



Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/dcan

Blockchain-enabled resource management and sharing for 6G communications

Hao Xu^a, Paulo Valente Klaine^a, Oluwakayode Onireti^a, Bin Cao^b, Muhammad Imran^a, Lei Zhang^{a,*}^a James Watt School of Engineering, University of Glasgow, Scotland, United Kingdom^b Beijing University of Posts and Telecommunications of China, Beijing, China

ARTICLE INFO

Keywords:

6G
Blockchain
Resource management
Network slicing
Wireless blockchain

ABSTRACT

The sixth-generation (6G) network must provide better performance than previous generations to meet the requirements of emerging services and applications, such as multi-gigabit transmission rate, higher reliability, and sub-1 ms latency and ubiquitous connection for the Internet of Everything (IoE). However, with the scarcity of spectrum resources, efficient resource management and sharing are crucial to achieving all these ambitious requirements. One possible technology to achieve all this is the blockchain. Because of its inherent properties, the blockchain has recently gained an important position, which is of great significance to the 6G network and other networks. In particular, the integration of the blockchain in 6G will enable the network to monitor and manage resource utilization and sharing efficiently. Hence, in this paper, we discuss the potentials of the blockchain for resource management and sharing in 6G using multiple application scenarios, namely, Internet of things, device-to-device communications, network slicing, and inter-domain blockchain ecosystems.

1. Introduction

The fifth generation of mobile networks, 5G, is already being commercialized in some parts of the world, with the expectation of addressing limitations of current cellular systems and providing an underlying platform for new services to emerge and thrive [1]. 5G was envisioned to be not only a faster 4G, but also an enabler for several other applications, such as the Internet of Everything (IoE), industry automation, intelligent transportation, and remote healthcare, to name a few, by providing ultra-high reliability, latency as low as 1 ms, and increased network capacity and data rates [2]. However, despite the emergence of new technologies, such as millimeter waves, massive Multiple-Input-Multiple-Output (MIMO), and the utilization of higher frequency bands, it is clear that 5G will not be able to attend all of these requirements, albeit improving significantly from its predecessors. As such, research has already shifted towards the next generation of mobile networks, 6G [2–5].

It is expected that by 2030 our society will shift towards a more digitized, data-driven and intelligently inspired society that needs a near-instant and ubiquitous wireless connectivity [4,6]. Thus, several novel applications that provide such interaction and integration are bound to

emerge in the next decade [4]. As such, some key trends that are foreseen to emerge in the near future are: virtual and augmented reality, 8K video streaming, holograms, remote surgery, the industry 4.0, smart homes, fog computing, artificial intelligence integrated services, Unmanned Aerial Vehicles (UAV), and autonomous vehicles, to name a few [4,5,7]. These, by their turn, will demand much more from mobile networks in terms of reliability, latency and data rates than 5G, and its improvements can support [2,4,5]. As such, several research initiatives around the globe have been working to shape the direction of 6G, and some of its key requirements are already being speculated, as in Refs. [2–4]:

- Provide peak data rates of at least 1 Tb/s and latency of less than 1 ms;
- Support user mobility up to 1000 km/h;
- Operate in GHz to THz frequency range;
- Increase the network spectral efficiency, energy efficiency, and security;
- Harness the power of big data, enabling a self-sustaining wireless network;
- Support for a massive number of devices and things, enabling the IoE.

* Corresponding author.

E-mail addresses: h.xu.2@research.gla.ac.uk (H. Xu), Paulo.ValenteKlaine@glasgow.ac.uk (P.V. Klaine), Oluwakayode.Onireti@glasgow.ac.uk (O. Onireti), caobin65@163.com (B. Cao), Muhhammad.Imran@glasgow.ac.uk (M. Imran), Lei.Zhang@glasgow.ac.uk (L. Zhang).<https://doi.org/10.1016/j.dcan.2020.06.002>

Received 17 January 2020; Received in revised form 30 May 2020; Accepted 4 June 2020

Available online 15 July 2020

2352-8648/© 2020 Chongqing University of Posts and Telecommunications. Publishing Services by Elsevier B.V. on behalf of KeAi Communications Co. Ltd. This is an

open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

According to Shannon's information theory, in order to achieve all of the above and increase the system's total capacity, two different approaches are feasible: either increasing the system bandwidth or improving the spectral efficiency [4,8,9]. It is well-known that spectrum management is a key to efficient spectrum utilization, but there are still some problems. For example, it is known that current fixed paradigms for spectrum assignment and resource management is a major challenge in mobile networks. This will become even more challenging in 6G, due to the ever-growing number of subscribers and their need for intermittent connectivity as well as the development of more data-hungry applications. Moreover, a number of studies have shown that although fixed spectrum allocation is not so complicated, the spectrum efficiency is low since license holders of that spectrum do not utilize it all the time (see Ref. [8] and references therein).

Several approaches have been proposed to improve spectrum management, such as Opportunistic Spectrum Access (OSA) or auction mechanisms. Despite the advantages of these approaches, they still have problems in terms of security, high computing power, and convergence. Most importantly, even if such protocols provide some collaborations at the system level, the collaboration between users is still not considered, which hinders the overall performance of those solutions. As 6G is expected to be much more cooperative than its preceding generations, with new technologies, such as wireless power transfer, mobile edge computing, the IoE, and Device-to-Device (D2D) communications, heavily relying on the cooperation between devices, novel approaches that do not rely on a central authority controlling spectrum and resource management, such as the blockchain, are needed [2,3].

Due to its inherent characteristics, the blockchain is being regarded as the next revolution in wireless communications, with even the Federal Communications Commission (FCC) emphasizing the crucial role that it can play in 6G and beyond [10]. The main idea behind the blockchain is that of an open and distributed database (ledger), where no single party has control, and transactions¹ are securely recorded in blocks. Each block is chained together to its predecessor in a sequential, verified, and secure manner, without the need of a trusted third party. As such, the blockchain is expected to revolutionize resource management and spectrum sharing by eliminating the central authority and replacing it with a distributed one to realize asset transactions without central authorization, improve network security, and reduce costs [11,12].

This integration between wireless networks and the blockchain will allow the network to monitor and manage spectrum and resource utilization in a more efficient manner, reducing its administration costs and improving the speed of spectrum auction. In addition, due to its inherent transparency, the blockchain can also record real-time spectrum utilization and massively improve spectrum efficiency by dynamically allocating spectrum bands according to the dynamic demands of devices [9]. Moreover, it can also provide the necessary but optional incentive for spectrum and resource sharing between devices, fully enabling new technologies and services that are bound to emerge [12]. Furthermore, with future wireless networks shifting towards decentralized solutions, with thousands of cells deployed by operators and billions of devices communicating with each other, fixed spectrum allocation and operator-controlled resource sharing algorithms will not be scalable nor effective in future networks. By designing a communications network coupled with the blockchain as its underlying infrastructure from the beginning, 6G and beyond networks can be more scalable and provide better and more efficient solutions in spectrum sharing and resource management. Moreover, with privacy in mobile networks becoming more and more critical, due to the emergence of novel applications, such as automated vehicles, industry 4.0 and medical applications, where even a minor failure can lead to disastrous consequences, the blockchain

can be of great advantage in securing and storing sensitive information. Since all information in a blockchain is verified by all peers and is immutable, the future mobile network can permanently record all events with its corresponding time-frame [8].

Compared with other papers in this field, which analyze the impact of applying blockchain in wireless networks and spectrum management [8–10], in this article, we dive deeper into the field of blockchain-enabled resource sharing and spectrum management. Based on that, in this paper, it is envisaged that 6G-enabled blockchain resource management, spectrum sharing and computing, and energy trading can serve as the driving force for future use cases. These resources are considered to be in a resource pool, in which spectrum is dynamically allocated, network slices are managed, and hardware is virtualized in order to enable the blockchain resource, and spectrum management. Based on this envisioned framework, a discussion on how the blockchain can enable resource sharing between devices, such as energy, data, spectrum lease, and computing power, is presented. In addition, the motivation to utilize the blockchain for different use-cases is highlighted, mainly in terms of the Internet of things (IoT) and D2D communications, network slicing, and network virtualization. Lastly, some future trends expected in the realm of blockchain-enabled wireless networks are discussed, and conclusions are drawn.

The remainder of this paper is organized as follows. Section 2 presents an overview of current spectrum management, allocation techniques, and a link between the blockchain, and spectrum management. Section 3 discusses the motivations behind blockchains and outlines its fundamentals. Section 4 discusses some key applications of the blockchain and how it can transform current wireless networks. Lastly, Section 5 concludes the article.

2. Spectrum management

In order to meet the growing demand for high data rate for 5g and above applications, the capacity of the networks must be increased. Hence, there is also an increase in the demand for spectrum. A dynamic policy for managing the spectrum license has recently been proposed to manage the spectrum efficiently [13]. It allows unlicensed secondary users to opportunistically access the licensed spectrum without interfering with the licensed primary user. One of the options for using the new spectrum license is to distribute operation parameters to policy-based radio via a database. Such a model has been established for sharing the Television White Space (TVWS), and the Citizen Broadband Radio Service (CBRS) [14]. Recently, the application of the blockchain as a trusted database has emerged [15]. Various information, such as spectrum sensing and data mining results, spectrum auction results, spectrum lease mappings, and the idle spectrum information, are safely recorded on the blockchain. Blockchain thus brings new opportunities to Dynamic Spectrum Management (DSM) [9,10,15], and it has recently been identified as a tool to reduce the administrative expenses associated with DSM [16]. In particular, the blockchain features can improve conventional spectrum management approaches, such as spectrum auction [8]. Further, the blockchain can help overcome the security challenges and the lack of incentives related to DSM [15]. Since the blockchain is a distributed database, it borrows this property, so that the records in the DSM system are recorded in a decentralized manner.

One of the key applications of the blockchain in spectrum management is to record its information. Note that the blockchain can record information as transactions, while spectrum management relies on databases, such as the location-based database, for protecting the primary users in the TVWS [17]. With the blockchain, information about spectrum management, such as 1) the TVWSs, 2) spectrum auction results, 3) the spectrum access history, and 4) the spectrum sensing outcomes, can be made available to the secondary user. As such, the benefits of recording the spectrum management information with the blockchain are discussed here:

¹ These transactions can mean anything, such as holdings of a digital currency (i.e., Bitcoin), movement of goods across a supply chain, spectrum and resource allocation in wireless networks, etc. [9].

- Contrary to conventional third-party databases, the blockchain enables users to directly control the data in the blockchain, thus guaranteeing the accuracy of the data. In particular, information on TVWS, and other underutilized spectra can be recorded in a blockchain. Such data could include the usage of the spectrum in frequency, time, and the geo-location of TVWS, and the primary users' interference protection requirement.
- By effectively managing the mobility of secondary users and the changing traffic demands of primary users, the spectrum utilization efficiency is improved. This is supported by the decentralized nature of the blockchain with primary users recording information on the idle spectrum, which can be readily accessed by unlicensed secondary users. Moreover, secondary users can make their arrival in the network or departure from it known to other users by initiating a transaction.
- Access fairness can be achieved with blockchain-based approaches, where the access history is recorded. This is not the case with the traditional Carrier Sensing Multiple Access (CSMA) schemes, where their access is not coordinated. Access can be managed in the blockchain via smart contracts, where a threshold is defined, and users can be denied access to a specific band for a specified period when they reach the predefined access threshold.
- Blockchains provide a secure and verifiable approach to record information related to spectrum auction. Spectrum auction has been established as an efficient approach for the dynamic allocation of spectrum resources [18]. The benefits of the blockchain-based approach include: 1) it prevents frauds from the primary users by providing transparency; 2) it guarantees that the auction payments are not rejected because all transactions are verified before they are recorded on the blockchain; 3) it prevents unauthorized secondary users from accessing the spectrum since all secondary users can cooperatively/collaboratively supervise, and prevent such unauthorized access.

In [9], the authors explored the applications of the blockchain in spectrum management, including primary cooperative sharing, secondary cooperative sharing, secondary non-cooperative sharing, and primary non-cooperative sharing. Moreover, in Ref. [19], the authors utilized a blockchain verification protocol for enabling and securing spectrum sharing in cognitive radio networks. The spectrum usage based on the blockchain verification protocol was shown to achieve significant benefits compared with the traditional Aloha medium access protocol. The authors in Ref. [20] proposed a privacy-preserving secure spectrum trading and sharing scheme based on the blockchain technology for Unmanned Aerial Vehicle (UAV)-assisted cellular networks. Furthermore, in Ref. [21], the authors proposed a consortium blockchain-based resource sharing framework for V2X, which couples resource sharing and consensus process together by utilizing the reputation value of each vehicle. In Ref. [10], the authors proposed the integration of the blockchain technology and Artificial Intelligence (AI) into wireless networks for flexible and secure resource sharing.

3. Benefit of using the blockchain

3.1. Blockchain basis

Blockchain plays an important role in the cryptocurrency and ledger keeping industry. Due to the vitality of the community, the technology has gained much attention from policymakers, mobile operators, and infrastructure commissioners [22]. Blockchains are distributed databases organized using a hash tree,² which is naturally tamper-proof and

irreversible [24]. It has the attribute of adding distributed trust, and it is also built for enabling transaction consistency in a database. Furthermore, the blockchain allows for atomicity, durability, auditability, and data integrity [25]. Besides the nature of its chain-link data structure, the Consensus Mechanism (CM), which ensures an unambiguous ordering of transactions, and the integrity and consistency of the blockchain across geographically distributed nodes, is of great importance to blockchains. The CM largely determines the performance of the blockchain system, such as transaction throughput, delay, node scalability, and security level, etc. As such, depending on application scenarios and performance requirements, different CMs can be considered. Commonly used CMs include Practical Byzantine Fault Tolerance (PBFT), Proof of Work (PoW), or Proof of Stake (PoS), and the detailed analyses of performance and security of consensus, and how they can be used in different resource management and sharing scenarios are presented in Section 3.2.

The blockchain opens up a transparent and distributed information reform, which can benefit all aspects of the industry and adapt to the centralization of all scopes using different CMs. In the perspective of using the blockchain technology in 6G, the large-scale deployment of the blockchain may take the communication industry and all other economic sectors a big step forward.

The transparent information flows on the blockchain are valuable assets for users, operators, and service providers and societies. In social practice, the authority has always attempted to grip every detail for every operation and transaction. However, it would never track down every happened transaction if they are not born to be recorded. The blockchain is an ideal tool for tracking transactions if the blockchain native transactions are de facto in panoptic scenarios. The blockchain native resources and assets will stimulate a new era of information revolution. Such reform will significantly improve the efficiency and security of the system due to the improvement of public order [32]. It enables the Infrastructure as a Service (IaaS), Blockchain as a Service (BaaS) [33] to spread out in terms of feasibility, and now the infrastructure can be organized in a distributed way by allowing the infrastructure transactions without further centralized management.

Later, such an ecosystem incubates the Blockchain as an Infrastructure (BaaS), which provides a solid tool-chain for settlements between the producer, the trader, and the consumer, as shown in Fig. 1. As seen in Fig. 1, blockchains can be used as the information backbone of a locally distributed resource management system that organizes the customers and producers in an open, transparent market, breaking the information barriers to publicize the resources and accelerate the process of transactions.

The blockchain has incubated the new horizon of resource trading for fixed assets, such as licensed spectrum and computing hardware. In our proposed blockchain 6G resource management scheme, trade-able spectrum and computing resources are integrated parts of the resource pool, where spectrum is dynamically allocated, and network slices are managed, and the hardware is virtualized to facilitate blockchain-enabled resource management. The automated blockchain-enabled resource management relies on the programmable blockchain functionality, which in most cases is described as a smart contract.³ The contract's content is transparent for both public and agreement-making parties, making it publicly traceable. The virtual machine concept is used for the execution of smart contracts, where the code will be executed by a node on the virtual stack, and its results will be stored on the chain as transaction records. The temper-proof ability and fully automatic process give the contract a high degree of immutability against breaches of the contract and misrepresentations.

² A hash tree or Merkle tree is a tree in which every leaf node is labeled with the hash of a data block, and every non-leaf node is labeled with the cryptographic hash of the labels of its child nodes [23].

³ The smart contract is essentially an executable program code stored on the chain, representing terms of agreements triggered automatically when certain conditions are met [34].

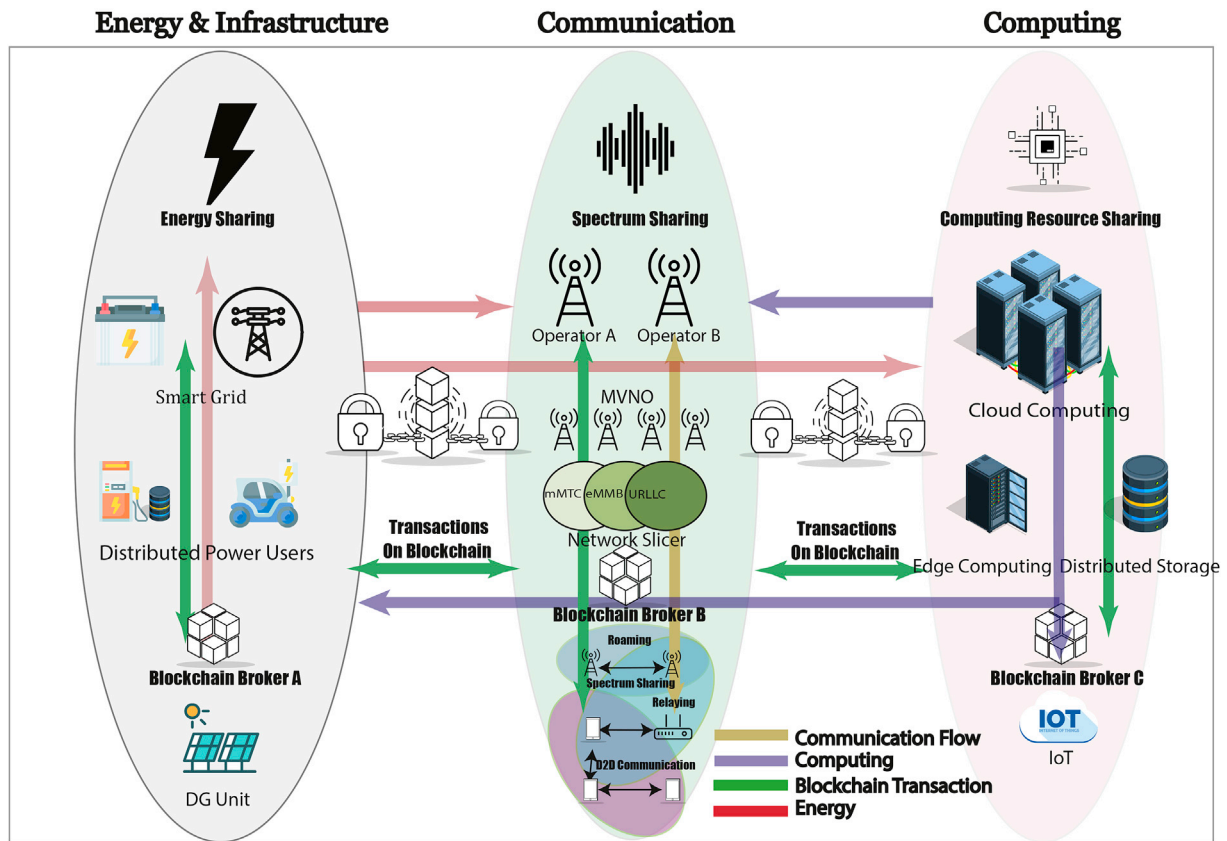


Fig. 1. Blockchain-enabled resource management framework.

3.2. Impact of consensus and security performance

If the impressive and resistive data structure of the blockchain is the facade of a building, the consensus is the pillars. Blockchain has various options on the CM. Choosing a suitable consensus for 6G resource management is the most critical step of making a secure and efficient blockchain system. The CM, which ensures an unambiguous ordering of transactions and the integrity and consistency of the blockchain across geographically distributed nodes, is of importance to blockchains since it determines its performance in terms of TPS, delay, node scalability, security, etc.

According to the access criteria, the chain can be divided into the public chain and private one. The public chain is permission-less, which uses proof-based consensus to provide a secure, reliable network for every participant without requiring their identities at entry points. In the 6G resource pool, there are potential anonymous clients and providers on an ad-hoc basis [4]. The benefit of adopting a public chain is significant for ad-hoc networks, where the barriers of identification and security are broken down for panoptic information exchanges. As such, public chains can potentially promote the efficiency of the community and regulate the order of participants [32]. However, if participants are concealed, violations and malicious activities will pose threats to the system. The consortium/private chain, in contrast, is permitted, which means that the entry is controlled. It has a rather stable community composition, where the identity of the participant is not kept secret. The network faces fewer threats from unknown attacks, but has challenges within the network, for instance, the malicious byzantine node.⁴

⁴ A byzantine node is a malicious node that conceals its existence, and tempts the consensus, which tampers with the security of the network.

Before adapting to any new technologies, security and reliability are always the first concerns. Blockchain technology is born to be superior to existing solutions in terms of security performance and robustness. Table 1 shows the comparison of CMs widely used in the blockchain in six aspects: latency, TPS, complexity, security, energy consumption, and scalability. As can be seen, private/consortium consensus shows better latency, TPS, and energy consumption performance alongside lower ability to scale up; however, the applied application prioritizes latency and TPS over scalability. On the other hand, proof-based mechanisms have decent performance in scalability, but at the expense of latency and TPS. In some cases, like proof of work, it also consumes a huge amount of power. However, their good scalability enables them to grow fast in the public network without being affected by the surge of users, which makes them perform well in mass market transactions and distributed file storage system. Regarding the security performance, it is worth noting that the non-byzantine consensus is assumed to be non-malicious activities, but the byzantine consensus is not only tolerant of inactivity but also tolerant of false and erroneous messages. PBFT functions with less than $(n-1)/3$ byzantine nodes, and some variants of PBFT provide higher tolerance with trades-off of latency, such as multi-layer PBFT [35].

Besides the consensus of ensuring that the blockchain is free from top-level threats, the communication links should be strengthened to prevent external security breaches. The wireless communication is in peril of jamming and spoofing because of open channels. In the practice of wireless blockchain network, the communication failure will result in the node failure, thus lowering the security level. To mitigate the transmission success rate, a collision-avoidance mechanism, such as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) and physical layer security, can be considered.

Table 1
Comparison of blockchain consensus.

Consensus	Suitable Type of Blockchain	Latency/TPS	BFT*	Communication Complexity ¹	Security Threshold ²	Energy Usage	Scalability
PBFT	Consortium/Private	Low/High [26]	Yes [26]	$O(n^2)$ [26]	33% [26]	Low	Low [26]
RAFT	Consortium/Private	Very Low/Very High [27]	No [27]	$O(n)$ [28]	50% [27]	Low	Medium [28]
PoW/PoS	Public	High/Low [29]	Yes [30]	$O(n)$ [29]	50% [29]	High	High [29]
Proof of Storage	Public	High/Low [31]	Yes [30]	$O(n)$ [31]	50% [31]	Low	High [31]

* The ability to tackle byzantine fault.

¹ n indicates the number of participants.

² The given percentage stands for the maximum acceptable faulty nodes or attack.

4. Application scenarios

4.1. IoT and D2D communications

The IoT is an example which envisions that all of our daily objects and appliances will be connected to each other, collecting and sharing information. This will allow for the automation of specific tasks and enable the emergence of other applications, such as smart homes, smart transportation, wearable devices, smart farming, healthcare, and machine-to-machine communications, etc. [36]. In order to achieve such automation and growth, it is necessary to have proper standards and protocols for IoT devices. However, current solutions still rely on a centralized model, which incurs a high maintenance cost for manufacturers, while consumers also lack trust in these devices. Combined with the resource constraints of IoT devices, privacy and security concerns as well as poor interoperability among different vendors make IoT a challenging domain [37,38]. Similarly, D2D communications, a paradigm that envisions the communications and share of data between devices, also share similar challenges to the IoT [39]. For example, mobile devices are constrained by battery, while security is an ever-present concern in mobile communications. Moreover, in order to fully realize D2D communications, a proper incentive is needed to trade and share resources, such as power or data, because current D2D paradigms lack the motivation to do so [39].

In this context, the blockchain is an excellent complement to both IoT and D2D communications, as it can provide the underlying infrastructure with improved interoperability, privacy, reliability and scalability [38]. For example, in the context of resource management, blockchains can be used to perform spectrum sharing and record all the spectrum utilization and lease requests [9]. Moreover, it can provide the incentive needed for devices to share and trade resources, as current protocols lack the incentive to do so. Integrating the blockchain into the IoT and D2D, it can provide rewards every time devices share their power or data, allowing for a more cooperative and trusted network environment [22,38]. Moreover, this reward mechanism can also be applied to spectrum sharing, in which whenever a user leases spectrum to another, a reward can be assigned, creating a more collaborative environment and improving spectrum efficiency [8,9]. Furthermore, blockchains can be utilized in the realm of Vehicular-to-Anything (V2X) communications by encouraging vehicles to trade energy or information with each other [10]. In addition, another key aspect of V2X communications is how to guarantee a secure communication between vehicles and Public Key Infrastructures (PKI). In this context, the blockchain can be utilized as the infrastructure to provide secure and private communications to the PKI, or also the communication between PKIs from different vendors [22].

However, despite all of these benefits, the integration of blockchains in the IoT and D2D domains is still challenging [9–11]. In the case of public chains, for example, the decentralized CMs often require extensive computing power from network nodes (such as PoW-based blockchains). This can be a problem as most IoT devices are power-constrained. This is especially true for devices powered by the cellular IoT, which can be deployed in very remote or inaccessible areas, with an expected battery life of more than 10 years [40]. Thus, the utilization of the blockchain in the cellular IoT, especially when

considering the computation of the consensus algorithm, can significantly reduce the life-time of cellular IoT devices, limiting their communication capabilities and effectiveness. As such, it is still unclear how the generation of the PoW could be done when public blockchains are integrated with IoT or D2D communications [38]. Hence, other CMs, such as PBFT, are being proposed in the context of IoT applications [38,41]. Another challenge in integrating the blockchain into small devices comes due to their limited memory capabilities. Since in the blockchain, every node needs to have a record of all the current and previous blocks in the chain, it can be infeasible to store such a huge amount of data in IoT devices. Thus, it is still not clear how the blockchain can be fully integrated into IoT. Moreover, the blockchain still has privacy issues, as other studies have shown, identities of users could be inferred by analyzing transaction patterns[11].

On top of that, it is also known that the blockchain introduces delay due to its decentralized approach and its CMs. As such, this additional delay might also affect the performance of certain wireless communication use-cases, such as in V2X, industrial applications, or D2D, and it is still an area to be investigated. Moreover, in V2X scenarios, information security and resilience are critical since any small failure can lead to catastrophic and even fatal consequences. In those cases, the blockchain can provide an additional security layer for vehicles to perform key management exchange, as in Ref. [42], or even to protect a vehicle's identity and location in what is known as pseudonym management [43]. Lastly, another important challenge in this realm, which has not been largely explored, is how the performance of the wireless link affects the performance of the blockchain [12]. Despite recent works investigating the applicability of the CSMA/CA protocol in wireless blockchain networks [44], or the security performance and optimal node deployment of blockchain-enabled IoT systems [45], more researches are needed in this area.

4.2. Network slicing

Network slicing is an up-and-coming technology in the future cellular architecture, and it is aimed at meeting the diverse requirements of different vertical industry services. Network slicing is a specific form of virtualization that allows multiple logical networks to run on top of a shared physical network infrastructure [46]. A network slice is realized when a number of Virtualized Network Functions (VNF) are chained-based on well-defined service requirements, such as the massive Machine Type Communication (mMTC), enhanced Mobile BroadBand (eMBB) and the ultra-Reliable Low Latency Communication (uRLLC). The management and orchestration of network slices must be trusted and well secured, in particular for accommodating applications that require high security, such as in the case of remote robotic surgery and V2X communications [47].

Network slicing also enables Mobile Network Operators (MNO) to slice a single physical network into multiple virtual networks, which are optimized according to specified business and service goals [48]. Hence the term Mobile Virtual Network Operators (MVNOs) is used. The implementation of MVNOs necessitates the integration of a network slice broker into the architecture, as shown in Fig. 2.

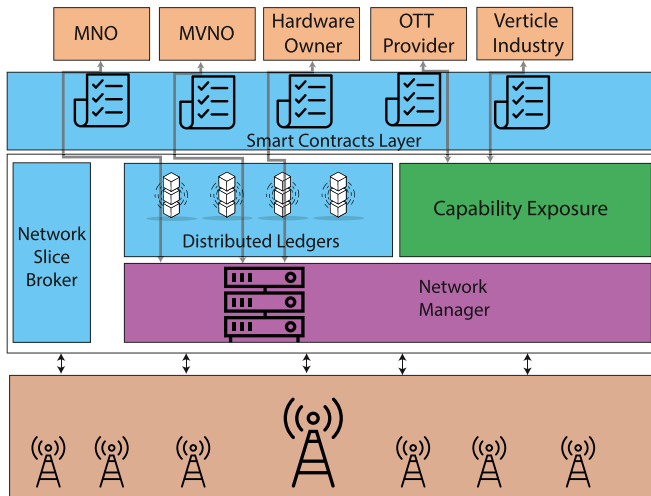


Fig. 2. Spectrum management using the blockchain and smart contract.

4.2.1. Network slicing broker

A network slice broker aims to enable MVNOs, industry vertical market players, and Over-The-Top (OTT) providers to dynamically request and release the network resources from the infrastructure provider entity based on their needs [49]. The network slicing brokering relies on the ability of the MNO/Communication Service Providers (CSP) to automatically and easily negotiate with the requests of the external tenants of the network slice based on the currently available resources with the infrastructure provider. In Ref. [49], the authors proposed the concept of a 5G network slice broker that could lease network resources on-demand.

The 3GPP's study on orchestration and management of network slicing for 5G & beyond networks indicated the establishment of mutual trust among participants (MVNOs, MNOs, OTT providers) as a prerequisite for an effective and efficient multi-operator slice creation [50]. Hence, trust and security are important factors to be considered in the implementation, design and integration of a network work slice broker.

4.2.2. Integration of blockchain to network slicing and resource brokerage

A major challenge associated with network slicing and resource brokerage is the need to keep a transparent, fair and open system within the available number of resources and several suspicious players.

Blockchain and Distributed Ledger Technology (DLT) functionalities can be utilized to address the aforementioned trust and security issues associated with the implementation of network slicing either for the coexistence of various applications and services, or for both the service and operational use-cases of CSPs. The trading of a network slice can be blockchain-based, where the blockchain smart contract orders the slice orchestration based on the agreed SLA from the 5G network slice broker. The blockchain can be integrated to take the record of how each resource has been used and how each service provider has performed against the SLA. The blockchain combines a distributed network structure, CM and advanced cryptography to present promising features that are not available in the existing structures. The key benefit that is achieved through the blockchain is the integration of the trust layer, which lowers the collaboration/cooperation barrier and enables an effective and efficient ecosystem. Further, the distributed nature of the blockchain prevents the single point of failure problem and thus enhances security.

Fig. 3 illustrates the provision of the remote surgery/consultation and remote control of drones over a long distance (with network operators in different geographical regions) while leveraging on network slicing and blockchain technologies. Here, a blockchain-based approach is used to automate the reconciliation and the payment between providers in different geographies. Without this approach, a more costly manual intervention or the integration of a third party for settlement would be required. The blockchain can also enable the seamless access of devices to a diverse number of networks. However, this might require the network provider to manage rules, protocols, and transactions at an increasing number of access points. The blockchain can play a reinforcing role, such as in the case of auditing agreement. Once the information is stored on a blockchain, it can be operated through “smart contracts” [24].

In [51], the authors proposed a model where brokering is managed by the 5G network slice broker [49] while the payout, billing and leasing are managed by the blockchain-based slice leasing ledger which is incorporated in the service layer. The blockchain can enable secure and

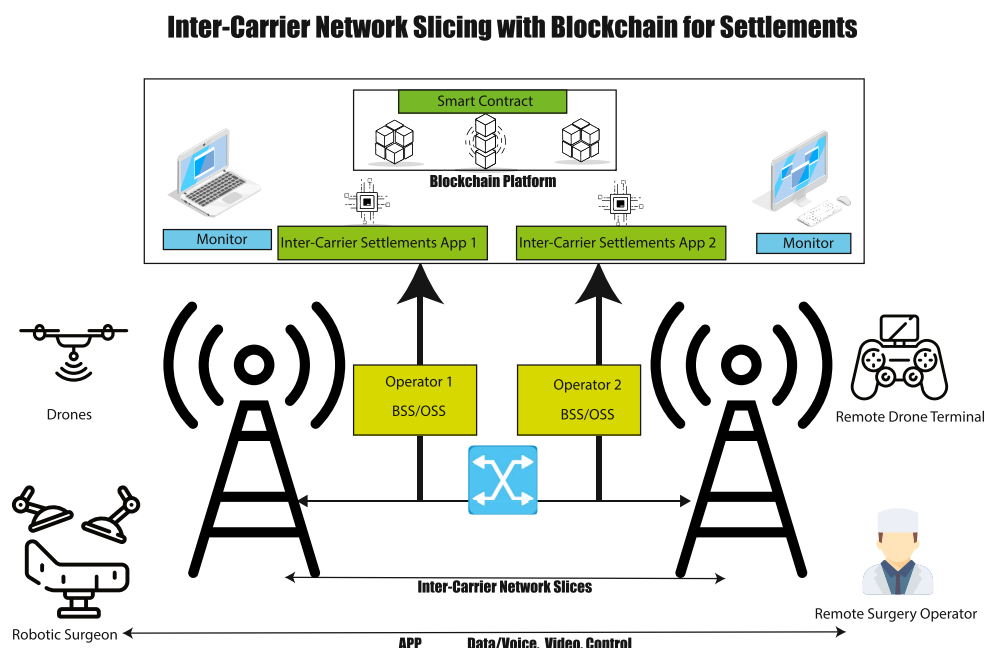


Fig. 3. Network slicing applied with the use of the blockchain.

automated brokerage of network slicing while proving the following gains:

- Significant savings in the operational (transaction and coordination) cost;
- Speed up the slice negotiation process and reduce the cost of slicing agreement;
- Increased efficiency of operation for each network slice [52];
- Increased security of the network slice transactions;
- The creation of a blockchain-enabled contract for MVNOs and MNOs that cannot afford the required network capital investment which could be on the high side. In particular, the frequency spectrum could be leased by large operators or players on a pay-as-you-go basis or in real time.

The blockchain can also enhance the enforcement of quite straightforward agreement, which is related to many brokering operations. Furthermore, the negotiation on SLAs can be more efficient when pricing and Quality of Service (QoS) levels are identified as smart contract parameters.

Other opportunities associated with the blockchain in the next generation networks include:

- The settlement of transactions between multiple carriers, including voice transactions and Call Detail Records (CDRs) of all involved call participants;
- Managing the Service Level Agreement (SLA);
- Simplification of roaming terms and agreements between multiple operators;
- Managing money transfers across borders and cross-carrier payment platform;
- Managing user/nodes identity and authentication process;
- Managing Licensed Spectrum Access (LSA) via the blockchain-based carrier marketplace.

4.3. Inter-domain blockchain ecosystem

Shareable resources are the new assets defined by the distributed resources operators, which are not limited to communication but energy and computing sections. While the communication infrastructure also relies on the energy and computing resource provision, as shown in Fig. 1. Thus, a trusted blockchain-enabled trading ecosystem, including energy, computing and communication, can be built to enable an efficient and sustainable 6G.

In the ecosystem, we can find various streams of the blockchain transaction, energy and computing flow using shared communication assets in the resource management scheme, as seen in Fig. 1. Arrows in Fig. 1 represent the flow directions, and they are started with the provider through the inter-domain sharing scheme to reach the final consumers at both the local level with consortium blockchain and national or global level via public blockchain. The ecosystem is not limited to the scope of energy, communication and computing as it can expand itself to a wider range through cross-field integration to reach, for instance, automotive, finance, manufacturing, logistic chain, and so on.

Organizations that intend to fuse such resources can be recognized as Virtual Infrastructure Operators (VIO) since they do not own all of the resources but a vendor of combined sets of resources. An example of VIO can be found in remote regions, where local infrastructure investors tend to have off-grid Distributed Generation (DG) units [53], for instance, solar and wind farms and micro Combined Heat and Power (microCHP) to offer energy and heat to remote users in the form of Distributed Energy Resources (DER) [54]. A local-based integration of such resources as aka, Virtual Power Plant (VPP) plays the role of the vendors for electricity and heat and also buys from, or sells, to other grids, with unfilled demands and excess electricity. Since these establishments are far from the central network and lack a cost-effective way of trading regarding the communication and

delivery cost, it is ideal to break with other local providers and exchange the electricity for other goods. For example, the communication relay service and computing service of DG sensor are used as the exchange of hardware power supply, so as to cultivate the ecosystem while the internal demand grows. In addition to the resources owned by the operator, there are many common resource containers among all participants.

However, the blockchain ecosystem has to accommodate the performance and security requirements of the intended application. In terms of the performance and security, the consensus is the major concern in the phase of planning. Different consensus can be applied to the sharing scheme. For example, a public chain is more suitable for inter-domain transactions on top-level operators like the national grid and first-tier MNO. However, if the resources are local-oriented, the private chain can be hosted for IoT and local/off-grid nodes, where the information from a private chain is kept within the network with confidence for external auditing. An ecosystem may introduce multiple consensus on different chains to achieve its best results.

Beyond the deployment of blockchains, the actual hardware plays an important role in the ecosystem, as current blockchain applications are designed for upper-layer applications. It lacks the understanding of portable solutions for mobile devices, such as drones, cars, and IoT. It is worth noting that the wireless capability for the blockchain is essential in 6G deployment. Wireless blockchain-enabled nodes empower the Machine-to-Machine (M2M) trade among distributed and shared resources; therefore, it becomes essential that the remote nodes are wireless-enabled. In the near future, the VANET-enabled car equipped with blockchain nodes can recharge the battery from multiple wireless charging points while moving and trade the information it carries, for instance, the Light Detection and Ranging (LiDAR) mapping data, relaying the internet access, edge computing resources and anything that can be used by the remote DG unit using wireless communication, D2D, and edge computing. The transactions are kept in the blockchain and carried by the vehicular network then mined by the local infrastructure or base station blockchain nodes. Later, the mined blocks will be relayed by satellite-linked base stations for a fee [55]. The auction of spectrum and network slices can be found on data relay and short-range Vehicle to Ground (V2G) communication, which requires huge local bandwidth to achieve lower latency. This example intends to give an insight into the inter-domain blockchain ecosystem, and further additional features are all made possible based on the inter-domain transactions.

4.4. Challenges of applying the blockchain technology in resource sharing and spectrum management

Though the blockchain has many advantages, some features need to be eliminated when applied to the resource sharing and spectrum management scenarios. Here we highlight some of the challenges of applying the blockchain technology in resource sharing and spectrum management.

Storage: Each replica node in the conventional blockchain network must process and store a copy of the completed transaction data. This can give rise to both storage and computation burden on IoT devices, which are generally resource-constrained, thus limiting their participation in the blockchain network.

Underlying networking: Implementing a consensus mechanism within the blockchain is computationally expensive, and it also requires significant bandwidth resources. Meanwhile, resources are very limited in the future network. Thus, meeting the resource requirement for large transaction throughput might be hard to achieve with the current system.

Scalability of the blockchain network: The scalability of the blockchain network is a serious issue in current systems. The number of replicas in the blockchain network relates directly to the throughput (i.e., number of transactions per second) and latency (i.e., the time required to add a transaction to the blockchain). Hence, sustaining the huge volume of transactions expected in blockchain-enabled future networks demands solutions for improving the throughput of the blockchain system.

5. Conclusion

In this article, blockchain-enabled 6G resource management, spectrum sharing, and computing and energy trading were envisioned as enablers for future use-cases. We first briefly introduced the current spectrum management and allocation techniques and discussed the link between the blockchain and spectrum management. We have then given the motivation behind the blockchain as well as an overview of its fundamentals. Moreover, we have discussed a set of key applications of the blockchain and the transformation that brings to the current wireless networks. The discussed applications include IoT and D2D communications, network slicing, and the inter-domain blockchain ecosystem.

In order to achieve a complete ecosystem and manage the resources of 6G, we identified the following open problems: 1) development of lightweight blockchain solutions for low-cost IoT devices; 2) high-performance blockchain and decentralization for the vertical industries and future networks; 3) development of blockchain solution ecosystem by considering the security and privacy issues; 4) implementation of blockchain protocols over the wireless channel and evaluation of fundamental limits relating to the performance and security.

Funding

This work was supported in part by the U.K. EPSRC (EP/S02476X/1), Sichuan International Science and Technology Innovation Cooperation/Hong Kong, Macao and Taiwan Science and Technology Innovation Cooperation Project (2019YFH0163), Key Research and Development Project of Sichuan Provincial Department of Science and Technology (2018JZ0071).

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A. Supplementary data

Supplementary data to this article can be found online at <https://doi.org/10.1016/j.dcan.2020.06.002>.

References

- [1] J.G. Andrews, S. Buzzi, W. Choi, S.V. Hanly, A. Lozano, A.C.K. Soong, J.C. Zhang, What will 5G be? *IEEE J. Sel. Area. Commun.* 32 (6) (2014) 1065–1082, <https://doi.org/10.1109/JSAC.2014.2328098>.
- [2] W. Saad, M. Bennis, M. Chen, A vision of 6G wireless systems: applications, trends, technologies, and open research problems, 2019, p. 10265, <https://doi.org/10.1109/MNET.001.1900287>, arXiv:1902.
- [3] F. Tariq, M. Khandaker, K.-K. Wong, M. Imran, M. Bennis, M. Debbah, A speculative study on 6G, 2019 arXiv:1902.06700. URL, <http://arxiv.org/abs/1902.06700>.
- [4] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G.K. Karagiannis, P. Fan, 6G wireless networks: vision, requirements, architecture, and key technologies, *IEEE Veh. Technol. Mag.* 14 (3) (2019) 28–41.
- [5] P. Yang, Y. Xiao, M. Xiao, S. Li, 6G wireless communications: vision and potential techniques, *IEEE Network* 33 (4) (2019) 70–75.
- [6] K. David, H. Berndt, 6G vision and requirements: is there any need for beyond 5G? *IEEE Veh. Technol. Mag.* 13 (3) (2018) 72–80.
- [7] J. Chen, Z. Wei, S. Li, B. Cao, Artificial intelligence aided joint bitrate selection and radio resource allocation for adaptive video streaming over f-ran, *IEEE Wireless Communications* 27 (2) (April 2020) 36–43, <https://doi.org/10.1109/MWC.001.1900351>.
- [8] K. Kotobi, S.G. Bilén, Secure blockchains for dynamic spectrum access: a decentralized database in moving cognitive radio networks enhances security and user access, *IEEE Veh. Technol. Mag.* 13 (1) (2018) 32–39, <https://doi.org/10.1109/MVT.2017.2740458>.
- [9] M.B. Weiss, K. Werbach, D.C. Sicker, C.E. Bastidas, On the application of blockchains to spectrum management, *IEEE Transactions on Cognitive Communications and Networking* 5 (2) (2019) 193–205, <https://doi.org/10.1109/TCCN.2019.2914052>.
- [10] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, Y. Zhang, Blockchain and deep reinforcement learning empowered intelligent 5G beyond, *IEEE Network* 33 (3) (2019) 10–17, <https://doi.org/10.1109/MNET.2019.1800376>.
- [11] H.N. Dai, Z. Zheng, Y. Zhang, Blockchain for internet of things: a survey, *IEEE Internet of Things Journal* 6 (5) (2019) 8076–8094, <https://doi.org/10.1109/JIOT.2019.2920987>, arXiv:1906.00245.
- [12] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, M. Imran, Performance analysis for blockchain driven wireless iot systems based on tempo-spatial model, in: 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC), 2019, pp. 348–353, <https://doi.org/10.1109/CyberC.2019.00066>.
- [13] A. Li, G. Han, J.J. Rodrigues, S. Chan, Channel hopping protocols for dynamic spectrum management in 5G technology, *IEEE Wireless Communications* 24 (5) (2017) 102–109, <https://doi.org/10.1109/MWC.2017.1700046>.
- [14] Federal Communications Commission, NPRM: Amendment of the commission's rules with regard to commercial operations in 3550–3650 MHz band, Tech. Rep. i, FCC Washington (Apr 2013).
- [15] Y.C. Liang, *Blockchain for Dynamic Spectrum Management, Signals and Communication Technology*, Springer, Singapore, 2020.
- [16] J. Eggerton, FCC's Rosenworcel Talks up 6G.
- [17] D. Gurney, G. Buchwald, L. Ecklund, S. Kuffner, J. Grosspietsch, Geo-location database techniques for incumbent protection in the TV white space, in: 2008 IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2008, 2008, pp. 232–240, <https://doi.org/10.1109/DYSPAN.2008.31>.
- [18] Y. Zhang, C. Lee, D. Niyato, P. Wang, Auction approaches for resource allocation in wireless systems: a survey, *IEEE Communications Surveys and Tutorials* 15 (3) (2013) 1020–1041, <https://doi.org/10.1109/SURV.2012.110112.00125>.
- [19] K. Kotobi, S.G. Bilén, Blockchain-enabled spectrum access in cognitive radio networks, in: 2017 Wireless Telecommunications Symposium, WTS), 2017, pp. 1–6, <https://doi.org/10.1109/WTS.2017.7943523>.
- [20] J. Qiu, D. Grace, G. Ding, J. Yao, Q. Wu, Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: an operator's perspective, *IEEE Internet of Things Journal* 7 (1) (2020) 451–466, <https://doi.org/10.1109/JIOT.2019.2944213>.
- [21] H. Chai, S. Leng, K. Zhang, S. Mao, Proof-of-reputation based-consortium blockchain for trust resource sharing in internet of vehicles, *IEEE Access* 7 (2019) 175744–175757, <https://doi.org/10.1109/ACCESS.2019.2956955>.
- [22] H. Liu, Y. Zhang, T. Yang, Blockchain-enabled security in electric vehicles cloud and edge computing, *IEEE Network* 32 (3) (2018) 78–83, <https://doi.org/10.1109/MNET.2018.1700344>.
- [23] R.C. Merkle, *A Certified Digital Signature*, 1990, pp. 218–238.
- [24] S. Underwood, Blockchain beyond bitcoin. Tech. Rep. 11, jun 2016, <https://doi.org/10.1145/2994581>. Sutardja Center for Entrepreneurship & Technology Technical Report. UC Berkeley.
- [25] P. Bhattacharya, S. Tanwar, R. Shah, A. Ladha, Mobile Edge Computing - Enabled Blockchain Framework - A Survey, Springer, Cham 597.
- [26] M. Castro, B. Liskov, Practical byzantine fault tolerance, in: *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, 1999, pp. 173–186. OSDI '99, USENIX Association, USA.
- [27] H. Xu, L. Zhang, Y. Liu, B. Cao, Raft based wireless blockchain networks in the presence of malicious jamming, *IEEE Wireless Communications Letters* (2020) 1, <https://doi.org/10.1109/LWC.2020.2971469>.
- [28] D. Ongaro, J. Ousterhout, In search of an understandable consensus algorithm, in: 2014 USENIX Annual Technical Conference (USENIX ATC 14), USENIX Association, 2014, pp. 305–319. Philadelphia, PA, <https://www.usenix.org/conference/atc14/technical-sessions/presentation/ongaro>.
- [29] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system, Tech. Rep. (2019). Manubot.
- [30] J. Niu, C. Feng, H. Dau, Y.-C. Huang, J. Zhu, Analysis of Nakamoto Consensus, Revisited, arXiv preprint arXiv:1910.08510.
- [31] J. Benet, IPFS - Content Addressed, Versioned, P2P File System arXiv:1407.3561, 2014. URL, <http://arxiv.org/abs/1407.3561>.
- [32] M. Foucault, *Discipline and Punish: the Birth of the Prison*, Pantheon Books, 1977.
- [33] J. Singh, J.D. Michels, Blockchain as a service (BaaS): providers and trust, in: *Proceedings - 3rd IEEE European Symposium on Security and Privacy Workshops*, EURO S and PW 2018, Institute of Electrical and Electronics Engineers Inc., 2018, pp. 67–74, <https://doi.org/10.1109/EuroSPW.2018.00015>.
- [34] K. Werbach, The Blockchain and the New Architecture of Trust, 2019, <https://doi.org/10.7551/mitpress/11449.001.0001>.
- [35] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, A Scalable Multi-Layer PBFT Consensus, 2020.
- [36] T.M. Fernández-Caramés, P. Fraga-Lamas, A review on the use of blockchain for the internet of things, *IEEE Access* 6 (2018) 32979–33001, <https://doi.org/10.1109/ACCESS.2018.2842685>.
- [37] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, *IEEE Access* 4 (2016) 2292–2303, <https://doi.org/10.1109/ACCESS.2016.2566339>.
- [38] B. Cao, Y. Li, L. Zhang, L. Zhang, S. Mumtaz, Z. Zhou, M. Peng, When Internet of Things Meets Blockchain: Challenges in Distributed Consensus, *IEEE Network*, 1arXiv, 2019, <https://doi.org/10.1109/MNET.2019.1900002>, 1905.06022.
- [39] G. Fodor, E. Dahlman, G. Mildh, S. Parkvall, N. Reider, G. Miklós, Z. Turányi, Design aspects of network assisted device-to-device communications, *IEEE Commun. Mag.* 50 (3) (2012) 170–177, <https://doi.org/10.1109/MCOM.2012.6163598>.
- [40] N. Mangalvedhe, R. Ratasuk, A. Ghosh, Nb-iot deployment study for low power wide area cellular iot, in: 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), IEEE, 2016, pp. 1–6.
- [41] O. Onireti, L. Zhang, M. Imran, On the viable area of wireless practical byzantine fault tolerance (PBFT) blockchain networks, in: 2019 IEEE Global Communications Conference, GLOBECOM), 2019, pp. 1–6.

- [42] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C.P.A. Ogah, Z. Sun, Blockchain-based dynamic key management for heterogeneous intelligent transportation systems, *IEEE Internet of Things Journal* 4 (6) (2017) 1832–1843.
- [43] S. Bao, Y. Cao, A. Lei, P. Asuquo, H. Cruickshank, Z. Sun, M. Huth, Pseudonym management through blockchain: cost-efficient privacy preservation on intelligent transportation systems, *IEEE Access* 7 (2019) 80390–80403.
- [44] B. Cao, M. Li, L. Zhang, Y. Li, M. Peng, How does csma/ca affect the performance and security in wireless blockchain networks, *IEEE Transactions on Industrial Informatics* (2019) 1, <https://doi.org/10.1109/TII.2019.2943694>.
- [45] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, M.A. Imran, Blockchain-enabled wireless internet of things: performance analysis and optimal communication node deployment, *IEEE Internet of Things Journal* 6 (3) (2019) 5791–5802, <https://doi.org/10.1109/JIOT.2019.2905743>.
- [46] X. Foukas, G. Patounas, A. Elmokashfi, M.K. Marina, Network slicing in 5G: survey and challenges, *IEEE Commun. Mag.* 55 (5) (2017) 94–100, <https://doi.org/10.1109/MCOM.2017.1600951>.
- [47] B. Chang, L. Zhang, L. Li, G. Zhao, Z. Chen, Optimizing resource allocation in URLLC for real-time wireless control systems, *IEEE Trans. Veh. Technol.* 68 (9) (2019) 8916–8927, <https://doi.org/10.1109/tvt.2019.2930153>.
- [48] Ngmn, Description of network slicing concept by NGMN alliance, *Ngmn 5G P1* 1 (September) (2016) 19.
- [49] K. Samdanis, X. Costa-Perez, V. Sciancalepore, From network sharing to multi-tenancy: the 5G network slice broker, *IEEE Commun. Mag.* 54 (7) (2016) 32–39, <https://doi.org/10.1109/MCOM.2016.7514161>.
- [50] 3GPP, Study on Management and Orchestration of Network Slicing for Next Generation Network, May 2017.
- [51] J. Backman, S. Yrjola, K. Valtanen, O. Mammela, Blockchain network slice broker in 5G: slice leasing in factory of the future use case, in: Joint 13th CTTE and 10th CMI Conference on Internet of Things - Business Models, Users, and Networks vol. 2018, Janua, 2017, pp. 1–8, <https://doi.org/10.1109/CTTE.2017.8260929>.
- [52] P. Ridgewell, Blockchain: where's the value for telecoms? *Tech. Rep.* May (2019).
- [53] G.G. Talapur, H.M. Suryawanshi, L. Xu, A.B. Shitole, A reliable microgrid with seamless transition between grid connected and islanded mode for residential community with enhanced power quality, *IEEE Trans. Ind. Appl.* 54 (5) (2018) 5246–5255, <https://doi.org/10.1109/TIA.2018.2808482>.
- [54] P. Landsbergen, Feasibility, beneficiality, and institutional compatibility of a micro-CHP virtual power plant in The Netherlands, *Energy* 28 (2007) 13.
- [55] E. Yaacoub, M.-S. Alouini, A key 6G challenge and opportunity – connecting the remaining 4 billion: a survey on rural connectivity. *Tech. Rep.*, 2019 arXiv: 1906.11541. URL, <http://arxiv.org/abs/1906.11541>.