator during device and SIM card production. The private key is then securely written into the hardware, while

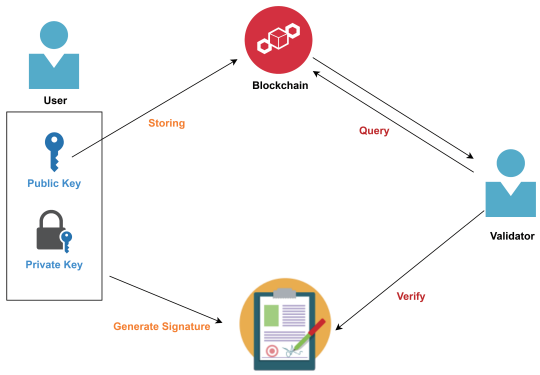

Figure 1 (Color online) Public key management.

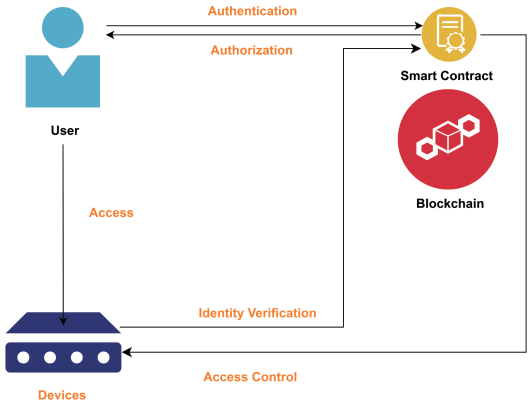

Figure 2 (Color online) Authorization, authentication, and access control.

the corresponding public key is stored on the blockchain for authentication and verification purposes.

• Key usage and protection. Keys are used for cryptographic operations such as encryption, decryption, digital signing, and verification. It is essential to enforce proper key usage policies and protect keys from unauthorized access or misuse through measures such as encryption, hardware security modules (HSMs), and access controls.

3.1.3 *Integration with blockchain*

• Blockchain identity. Public key management plays a pivotal role in blockchain ecosystems, where cryptographic keys are used to represent user identities and authenticate transactions. Public keys are associated with blockchain addresses, enabling participants to send and receive digital assets securely.

• Digital signatures. Cryptographic signatures generated using private keys provide proof of ownership and authorization in blockchain transactions. Public key management ensures the integrity and authenticity of digital signatures, enabling trustless interactions in decentralized networks.

Figure 1 illustrates the process of public key management. Users or devices generate a key pair, keeping the private key confidential while registering and publicizing the public key on the blockchain network. The public key is primarily used to verify transactions and messages signed by the private key, ensuring their authenticity and security. Over time, if necessary, these public keys may be updated or revoked to address security risks or change authentication information. This process takes place in the decentralized and tamper-proof environment of the blockchain, ensuring the transparency and trustworthiness of the entire system [42].

3.2 ID management

One of the major challenges facing 6G network operators is bringing all parties together and coordinating their efforts to provide economically viable and seamless connectivity to users. For each new participant, the demand for interfaces with secure authentication and authorization mechanisms will increase, along with the complexity and operational costs of the ID infrastructure required for the associated identity management. While today's centralized ID infrastructures have proven to be technically feasible in limited and trusted spaces, once centralized identity providers must be avoided and due to limited cross-domain interoperability or national data protection legislation and certification, they are unable to provide the required security for country-dependent institutions typically cannot be trusted, for example, geopolitical reasons [43].

A blockchain-based 6G network enables secure mutual authentication across networks with different trust domains. It also allows the network to be independent of trusted third parties while improving the auditability and transparency of IDs, better management of IDs in multiple trust domains. two use cases for ID management in 6G networks are Pseudo-name management and decentralized ID management.

Pseudonyms, as a data protection method strongly recommended by GDPR, emerge to prevent real information leakage. It is to use real public keys to create pseudonyms and record the mapping relationship

between pseudonyms, along with real public keys in the blockchain. This way ensures the leakage of real public key information, the authenticity of public keys and the auditability of related user behavior.

Although blockchain can provide a trustworthy third-party identity management platform, being an open system, it often leads to the leakage of identity privacy [44]. Even when users employ random addresses (or pseudonyms) while operating on the blockchain, it only offers limited identity privacy [45]. Certainly, some potential methods are available for us to use, helping us address the issue of identity leakage in blockchain. These include ring signatures, zero-knowledge proofs, and mixing services. We will also assess the benefits of using blockchain for ID management through "A framework for comparative evaluation of web authentication schemes" [46].

3.3 Authorization, authentication, and access control

In 6G networks, the total number of devices is growing at an increasing rate, which poses new security risks and challenges to the system. Failure to protect network devices from unauthorized access can often lead to serious data breaches, as these devices often contain large amounts of valuable and sensitive data. As for traditional access control technology, centralized management can lead to data leakage, as well as the difficulty of coordinating multiple parties as multiple organizations are involved. Therefore, it is not applicable to 6G networks. AAA can be ported to blockchain networks and, in particular, be implemented as a smart contract on a decentralized blockchain with no downtime, no fraud, and no third-party intervention. It also enables secure AAA in mutually untrusted administrations.

However, due to the public and transparent nature of blockchain, it easily leads to the leakage of identity information of both parties during AAA [47]. Over the past twenty years, there has been an ongoing discussion on how to achieve an efficient and secure identity authentication mechanism [48]. In the context of 6G identity AAA, we need to consider not only the convenience brought by blockchain but also the privacy issues it causes. Therefore, blockchain-based identity management requires a new privacy protection scheme. Additionally, this new privacy protection scheme needs to be evaluated, and certain methodologies can assist in this process [49, 50]. Figure 2 illustrates a simple AAA process.

3.4 Context information management

With the objective of providing high quality of service (QoS), 6G systems will need to be context-aware. using context information in a real-time mode depends on the network, devices, applications, and the environment of users [51]. There are several benefits to using blockchain to preserve context information. First, it enables easy access. Because different kinds of context information are kept in the blockchain, and there is no need to go through a third-party platform. Second, all the modification and deletion records of the context information can be audited, thus enhancing the security of the information. We propose two use cases for context information as follows:

• Personal context information is indexed by the user's identity and contains personal information, for example, the cached information such as ID and public key generated by individual users. For some data that needs to be shared, putting the personal context information into the blockchain can facilitate the base station to access the cached information quickly and also ensure the auditable record of information usage. For certain private user context data, we encrypt and store user context information in the distributed Hash table (DHT) network as shown in Figure 3, and store the context hash values in the blockchain, thus protecting the privacy of the user's context.

• Location information, which is very important context information, ensures that operators can better serve their customers. By storing location information in the blockchain, it can facilitate fast access by different operators. However, location information is private information. it needs to be placed in the blockchain by encryption and to access location information that needs to be approved by the owner.

3.5 Data management and data trading

As digitization accelerates, every element of society is generating large amounts of data all the time, and in turn, benefits from the proliferation of data [52]. As a result, data management and further data transactions have become one of the key technical building blocks of the 6G architecture. Considering that 6G is envisioned to assume an important role in enabling large-scale IoT devices to seamlessly collaborate to meet highly diverse business needs and to realize the vision of ubiquitous AI. In this paper, we mainly consider subscription data, AI model data, IoT data, and sensing data. All of these contain

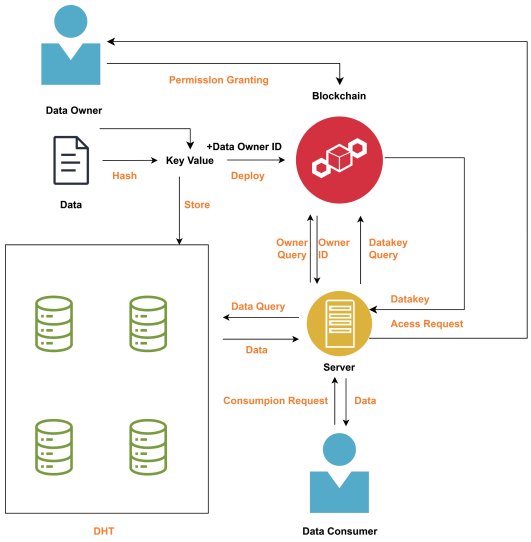

Figure 3 (Color online) DLT+DHT architecture.

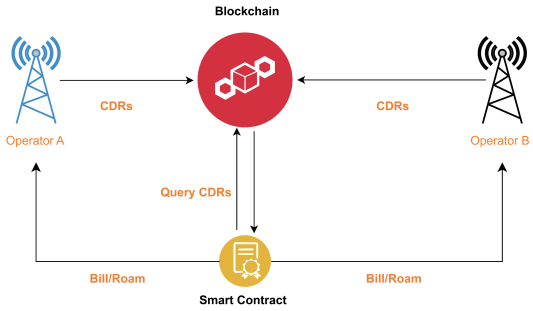

Figure 4 (Color online) Call detail records are recorded on the blockchain.

a large amount of private information and these data contain a large amount of private information and are of high commercial value. Therefore, there is an urgent need for secure systems that support data management and transactions. Blockchain is a distributed database maintained by multiple parties, and it is transparent, traceable, collaboratively maintained, and supports the flow of data and transactions. With these advantages, blockchain has emerged as one of the potential solutions for data management and transactions.

The biggest problem with current data management is the inability to provide transparency, trustworthiness, traceability, immutability, auditability, privacy, and security. Particularly for data operations, there is a lack of publicly transparent records for review by multiple parties [53]. In data trading, due to the presence of dishonest buyers/data brokers, traditional data trading platforms have many limitations [54]. For example, lack of price transparency and data manipulation by brokers.

However, storing data on the blockchain is very costly, and since the data on the blockchain is public and transparent, it can easily lead to privacy breaches. Therefore, we propose a blockchain-based data management architecture. We use both on-chain and off-chain architectures to manage data, as shown in Figure 3. DHT plays a crucial role in enhancing distributed ledger technology (DLT) systems. It offers decentralized storage and retrieval of data across the network, eliminating the need for centralized servers. DHTs employ a key-value storage mechanism, with each node responsible for a subset of data, ensuring efficient access through unique identifiers. Moreover, DHTs ensure scalability and fault tolerance by distributing data tasks across numerous nodes, enabling the network to handle large volumes of data and withstand node failures gracefully. The hash address of the original data is stored on the blockchain, while the original data is stored off-chain after encryption. For data deletion and update, the data activity should be recorded on the blockchain. The on-chain/off-chain architecture ensures the "right to forget" as required by GDPR and also ensures the expansion of the blockchain ledger due to excessive data size. By integrating DHT with DLT, systems benefit from decentralized storage, efficient data access, and enhanced resilience, making them capable of managing extensive data operations effectively.

We briefly explain how this system architecture achieves data storage and data access. During data storage, the hash value of the encrypted data block is first calculated and used as a key. Then, the encrypted data block and a signed copy are stored in the DHT network as key-value pairs. Finally, the data owner adds a timestamp, a summary of the encrypted data block, and their account message to an appendix file, and deploys the file to the blockchain for querying. Regarding data requests, first, the consumer sends a data request to the server. This request includes partial account information of the data owner, the timestamp when the data was generated, and the consumer's public key (PKconsumer). The server queries the blockchain for the data owner's ID (ownerID) using the timestamp and data owner's information, and then sends PKconsumer to the data owner. If the data owner agrees to grant access to the user, a permission file is uploaded to the blockchain; if access is denied, a denial file is uploaded.

Then, the server verifies through the blockchain whether the user has been successfully authorized. If access is denied, the edge server returns an apology statement. Otherwise, the server finds the summary (datakey) of the encrypted data block in the appendix file.

3.6 Resource sharing

To meet the demands of high-performance computing in the era of big data, cloud computing has begun to be utilized as a means of resource sharing. However, all resources in cloud computing are deployed in data centers, and dynamic data management in traditional network defense structures relies on third-party central nodes. Currently, there is significant research on how to share computing resources through blockchain. Shi et al. [55] proposed a new concept of worm computing, utilizing blockchain platforms to build basic decentralized systems. By using private chains to store collaborative data, they addressed the issues of data sharing and trust calculation in traditional collaboration models, ensuring the immutability of transactions through decentralized, trustworthy services. Hong et al. [56] focused on enhancing fairness in device-to-device (D2D) networks by recording users' collaborative computing tasks on a public blockchain ledger. They combined user mobility and credit balance for task scheduling, aiming to improve the fairness of resource sharing.

Besides the contribution of computing resources, there are other studies related to resource sharing [57–61]. To achieve efficiency and security of 6G resource sharing, wireless resources such as spectrum, compute, storage, and infrastructure will play a critical role. The cost of sharing wireless resources will be significant. Traditional studies rely on a centralized third party to verify each resource sharing transaction, which is vulnerable to many security threats, including single points of failure and denial of service attacks [62]. Moreover, they focus only on resource management and ignore privacy and security issues that are critical to resource sharing.

Resource sharing is a typical use case where blockchain can be used to efficiently exchange assets between multiple stakeholders without the need for a centralized third party to provide trust. In a blockchain, all resource sharing and transactions are transparent and secure. Not only that, all resource sharing executions can be consistent through smart contracts without human intervention in resource sharing. In 6G networks, there are several resources that can be shared, such as spectrum, computing resources, and networks.

3.7 Trading and settlement

Traditional asset transactions require the involvement of intermediaries, such as brokers or paying agents, to facilitate the clearing and settlement of transactions, making the settlement process very time-consuming and costly. Blockchain can be used to exchange assets between multiple stakeholders in a de-trusted environment as it provides a decentralized infrastructure and enables more flexible settlement cycles to speed up settlements. Through smart contracts, we can automate transactions and settlements without human intervention to ensure the security of assets and ease of transactions.

At the same time, due to the in-mutability of the blockchain, all transaction and settlement information can be accessed through the blockchain, which can also facilitate future inquiries and audits. In 6G, we propose two use cases that require the use of blockchain.

• In the wireless telecommunications environment, there is interconnection settlement, roaming settlement, and billing between different operators. The existing settlement methods take a long time and the results are not clear and ambiguous. With the introduction of blockchain, different stakeholders can transact and settle faster, more transparently, more accurately, and more securely.

• Call detail records (CDRs) are used to charge customers for using transportation network services at the end of the billing period. To make billing information auditable, CDRs can be periodically recorded on the blockchain or stored in an on-chain/off-chain architecture (Figures 3 and 4). When settlement and transactions are encountered, the CDRs are queried via smart contracts to automatically perform billing and roaming tasks.

The telecommunications operator integrates CDRs into a DLT + DHT architecture. In this setup, the actual CDR data is stored within the DHT, while the data hashes are stored within the DLT. When consumers need to access their own billing records for auditing or verification purposes, they first query the smart contract within the DLT to check for permission to access. Upon obtaining access rights, consumers retrieve the corresponding CDRs from the DHT and perform the audit. Similarly, when multiple operators need to access and audit the data, they utilize the same method to retrieve CDRs.

Algorithm 1 Evaluate blockchain suitability for 6G scenarios

```
Initialization
while new 6G scenario is found do
    Understand the need for blockchain in the scenario;
    if blockchain is beneficial then
        Determine how to use blockchain in this scenario;
        Identify what to record on the blockchain;
        Determine when to use blockchain (read/write transactions);
        Choose transaction arrival rate model (e.g., Poisson, Pareto);
        Input model into blockchain for performance evaluation;
        Calculate read/write performance of the blockchain;
        Compare calculated performance with maximum blockchain speeds;
        if blockchain meets scenario requirements then
            Scenario suitable for blockchain integration;
        else
            Scenario not suitable for blockchain;
        end if
    else
        Scenario not suitable for blockchain;
    end if
end while
```

4 Methodology of performance evaluation

In this section, we introduce a methodology that evaluates blockchain performance and scalability in 6G scenarios. We divide transactions in the blockchain into "read" and "write", and analyze when "read" and "write" are required in seven scenarios. Based on the above, we propose a model for the sending rate as a Poisson distribution. Finally, we calculate the transaction arrival rates of scenarios.

4.1 Methodology

From related work, it can be concluded that there is no common evaluation method for blockchain in 6G scenarios. In this section, we propose a methodology that can evaluate whether the blockchain performance meets the 6G scenario.

To simplify the evaluation process, we provide the Algorithm 1. When we find a new 6G scenario, first we understand why the scenario needs to use blockchain and the benefits of using blockchain. If there is no benefit to using blockchain in this scenario, or if the performance and usefulness of the entire scenario are not greatly improved by using blockchain, then the scenario cannot be combined with blockchain. After determining why we use blockchain, we should know how to use blockchain in this scenario and what should be recorded on the blockchain. After that, we need to know when to use blockchain. Here, we distinguish between "read" and "write" transactions, and know when to "read" and when to "write".

Next, after determining when to use the blockchain, we determine the read and write transaction arrival rate model. Examples include Poisson distribution model, Pareto distribution process, and Weibull distribution process. After determining the transaction arrival rate, we input the model into the blockchain for performance evaluation and get the "read" and "write" performance of the blockchain.

In Tables 2 and 3, we analyze the why, what, and when of the seven scenarios using blockchain. Usually, most 6G scenarios are upgrades of 5G scenarios, so we consider 6G scenarios to extend them by considering some of the 5G scenarios. We are inspired by 5G to calculate the "write" and "read" speeds for such scenarios in 6G.

Finally, we compare the calculated "read" and "write" transaction speeds with the maximum "read" and "write" transaction speeds of the blockchain transactions. If the "read" and "write" performance of the blockchain system meets the scenario, then the scenario can be considered for the blockchain.

4.2 Transaction arrival model

With our methodology, in Tables 2 and 3, we first analyze what and when to use blockchain in seven scenarios. Different scenarios and different times require different transaction types, so we divide blockchain transactions into "reads" and "writes".

• For the sake of brevity, the transaction query operation is referred to as "read" while the operation of originating and recording.

• For write operations, we need to change the state of the blockchain and wait for multiple nodes to reach consensus. so write transactions can only be done sequentially.

Table 2 6G scenario analysis based on blockchain: scenario 1–4 (W for write transaction; R for read transaction)

	Use cases	Why on-chain? Benefits?	What is recorded on chain? I.e., transaction definition	When is the transaction generated/query?
1 Public key management	Subscribers' public key management	• Decentralization, i.e., avoid centralized PKI; • Tamper-proof ensures the authenticity of public key; • Provide public key to the 3rd party to authenticate the user.	• Transaction content: {Hash(ID): Pseudonyms} • Transaction is digitally signed by operator's private key	• When an end user subscribes to the network provider. (W) • User query, operator query. (R)
	Network equipment's public key management	• Decentralization, i.e., avoid centralized PKI; • Tamper-proof ensures the authenticity of public key; • Provide public key to the 3rd party to authenticate the user.	• Transaction content: {Hash(NEID): Public key} • Transaction is digitally signed by operator's private key	• When network equipment is onboard. (W) • operator query. (R)
2 ID management	Pseudo-name management	• User's public key is endorsed by the central authority-authenticity. • Auditable users' behavior	• Transaction content: {pseudo-name: pseudo} • Transaction is digitally signed by central authority who creates the pseudo-name	• When the pseudo-name is created by central authority. (W) • When the pseudo-name is queried. (R)
	Decentralized ID (DID)	• publicly accessible, Transparent. • Trusted attestation.	• Identifiers and use schemas	• When the DID is created by central authority. (W) • When the identifier is verified. (R)
3 Authentication, authorization, and access control	Authentication	Traceable & auditable records of user's subscription data access activities as required by GDPR or PIPL	The data activity of inquiring the subscriber's data (subscriptions, profiles)	When a service request is initiated. (R & W)
	Authorization		The data activity of inquiring the subscription profile	When a specific service request. (R & W)
	Access control		The data activity of inquiring the user data which is not include in subscription profile.	When a 3rd party or a network function access to the user's data. (R & W)
4 Context	personal context information context		The data activity of inquiring the subscription profile and updating/deleting the context.	When a network function access to user's subscription data, or update/delete the context. (R & W)
	Location information		Location information access log.	When a 3rd party or a network function access to the user's data. (R & W)

Next, we pick a model for the transaction arrival rate, before that we clarify the following concepts.

• η – the number of concurrent events (CCE) refers to the total number of events that simultaneously occur. Different scenarios or use case has different CCE. CCE can be calculated based on some assumptions or can be observed through traffic monitoring on the real network.

• α – the number of "read" transactions. It is the number of query operations in a given scenario.

• β – the number of "write" transactions. It is the number of operations that record transactions in a given scenario on the blockchain.

In our case, traffic refers to blockchain transactions proposed or generated by the programs of the different scenarios we analyzed in Section 3. For all scenarios and use cases, the Poisson model is a good choice. In this model, the interarrival times have the following characteristics.

(1) They are independent.

(2) They are exponentially distributed, i.e., probability density function.

We assume that the seven scenarios listed satisfy the above two characteristics [63]. Therefore the inter-arrival times are exponentially distributed with a rate parameter λ:

$$p\{A_n \leqslant \lambda\} = 1 - \exp(-\lambda t). \tag{1}$$

The rate parameter λ is determined by the number of the "read" or "write" transactions performed

Table 3 6G scenario analysis based on blockchain: scenario 5–7

	Use cases	Why on-chain? Benefits?	What is recorded on chain? I.e., transaction definition	When is the transaction generated/query?
5 Data management & data trading	Subscription data	GDPR/PIPL, including forgettable/erasable	• Hash/address of the off-chain stored subscription profile • For removing data: the action of removing the off-chain data • For update: the action of updating the offchain data	• User subscribes to the service provided by network provider. (R & W) • User change his/her subscription. (R & W) • User de-register his/her service from the. (R & W) network provider. • User update his/her subscription. (W)
	AI model data	• Tamper-proof • Defend poison attack • Eliminate SPOF (e.g., the aggregator), mitigate the DDoS attacks (targets at centralized aggregator)	• The hash of the model data (on-chain/offchain) • Encrypted model data (on-chain store AI model data)	• When the model training is completed. (W) • When the gradient update is completed. (W) • Retrieve the model/gradient. (R)
	IoT data	• Privacy preserving, traceable, auditable • Avoid the problem of 'BC bloat'	Hash of raw data	• Periodically store the streaming/time series data. (W) • Audit and trading/sharing (R)
	Sensing data	• Auditability • Data sharing (automatic trading)	Hash of the sensing data	Periodically store the streaming/time series data. (W)
	Data trading/sharing	• Automatic trading (SC) • Trusted data source • Data cooperation	Data package exchanged between data owner and data requester	Data is shared or exchanged when the trading occurs. (R&W) • Audit (R)
6 Resource sharing	Spectrum	• Automatic settlement (via SC) • Automatic auction (via SC)	• Spectrum resource status • Geographic information is included	• When available spectrum is published. (W) • Trade deal (W) • Revoke (W) • Audit (R)
	Computing resource		• Computing resource status • Geographic information is included • Per device/NF/MEC/DC	• When available computational resource is published. (W) • Trade deal (W) • Revoke (W) • Audit (R)
	Network sharing (RAN, CN, etc.)	Precise, near-real-time (record), trusted automatic settlement (via SC) • Auditable • Tamper-proof	Hash of the following information needs to be recorded on-chain • User's network usage • NE's resource provision status	• When settlement occurs (W) • batch Log information (W) • Audit (R)
7 Trading & settlement	Interconnection settlement	• Auditable usage • Automatic settlement (via SC)	• Interconnection traffic volume/usage (per hour) • Settlement (per month)	• Periodic (W) • Per-hour/Perday/month (W) • Audit (R)
	Roaming settlement	• Auditable usage • Automatic settlement (via SC)	• CDR (periodically record on the chain in a batch) • Settlement (per-user) • Per-day/month	• Periodic settlement (W) • Per-hour/Perday/month (W) • Audit (R)
	Billing	Auditable usage	CDR (periodically record on the chain in a batch)	• Per-hour/Perday/month (W) • Periodic settlement (R) • Audit (R)

on the blockchain in a specific scenario or use case and the number of CCE.

$$\lambda_{\text{write transaction}} = \eta \times \beta = \lambda_\beta, \tag{2}$$

$$\lambda_{\text{read transaction}} = \eta \times \alpha = \lambda_\alpha. \tag{3}$$

4.3 Case study of transaction arrival analysis

In this subsection, we focus on the transaction arrival rate of the 6G scenario. Assuming a total number of 30 million subscriptions, we obtain λ_β and λ_α by using (2) and (3). Since the β data comes from existing 5G network operators, here we focus on how many read and write transactions are available for each scenario CCE. Finally, we have selected two typical scenarios to calculate their transaction arrival rates.

Table 4 The transaction arrival rate of 6G scenarios

Scenario	λ_β	λ_α
Public key management	0.0115	–
ID management	347.2	8333
AAA	8333	41665
Context	694.4	9721
Data management & data trading	705.9	9038
Resource sharing	1041.6	9374.6
Trading & settlement	347.2	8333

Due to space being limited, the specific calculations for the remaining scenarios are not given. In Table 4, we provide the values of λ_β and λ_α for the remaining scenarios.

4.3.1 *The transaction arrival rate of public key management*

The read operation in public key management is used in the AAA scenario, and the write transaction is mainly described here. The write transaction is mainly when the user opens an account or when a new device goes online (such as a new base station). There is one write transaction per public key managed CCE (the figure of 0.0015 is from the operator).

$$\lambda_\beta = \eta \times \beta = 0.0115 \times 1 = 0.0115. \tag{4}$$

4.3.2 *The transaction arrival rate of AAA*

Authentication is mainly about verifying the authenticity of the identity. Usually, a query on the chain is sufficient for authentication, so this scenario is a "read" transaction only. Each authentication requires the user to submit a signature for verification. So, only one "read" transaction is required. Authorization is the granting of certain information or rights to another person. It is often necessary to update their authorization information in the blockchain. Therefore, in each authorization, one "write" transaction is required to change the authorization information, and two read transactions are required to verify the information of the authorized person.

Complete access control requires authorization and authentication. Complete access control requires authorization and authentication. The number of authorizations and authentications required varies from one access control to another, so we refer to the FairAccess framework for evaluation [64]. In FairAccess, the complete process requires three authentications and one authorization (the figure of 8333 is from the operator).

$$\lambda_\beta = \eta \times \beta = 8333 \times 1 = 8333, \tag{5}$$

$$\lambda_\alpha = \eta \times \alpha = 8333 \times (1 \times 3 + 2 \times 1) = 41665. \tag{6}$$

5 Experimental evaluation

To confirm our methodology's correctness, ample experimentation is necessary. Utilizing our methodology, we investigate blockchain's benefits in seven scenarios, clarifying the reasons and timing for its use. We select the Quorum blockchain for evaluation, assessing both its fundamental performance and transaction arrival model. At this stage, theoretical results are derived by comparing data in Table 5 with our experimental findings. Comparing experimental results with theoretical ones validates the feasibility and accuracy of our methodology.

5.1 Security model

Before continuing, we provide a summary of our security model. Our model is based on the following assumptions:

- The network is semi-synchronous.
- The system consists of a fixed set of N nodes (servers). A subset of at most f nodes are Byzantine, and $N \geqslant 3f + 1$. It is known that N and f are protocol parameters.
- By the use of public key cryptography, messages are verified. The public keys are known to everyone.

Table 5 Our methodology evaluates blockchain's performance for 6G scenarios

Scenarios	Meets the write performance	Meets the read performance
Public key management	√	–
ID management	√	√
AAA	×	×
Context	√	√
Data management & data trading	√	√
Resource sharing	√	√
Trading & settlement	√	√

5.2 Experiment setup

5.2.1 *Consensus Quorum*

We choose blockchain based on the following 3 principles:

- Module Blockchain. This gives us more flexibility in configuring the blockchain.
- Abundant community support. Higher community supported products have better robustness.
- More components are available. Convenient for us to do research.

Summing up the above points, we choose the Quorum blockchain as the base environment for our experiments. It offers unified control over infrastructure management and blockchain network governance. Quorum's compatibility with Ether-related components yields improved results in our experiments. Upon investigating Quorum's performance, we find it meets our requirements [65]. Furthermore, our comprehensive performance and storage evaluation of Quorum yields even more favorable results.

In the context of 6G, a blockchain architecture with high concurrency and performance is essential. Within Quorum, we select the Byzantine fault tolerance (BFT)-style consensus algorithm IBFT. Our choice is driven by IBFT's robust fault tolerance and superior performance compared to other BFT algorithms [66]. Additionally, IBFT's effectiveness is validated by rigorous mathematical proofs.

5.2.2 *Cloud setup*

In each experiment, we deploy N consensus nodes in cloud-based virtual machines. Each virtual machine features a 4-core, 8-thread 2.6 GHz CPU, 16 GB RAM, and 100 GB of storage. The round-trip latency between any two virtual machines averages around 30 ms. These cloud servers are respectively deployed in Shanghai, Beijing, Guangzhou, Guiyang, and Ulanchabu.

5.3 Performance metrics

This paper primarily focuses on the system's storage, latency, performance, and resource costs. Concurrently, we distinguish between "read" and "write" operations, assessing their performance individually. We categorize the experiments into two groups: evaluations of "read" and "write" performance.

- Storage. Refers to storing scenario data on the blockchain network. The network must have enough storage capacity to accommodate the growing volume of data.
- Latency. The time required for the network to process and validate a transaction. Lower latency ensures quicker processing and a more efficient network. Transactions per second (TPS): the rate at which the blockchain network processes transactions. It encompasses (a) read transaction throughput and (b) write transaction throughput. Higher TPS signifies greater network efficiency and capacity to manage more transactions.
- Resource costs. Primarily focuses on memory and computational resource consumption.
- Scalability. The network's capacity to accommodate a growing number of users and transactions while maintaining performance.

5.4 Experiment result

We utilize Caliper to generate and simulate both read and write transactions for the system.

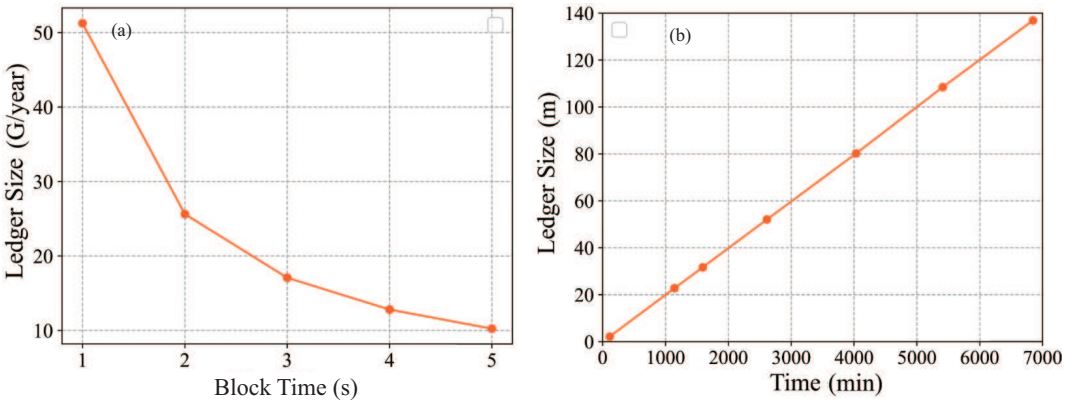

Figure 5 (Color online) (a) Block interval time and ledger size; (b) time and ledger size.

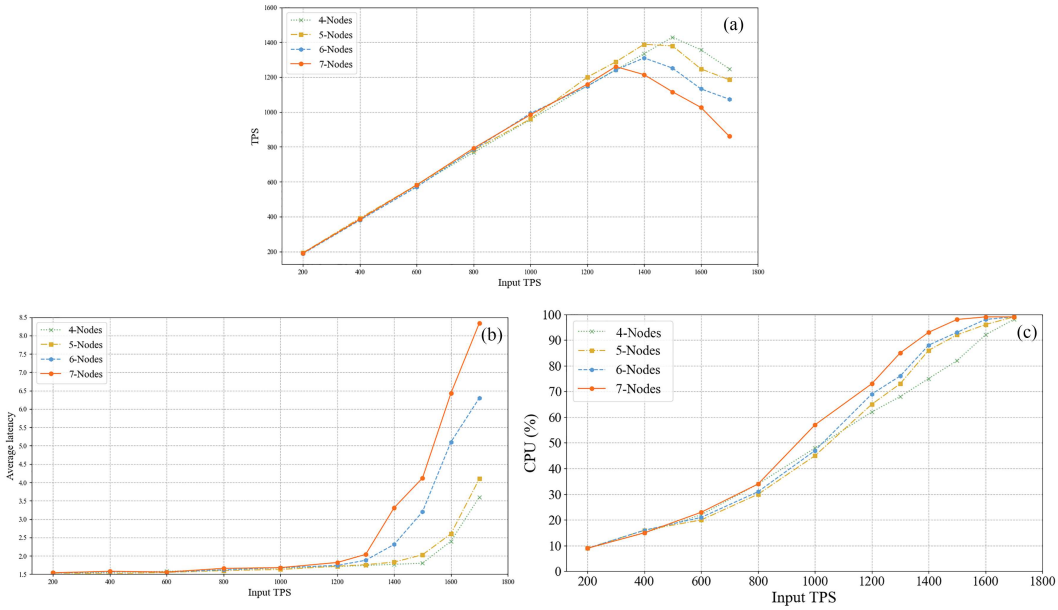

Figure 6 (Color online) (a) TPS; (b) latency; (c) CPU.

5.4.1 *Quorum basic storage performance*

To determine the storage requirements for 6G scenario data, we assess the fundamental storage performance of the Quorum blockchain. We record the ledger size of empty blocks without adding any data. We analyze the correlation between Quorum's block time and storage size, and the interrelation of time with storage size. The relationship between block time and storage is depicted in Figure 5(a). Additionally, Figure 5(b) shows a linear increase in the storage size of empty blocks over time. In our forthcoming storage experiment, subtracting the size of empty blocks from the total storage yields the data size for 6G scenarios.

5.4.2 *Quorum basic performance*

We assess the write performance of the blockchain across configurations with 4, 5, 6, and 7 nodes, as shown in Figures 6(a)–(c). We inject X (100, 200, ..., 1600) TPS into the blockchain. After the blockchain fully confirms these transactions, we obtain the average TPS processed by the blockchain during this period. We statistically calculate the latency generated from the injection to the completion of each transaction and derive the average latency. Finally, we compute the CPU utilization of all nodes at peak load, resulting in three graphs depicted in Figures 6(a)–(c).

Our analysis reveals that the system's TPS increases linearly with the transaction arrival rate until reaching maximum capacity. Beyond this peak, the system deviates from the steady-state (where the

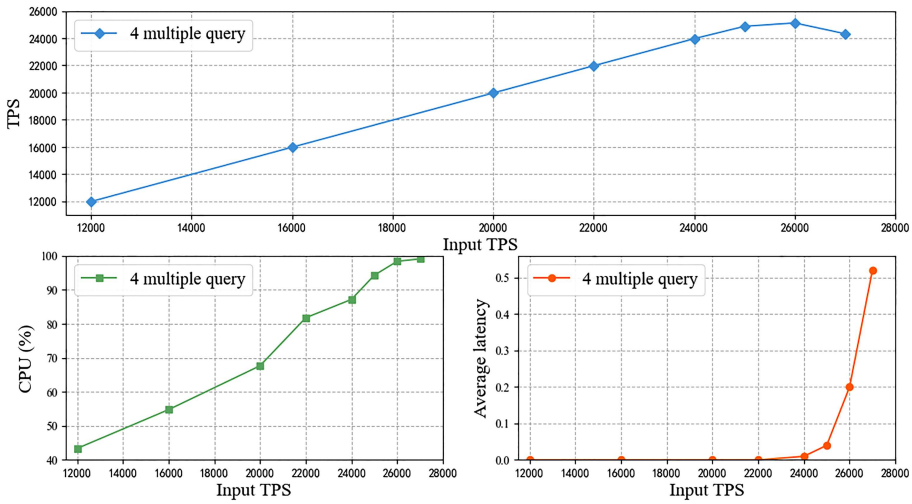

Figure 7 (Color online) Four multiple write.

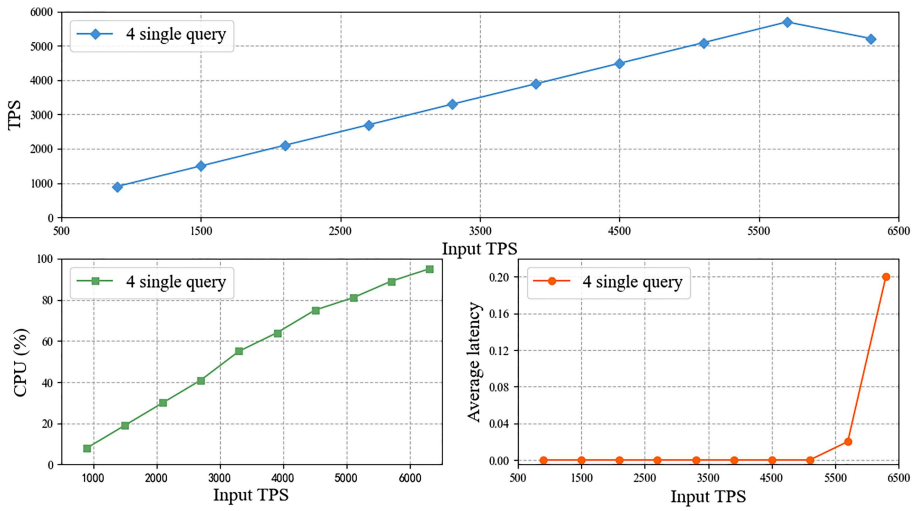

Figure 8 (Color online) Four multiple read.

transaction arrival rate equals the throughput rate), leading to a decline in TPS. Concurrently, as the arrival rate increases, CPU usage and latency also rise. Additionally, with more nodes, we observe a decrease in maximum TPS and an increase in latency, a result of the BFT algorithm's limitations. This indicates that while processing more transactions, the system requires additional resources and time.

In a four-node setup (Figures 7 and 8), we measure TPS, CPU utilization, and average latency for read transactions. Our findings suggest that the blockchain's structure does not limit the query rate; rather, the machine's performance does. Enhancing the read transaction performance could be achieved by increasing the number of non-consensus nodes.

In the Quorum blockchain, as the number of nodes increases, we observe a significant impact on both TPS and latency. Adding more consensus nodes in the future could challenge the blockchain's scalability. With more nodes, the TPS rapidly declines, and latency increases notably, suggesting scalability issues. This raises concerns about whether the blockchain's limited scalability can meet the demands of 6G networks. Interestingly, CPU utilization plateaus beyond a certain point, indicating that the CPU's role in system performance is relatively minor. In contrast, read operations exhibit higher scalability, as they are not constrained by the blockchain. Improving read operation performance may be as simple as upgrading the hardware.

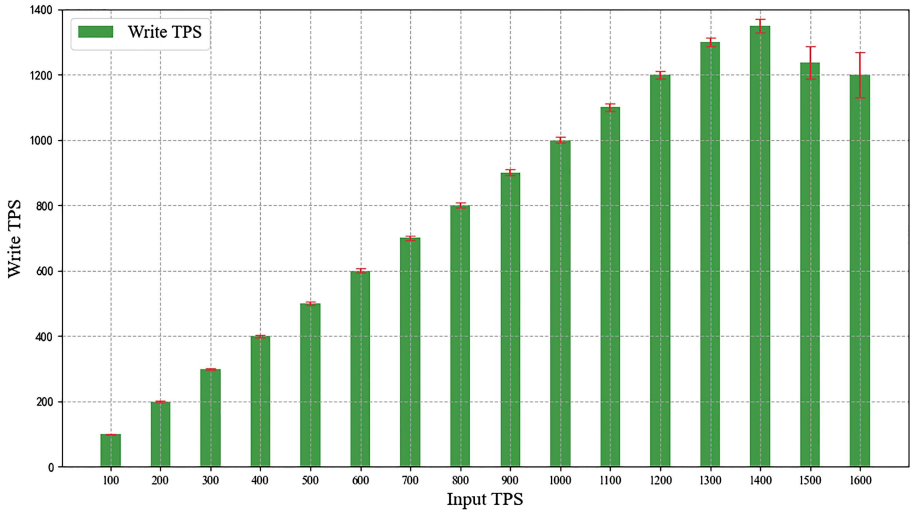

Figure 9 (Color online) Transaction arrival rate (use the Poisson distribution model) vs. 4 node write TPS.

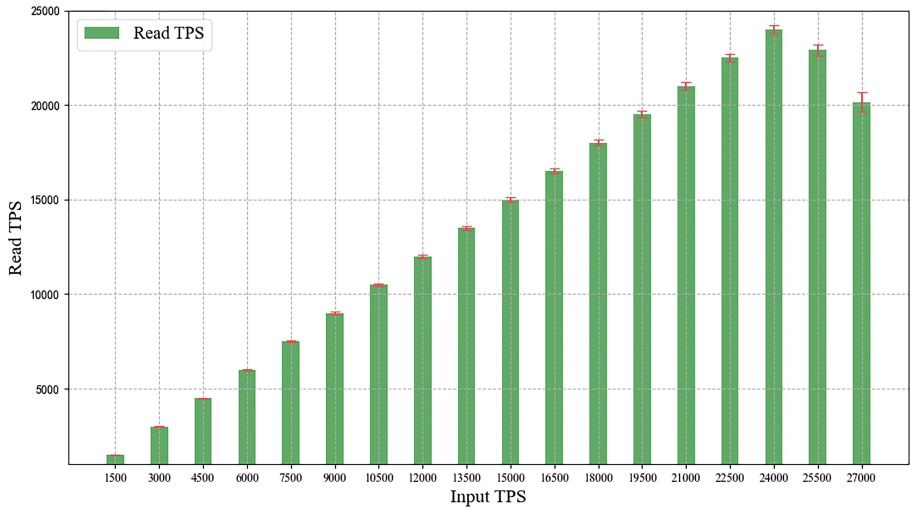

Figure 10 (Color online) Transaction arrival rate (use the Poisson distribution model) vs. 4 node multiple read TPS.

5.4.3 *Quorum Blockchain performance evaluation with Poisson distributed transaction arrival rate model*

For this experiment, we select four nodes for evaluation and divide it into two primary groups: "read" and "write". Each large group of experiments is further divided into multiple groups with different values of λ for each group. We conduct five measurements in each experiment. During each experiment, we inject transactions into the system using a Poisson distribution as the value of λ for ten minutes and record the corresponding average TPS, latency, and resource usage.

As shown in Figure 9, the system achieves maximum throughput when λ_α is equal to 20500 for query transactions. When the value of λ_α for read transactions on the four nodes exceeds 20500, the system performance begins to decline significantly.

As shown in Figure 10, the system achieves maximum throughput when λ_α equals 20500 for query transactions. However, when the input rate of read transactions for four nodes exceeds λ_α of 20500, the system's performance begins to degrade significantly. Compared to Figure 6(a), we observe that the system reaches a steady-state with a value of λ_β slightly lower than the peak. According to the Poisson model, there is a chance that a value greater than λ_β will occur, causing the system's transaction processing rate to be lower than the transaction arrival rate at some point.

Adopting the methodology provided in Section 4, we analyze whether the performance of the Quorum blockchain meets the criteria of the seven major scenarios. Figures 9 and 10 depict the maximum read and write transaction throughputs for the Quorum blockchain using the Poisson distribution traffic arrival model with $\lambda_\alpha = 20500$ and $\lambda_\beta = 1400$, respectively.

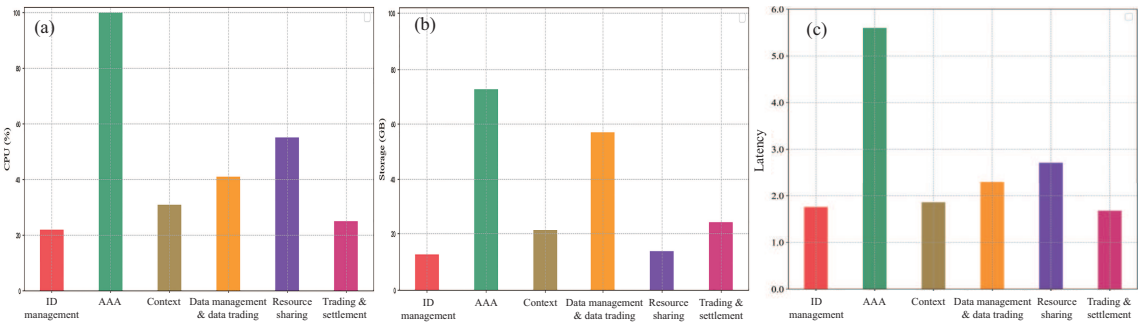

Figure 11 (Color online) (a) Scenario CPU; (b) scenario storage; (c) scenario latency.

In Section 4, we compare the read and write transaction arrival rates to the maximum throughput for the seven scenarios and conclude that our system is well-suited for most cases. For instance, the write transaction rate for the public key management scenario is $\lambda_\beta = 0.0115$, and the Quorum blockchain meets all performance requirements for this scenario.

However, the write transaction rate for the AAA case is $\lambda_\beta = 8333$, and the read transaction rate is $\lambda_\alpha = 41665$, which exceeds the maximum throughput of the Quorum blockchain. Therefore, the Quorum blockchain is not suitable for this scenario. This problem can be addressed by consolidating several transactions into a single one or by scaling the blockchain. We thoroughly investigate the remaining scenarios and found that they can be accommodated by the Quorum blockchain.

5.5 Scenario performance evaluation

To validate the correctness of our methodology, we simulate the performance of 6G scenarios on a blockchain. We measure TPS, storage, CPU, and latency for multiple scenarios respectively. Using data from Table 4 on transaction arrival rates for scenarios obtained from operators, we simulate the real-world performance of these scenarios on the blockchain. Initially, we simulate the performance of various machines in blockchain write transactions across different scenarios, including CPU utilization, storage usage, and system latency. We use a blockchain with four nodes, and Figures 11(a)–(c) show the average performance of these four nodes. Then, we simulate transactions with arrival rates based on a Poisson distribution and measure the throughput of the entire blockchain system for both read and write transactions. As the transaction arrival rates gradually reach their peak in scenarios, we randomly select 100 outcomes for presentation once the system stabilizes. We do not display the values for public key management in the figure because they are too small.

Figure 11(a) displays the CPU usage rates for different 6G scenarios. It can be observed that the CPU consumption in the AAA scenario reaches 100%. The reason for this is that the input TPS in the AAA scenario far exceeds the system's maximum capacity, which results in the system constantly operating under high load. Figure 11(b) shows the storage consumption for multiple scenarios. Generally, scenarios with higher input TPS also have larger data volumes. However, for data management and data transactions, more information is generated due to the complexity of control processes. Lastly, due to the excessively high input TPS, the latency in the AAA scenario is also significantly high, as shown in Figure 11(c). The latency in other scenarios is slightly higher than the write transaction generated by empty blocks due to additional processes and controls.

The experimental results once again corroborate the accuracy of the theoretical assessment in Table 5. As long as the output TPS exceeds the input TPS, we consider that the blockchain meets the requirements of the scenario; otherwise, it does not. Figures 12(a) and (b) show that in the AAA scenario, the input TPS for our write transactions reached 8300, and the input TPS for read transactions reached 41600. However, the system's output TPS for read and write transactions are 1180 and 18643, respectively, clearly not meeting the requirements of this scenario.

Using the methodology, we conclude that all scenarios except for the AAA scenario can be fulfilled by the Quorum blockchain. Our experiments also confirm this, as shown in Figures 12(a) and (b). Due to the excessively high input TPS, the AAA scenario results in an unstable system with significantly larger error values, especially in write transactions where the error value reaches an astonishing 4000. Meanwhile, the system throughput is less than the maximum system throughput because more resources are allocated to resource scheduling, thus reducing the system throughput.

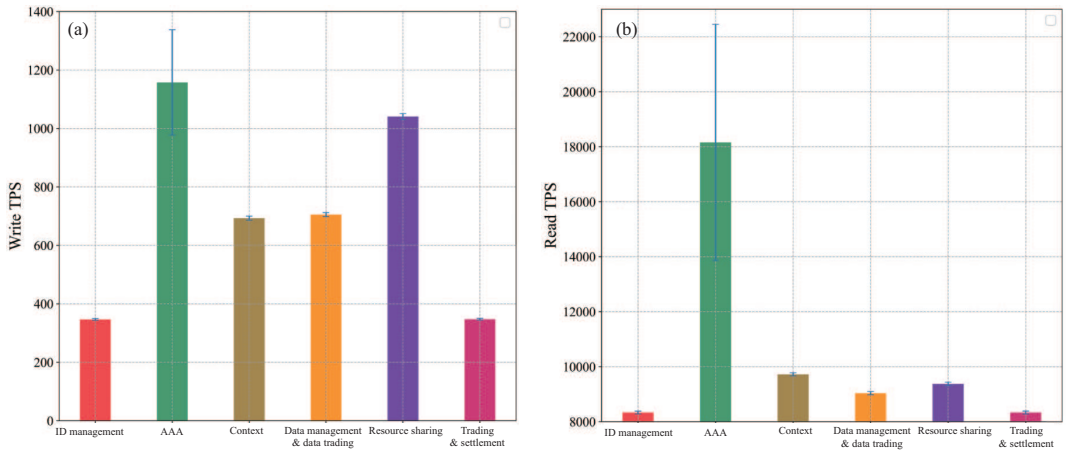

Figure 12 (Color online) (a) Write performance for Poisson distribution; (b) read performance for Poisson distribution.

5.6 Supplement experiment and discussion

Based on our analysis results, we have demonstrated the usability of the methodology. However, it is worth noting that the AAA scenario cannot be fully fulfilled by the Quorum blockchain. To overcome this limitation, we can bundle multiple transactions into a single transaction for uploading. This approach allows us to achieve the primary objective of the AAA scenario, which is traceability and auditability. However, it may require configuring the blockchain or exploring other alternatives to ensure optimal performance.

We conduct additional experiments by bundling 8 transactions from the AAA scenario into a single transaction. The results show that this approach can fulfill the requirements of the AAA scenario on the Quorum blockchain.

In the future, it is possible that multiple 6G scenarios may encounter similar limitations on the blockchain. To address such issues, we can explore various solutions, including configuring the blockchain or exploring alternative approaches. Finally, The aforementioned study indicates that a properly constructed federated blockchain is able to match the performance requirements of a 6G network scenario.

We measure seven scenarios, but find that the Quorum blockchain in the AAA scenario does not meet its performance requirements. However, in supplementary experiments, we address this issue. As we evaluate the performance of all scenarios, we discover that as long as we use and configure the blockchain appropriately, it meets the performance requirements of the vast majority of 6G scenarios. In particular, our experimental results indicate that these performance bottlenecks are not inherently unscalable as user numbers increase. For instance, in scenarios requiring high-concurrency write operations, we scale up servers to accommodate demand. For high-performance write operations, we optimize transaction content and adjust blockchain configurations to address them.

6 Conclusion

The integration of blockchain into 6G is still in its early stages but has attracted increasing interest from researchers and companies. This article analyzes seven 6G scenarios and proposes a methodology for evaluating their usability with blockchain. We investigate the why, how, and when aspects of these scenarios and propose an evaluation method for their usefulness. We also conduct a preliminary evaluation of the Quorum blockchain's performance using a Poisson distribution traffic model for transaction arrival rates. We evaluate 7 6G scenarios, with 6 of them aligning with Quorum blockchain configurations. We bundle multiple transactions into one transaction for the AAA scenario, resulting in Quorum blockchain being able to handle 8333 write transactions. Our experimental results show that a consortium blockchain with the proper settings can meet the performance and scalability requirements of a 6G network.

However, there are still challenges that need to be addressed. Firstly, we have only explored seven 6G scenarios, and there may be other scenarios, such as Telematics and Drones, that could use blockchain. It is essential to investigate more 6G application scenarios and evaluate their usability under blockchain. Secondly, our study only focuses on a single scenario, but a complete blockchain architecture is needed to

integrate all scenarios in a real 6G network. Communication and interaction between different scenarios must also be accomplished within this framework. Therefore, further efforts are crucial for the future of blockchain in 6G.

Acknowledgements This work was partially supported by National Natural Science Foundation of China (Grant Nos. U20A20173, 62125206).

References

1 Chettri L, Bera R. A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems. IEEE Int Things J, 2019, 7: 16–32
2 Xu W, Huang Y M, Wang W, et al. Toward ubiquitous and intelligent 6G networks: from architecture to technology. Sci China Inf Sci, 2023, 66: 130300
3 Hewa T, Gür G, Kalla A, et al. The role of blockchain in 6G: challenges, opportunities and research directions. In: Proceedings of the 2nd 6G Wireless Summit (6G SUMMIT), 2020
4 Nguyen D C, Ding M, Pathirana P N, et al. 6G Internet of Things: a comprehensive survey. IEEE Int Things J, 2021, 9: 359–383
5 Khan A H, Ul Hassan N, Yuen C, et al. Blockchain and 6G: the future of secure and ubiquitous communication. IEEE Wireless Commun, 2021, 29: 194–201
6 Maksymyuk T, Gazda J, Volosin M, et al. Blockchain-empowered framework for decentralized network management in 6G. IEEE Commun Mag, 2020, 58: 86–92
7 Rappaport T S, Sun S, Mayzus R, et al. Millimeter wave mobile communications for 5G cellular: it will work! IEEE Access, 2013, 1: 335–349
8 Giordani M, Polese M, Mezzavilla M, et al. Toward 6G networks: use cases and technologies. IEEE Commun Mag, 2020, 58: 55–61
9 Zhang J Y, Björnson E, Matthaiou M, et al. Prospective multiple antenna technologies for beyond 5G. IEEE J Select Area Commun, 2020, 38: 1637–1660
10 Hajiyat Z R M, Ismail A, Sali A, et al. Antenna in 6G wireless communication system: specifications, challenges, and research directions. Optik, 2021, 231: 166415
11 Tataria H, Shafi M, Molisch A F, et al. 6G wireless systems: vision, requirements, challenges, insights, and opportunities. Proc IEEE, 2021, 109: 1166–1199
12 Wu Q H, Wang W, Li Z G, et al. SpectrumChain: a disruptive dynamic spectrum-sharing framework for 6G. Sci China Inf Sci, 2023, 66: 130302
13 Zeng H, Zhu Z, Wang Y, et al. Periodic collaboration and real-time dispatch using an actor-critic framework for UAV movement in mobile edge computing. IEEE Int Things J, 2024, 11: 21215–21226
14 Gao H, Wang X, Wei W, et al. Com-DDPG: task offloading based on multiagent reinforcement learning for information-communication-enhanced mobile edge computing in the Internet of Vehicles. IEEE Trans Veh Technol, 2024, 73: 348–361
15 You X H. 6G extreme connectivity via exploring spatiotemporal exchangeability. Sci China Inf Sci, 2023, 66: 130306
16 He L, Li F C, Xu H K, et al. Blockchain-based vehicular edge computing networks: the communication perspective. Sci China Inf Sci, 2023, 66: 172301
17 Chaer A, Salah K, Lima C, et al. Blockchain for 5G: opportunities and challenges. In: Proceedings of IEEE Globecom Workshops (GC Wkshps), Waikoloa, 2019. 1–6
18 Nguyen D C, Pathirana P N, Ding M, et al. Blockchain for 5G and beyond networks: a state of the art survey. J Network Comput Appl, 2020, 166: 102693
19 Mistry I, Tanwar S, Tyagi S, et al. Blockchain for 5G-enabled IoT for industrial automation: a systematic review, solutions, and challenges. Mech Syst Signal Process, 2020, 135: 106382
20 Sotenga P, Chuku P, Olwal T. Analysis of IEEE 802.11n network access categories in EDCA non-saturated networks. In: Proceedings of International Conference on Computing, Communication and Security (ICCCS), 2015. 1–6
21 An S Y, Ngayo G, Hong S P. Enhancing 5G antenna manufacturing efficiency and reliability through blockchain and smart contract integration: a comprehensive AHP analysis. Appl Sci, 2024, 14: 2507
22 Qin Z, Deng S, Yan X, et al. 6G data plane: a novel architecture enabling data collaboration with arbitrary topology. Mobile Netw Appl, 2023, 28: 394–405
23 Xu H, Klaine P V, Onireti O, et al. Blockchain-enabled resource management and sharing for 6G communications. Digital Commun Netw, 2020, 6: 261–269
24 Cheng G, Chen Y, Deng S, et al. A blockchain-based mutual authentication scheme for collaborative edge computing. IEEE Trans Comput Soc Syst, 2021, 9: 146–158
25 Jiang W, Han B, Habibi M A, et al. The road towards 6G: a comprehensive survey. IEEE Open J Commun Soc, 2021, 2: 334–366
26 Refaey A, Hammad K, Magierowski S, et al. A blockchain policy and charging control framework for roaming in cellular networks. IEEE Netw, 2020, 34: 170–177

27 Velliangiri S, Manoharan R, Ramachandran S, et al. Blockchain based privacy preserving framework for emerging 6G wireless communications. IEEE Trans Ind Inf, 2022, 18: 4868–4874

28 Wang X, Shankar A, Li K, et al. Blockchain-Enabled decentralized edge intelligence for trustworthy 6G consumer electronics. IEEE Trans Consumer Electron, 2024, 70: 1214–1225

29 Wei Y, Gai K, Yu J, et al. Trustworthy access control for multiaccess edge computing in blockchain-assisted 6G systems. IEEE Trans Ind Inf, 2024, 20: 7732–7743

30 Chaer A, Salah K, Lima C, et al. Blockchain for 5G: opportunities and challenges. In: Proceedings of IEEE Globecom Workshops (GC Wkshps), 2019

31 Chowdhury M Z, Shahjalal M, Ahmed S, et al. 6G wireless communication systems: applications, requirements, technologies, challenges, and research directions. IEEE Open J Commun Soc, 2020, 1: 957–975

32 Manogaran G, Rawal B S, Saravanan V, et al. Blockchain based integrated security measure for reliable service delegation in 6G communication environment. Comput Commun, 2020, 161: 248–256

33 Deb P K, Misra S, Sarkar T, et al. Magnum: a distributed framework for enabling transfer learning in B5G-enabled industrial IoT. IEEE Trans Ind Inf, 2021, 17: 7133–7140

34 Zhao Y, Yang X, Yu Y, et al. Blockchain-based auditable privacy-preserving data classification for Internet of Things. IEEE Internet Things J, 2021, 9: 2468–2484

35 Liu L, Liang W, Mang G, et al. Blockchain based spectrum sharing over 6G hybrid cloud. In: Proceedings of International Wireless Communications and Mobile Computing (IWCMC), 2021. 492–497

36 Hu S, Liang Y C, Xiong Z, et al. Blockchain and artificial intelligence for dynamic resource sharing in 6G and beyond. IEEE Wireless Commun, 2021, 28: 145–151

37 Asheralieva A, Niyato D. Distributed dynamic resource management and pricing in the IoT systems with blockchain-as-a-service and UAV-enabled mobile edge computing. IEEE Int Things J, 2019, 7: 1974–1993

38 Otoum S, Ridhawi I A, Mouftah H. Securing critical IoT infrastructures with blockchain-supported federated learning. IEEE Int Things J, 2021, 9: 2592–2601

39 Nguyen T, Tran N, Loven L, et al. Privacy-aware blockchain innovation for 6G: challenges and opportunities. In: Proceedings of the 2nd 6G Wireless Summit (6G SUMMIT), 2020

40 Yang Y, Wei L, Wu J, et al. A blockchain-based multidomain authentication scheme for conditional privacy preserving in vehicular ad-hoc network. IEEE Int Things J, 2022, 9: 8078–8090

41 Li J, Wu J, Chen L, et al. Blockchain-based secure key management for mobile edge computing. IEEE Trans Mobile Comput, 2021, 22: 100–114

42 Yang K, Sunny J, Wang L. Blockchain-based decentralized public key management for named data networking. In: Proceedings of the International Conference on Computer Communications and Networks (ICCCN 2018), 2018

43 Garzon S R, Yildiz H, Küpper A. Decentralized identifiers and self-sovereign identity in 6G. IEEE Netw, 2022, 36: 142–148

44 Wang D, Cheng H, He D, et al. On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices. IEEE Syst J, 2016, 12: 916–925

45 Feng Q, He D, Zeadally S, et al. A survey on privacy protection in blockchain system. J Netw Comput Appl, 2019, 126: 45–58

46 Bonneau J, Herley C, van Oorschot P C, et al. The quest to replace passwords: a framework for comparative evaluation of web authentication schemes. In: Proceedings of IEEE Symposium on Security and Privacy, 2012. 553–567

47 Wang D, Wang P. On the anonymity of two-factor authentication schemes for wireless sensor networks: attacks, principle and solutions. Comput Netw, 2014, 73: 41–57

48 Wang D, Wang P. Two birds with one stone: two-factor authentication with security beyond conventional bound. IEEE Trans Dependable Secure Comput, 2018, 15: 708–722

49 Wang D, Li W, Wang P. Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. IEEE Trans Ind Inf, 2018, 14: 4081–4092

50 Wang D, Gu Q C, Cheng H B, et al. The request for better measurement: a comparative evaluation of two-factor authentication schemes. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, 2016. 475–486

51 Alam M, Yang D, Huq K, et al. Towards 5G: context aware resource allocation for energy saving. J Sign Process Syst, 2016, 83: 279–291

52 Liu G, Li N, Deng J, et al. 6G mobile network architecture-SOLIDS: driving forces, features, and functional topology.

53 Yaqoob I, Salah K, Jayaraman R, et al. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Comput Applic, 2022, 34: 11475–11490

54 Dai W, Dai C, Choo K K R, et al. SDTE: a secure blockchain-based data trading ecosystem. IEEE Trans Inform Forensic Secur, 2019, 15: 725–737

55 Shi L, Li X, Gao Z, et al. Worm computing: a blockchain-based resource sharing and cybersecurity framework. J Netw Comput Appl, 2021, 185: 103081

56 Hong Z, Wang Z, Cai W, et al. Blockchain-empowered fair computational resource sharing system in the D2D network.

Future Int, 2017, 9: 85
57 Le Y, Ling X, Wang J, et al. Resource sharing and trading of blockchain radio access networks: architecture and prototype design. IEEE Int Things J, 2023, 10: 12025–12043
58 Hamdaoui B, Alkalbani M, Rayes A, et al. IoTShare: a blockchain-enabled IoT resource sharing on-demand protocol for smart city situation-awareness applications. IEEE Int Things J, 2020, 7: 10548–10561
59 Giupponi L, Wilhelmi F. Blockchain-enabled network sharing for O-RAN in 5G and beyond. IEEE Netw, 2022, 36: 218–225
60 Gao Y, Wu W, Si P, et al. B-ReST: blockchain-enabled resource sharing and transactions in fog computing. IEEE Wireless Commun, 2021, 28: 172–180
61 Ali M, Qaisar S, Naeem M, et al. Energy efficient resource allocation in D2D-assisted heterogeneous networks with relays. IEEE Access, 2016, 4: 4902–4911
62 Zhou Z, Chen X, Zhang Y, et al. Blockchain-empowered secure spectrum sharing for 5G heterogeneous networks. IEEE Netw, 2020, 34: 24–31
63 Jain R, Routhier S. Packet trains-measurements and a new model for computer network traffic. IEEE J Sel Areas Commun, 1986, 4: 986–995
64 Ouaddah A, Elkalam A A, Ouahman A A. FairAccess: a new blockchain-based access control framework for the Internet of Things. Secur Comm Netw, 2016, 9: 5943–5964
65 Baliga A, Subhod I, Kamat P, et al. Performance evaluation of the Quorum blockchain platform. 2018. ArXiv:1809.03421
66 Moniz H. The Istanbul BFT consensus algorithm. 2020. ArXiv:2002.03613