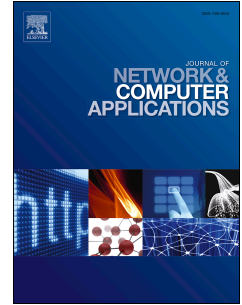# Journal Pre-proof

Blockchain for 5G and beyond networks: A state of the art survey

Dinh C. Nguyen, Pubudu N. Pathirana, Ming Ding, Aruna Seneviratne

Please cite this article as: Nguyen, D.C., Pathirana, P.N., Ding, M., Seneviratne, A., Blockchain for 5G and beyond networks: A state of the art survey, *Journal of Network and Computer Applications* (2020), doi: https://doi.org/10.1016/j.jnca.2020.102693.

This is a PDF file of an article that has undergone enhancements after acceptance, such as the addition of a cover page and metadata, and formatting for readability, but it is not yet the definitive version of record. This version will undergo additional copyediting, typesetting and review before it is published in its final form, but we are providing this version to give early visibility of the article. Please note that, during the production process, errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Blockchain for 5G and Beyond Networks:
A State of the Art Survey

Dinh C. Nguyen[1*], Pubudu N. Pathirana[1], Ming Ding[2], and Aruna Seneviratne[3]

[1]*School of Engineering, Deakin University, Waurn Ponds, VIC 3216, Australia*
[2]*Data61, CSIRO, Australia*
[3]*School of Electrical Engineering and Telecommunications, UNSW, NSW, Australia*
* *Corresponding author: cdnguyen@deakin.edu.au*
Emails: pubudu.pathirana@deakin.edu.au, ming.ding@data61.csiro.au, a.seneviratne@unsw.edu.au

Abstract

The fifth generation (5G) wireless networks are on the way to be deployed around the world. The 5G technologies target to support diverse vertical applications by connecting heterogeneous devices and machines with drastic improvements in terms of high quality of service, increased network capacity and enhanced system throughput. However, 5G systems still remain a number of security challenges that have been mentioned by researchers and organizations, including decentralization, transparency, risks of data interoperability, and network privacy vulnerabilities. Furthermore, the conventional techniques may not be sufficient to deal with the security requirements of 5G. As 5G is generally deployed in heterogeneous networks with massive ubiquitous devices, it is quite necessary to provide secure and decentralized solutions. Motivated from these facts, in this paper we provide a state-of-the-art survey on the integration of blockchain with 5G networks and beyond. In this detailed survey, our primary focus is on the extensive discussions on the potential of blockchain for enabling key 5G technologies, including cloud computing, edge computing, Network Function Virtualization, Network Slicing, and D2D communications. We then explore and analyse the opportunities that blockchain potentially empowers important 5G services, ranging from spectrum management, data sharing, network virtualization, resource management to interference management, federated learning, privacy and security provision. The recent advances in the applications of blockchain in 5G Internet of Things are also surveyed in a wide range of popular use-case domains, such as smart healthcare, smart city, smart transportation, smart grid and UAVs. The main findings derived from the comprehensive survey on the cooperated blockchain-5G networks and services are then summarized, and possible research challenges with open issues are also identified. Lastly, we complete this survey by shedding new light on future directions of research on this newly emerging area.

Keywords: 5G networks, Blockchain, 5G Internet of Things, 5G services, Machine Learning, Security and Privacy.

1. Introduction

The fifth generation 5G technology, referred to as beyond 2020 communications systems, represents the next important phase of the global telecommunication evolution, with recent successful deployments in several areas across almost all the continents[1]. The 5G cellular networks are char-

---

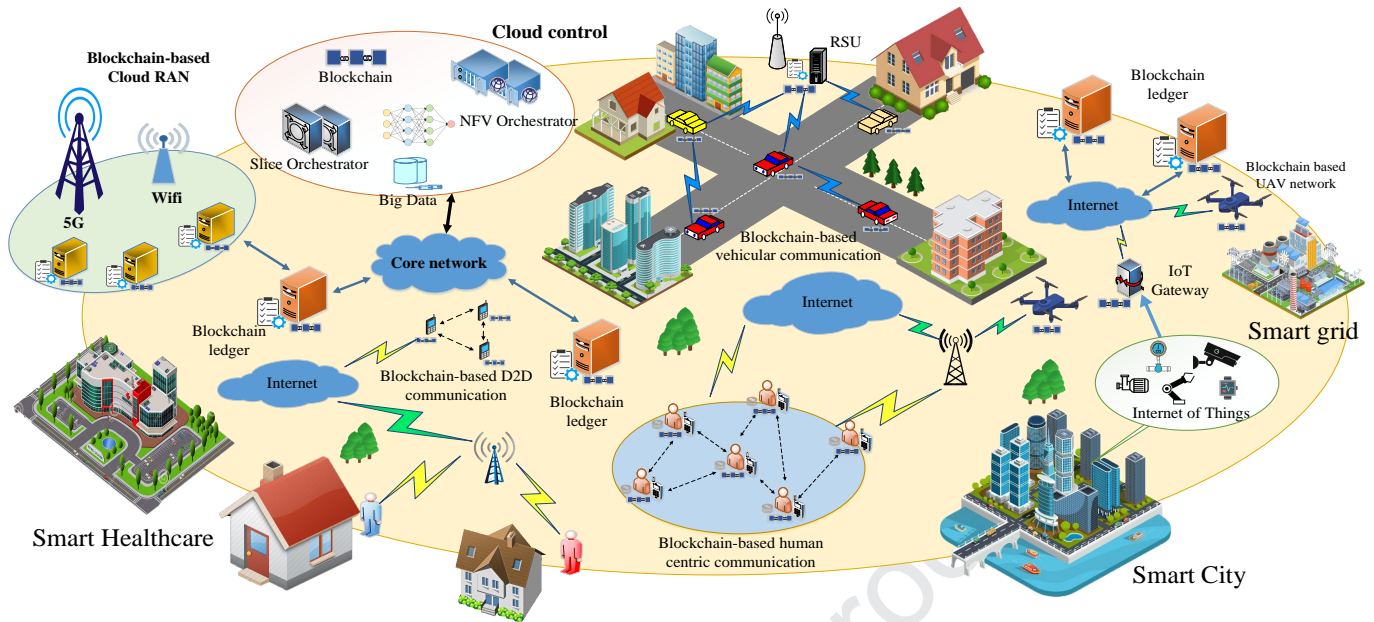[1]https://www.speedtest.net/ookla-5g-map

Figure 1: The convergence of blockchain and 5G.

acterized by three major features supporting for Enhanced Mobile Broadband, Massive Machine Type Communication and the provisioning of Ultra-reliable Low Latency Communication services [1]. Here, the definition of 5G networks refers to the 5G cellular networks that has been empowered by the evolution of cellular technology over the long history, from 1G cellular networks to 4G cellular networks [2]. Driven by the explosion of smart mobile devices and the rapid advances of communication technologies, 5G could be a technical enabler for a plethora of new innovative business opportunities and industrial applications, and facilitates the seamless collaboration across domains by interconnecting billions of devices. The 5G cellular networks promise to revolutionize global industries and provide immediate impacts on customers and business stakeholders. The main vision of future 5G services is to provide a customized and advanced user-centric value, enabling human interconnection to meet the ever growing demands of user traffic and emerging services. To achieve these objectives, according to [2], [3], [4], several underlying wireless technologies have been proposed to enable 5G cellular networks, including cloud computing, edge computing, Network communication. Function Virtualization (NFV), Network Slicing, and D2D. However, the rapid surge and breakneck expansion of 5G wireless services also pose new security challenges such as network reliability, data immutability, privacy that must be considered and solved before wide deployments.

The 5G cellular technologies will support new service delivery models and thus further exacerbate the security challenges. Unlike the legacy cellular networks, 5G wireless networks are going to be decentralized and ubiquitous service-oriented which have a special emphasis on security and privacy requirements from the perspective of services. In particular, the security management in 5G is more complex due to various types of and a massive number of devices connected. How to provide an open data architecture for flexible spectrum sharing, data sharing, multiuser access, for example, to achieve ubiquitous 5G service provisions while ensuring high data immutability and transparency is a critical issue. Succinctly, the security architectures of the previous generations lack the sophistication needed to secure 5G networks.

In the 5G era, immutability, decentralization and transparency are crucial security factors that ensure the successful roll-out of new services such as IoT data collection, driverless cars,

Unmanned Aerial Vehicles (UAVs), Federated Learning (FL). Among the existing technologies, blockchain is the most promising one to meet these new security requirements and reshape the 5G communication landscape [5], [6]. Hence, 5G needs blockhain for its wide 5G service deployments. Technically, blockchain is a distributed ledger that was firstly used to serve cryptocurrency Bitcoin [7] for economic transactions. The blockchain is basically a decentralized, immutable and transparent database. The concept of blockchain is based on a peer-to-peer network architecture in which transaction information is managed flexibly by all network participants and not controlled by any single centralized authority. In particular, the blockchain technology boasts a few desirable characteristics of decentralization, immutability, accountability, and truly trustless database storage which significantly improve network security and save operational costs [8]. The rapid development and the adoption of blockchain as a disruptive technology are paving the way for the next generation of financial and industrial services. Currently, the blockchain technology has been investigated and applied in various applications, such as Internet of Things (IoT), [9], edge computing [10], smart city [11], vehicular networks [12], and industries [13].

For the inherent superior properties, blockchain has the potential to be integrated with the 5G ecosystems to empower mobile networks and services as shown in Fig. 1. Due to the advanced technical capabilities to support future network services, blockchain was regarded as one of the key technical drivers for 5G at the 2018 Mobile World Congress (MWC) [14]. It is also predicted that blockchains would be a key technology in reaping real benefits from 5G networks, for giving birth to novel applications from autonomous resource sharing, ubiquitous computing to reliable content-based storage and intelligent data management [15].

The combination of blockchain and 5G is also expected to pave the way for emerging mobile services [16]. In fact, 5G is all about connecting heterogeneous devices and complex networks interconnecting more than 500 billion mobile devices by 2030 [17]. Besides, the emerging Internet of Things (IoT), and Massive Machine Communications (MMC) are predicted to create over 80 billion connections by 2020 [18]. In such a context, the ultra-dense small cell networks, a fundamental component of 5G infrastructure, will provide connections and energy efficiencies of radio links with high data rates and low latencies. However, it introduces trust and secure interoperability concerns among complex sub-networks. Therefore, providing a reliable cooperation among heterogeneous devices is vitally important for 5G mobile networks. In this regard, blockchain with its immutable and decentralized transaction ledgers can enable distributed massive communication with high security and trustworthiness [19]. Moreover, network slicing associated with other emerging technologies such as cloud/ edge computing, NFV, and D2D communication are also key enablers for future 5G networks and services. A big challenge for current 5G platforms is the need to guarantee an open, transparent, and secure system among the extraordinary number of resources and mobile users. Blockchain with its innovative concepts of decentralized operation can provide a high level of data privacy, security, transparency, immutability for storage of 5G heterogeneous data [20]. Blockchain is thus expected to be an indispensable tool to fulfill the performance expectations for 5G systems with minimal costs and management overheads.

1.1. Comparisons with the existing surveys

There are several survey articles in the literature that considers issues of the integration of blockchain and 5G networks. The authors in [21] only provided a brief introduction of the blockchain adoption in secure 5G resource management and reliable network orchestration. The survey in [22] provided a short survey on the potential of blockchain for 5G networks in Industry 4.0. Similarly, the study in [23] presented a brief review on the benefits of blockchain for 5G-based industrial IoTs. The survey in [24] gives a brief introduction of the potential combination
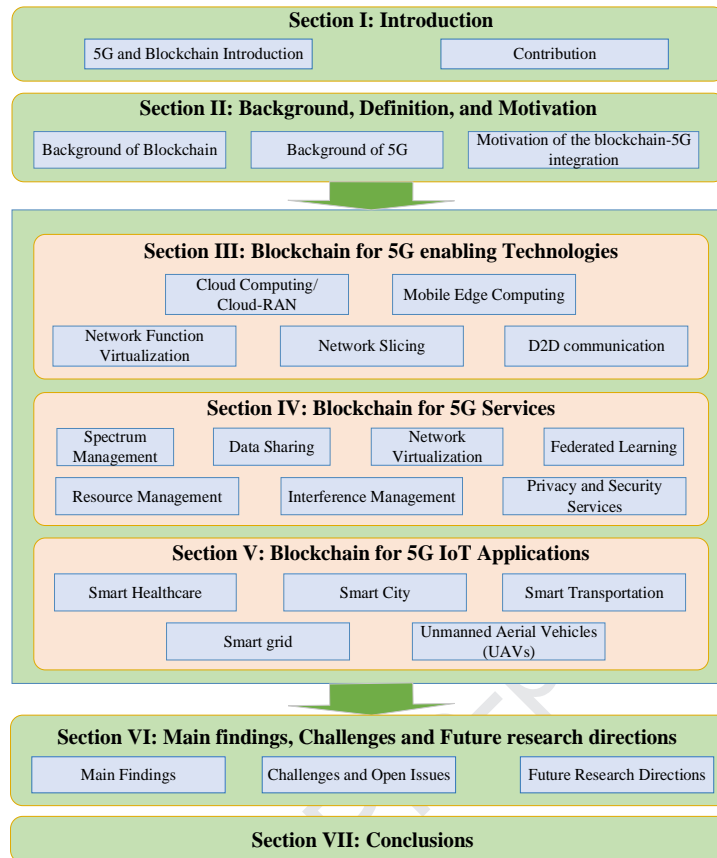
Figure 2: The structure of the paper.

of blockchain and 5G networks. Furthermore, the authors in [25] analyse the use of blockchain for solving privacy and security issues in smart communities with a number of key industrial applications such as healthcare, transportation, IoT, and smart grid. Another paper in [26] presents a survey on the security properties of blockchain that can apply to IoT networks for solving security, privacy and network performance challenges. The authors in [27] present a survey on the use of blockchain for UAV, a 5G IoT application in future networks. Meanwhile, the paper in [28] provided a systematic survey of various D2D based content caching techniques used for popular content sharing among different devices in the 5G.

1.2. Motivations and contributions

1.2.1. Motivations

Currently, there are a number of research proposals working around the combination of blockchain and 5G networks. However, there is no existing survey which provides a comprehensive discussion and analysis on the use of blockchain for 5G, including 5G technologies, 5G services and 5G IoT. Motivated by this limitation, in this paper we present a review on the combination of blockchain and 5G with extensive discussions in various 5G aspects. We identify a number of key research questions that motivate our survey in this paper as summarized in TABLE II.

1.2.2. Contributions

To our best knowledge, we are the first to provide a comprehensive survey on the integrated use of blockchain and 5G technologies and services. In this paper, we provide an extensive survey on

Table 1: Relative comparison of the existing surveys.

Related Surveys	Topic	Technology used	Key contributions	Limitations and Open issues
[21]	Blockchain for 5G network management	Blockchain, Deep Reinforcement Learning (DRL)	The authors presented a brief introduction of the blockchain adoption in secure 5G resource management and reliable network orchestration.	The potential of blockchain in enabling 5G technologies such as secure edge/cloud computing, D2D communication is lacked. Combining blockchain and DRL for 5G IoTs needs to be considered.
[22]	Blockchain for industrial 5G networks	Blockchain, IoT	The authors provided a short survey on the potential of blockchain for 5G networks in Industry 4.0.	The paper only provided the concept of blockchain for 5G. The specific use cases need to be provided.
[23]	Blockchain for 5G IoTs	Blockchain, IoT	The authors presented a brief review on the benefits of blockchain for 5G-based industrial IoTs.	The applications of blockchain for 5G technologies and services have been not analysed. The role of blockchain for 5G services should be considered.
[24]	Blockchain for industrial 5G	Blockchain, IoT	The authors provided a brief introduction of the potential combination of blockchain and 5G networks.	The potential of blockchain for 5G IoT have been not covered. More discussions of using blockchain in 5G services need to be updated.
[25]	Blockchain for smart communities	Blockchain, IoT	The authors presented a survey on the use of blockchain for smart communities, such as healthcare, transportation, IoT, and smart grid.	The discussion of blockchain is limited to smart IoT applications. The potential of blockchain for securing 5G services need to be explored.
[26]	Blockchain for IoT	Blockchain, IoT	The authors identified the security and privacy challenges in IoT networks and propose blockchain-based solutions in various IoT scenarios such as smart transportation, smart home, supply chain.	There is a lack of discussion on the roles of blockchain for 5G technology. The discussions of blockchain-5G services like spectrum sharing, resource management should be updated.
[27]	Blockchain for UAV	Blockchain, UAV	The authors in [27] present a survey on the use of blockchain for solving security in UAV networks.	The analysis of blockchain applications in other 5G domains such as edge/cloud, SDN, D2D networks has not been considered. Analysis of security and privacy should be provided.
[28]	D2D based content caching	D2D	The paper provided a systematic survey of various D2D based content caching techniques used for popular content sharing among different devices in the 5G.	The use of blockchain is only analysed in the edge catching. The role of blockchain in 5G services such as the discussions on data sharing, network management, spectrum sharing have been overlooked.
Our paper	Blockchain for 5G networks	Blockchain, cloud and edge computing, SDN, D2D, NFV, UAVs, IoT	We present a comprehensive survey on the integration of blockchain with 5G networks and beyond. The key focus is on the analysis of the blockchain adoption in 5G technologies, 5G services and 5G IoT.	-

5

Table 2: Research questions and discussions.

Research questions	Motivations
What are the current security challenges of 5G networks?	The current 5G networks and systems have faced various critical challenges in terms of decentralization, security, privacy and performance limitations due to centralized architecture.
What are the key requirements of 5G networks?	5G considered in this paper refers to the latest generation wireless networks which are envisioned to provide higher capacity, higher data rate, lower latency, massive device connectivity, enhanced enduser quality-of-experience (QoE), reduced operation cost, and consistent service provisioning.
What is the importance of security for 5G?	Security is the key for full realization of 5G in practical wireless networks and systems. Security ensures reliable 5G service delivery, data availability and better user experience.
What are the key characteristics of blockchain?	The key characteristics of blockchain includes decentralization, immutability, and transparency.
What are the potential benefits of blockchain for 5G?	With its promising security properties, blockchain promises to provide a new set of innovative solutions for 5G networks and services for better security, privacy, decentralization and transform the network management architectures for improved QoS as well as better 5G performances.
What is the key advantages of blockchain over the traditional technique for supporting 5G?	Blockchain can offer a number of new features over the existing technique such as decentralization, the limitation of third party involvement, automatic network management thanks to cooperative blockchain nodes and high immutability.
How is the current blockchain-5G research progress?	The potential of blockchain in 5G networks has been explored recent years with a growing interests from both academic and industry, mostly falling into three domains, including blockchain for 5G technology, blockchain for 5G services and blockchain for 5G IoT.

the integration of blockchain and 5G technologies for providing services, including cloud computing, edge computing, Network Function Virtualization, Network Slicing, and D2D communication. We also detail the use of blockchain for supporting important 5G services, ranging from spectrum management, data sharing, network virtualization, resource management to mitigating interference, federated learning, privacy and security attacks. The potential of blockchain in 5G IoT networks is also discussed through a number of use-case domains, such as smart healthcare, smart city, smart transportation, smart grid and UAVs. Besides, we highlight the research challenges and open issues, and point out the promising future research directions related to the blockchain-5G integrations. The main contributions of this survey article are highlighted as follows:

1. We conduct a state-of-the-art survey on the convergence of blockchain and 5G, starting with an analysis on the background, definitions as well as highlighting the motivations of the integration of these two emerging technologies.
2. We provide a review on the adoption of blockchain for enabling key 5G technologies, with a particular focus on cloud computing, edge computing, Network Function Virtualization, Network Slicing, and D2D communication.
3. We present a systematic discussion on opportunities that blockchain brings to 5G services, including spectrum management, data sharing, network virtualization, resource management, interference management, federated learning, privacy and security services.
4. We investigate the potential of leveraging blockchains in 5G IoT networks and review the latest developments of the integrated blockchain-5G IoT applications in a number of domains, ranging from smart healthcare, smart city, smart transportation to smart grid and UAVs.
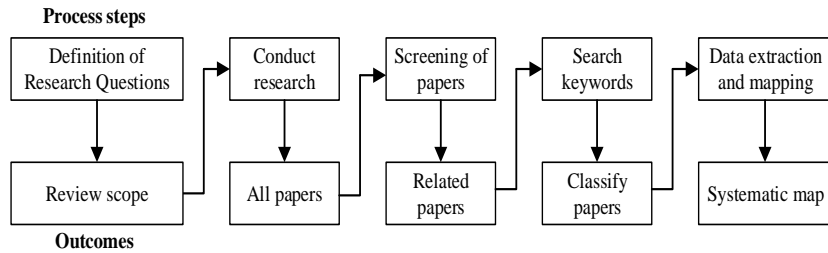
Figure 3: The systematic mapping process.

5. Based on the comprehensive survey, we summarize the main findings, highlight research challenges and open issues, and point out several future research directions.

1.3. Methods and Materials

A systematic mapping study was selected as the research method for this paper, aiming to provide an overview of the research related to the conjunction of 5G and blockchain. We follow the systematic mapping process as shown by [12] because our objective is to explore the existing studies on the blockchain-5G integration. The systematic mapping process is depicted in Fig. 3 with five key steps. *The first stage* is the definition of the research questions, which are listed in TABLE II. By identifying the key research questions, we can provide an overview on the blockchain and 5G networks, and recognize the key issues of 5G that can be solved by using the blockchain technology. *The second stage* is to search for all the relevant scientific papers on the research topic. We map the papers related to technical aspects of blockchain and 5G and using only the terms Blockchain and 5G as the search strings so that we can filter and select the most relevant technical papers for our survey. Then we chose the scientific databases for the searches. We decided to focus on peer-reviewed, high-quality papers published in conferences, workshops, symposiums, books and journals related to the research topic. We used four scientific databases for paper retrieval, including (1) IEEE Xplore, (2) ACM Digital Library, (3) Springer Link, and (4) ScienceDirect. *The third stage* is to screen all related papers based on their titles. For example, we screen all technical papers that mention blockchain and 5G technologies, i.e. D2D, cloud/edge computing. Meanwhile, we exclude papers without high content quality, papers without text availability and papers that were not written by English. *The fourth stage* is keywording. We read the abstract and identified keywords and concepts that reflected the contribution of the paper. Then, we used the keywords to cluster and form categories for the mapping of the studies. *The final stage* is data extraction that gathers all information needed to address the research questions of this mapping study. We focus on the analysis of the key findings of technical studies according to the sub-sections as pre-defined in Fig. 2.

1.4. Structure of this survey

The structure of this survey is shown as Fig. 2. Section 2 presents an overview of blockchain and 5G networks, and then highlight the motivations for the integration of blockchains in 5G networks and services. In Section 3, we present a state-of-the-art survey on the convergence of blockchain and key 5G technologies, namely cloud computing, edge computing, Network Function Virtualization, Network Slicing, and D2D communication. We also provide a comprehensive discussion on the use of blockchain for supporting fundamental 5G requirements, ranging from spectrum management, data sharing, network virtualization, resource management to interference management, federated learning privacy and security services in Section 4. The benefits of blockchain for 5G

IoT applications are analysed in details in Section 5, with a focus on popular applications such as smart healthcare, smart city, smart transportation, smart grid and UAVs. We summarize the key main findings in Section 6, and the potential research challenges and future research directions are also outlined. Finally, Section 7 concludes the paper.

2. Blockchain and 5G: background, definition and motivation

2.1. Blockchain

Blockchain is mostly known as the technological platform behind Bitcoin [7]. The core idea of a blockchain is decentralization. This means that its database does not place in a central location, but is distributed across a network of participants (i.e. computers). This decentralized concept provides high robustness and security for database stored on blockchain with no single-point failure. Importantly, blockchain is visible to each member in the network. This is enabled by a mechanism called consensus which is a set of rules to ensure the agreement among all participants on the status of the blockchain ledger. A concept on how a blockchain works is shown in Fig. 4.

In general, blockchains can be classified as either a public (permission-less) or a private (permissioned) blockchain [29]. A public blockchain is accessible for everyone and anyone can join and make transactions as well as participate in the consensus process. The best-known public blockchain applications include Bitcoin and Ethereum. Private blockchains on the other hand are an invitation-only network managed by a central entity. A participant has to be permissioned using a validation mechanism. In order to realize the potential of blockchain in 5G networks, it is necessary to understand the the concept and key characteristics of blockchain, and understand the potentials that blockchain can bring to 5G networks. We first provide an introduction of the major components of a blockchain network. Then, the key components of blockchains are presented in terms of immutability, decentralization, transparency, security and privacy, which can benefit for 5G networks and services.

2.1.1. Blockchain components

Blochain features several key components which are explained as follows.

- *Data block:* Blockchain can be defined as a series of blocks, starting with a genesis block and interconnecting with every newly updated block to create a chain. Each block is strongly linked to the previous one via a hash label, which provide a robust interconnection among block and prevent any modification risks. Each data block contain two main parts: transaction records and a blockchain header [30]. The transaction records are arranged under a Merkle tree architecture of a conjunction of all transactions. Besides, the block header mainly includes four small parts, including hash value, Merkle root, nonce value and timestamp. A typical blockchain structure is illustrated in Fig. 5.

- *Distributed ledger (database):* Distributed ledger is a kind of database that is replicated over all network participants. It records and stores transactions which are created by users and ensured consensus among utilities by the mining process (i.e. Proof of Work). In the distributed ledger, each record contains a unique cryptographic signature decoupled with a timestamp which makes the ledger resistant to be modified.

- *Consensus algorithms:* The process of transacting the block over the chain should not be controlled by any entity so that each block is managed by all participants with equal rights to avoid security issues, i.e. double-spending attacks [31]. This can be done by a mechanism called consensus. From the view of blockchain, the consensus process mainly provides a guarantee for agreement on each data blockchain among entities. For instance, Bitcoin uses Proof of Work
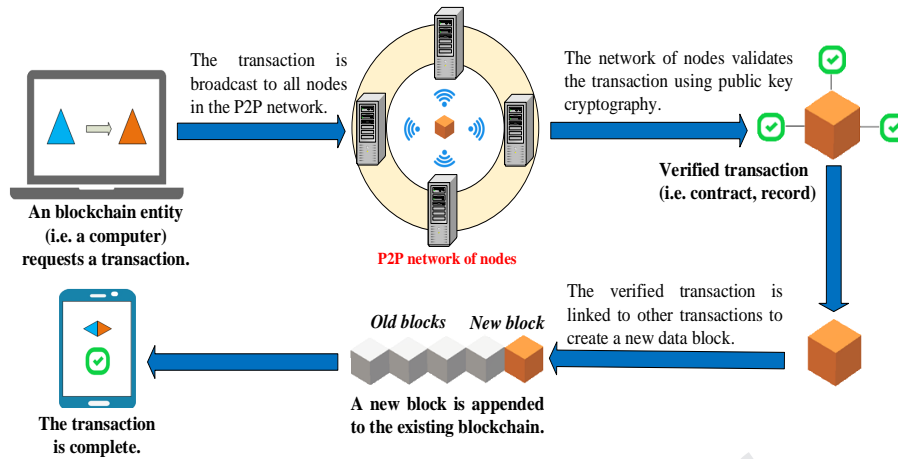
Figure 4: The concept of blockchain operation.

algorithm (PoW) [7] as a main consensus scheme for its transaction management. The nodes with high computational capability can join the mining process and compete each other to be a first one to verify the block. In return, the winner can receive a certain amount of coin as the reward for its mining effort. Along with the advance of blockchain, there are some new consensus algorithms such as Proof-of-stake (PoS), Byzantine Faulty Tolerant (BFT). More information of these mechanisms can be found in [5], [29].

- *Smart contracts:* A smart contract is a self-executing application running on top of blockchain. Since the first smart contract of Ethereum platform [5] was created in 2015, this technology has experienced a fast growth. Smart contracts are capable of execute clauses predefined in the contract in an automatic manner. The users can execute the smart contract by sending a transaction or message to it. Besides, running smart contracts costs a certain amount of coin (i.e. gas in Ethereum blockchain). No any entities can alter or change the rules defined in the smart contract, and the operation of contract does not depend on any third party. These features ensures high resistance to external attacks [32]. Based on its interesting characteristics, smart contracts have been used widely in various applications, such as money transfer, healthcare data sharing, supply chain management [33].

While such features can bring benefits, it also poses a legal and regulatory challenge if there is no central party that is responsible and can be held accountable. In a public blockchain system, it will be important to consider what law might apply to transactions and what appropriate risk management should be put into place. However, with a permissioned blockchain system, it is easier to create some forms of legal schemes and internal governance models that will dictate the governing law for blockchain transactions. In private blockchain systems, it would also be essential to take advantage of some form of agreed dispute resolution processes. Specially, we also consider legal issues about content and executions of smart contracts, programmed software running on blockchain [5], such as problems with copyright infringement and defamation. Blockchain proponents contend that it could disrupt the entire banking industry as well as industrial applications. Nowadays, many companies are collaborating together to implement and apply distributed blockchain ledger technologies to global financial markets, which could bring huge economic impacts on every corner of businesses and social activities [8].

2.1.2. Main characteristics of blockchain

We describe some key characteristics of blockchain and show its benefits to 5G networks. *Immutability:* It is the capability of a blockchain ledger to ensure that transaction data is unchange-
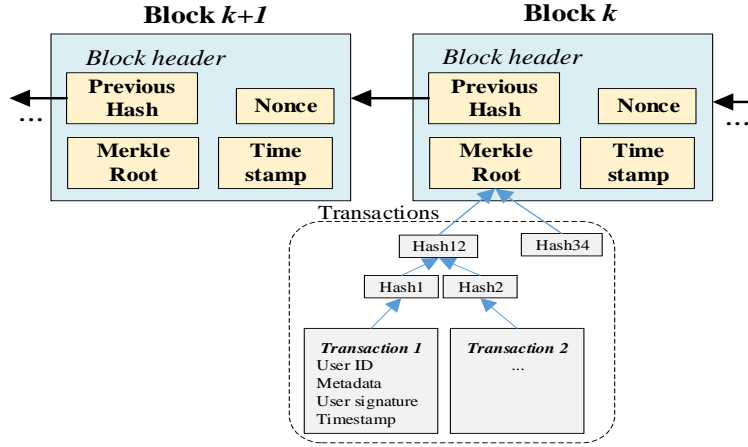
Figure 5: The data block structure.

able once it is stored on blockchain. This is because each block is hashed and linked with other blocks in a way any entities are unable to break the chain and modify the content of each block. Further, thanks to the consensus mechanism governed by the miners, each block is verified and appended immutably to the chain. The conjunction of block establishment concept and mining makes the chain data strongly immutable and unalterable. This property of blockchain supports secure data storage and sharing in 5G scenarios, i.e. secure spectrum sharing, D2D communication or privacy-preserved network virtualization. Further, by deploying immutable transaction ledgers, the network operators can establish secure communications to perform heterogeneous networking and computing, such as large-scale IoT collaborations or mobile edge/cloud computing over the trustless IoT environments.

Decentralization: Decentralization means that the blockchain does not depend on a signal entity or a central authority for managing the database. Blockchain employs consensus mechanisms such as PoW to create a secure chain of blocks and maintain the security of the database without the need of external control points. This important feature enables building the database platform with high immutability and robustness associated with low latency in data retrieval.

Transparency: The transparency of a blockchain stems from the fact that all information of transactions on blockchains (i.e. permission-less ones) is viewable to all entities. In other words, the copy of data records replicates over the network of participants for public validation. By this way, each entity can contribute their power to verify the transactions based on their functionalities (i.e. mining for miners and metadata checking for slight nodes). The corporation of all nodes helps achieve a transparency within the blockchain network, which in return enhance data integrity. This feature is particularly suitable for 5G ecosystems where the openness and fairness are required. In the cooperative network slicing, for instance, the blockchains can offer transparent ledger solutions to support open and secure data delivery and payment such that the resource providers and slice customers can trace and monitor transactions. Moreover, service trading applications (i.e. mobile resource trading in 5G IoT) can be performed automatically on blockchain by triggering smart contracts, which ensures transparent and reliable data exchange among different service providers and IoT users.

Security and privacy: Security of blockchain can be achieved by the utilization of private and public keys. The key concept behind blockchain security is the adoption of asymmetric cryptography which provide random strings for key creation so that attackers are unable to breach transactions [34]. Besides, the nature of immutability and consensus ensures privacy for database stored in the blockchain. Each user can verify and keep track of their data over the network.

10

Data stored inside the block is preserved by data leakage bottlenecks through hashing concept and mining process.

Table 3 presents the mapping of the blockchain characteristics with the potential applications in 5G networks. Each feature woudld enhance the quality of 5G systems from the performance and security perspectives which show the great potential of using blockchain in 5G. Recently, some projects have been implemented towards the integration of blockchain into 5G systems via real-world case studies. China's Ministry of Industry and Information Technology (MIIT) has launched a national blockchain-5G project that allows the majority of blockchain mobile phone manufacturers such as China Mobile, China Unicom and China Telecom to deploy blockchain on existing 5G platforms in the large cities across the country. Very recently, the 5G China Unicorn company has recently partnered with a blockchain company Wanxiang Blockchain, to combine the two technologies for IoT supply chain [35]. The blockchain application ecosystem in this project intends to solve major issues in operating 5G mobile networks, including fraud, harassment, loss of data and crimes related to identity theft. Korea Telecom also announces secure IoT, 5G blockchain projects [36]. The projects include a 5G blockchain network called GiGA Chain, a blockchain to secure IoT devices, a Blockchain as a Service offering and a local currency platform. The company also plans to use blockchain for IoT security market with its eye on connected cars and smart factories. It also works with existing systems with plans to enable blockchain on the 5G network.

2.2. 5G networks

In this subsection, we present an overview of the 5G networks. Also, 5G design principles are highlighted to provide insights into integrating blockchain in future networks and services.

2.2.1. Overview of 5G networks

Over the past few decades, the world has seen a steady development of communication networks, initializing from the first generation and moving towards the fourth generation. The global communication traffic has shown a drastic increase in recent years and is expected to continue, which triggers the appearance of the forthcoming generation of telecommunication networks, namely 5G, aiming to address the limitations of previous cellular standards and scope with such ever-increasing network capacity. The 5G network can outperform earlier versions of wireless communication technology and provide diverse service abilities as well as encourage full networking among countries globally [37], [38]. The advances in 5G communication are envisioned as opening up new applications in various domains with great impacts on nearly aspects of our life, such as IoT [39], smart healthcare [40], vehicular networks [41], smart grid [42], smart city [43]. Particularly, according to 3GPP and IMT-2020 vision [44], [45], the 5G technology is able to provide the following key capabilities:

- Provide 1-10Gbps connections for the field and can reach up to 20Gbps in certain scenarios.

- Provide ultra-low latency services (1ms or less than 1ms).

- Achieve high mobility, up to 500km/h.

- Enable Perception of 99.999% availability and 90% reduction in network energy usage.

- Enable 10-100x number of connected devices with the ability to achieve 10-year battery life.

- Enable 1000x band-width/unit area.

11

Table 3: Main characteristics of blockchain and their potentials to 5G.

Key characteristics of blockchain	Description	Potential applications to 5G networks and services
Decentralization	No central authority or trusted third party is needed to perform transactions. Users have full control on their own data.	Eliminate the need of trusted external authorities in 5G ecosystems, i.e. spectrum licenses, band managers, and database managers in spectrum management; central cloud/edge service manager in mobile computing and D2D networks; UAV control center in 5G UAV networks; and complex cryptographic primitives in 5G IoT systems. Decentralizing 5G networks potentially eliminates single-point failures, ensures data availability and enhance service delivery efficiency.
Immutability	It is very difficult to modify or change the data recorded in the blockchain.	Enable high immutability for 5G services. Spectrum sharing, data sharing, virtualized network resource provisions, resource trading can be recorded immutably into the only-appended blockchain. Besides, D2D communications, ubiquitous IoT networking and large-scale human-centric interconnections can be achieved via peer-to-peer networks of ubiquitous blockchain nodes without being modified or changed. The high immutability is very useful for 5G networks to performing accounting tasks, i.e. immutable database sharing, service transparency, secure user behaviour monitoring.
Transparency	All information of transactions on blockchain (i.e. public ledgers) can be viewable to all network participants.	Provide better localized visibility into 5G service usage. The same copy of records of blockchain spreads across a large network for public verifiability. This enables service providers and users to fully check and monitor transactions with equal rights. Also, blockchains potentially offer transparent ledger solutions for truly open 5G architectures (i.e. decentralized network virtualization, distributed edge computing, distributed IoT networks). Blockchain ledgers also support fair service trading applications (i.e. resource trading, payment) under the control of all network entities.
Persistency	All data stored in the blockchain would be verified its correction to detect modifications or malicious behaviours.	Provide better persistency for 5G services. Transactions created from activities of spectrum sharing, data sharing, virtualized network resource provision are recorded and verified by all network operators and users. It also enhances the reliability of 5G IoT communications thanks to the ability of malicious access detection by using blockchain ledger.
Auditability	Any information and data is audited and traced once uploading to the blockchain.	Enable network operators keep track of 5G services and operations over the wireless network. It also provide an equal right to the users to audit the 5G data over the network to strengthen the roles of mobile users in the 5G ecosystem.
Security and privacy	Blockchain employs asymmetric cryptography for security with high authentication, integrity, and non-repudiation. Smart contracts available on blockchain can support data auditability and access control for privacy.	Provide high security for 5G networks involved in decentralized ledgers. Blockchain helps secure the 5G networks by providing distributed trust models with high access authentication, in turn enabling 5G systems to protect themselves and ensure data privacy. By storing data information (i.e. IoT metadata) across a network of computers, the task of compromising data becomes much more difficult for hackers. Besides, smart contracts, as trustless third parties, potentially support 5G services, such as data authentication, user verification, and preservation of 5G resource against attacks.

In order to achieve such promising performance targets, the 5G networks leverage a number of underlying technologies, such as cloud/ edge computing, Network functions virtualisation (NFV), network slicing, Device-to-Device Communications, Millimeter wave communication [3].

- *Cloud/edge computing:* Cloud computing has been introduced to meet the increasing demands for resource management, data storage, and mobile sensing in the 5G era. In specific, cloud computing paradigms with resourceful virtual computation centers can well support 5G services such as mobility/network management, resource offloading, and sensing services in various application domains [46]. Meanwhile, as an extended version of cloud computing, edge computing has been regarded as the promising technology to empower 5G ecosystems. It provides computing services at the edge of the mobile network, which enables computation and storage services with much lower transmission delays.

- *Network functions virtualisation (NFV):* In network functions virtualisation, it is possible to run the different network functions purely using software. NFV enables decoupling the network functions from proprietary hardware appliances so that they can operate using standardized hardware [3]. The key purpose of NFV is to transform the way networks are built and services are delivered. With NFV, any 5G service operators can simplify a wide array of network functions, as well as maximize efficiencies and offer new revenue-generating services faster and easier than ever before [3].

- *Network slicing:* Network slicing is a kind of virtual networking architecture which allows to create multiple virtual networks on top of the physical network infrastructure. By integrating with NFV, network slicing provides virtual applications which can directly deployed on each slice so that services can be instantly provided to the users. As a result, mobile applications running on slices can exhibit low-latency services with specific service provisions, which provide high quality of user experience.

- *Device-to-Device (D2D) communication:* It allows IoT devices in close proximity to communicate together using a direct link rather than long signal transmissions via traditional base stations. By using D2D communication, 5G heterogeneous data can be transferred quickly between mobile devices in short range, which promises ultra-low latency for communication among users. Moreover, D2D connectivity will make 5G operators more flexible in terms of offloading traffic from the core network, improve spectral efficiency and eliminate unnecessary energy loss due to long data transmissions [47].

- *Millimeter wave (mmWave) communication:* The mmWave communication technology gives new facilities with a tremendous amount of spectrum to 5G mobile communication networks to supply mobile data demands. It comes with a number of benefits including huge bandwidth, narrow beam, and strong data access ability to overcome shortcomings caused by the explosive growth in mobile traffic volumes, unprecedented connected devices, and diversified use cases [48].

In the 5G networks, these above technologies will be used to meet the demands of diverse applications from the ongoing traffic explosion of connected devices. For example, the combination of cloud/edge computing and Software Defined Networking and Network Function Virtualization (NFV) is regarded as the potential facilitators for flexible network deployment and operation. Moreover, the network slicing and D2D communication will enable ultra-reliable, affordable broadband access and intelligent use of network data to facilitate the optimal use of network resources

with extremely low latency and high-speed device connection [4], [5]. The proliferation of 5G networks was initially shaped by the Next Generation Mobile Networks (NGMN) alliance [49] with a 5G initiative for enabling emerging services and business demands with the time target of 2020 and beyond.

2.2.2. 5G design principles

The rapid advances of new 5G technologies provide an impetus for new fundamental design principles toward 5G networks. The 5G design principle was outlined by the NGMN alliance [50]. Specifically, 5G systems can employ software and virtualisation to achieve the service objectives on flexibility, configurability, and scalability. Particularly, one of the key design concepts behind the 5G networks will be network slicing which separates the user and control planes and enables dynamic network function placement [3] for a ubiquitous flexible and extensible infrastructure for all types of communication services on top of which a dynamic service and business environment can involve. The vision of 5G lies in providing smart services with very high data rates, extremely low network latency, manifold increase in base station density and capacity, and brings about significant improvements in the quality of services, quality of user experience, compared to 4G systems. It provides a convergence of pervasive broadband, sensing, and intelligence to establish a greater scale for the fourth industrial revolution that will stimulate the development of society and industrial markets.

In the future, the 5G operation need to be simplified that can be achieved thanks to the support of emerging technologies including NFV with networking slices. The control plane empowered by potentially provides a logic control for the local network so that system operations and services can be monitored in a better organized manner. NFV implements network functions virtually through decoupling hardware appliances to provide virtual services, virtual edge nodes for extending the network functions. Meanwhile, cloud computing/cloud RAN supports unlimited data storage and data processing to cope with the growing IoT data traffic in 5G. The combinations of 5G enabling technologies promise to foster mobile networks with newly emerging services such as intelligent data analytics, big data processing. Specially, different from previous network generations (i.e. 3G/4G), 5G is promising to provide mobile services with extremely low latency, energy savings due to flexibility (i.e. network slicing and proximity of edge computing), all of which will enhance QoS of the network and ensure high QoE for users.

2.3. Potentials of the Blockchain and 5G integration

In this subsection, we explain the potentials behind the blockchain and 5G integration.

2.3.1. Definition of the integration of Blockchain and 5G

To highlight the motivation, we recall the most significant features of both technologies for the integration. Blockchain can provide secure 5G data services through its secure distributed ledger. This is enabled by some interesting features such as immutability, decentralization, transparency and privacy. Thus, the key points of blockchain here are its capabilities to support security and network management for 5G networks and applications. On the other side, 5G considered in this paper refers to the latest generation wireless networks which are envisioned to provide higher capacity, higher data rate, lower latency, massive device connectivity, enhanced end-user quality-of-experience (QoE), reduced operation cost, and consistent service provisioning. Therefore, the key points of 5G here are its advantages of providing fast and high-quality services and the need for security and networking improvement.

Then, the motivation behind the conjunction of blockchain and 5G stems mainly from the promising benefits of blockchain for solving challenges in 5G networks in terms of security, privacy, networking and service management. With the help of innovative blockchain designs, 5G is expected to overcome the existing challenges and open up new opportunities to empower blockchain 5G-based services and applications. In the following, we discuss the motivation of the integration coming from current 5G challenges and then present opportunities brought from the blockchain-5G integrations.

2.3.2. Security challenges in 5G networks

The security associated with 5G technologies has been regarded as one of the key requirements for 5G and beyond systems. The existing 5G technology infrastructure has remained unsolved challenges in terms of security, networking and computing performance degradation due to its centralized architecture [50]. For example, edge/cloud computing models current rely on centralized service providers (i.e. Amazon cloud), which reveals various security bottlenecks. Indeed, this configuration is vulnerable to single-point failures, which bring threats to the availability of cloud/edge services for on-demand user access.

Moreover, network function virtualization (NFV) and service function chaining in 5G networks, however, also incur new security challenges [51], [52]. Since end-to-end service function chains may deploy NFVs in an environment involving multiple cloud providers, such data transmissions can be compromised by curious cloud entities, leading to data leakage concerns. Furthermore, in a virtualized scenario, tenants often share the same cloud infrastructure. In this context, the possibility of attacks inside the cloud can increase, which damages the transparency and accountability of service providers. In NFVs, virtualization servers can run on virtual machines (VM) to offer specific functions to execute distinct operating systems such as VM migration or resource allocation using orchestration protocols. However, the security for the communication between the orchestrator and the physical machine VM manager is a real challenge.

The rapid proliferation of mobile data traffic and the increasing user demands on 5G infrastructure also introduce new challenges in terms of security and performance degradation. For example, the increasing requirement for bandwidth-hungry applications for 5G services such as mobile video streaming, big data processing requires a proper 5G spectrum resource management strategy to avoid resource scarcity issues for ensuring continuous service functionalities. Therefore, spectrum sharing between mobile network operators (MNOs) and mobile users is necessary. However, spectrum sharing in such scenarios also raises security concerns and provides a central point of attacks for malicious users [53]. A possible approach is to use certification authorities, providing provide certificates for cognitive radios inside each cell. Further, it requires greater computation complexity which increases spectrum sharing overheads and thus reduces the Quality of Services (QoS) of the involved system. Importantly, the use of such centralized architectures also adds single-of-failure bottlenecks when the authority is attacked or out of services, which leads to the disruption of the entire spectrum sharing network.

In the 5G IoT scenarios such as smart healthcare, smart cities where mobile environments are highly dynamic with the conjunction of IoT devices, complex networks and ubiquitous services, security and privacy issues become much more complex to be solved [54]. In fact, a prohibitively large amount of IoT data will be generated continuously from ubiquitous IoT sensor devices. It is very difficult to immediately identify the objects of interest or detect malicious actions from thousands of data transactions on a large scale. The solution of using a centralized management may be infeasible to such use cases due to long latency, privacy risks due to curious third parties and network congestion. Obviously, how to provide efficient mobile services (i.e. data sharing,

data processing, user management) in terms of low latency and increased network throughput while still ensure high degrees of security is a critical challenge. Therefore, there are urgent needs of innovative solutions to overcome the above security and network performance limitations for future 5G networks.

2.3.3. Opportunities brought by blockchain to 5G networks and services

With its promising security properties, blockchain promises to provide a new set of innovative solutions for 5G networks and services for better security, privacy, decentralization and transform the network management architectures for improved QoS as well as better 5G performances. Therefore, 5G should use the benefits of blockchain to accommodate flexibility and security in providing mobile network services and ubiquitous coverage. In short, we highlight the significant opportunities that blockchain can bring to 5G networks and services, with a focus on three main aspects, including security enhancements, system performance improvements, and network simplification.

1. *Security enhancements:* Blockchain promises to enhance the security and privacy of 5G ecosystems, by offering many promising technical properties such as decentralization, privacy, immutability, traceability, and transparency. Blockchain can eliminate the centralized network management concept by decentralizing the network infrastructure where there are no third party authorities needed. As an example, the concept of blockchain-based cloud computing enables decentralization of cloud/edge 5G networks which removes centralized control at the core network and provides a decentralized fair agreement with blockchain consensus platform, which eliminates single point failure bottlenecks and improves significantly system trust. Besides, the security of D2D communication can be achieved by building a peer to peer network via blockchain, which transforms each D2D device as blockchain node to hold a ledge copy with the ability of verifying and monitoring transactions for better system transparency and reliability.

   Especially, different from the conventional database management systems which often use a centralized server to perform access authentication and security mechanisms, blockchain with smart contracts can implement decentralized user access validation by using the computing power of all legitimate network participants. This makes the 5G services (i.e. spectrum sharing, data sharing, resource allocation) strongly resistant to data modifications. Many research works on blockchain [11], [12], [13] demonstrate that the blockchain adoption is beneficial to spectrum 5G management in terms of better verification of spectrum access with blockchain contracts, improved accessibility thanks to the transparency of blockchain. Moreover, the use of blockchain fosters scalable spectrum sharing over the peer-to-peer ledge network where spectrum license holders and band managers are eliminated for high trustworthiness. The ledger services with strong immutability from blockchain also provide a high degree of security and better system protection capability against DoS attacks and threats. Empowered by smart contracts, which provide highly flexible efficient user access control mechanisms via access rules and intelligent coding logics, blockchain potentially introduce new authentication solutions for 5G cellular networks. Instead of relying on external public key infrastructure, contracts can authenticate automatically user access, detect threats and discard malicious access from the networks in an autonomous manner without revealing user information. Besides, by publishing user data to ledger where data is signed by hash functions and appended immutably to blocks, blockchain platforms ensure strong data protection. Blockchain is capable of providing a full control of personal data when sharing over the untrusted network, which is unique from all traditional approaches which hinder users from tracking their data [14].

16

2. *System performance improvements:* The use of blockchain also potentially improves the performances of 5G systems. In comparison to traditional database platforms such as SQL, blockchain can provide better data storage and management services with low latency data retrieval. In fact, resource requests (i.e. data access) can be verified by decentralized blockchain nodes with the support of intelligent smart contracts without passing a centralized authority, which is promising to reduce network latency. Moreover, motivated by the removal of decentralization, blockchain is able to establish direct communications between 5G service providers and mobile users so that the management cost can be significantly reduced. This would provide a much more flexible and efficient data delivery model for 5G ecosystems but still meet stringent security requirements [12]. For example, blockchain can help establish secure peer-to-peer communication among users (i.e. in D2D communication) using the computing power of all participants to operate the network instead of passing a third party intermediary. This would potentially reduce communication latency, transaction costs, and provide the global accessibility for all users, all of which will enhance the overall system performance. Specially, even when an entity is compromised by malicious attacks or threats, the overall operation of the involved network is still maintained via consensus on distributed ledgers, which in return ensures no single-point failure vulnerabilities for better security.

3. *Network simplification:* It is believed that blockchain can simplify the 5G network deployments thanks to its decentralized architectures. Indeed, by leveraging blockchain, the mobile operators now can have no worries about the establishment of centralized control servers. The 5G service delivery can be achieved by the blockchain network where user access, service responses and service trading (i.e. resource trading and payment) can be implemented on the decentralized ledgers among network participants including service providers and mobile users without the need for additional management infrastructure [5]. Therefore, the blockchain adoption potentially reduces network complexity and thus saves significantly operational costs. Furthermore, the transactions for 5G services (i.e. data sharing, spectrum sharing) are controlled by the blockchain network itself where all entities hold the same rights to manage and maintain the network. The capability of exploiting internal resources from participants is also another great advantage that blockchain can provide to simplify the network organization and management for better user experience and facilitation of service transactions, especially in complex mobile environments in the future 5G networks [6].

3. Blockchain for enabling 5G technologies

Reviewing state-of-the-art literature works [1], [3], [4], we found that blockchain has mainly cooperated with the key 5G enabling technologies including cloud computing, edge computing, Network Function Virtualization, Network Slicing, and D2D communication. Motivated by this, in this section, we present a review on the integration of blockchain and such 5G technologies. The benefits of blockchain for different 5G use cases and applications empowered from the integration are also analysed in details.

3.1. Blockchain for cloud computing/ Cloud RAN

Cloud computing has drawn significant attention in the last decades thanks to its unlimited resources of storage and computation power, which can provide on-demand, powerful and efficient services with minimum management efforts. Cloud computing has been investigated and integrated extensively with 5G networks, paving the way for the computing-intensive applications involving multi-dimensional massive data processing assisted by the cloud [55], [56]. In fact, cloud computing

17

paradigms provide a number of technical solutions for realizing 5G services, such as optimizing the communications, processing and storage processes [57], 5G data content delivery and catching [58], resource allocation and data transmission management [59], and cloud-enabled small cell networking for 5G media services [60]. Specially, in order to meet the ever-increasing demand of user association and resource allocation in cellular 5G networks, the architecture of cloud radio access networks (Cloud-RANs) is envisioned as an attractive model that manages the large number of small cells through the centralized cloud controller as baseband unit (BBU) pool [61]. Cloud-RAN is able to offer high-speed interconnection and shared powerful processing to facilitate optimal multicell cooperation and collaborative radio, real-time cloud computing [62], [63], which makes Cloud-RAN become a promising candidate of next-generation 5G access networks.

However, the existing cloud computing models remain unsolved challenges in terms of security, networking and computing performance degradation due to its centralized architecture. Indeed, in the 5G era, the massive data traffic outsourced from IoT devices to the cloud has brought about a series of new security challenges, such as data availability [64],privacy management [65], [66], and data integrity [67]. As an example, the dynamic process of 5G data to clouds and data exchange between cloud providers and mobile users are vulnerable to information modifications and attacks caused by adversaries or third parties. Even entities within the network may be curious about transmitted data over the sharing and unauthorized obtain personal information (i.e. customer data of 5G smart grid or location information of vehicles in vehicular networks). These issues may lead to serious data leakage bottlenecks and consequently damage data availability. Besides, in the conventional cloud systems, cloud resource providers have full control over outsourced network data (i.e. IoT data) while users are not aware of it and lacks the ability of tracking data after offloading to the cloud. This poses critical challenges on data users to perform verification and monitoring of data flows or usage, especially in the 5G scenarios where transparency among networks members is highly required to ensure fairness and openness, i.e. cloud service providers and slice users in cloud-based network slicing, or between healthcare providers and patients in cloud e-health.

Recently, blockchains have been investigated and integrated in cloud computing to effectively address the above security challenges in the cloud-based 5G networks. For example, the work in [68] takes advantage of blockchain to develop a framework called BlockONet for 5G access scenarios, aiming to improve the network credibility and security in 5G fronthaul. Blockchain is employed to build a verification platform between IoT devices, BBU unit, and manufacturer, where user access information is stored immutably on the chain, while smart contracts are also leveraged to perform automatic user authentication. The benefits from the use of blockchain in Cloud-RAN 5G networks are twofold. First, the concept of blockchain-based Cloud-RAN gets rid of centralized control at the core network and offers a decentralized fair agreement with blockchain consensus platform, which eliminates single point failure bottlenecks and improves significantly system trust. Second, by applying a decentralized blockchain without third parties, the blockchain-based cloud-RAN strategy can achieve optimal resource utilization and save a large amount of signalling and connection costs. In the same direction, the study in [69] applies blockchain to build a trusted authentication architecture for cloud radio access network (Cloud-RAN) in the 5G era.

Blockchain is also integrated with cloud computing for 5G IoT networks. The study [70] introduces a blockchain-based cloud-centric IoT scheme using smart contracts for security of data provenance. The use of blockchain enables secure data storage by keeping the metadata in the ledgers while the actual database is placed in cloud storage servers. Smart contracts support security properties, such as transparency and immutability for cloud data exchange and sharing. Meanwhile, a secure data sharing architecture was introduced in [71] with a attributed based-access control system. The main components of the network consist of IoT devices, a data owner,

a blockchain network and cloud computing. To manage IoT data and transactions, a permissioned blockchain is deployed on top of the cloud IoT so that user access can be verified and data usage is monitored. Similarly, a hierarchical access control scheme for cloud blockchain is investigated in [72] with a blockchain-empowered key management system. The blockchain network topology is the combination of distributed side blockchains running at fog nodes and a multi-blockchain hosted in the cloud, which would provide efficient network management and flexible storage for scalable cloud IoT networks. Moreover, to preserve cloud applications, a forensic investigation system is proposed using decentralized blockchain [73]. The key focus of this work is on the analysis of the security for interactions among cloud service providers, clients, and IoT devices. With the support of blockchain, data immutability checking is done in a decentralized manner with the involvement of all entities, therefore avoiding single points of failure on the cloud storage.

In addition, blockchain has also incorporated with the cloud federation architectures to further improve the performance of complex 5G-IoT networks in terms of transparent collaboration and interconnected services. As an example, a blockchain framework was proposed on a joint cloud collaboration environment where multiple clouds are interconnected securely by peer-to-peer ledges [74]. The proposed scheme contains three tiers with an IoT sensor network, a federation of multiple clouds, and a service platform. Typically, the blockchain platform can exhibit superior advantages over the single cloud-based systems. For instance, since IoT data at each area is placed in a private cloud, its data security is improved. Further, the single cloud can offer instant services for IoT users thanks to a private blockchain, which reduces risks of attacks on cloud systems [75]. Besides, a cloud blockchain model with micro-clouds was introduced by [76] using blockchain-enabled distributed ledgers. The authors pay special attention to building a cloud blockchain platform for decentralized collaborative governance services, i.e. immutable data storage, transparent monitoring and resource management for better performance on lightweight computing nodes like IoT devices.

For hierarchical networking in 5G-based cloud computing, the work in [77] proposes a hierarchical trust networking architecture based on permissioned blockchain to implement JointCloud (HTJC). This research aims to solve some critical limitations in cloud-based IoT networks, namely trust, privacy leakage, and weak security of IoT devices. This can be done by introducing a trust hierarchy model that builds a secure credit-based trading environment using blockchain. In this context, the trading requires credits to ensure that the members of network can maintain normal behavior rather than engage in malicious behaviors. Besides, a mechanism of rewards and punishments empowered by credits is designed to manage the members of network based on credits for security and trust guarantees.

3.2. Blockchain for mobile edge computing

As an extension of cloud computing, mobile edge computing (MEC) is a promising technology for supporting 5G services. Edge computing, located at the edge of the network, can provide low-latency services for mobile users. [78]. The distributed structure of edge computing has the potentials to enabling ubiquitous computing provisions, scalability improvement and simplification of network management to cope with the explosion of IoT devices and rapid growth of 5G service demands [79]. However, its security is a significant challenge [80], [81]. Indeed, the migration of 5G services, i.e. data computation, in the dynamic edge computing environments can be vulnerable to malicious attacks (such as jamming attacks, sniffer attacks, denial-of-service attacks, etc.). Further, the setting and configuration information by the edge service providers (ESP) must be trustworthy and secure, but in fact these are actually challenged due to the high dynamism and openness of the MEC system. Another challenge is to ensure data privacy and immutability for outsourced
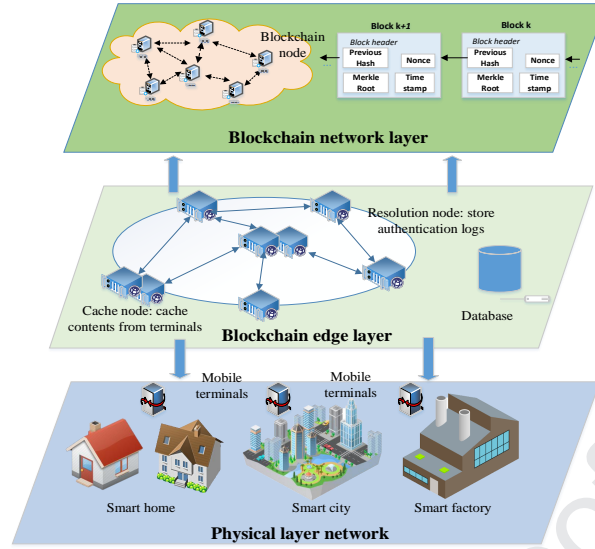
19

Figure 6: The convergence of blockchain and edge computing for 5G services.

5G heterogeneous data from external modifications or alternations. Importantly, how to avoid the system disruption caused by the attack on an edge node in the multi-edge computing [80] is of paramount importance for 5G-based edge computing networks. Fortunately, blockchain has come as a promising technical enabler to overcome most of security and networking challenges faced by the existing edge computing architectures. The same decentralization characteristic of both the blockchain and MEC built on the networking, storage, computation, communications makes their combination become natural. The recent research results have demonstrated that blockchain can be applied to the edge computing systems to support a number of services of security and management in edge computing [82]. Generally, the blockchains can support edge computing-based 5G services in three main aspects: networking, storage and computation as shown in Fig. 6.

In fact, with the help of blockchain, the networking capability of edge networks can be optimized. The blockchain is employed in [83] to build a distributed and trusted authentication system to realize reliable authentication and information sharing among different edge-based IoT platforms. In the system, authentication data and user access information can be stored securely on blockchain, which is also capable of automatically tracking activities of mobile terminals (devices) without the need of central authorities. In particular, smart contracts are also utilized to perform trusted content catching in the edge computing network. Meanwhile, the works in [84], [85] suggest a blockchain-based architecture for vehicular edge computing. Vehicular edge computing is introduced to provide data processing services with low latency, but it also raises privacy concerns since user information can be disclosed during the sharing process. The adaption of blockchain potentially solves such challenges by establishing a secure communication channel empowered by immutable transaction ledgers. Then, this robust and secure concept enables the energy flow and information flow to be protected against external malicious attacks when performing vehicular networking. Furthermore, ensuring security in the transmission process is one of the achievements of blockchain. The authors in [86], [87] take advantage of blockchain to establish a security mechanism for edge computing-based energy systems where smart contracts are leveraged to build a trusted access control scheme for energy sharing and distribution. Further, the blockchain-based solutions can support efficient conditional anonymity and key management for the privacy-preserving authentication protocol without the need for other complex cryptographic

primitives between network users. Moreover, to achieve a trustworthy and efficient edge computing system, the blockchain functionality is applied to the resource management [88], data sharing [89] or resource allocation [90], all of which improve edge computing performances while guaranteeing security properties of the network.

In addition, blockchain also provides security features for efficient data storage for edge computing systems. Indeed, blockchain can offer decentralized data storage enabled by the combined storage capacity of a network of peers to store and share contents. The work in [91] proposes a MEC-based sharing economy system by using the blockchain and off-chain framework to store immutable ledgers. Specifically, in a smart vehicular network, blockchain can keep information of the driver and the car profile with the history of maintenance, accident, and other car usage information. The raw vehicular data, i.e. vehicle sensor data, can be captured and processed by the MEC node under the control of the blockchain. The work in [92] also proposes a blockchain database to secure communication between the home devices and sensors in the MEC-based smart city. In the sense of the ledger, blockchain can be regarded as a distributed database which keeps data by interconnecting a network of strongly immutable blocks. It is noting that the scalability of blockchain is a critical challenge due to the constrained ledger size, throughput and latency [82]. In this regard, the on-chain and off-chain storage concept can be very useful. For example, in the vehicle context, the real-time updates regarding traffic information can be placed locally in a cache unit,, while data hash values can be kept securely in blockchain. Any modifications on the storage unit can be acknowledged by blockchain via decentralized ledgers, improving the trustworthiness of the MEC-based network. Moreover, to facilitate easy access to data in a distrusted MEC blockchain setting, a decentralized big data repository platform, such as Inter-Planetary File System (IPFS) can be necessary for improving storage capability on blockchain [93]. On top of IPFS, several blockchain-based storage platforms such as Filecoin or Storij [9] have been applied as an incentive layer to form an entirely distributed file storage system. These blockchain database systems contain the off-chain service data while providing the on-chain identifier, so that data integrity can be checked by the identifier from the data and hash values in the blockchain and comparing it for monitoring. Such a blockchain platform is integrated with edge computing to solve storage risks caused by dynamic MEC [94].

Moreover, the potential of blockchain for MEC collaboration has been also investigated recently. The authors in [95] introduce a distributed blockchain-based trusted MEC collaboration (BlockTC) architecture that is able to enable cross-domain collaboration among multiple MEC servers verification. The proposed BlockTC achieves multi-server trusted routing and privacy protection with three main features, including a backup dual-link that supports maintenance and verification of MEC collaboration routing without exposing privacy across the network; distributed ledger that ensures data consistency over the MEC network, and collaboration routing consensus that verifies the routing among MEC servers. The experiment shows good performances in terms of low mistrust rate, efficient resource utilization, low path provisioning latency, and low error detection latency.

Lastly, blockchain can support the computation processes in MEC networks. Specifically, blockchain can provide authentication capability to protect MEC systems. The study in [96] leverages blockchain features such as decentralization, tamper-proofing and consistency to build an authentication layer between edge/fog servers and IoT devices. The main objective is to monitor and verify all computing tasks offloaded to the MEC servers, which preserves edge computing from external attacks. In [97], smart contracts are employed for MEC to improve the efficiency of IoT computing, i.e. video coding, by providing a self-organized video transcoding and delivery service without a centralized authentication. Blockchain can protect the accuracy, consistency, and origins
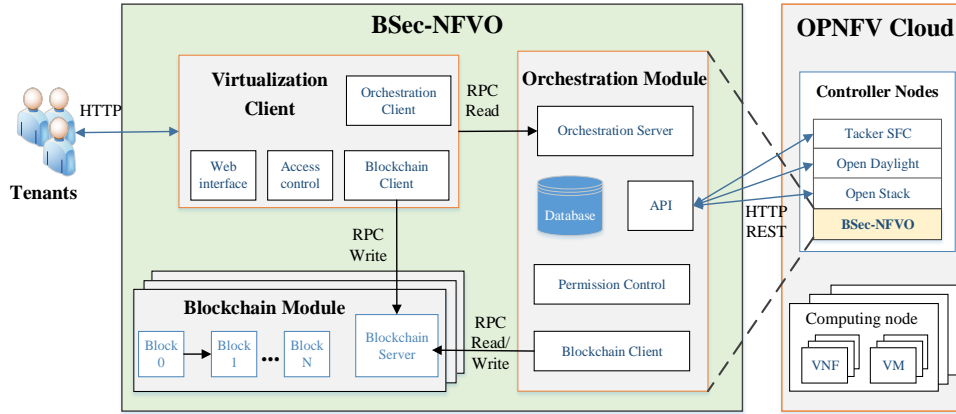
Figure 7: The conceptual blockchain-based NFV architecture.

of the data files in a transparent way. Further, the transactional data are also encrypted and stored on blocks, which has the potential to achieve privacy and security for MEC [98].

3.3. Blockchain for Network Function Virtualization (NFV)

Network Functions Virtualization (NFV) is a network architecture concept, standardized by the European Telecommunications Standards Institute (ETSI) that employs standard hardware for hosting various independent and network software components [99]. Basically, NFV includes three main architectural components, namely Network Function Virtualization Infrastructure (NFVI) which supports the execution of VNFs, Virtualized Network Functions (VNFs) that are the functions running on the NFVI, and Management and Network Orchestration (MANO) which cover the lifecycle management and orchestration of physical and software resources [100]. By decoupling hardware appliances, the network operators can save significantly equipment costs and reduce operational expenditures as well as automate network operation tasks without concerning about hardware installation. Particularly, NFV envisions to provide a diverse number of benefits for 5G networks, including enhancing flexibility and scalability of NF deployments and connections thanks to the decoupling of software from hardware, optimizing resource provision of the VNFs for better cost and energy usage, and optimizing VNFs operations with maximum failure rate and tolerable unplanned packet loss [101].

Network function virtualization and service function chaining, however, also incur new security challenges [102], [103]. Since end-to-end service function chains may deploy NFVs in an environment involving multiple cloud providers, such data transmissions can be compromised by curious cloud entities, leading to data leakage concerns. Furthermore, in a virtualized scenario, tenants often share the same cloud infrastructure. In this context, the possibility of attacks inside the cloud can increase, which damage the transparency and accountability of service providers. In NFVs, virtualization servers can run on virtual machines (VM) to offer specific functions to execute distinct operating systems such as VM migration or resource allocation using orchestration protocols. However, the security for the communication between the orchestrator and the physical machines is a current challenge. In fact, these architectures are very sensitive to attacks that can come from different horizons. In fact, a VM can be created by an attacker to run in a server and leveraged to carry out external denial-of-service attacks. Besides, internal attacks from curious VMs are another concern which can adversely impact data integrity and confidentiality [104].

In such a context, the blockchain technology has emerged as an efficient tool to help with these challenges. With the authenticity, integrity and non-repudiation natures, blockchain can facilitate

NFV networks in three main aspects [105], [106]. First, blockchain can enable reliable, easy and flexible orchestration of VNF services for better orchestration and network management. Second, blockchain can secure delivery of network functions and ensure system integrity against both insider attacks and external threats, i.e. malicious VM modifications and DoS attacks. Final, blockchain can perform data auditing and monitoring of system state during the network communication. We here review the latest advances in the use of blockchain to solve the above challenges for NFVs in 5G scenarios.

The authors of [107] propose a blockchain-based system called BSec-NFVO for secure management of service function chain orchestration operations in the Open Platform for Network Function Virtualization (OPNFV). A Practical Byzantine Fault Tolerance (PBFT) consensus protocol is employed to prevent collusion attacks without compromising latency and throughput. The architecture of BSec-NFVO is depicted in Fig. 7, consisting of three main modules: the visualization module, which provides an interface between tenants and the NFV and Service Function Chaining (SFC) services; the orchestration module, which executes instructions transmitted by tenants via the visualization module; and lastly the blockchain module that verifies and confirms transactions before execution by the orchestration module. By immutably logging all instructions enabled by blockchain, the proposed scheme can ensure authenticity, integrity and non-repudiation of instructions, which also provide data provenance for multi-domain NFV environments.

The work in [108] builds a blockchain-based Virtual Machine Orchestration Authentication (VMOA) framework to secure NFV/cloud orchestration operations for better authentication of orchestration commands in the lifecycle of cloud services. Here, blockchain acts as a decentralized database ledger shared between the virtualization server, the orchestrator and VM agents. The virtualization server is able to authenticate the orchestration command via blockchain VMOA ledger in an immutable and secure manner. Due to the removing of the requirement of third parties in the VMOA and using security features of blockchain, the proposed solution potentially achieves superior advantages such as records integrity, fault tolerance, and network trustworthiness, compared to its centralized counterparts.

Additionally, to realize a faulty or compromised VNF configuration, the study in [109] introduces a blockchain-based architecture to provide auditability to orchestration operations of network slices for securing VNF configuration updates. The prototype implements two smart contracts with specific transaction formats for safeguarding network slice management and VNF configuration operations. Especially, a Hyperledger Fabric blockchain platform associated with certificate authorities is integrated to manage digital certificates of every node, improving auditability and that only certified and authorized nodes participate in the blockchain-based NFV network.

The authors of [110] introduce a scheme called BRAIN, a Blockchain-based Reverse Auction solution for Infrastructure supply in NFV scenarios for dealing with challenges of discovery and selection of infrastructures to host VNFs acquired by end users. Smart contracts are designed to achieve a trustworthy agreement between stakeholders such as users and infrastructure providers regarding resources contracted and configurations required. Meanwhile, to support efficiency and security in wireless virtualization, blockchain is proposed in [111] to improve the trust and transparency among participants and stakeholders and enable more seamless and dynamic exchange of spectrum and computing resources in the 5G wireless networks.

Another work [112] presents a blockchain-based architecture for the secure configuration management of virtualized network functions (VNFs). The use of blockchain can provide security for VNF configuration state migration, building a trust mechanism between different infrastructure providers (tenants) and VNF vendors. Asymmetric keys are employed to develop a transaction

model for building anonymous authentication of tenants and VNFs and gaining confidentiality of configuration data through encryption. Such transactions are then appended in the blockchain data structure which also gives traceability and accountability of the VNF configuration updates.

Meanwhile, to realize the orchestration/management capabilities and business support systems in the context of architectural NFV, the research in [113] analyses blockchain-based Decentralized Applications (DApps) in support of multi-administrative domain networking. Blockchain can be an effective approach to establish an authentication layer for NFV Management and Orchestration (MANO) services across administrative domains. For example, blockchain can verify user access and grant access permission to resources between providers NFV-MANO components. In such a context, a smart contract can be leveraged to store access permission and assets information for MANO components as well as perform mappings of the structure of quotas, access grants and capacity of NFV users for efficient resource usage.

3.4. Blockchain for network slicing

To support IoT applications, 5G relies on the Network Slicing concept, which enables the separation of multiple virtual networks operating on the same physical hardware [114]. It enables telecom operators to portion their networks for specific services and applications. Network slicing is well envisioned by Network Softwarization which includes Virtual Network Functions (VNFs) running in the cloud inside virtual machines or containers. A network slice consists of a set of VNFs coupled with physical network functions to enable network services using cloud infrastructure [115]. Besides, network slicing also brings many unprecedented security challenges which consist of inter-slice security threats and the issues of resource harmonization between inter-domain slice segments [116], [117]. For example, due to the design of network slice instances sharing on open cloud-based architectures, attackers may abuse the elasticity of one slice to use the resources of other slices, which leads to the resource shortage of the target slice. Further, since multiple slices have often common control plane functions, attackers can exploit this network weakness to compromise the data of the target slice by maliciously accessing the common functions from another slice, leading to serious data leakages and damage of the system integrity [115].

In such contexts, blockchains can bring great opportunities for the security of 5G network slicing management. Blockchain can be exploited to build reliable end-to-end network slices and allow network slide providers to manage their resources. The work of [118] uses blockchain for reliability of resources in vehicle-to-vehicle communications over the vehicular network slices. The blockchain acts as the middle-security layer between vehicles and network controllers (i.e. roadside equipment), which eliminates the need of installing additional hardware from the operator side. This not only solves trust issues thanks to no required external authorities but also improves significantly vehicular network performances with low latency and enhanced throughput. Further, the blockchain-based approach can allow for the dynamic control of resource reliability, and improved the integrity and validity of the information exchanged among vehicles in the untrusted vehicular environments.

In order to guarantee secure and private transactions between the network slice provider and the resource provider for 5G services, blockchain is employed to build a brokering mechanism in network slicing [119]. When a slice provider receives a request or query to establish an end-to-end slice, it submits this request to blockchain for tracking and sharing. To support the deployment of the sub-slice components, smart contracts are designed, called as slice smart contracts (SSCs), where each SSC specifies the essential resources needed by the sub-slice. In this way, the resource providers can perform resource trading on contracts with sub-slice components. All related information about the sub-slice deployment is immutably recorded and stored in a permissioned blockchain controlled

by the slice provider. The proposed blockchain-based broker not only adds security abilities, but also supports privacy and accountability in network slicing.

The authors in [120] consider a blockchain slice leasing ledger concept using the 5G network slice broker in a blockchain to reduce service creation time and enable autonomous and dynamic manufacturing process. The works in [121], [122] also present how the blockchain technology can support the resource configuration value creation micro-processes and the 5G network slice broker use case in industrial automation use and smart grid. Manufacturing equipment leases independently the network slice needed for operations on-demand, approve service-level agreement (SLA) and pay for the service fee based on actual usage. In this context, blockchain performs the network slice trading, while smart contract orders slice orchestration based on agreed SLA from a slice broker.

In an effort to virtualize the slicing network, the authors in [123] propose a blockchain based wireless virtualization architecture where wireless resources such as RF channels are sliced into multiple (time/frequency) slices for mobile virtual network operators (MVNOs). Each transaction in blockchain for wireless virtualization contains information of bandwidth allocation, maximum channel power, and data rate which are used by the MVNOs when serving their users, and such a transaction is recorded immutably in the block for sharing. The blockchain based distributed scheme creates new MVNOs securely without revealing their private information to the public. Similarly, the work in [124] also proposes a blockchain-based wireless network virtualization approach to optimally allocate wireless resources for wireless network virtualization where the blockchain technology helps Virtual Network Operators (MVNOs) to sublease the RF slices from trustworthy Wireless Infrastructure Providers (WIPs). Blockchain is mainly used to build a reputation-based scheme for RF allocation of network slices with the objective of minimizing the extra delay caused by double-spending attempts in NFVs.

3.5. Blockchain for D2D communication

The exponential growth of mobile 5G data traffic has given impetus to the demand for high network rate proximity services. Device-to-device (D2D) communication has been envisioned as an allied technology for such 5G scenarios [125]. Conceptually, D2D communications refers to a type of technology that enables mobile devices (such as smartphone, tablet, etc.) to communicate directly with each other without the involvement of an access point or a core network of a cellular infrastructure. D2D takes advantage of the proximity of device communication for efficient utilization of available resources, enabling to improve the overall system throughput, mitigate communication delays and reduce energy consumption and traffic load [126]. D2D communication thus can facilitate new peer-to-peer and location-based applications and services, making it well suitable for the next mobile 5G communication networks and services.

However, direct communication between mobile devices also introduces new non-trivial challenges for D2D-based 5G networks in terms of security, network management and performance loss. Indeed, data sharing between devices may face risks of data leakage due to the malicious threats on the untrusted D2D environments. How to exchange mobile data to achieve low latency but ensure security is a critical challenge [127]. Furthermore, D2D devices may not be trusted, and can obtain illegal access to resources on servers (i.e. edge/cloud servers) if there is no an authentication mechanism on the network. Besides, the existing D2D architectures rely on the external authorities to grant data permission and request authentication during the D2D communication, which can incur unnecessary communication latency and degrade the overall network performance [128].

Blockchain can be a good solution to help overcome such challenges to facilitate D2D communication in 5G networks. For example, the work in [129] employs blockchain to build a secure content catching and sharing scheme among mobile devices for D2D networks. To mitigate the computation burden on devices, edge servers with high computing power are used to run mining puzzles for blockchain. In particular, blockchain demonstrates its efficiency in providing an incentive solution, which encourages caching-enabled users to store and share the contents with other mobile devices via D2D for better content sharing among mobile devices. The award policy empowered by blockchain stimulates the mining process in D2D devices, improving the robustness and security for the D2D network.

In order to support the authenticity of channel state information (CSI) of mobile users in D2D underlying cellular network, blockchain is applied in [130] to develop a secure mechanism using a consensus protocol. The mobile users can verify and validate the received broadcast CSI messages through the consensus mechanism before signing and adding immutably to the decentralized ledgers for sharing and storage. The authors also suggest that the blockchain-based approach is potential to dramatically improve the spectral efficiency while providing efficient CSI authenticity services for D2D networks.

Blockchain is also useful in another D2D scenario for supporting computation offloading [131]. In this work, a decentralized computation offloading coordination platform is developed and empowered by the blockchain which is able to manage the computation offloading requests and perform user matching. Each mobile user can participate in the computation offloading process and submit offloading requests to the blockchain platform. The other users in the D2D network and edge servers perform user matching to decide whether to participate in the offloading process to execute the requested computation tasks. The blockchain platform will incentivize COP which agrees to compute the task, and all request information is recorded and appended into blockchain for secure offloading management.

The work in [132] presents a delegated authorization architecture using blockchain-based smart contracts that enable users to use D2D communication to access IoT resources with respect to the preservation of the authorization information and network trust. Blockchains can immutably record hashes of the information exchanged during user authorization and payment events, while smart contracts can support for the concatenation of authorization requests. Here, smart contracts are placed on blockchain and run on all ledger nodes so that the resource access from D2D users can be handled automatically and quickly. The authentication mechanism can also protect network resource against DoS attacks that involve a very high resource request rate.

The authors in the works [133], [134] integrate blockchain with D2D communication to support the computation and offloading of the mobile data tasks as Fig. 8. With the trust and traceability features of the blockchain, a decentralized incentive approach is introduced to foster the collaboration of content creators and D2D users without the intervention of any third party. Mobile data can be transferred securely over the D2D network via blockchain ledgers, and computation offloading and content caching can be performed by edger servers for efficient execution.

In [135], a consortium blockchain is considered for further security and efficiency in the feature extraction application for encrypted images in D2D systems. Smart contracts are stored in blockchain, which solves the privacy leaking problem of image features. In a different direction, the study [136] exploits blockchain and smart contracts for the design and implementation of a trading application between the seller and the buyer via D2D communication. The trading can be performed automatically on blockchain by triggering the contract, which ensures transparent and reliable data exchange among different users. Moreover, to build a distributed secure monitoring system in D2D systems, blockchain is also considered in [137] to provide a high level of security
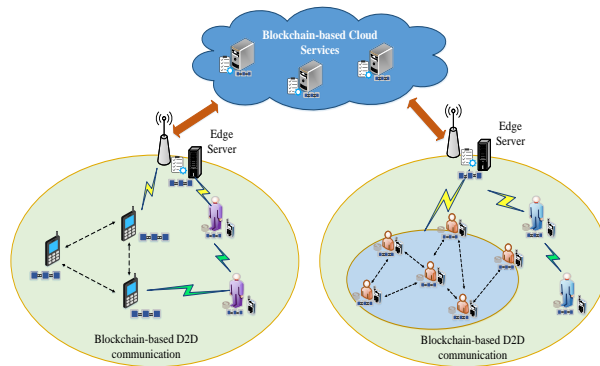
26

Figure 8: Blockchain for supporting D2D computation [133].

with reduced computational and communication costs. In particular, a secure access control using blockchain is also integrated to support identity authentication in a lightweight and scalable manner.

In summary, blockchain brings numerous opportunities to support 5G technologies and provides emerging services for 5G systems. Reviewing the state of the art works, we find that blockchain can provide security, networking solutions to protect 5G services and improve the performance of 5G-based systems. In the next section, we will present a systematic analysis and survey on the benefits of blockchain in a number of 5G services. We list blockchain use cases in the taxonomy Table 4 to summarize the key contributions of each reference work.

4. Blockchain for 5G services

Blockchains offer tremendous potential for improving existing 5G services and applications by supporting 5G technologies as discussed in the previous section. This vision can be achieved by taking advantage of interesting features that blockchains offer such as decentralization, privacy, immutability, and traceability. Blockchain can be regarded as a natural choice to facilitate the next-generation mobile communication networks for better 5G services. In this section, we provide an extensive discussion on the use of blockchain for important 5G services, including spectrum management, data sharing, network virtualization, resource management, interference management, federated learning, privacy and security services.

4.1. Spectrum management

With the increasing demand for bandwidth-hungry applications for 5G services such as mobile video streaming, big data processing, a foreseen network capacity shortage has become a key threat to mobile network operators (MNOs). Despite the technological achievements of 5G networks, the physical constraints such as spectrum limitations are still major limiting factors, which prevent operators from scaling their services properly. Spectrum scarcity in wireless networks hinders the fast improvement of throughput and service quality. Operators are forced to invest a large amount of money in their infrastructure to optimize the capacity by network densification and higher frequency reuse factors. Currently, MNOs have to face the challenges from the unavailability of usable frequency resources caused by spectrum fragmentation and the current fixed allocation policy, which prevents from meeting the requirements of the expanding market of wireless broadband and multimedia users [138]. To deal with the desire of mobile users to be connected at all times, anywhere, and for any application, more spectrum bandwidth and/or more efficient usage of that bandwidth is urgently needed. Some solutions have been proposed, including the fixed

Table 4: Taxonomy of Blockchain applications for key 5G technologies.

5G technology	Ref.	Use case	Main contributions	Limitations
Cloud computing	[68]	Blockchain for data verification on cloud	A framework called BlockONet for 5G access scenarios, aiming to improve the network credibility and security in 5G cloud fronthaul by data verification.	Security issues on cloud computing such as access authentication with blockchain have not been considered.
	[70]	Blockchain for data cloud data provenance	A blockchain-based cloud-centric IoT scheme using smart contracts for security of data provenance.	There is a lack of security analysis from the network perspective.
	[72]	Blockchain for access control on cloud	A hierarchical access control scheme for cloud blockchain.	Prototype of blockchain implementation is lacked.
	[74]	Blockchain for secure collaborative cloud	A blockchain solution for a joint cloud collaboration environment.	The feasibility of the proposed scheme has not been evaluated.
Edge computing	[91]	Blockchain for secure MEC sharing economy.	A MEC-based sharing economy system by using the blockchain.	Blockchain optimization in terms of latency has been overlooked.
	[92]	Blockchain for MEC-based smart city	A blockchain solution for secure communication between the home devices and sensors in the MEC-based smart city.	Blockchain optimization in terms of latency has been overlooked.
	[96]	Blockchain for MEC authentication	An authentication layer between edge/fog servers and IoT devices.	Only blockchain simulation have been given.
Network Function Virtualization	[107]	Blockchain for secure function management	A blockchain-based system called BSec-NFVO for secure management of service function chain orchestration.	Privacy for users has not been taken into consideration.
	[109]	Blockchain for audit of network slicing/ NFV	A blockchain-based architecture to provide auditability to orchestration operations of network slices.	NFV controller remains single-point failures.
	[112]	Blockchain for NFV secure configuration	A blockchain-based architecture for the secure configuration management of NFV.	The risks of NFV communications from attack should be considered practically.
	[113]	Blockchain for NFV management	A blockchain solution for multi-administrative domain networking for NFV management.	Security needs to be analysed.
Network slicing	[120]	Blockchain for reliable slice leasing	A blockchain slice leasing ledger concept for autonomous and dynamic manufacturing process.	Privacy of users has not been investigated.
	[123]	Blockchain for immutable network slicing	A blockchain based wireless virtualization architecture for network slicing.	This work lacks a testbed to evaluate the practicality of the proposed scheme.
	[124]	Blockchain for network slices resource allocation	A blockchain-based wireless network virtualization approach to optimally allocate wireless resources.	Performance for blockchain implementation has not been done.
D2D communication	[129]	Blockchain for secure D2D communication	A blockchain-based secure content catching and sharing scheme among mobile devices for D2D networks.	System scalability and communication costs have not been considered.
	[130]	Blockchain for D2D underlying cellular networks	A secure mechanism using a consensus protocol for D2D underlying cellular networks.	An experiment needs to set up to evaluate the scheme.
	[131]	Blockchain for secure D2D offloading	A decentralized computation offloading coordination platform for D2D.	Privacy is not taken into consideration

28

spectrum allocation strategies, but these approaches are inefficient in terms of wasteful spectrum usage because the license holders (or primary users) do not continuously utilize their full spectrum allocation. One solution for addressing the spectrum scarcity problem in radio 5G networks is to introduce secondary users that opportunistically monitor the spectrum and then transmit their data whenever the spectrum is idle [139]. However, spectrum sharing in such scenarios also raises security concerns and provides a central point of attack for malicious users. Another approach is to use certification authorities, providing provide certificates for cognitive radios inside each cell. Importantly, the use of such centralized architectures also adds single-of-failure bottlenecks when the authority is attacked or out of services, which leads to the disruption of the entire spectrum sharing network [140].

In comparison to such conventional spectrum management schemes, blockchain can be a much better solution to overcome the security and performance issues for spectrum management in 5G. Since blockchain is a form of decentralized database where no single party has control, blockchain can be applied to build spectrum sharing and management models with improved security and better performances, i.e. low latency and enhanced throughput. Especially, blockchain envisions to support spectrum management by providing the following benefits [141].

- *Decentralization:* The blockchain adoption eliminates the need of trusted external authorities such as spectrum licenses, band managers, and database managers. The inherent benefits are twofold: reducing unnecessary network overhead due to communicating with the authorities during the spectrum sharing, and improving system integrity and privacy due to no concerns about data leakage caused by curious third party intermediaries.

- *Transparency:* Since all transactions between spectrum users and service providers are reflected and recorded on distributed blockchain ledgers, the blockchain-based solution is able to provide better localized visibility into spectrum usage. Besides, blockchain can employ smart contracts, a self-executing platform, to perform auditability of spectrum sharing activities according to the pre-defined sharing policies.

- *Immutability:* The spectrum services, i.e spectrum sharing, monitoring or user payment is recorded to the only-appended blockchain in an immutable manner. By using consensus mechanisms empowered by blockchain miners, blockchain ledgers is well resistant to modifications caused by attacks or malicious users. This also ensures the reliability of the spectrum services and enhances the accuracy of the network implementation.

- *Availability:* Any network participants such as mobile users can access to spectrum resources managed by service providers to perform spectrum sharing and payment. Moreover, as blockchain broadcasts all service information to all entities, the spectrum sharing databases are also assessable to everyone in the network. Furthermore, there is no central authority to verify or record the data and transactions, which potentially enables a more transparent system without a loss of security properties.

- *Permissionless:* Because there is no single trusted entity as the central authority to control the network, new users or applications can be added to the overall system without seeking the approval of other users, providing a flexible sharing environment.

- *Security:* Blockchains enable efficient communication between users and service providers with strong security capabilities against threats, DoS risks and insider attacks.

In spectrum management, verification and access management is also of significant importance for enabling secure spectrum sharing [142]. In this work, blockchain can secure distributed medium-access protocol for cognitive radios (CRs) to lease and access available wireless channels. Blockchain is responsible for verifying and authenticating each spectrum-leasing transactions between primary and secondary users. Here, primary users are defined as spectrum license holders and can lease their allocated spectrum to increase spectrum efficiency as well as gain profits via a spectrum coin protocol. The blockchain performs exchanging currency, mining and updating the transactions, and leasing available spectrum through an auction. The authors also demonstrated that the blockchain adoption is beneficial to spectrum management in terms of better scalability, power efficiency in spectrum usage, improved accessibility with high degree of security and better system protection capability against DoS attacks and threats.

The work presented in [143] also describes a verification solution by taking advantage of blockchain for securing spectrum sharing in cognitive radio networks. The authors focus on building an auction protocol for spectrum payment services among primary users. Blockchain is regarded as a middle layer to perform spectrum trading, verify sharing transactions and lease securely the spectrum provided by a license holder. Besides, to solve the issues of privacy risks in spectrum sharing, a blockchain-based trustworthy framework called TrustSAS is presented in [144] to empower seamless spectrum sharing among secondary users (SUs) and incumbent users. The TrustSAS scheme relies on permissioned blockchains to monitor and control systems and cluster activities as well as tackle spectrum sharing events by using a Byzantine fault tolerant (BFT) consensus mechanism. All spectrum sharing transactions are validated by BFT and signed by blockchain miners for immutable recording on blocks. The experimental results show the superior advantages in terms of efficient auditability, improved privacy and lower end-to-end latency for spectrum access.

In addition, a spectrum sensing platform empowered by blockchain has been proposed and referred to as Spectrum Sensing as a Service (Spass) [145], [146], which provide services of spectrum sensing trading and payment. Smart contract acts as the core component which is responsible for scheduling spectrum sensing among secondary users and helpers which are the nodes offering sensing service in the secondary user network. Based on operation rules defined in the contract, smart contracts also perform access verification by using a malicious helper detection mechanism to identify whether a helper is honest or malicious. The proposed solution not only maximizes the profits of MNOs to encourage spectrum provision for user applications but also guarantees security requirements in an untrusted and decentralized spectrum sharing setting.

One of the biggest problems for unlicensed spectrum utilization is the unfair competition between MNOs for the utilization of unlicensed spectrum resources which are free to use and quite often available. To cope with this challenge, the authors of [147] introduce a new unlicensed spectrum sharing among MNOs on blockchain. For this purpose, authors use smart contracts in conjunction with virtual cryptocurrency to develop a coalitional spectrum sharing game for optimizing spectrum allocation. The account balance of each MNO can be achieved fairly through a transparent sharing enabled by smart contracts, aiming to mitigate the conflict between MNOs during the sharing. To further improve spectrum sharing for sustainability in unlicensed frequency bands, the work in [148] proposes to build a brokering platform to facilitate the collaboration between the network stakeholders. In this context, blockchain is feasible to establish a secure sharing to implement automatic negotiation processes for spectral resources between access point (AP) operators in a reliable manner.

Meanwhile, in the spectrum sharing environment between the aerial and terrestrial communication systems, unmanned aerial vehicles (UAVs) has been used for facilitating communication

on the sky. Currently, most UAVs in the market operate on the unlicensed spectrum (i.e., the industrial, scientific and medical bands) over the untrusted environment with significant security and privacy threats because of untrusted broadcast features and wireless transmission of UAV networks. To overcome such challenges, a spectrum blockchain architecture is considered in [149] to improve the spectrum sharing. To avoid wasteful spectrum usage in UAV network, a pricing-based incentive mechanism is proposed to encourage MNOs to lease their idle spectrum to a secondary UAV network to obtain some revenue from the UAV operators. Then, a secure spectrum sharing framework is introduced where blockchain uses immutable distributed ledgers to implement spectrum exchange while protect the sharing system from threats. The authors focus on developing a Stackelberg game for an optimal spectrum sharing strategy, which can maximize the profits of MNOs while provide security services for UAV-based networks.

4.2. Data sharing

One of the prominent characteristics of 5G is the strong data sharing capability in order to cope with the increasing content demands and data usage, especially in the 5G IoT scenarios. According to the latest release of Cisco [150], global mobile data traffic on the Internet will increase sevenfold between 2017 and 2022, reaching 77.5 exabytes per month by 2022. The rapid increase of content delivery over mobile 5G networks has revealed the need for new innovative data protection solutions to ensure secure and efficient data sharing over the untrusted environments [151]. In fact, sharing data in mobile networks is highly vulnerable to serious data leakage risks and security threats due to data attacks [152]. Mobile users tend to use information without caring about where it is located and the level of reliability of the information delivery, and the ability to control a large scale of information over the Internet is very weak. Blockchain may be an answer for such data sharing challenges. Indeed, blockchain can provide a wide range of features to improve the efficiency of data sharing in the 5G era such as traceability, security, privacy, transparency, immutability and tamper-resistance [153]. To control the user access to data resources, blockchain miners can check whether the requester meets the corresponding access control policy. Due to the decentralized architecture which enables data processing for user requests over the distributed nodes, the overall system latency for data delivery is greatly reduced and the network congestion can be eliminated, which improves the performance of data sharing with blockchain.

The problem of secure storage for data sharing is considered and discussed in [154]. The authors leverage blockchain as an underlying mechanism to build a decentralized storage architecture called as Meta-key wherein data decryption keys are stored in a blockchain as part of the metadata and preserved by user private key. Proxy re-encryption is integrated with blockchain to realize ciphertext transformation for security issues such as collusion-attack during the key-sharing under untrusted environments. In this context, the authors in [155] study blockchain to develop a data storage and sharing scheme for decentralized storage systems on cloud. Shared data can be stored in cloud storage, while metadata such as hash values or user address information can be kept securely in blockchain for sharing. In fact, the cloud computing technology well supports data sharing services, such as off-chain storage to improve the throughput of blockchain-sharing [156] or data distribution over the cloud federation [157].

In IoT networks, data transmission has faced various challenges in terms of low security, high management cost of data centre and supervision complexity due to the reliance on the external infrastructure [158]. Blockchain can arrive to provide a much more flexible and efficient data delivery but still meet stringent security requirements. A secure sharing scheme for industrial IoT is proposed in [159], which highlights the impact of blockchain for security and reliability of IoT data exchange under untrustworthy system settings. In comparison to traditional database

such as SQL, blockchain can provide better sharing services with low-latency data retrieval and higher degrees of security, reliability, and stronger resistance to some malicious attacks (DoS, DDoS) for data sharing. Further, the privacy of data is well maintained by distributed blockchain ledgers, while data owners have full control on their data shared in the network, improving the data ownership capability of sharing models [160].

The work in [161] also introduces a sharing concept empowered by blockchain and fog computing. The proposed solution constitutes a first step towards a realization of blockchain adoption as a Function-as-a-Service system for data sharing. Fog nodes can collect IoT data arising from private IoT applications and securely share each other via a blockchain platform which can verify all data requests and monitor data sharing behaviours for any threat detection.

Smart contracts running on blockchain have also demonstrated efficiency in data sharing services [162]. Smart contracts can take the role of building a trusted execution environment so that we can establish a set of information exchange frameworks working on blockchain. For example, the study in [163] leverages smart contracts to build a trustless data sharing in vehicular networks. The roadside units (RSU) can set the constraints for data sharing by using smart contracts which define shared time, region scope, and objects to make sure the data coins is distributed fairly to all vehicles that participate in the contribution of data. In addition, the authors of [164] introduce a smart contract-based architecture for consent-driven and double-blind data sharing in the Hyperledger Fabric blockchain platform. In the system, confidential customer data can be authorized and validated by smart contracts, and the service providers can execute the data tasks, add attributes and metadata, and submit it to the blockchain for validation and recording in a transparent manner.

4.3. Network virtualization

Wireless network virtualization is considered as an emerging paradigm in 5G to build different virtual wireless networks (VWNs) through mobile virtual network operators (MVNOs) to support rapidly increasing data demands caused by emerging 5G IoT applications [165]. Network virtualization is able to enhance wireless resource (RF slice) utilization, provide better coverage, and increase network capacity and energy efficiency [166]. The blockchain technology can provide the required characteristics of nonrepudiation and immutability to overcome the shortcomings of the previous configuration models. More precisely, blockchain is capable of creating secure virtual wireless networks (VWNs) so that wireless resource-owners sublease their wireless resources to provide for mobile virtual network operators (MVNOs) [123]. All participants of each virtual network slice is managed by a slice blockchain, which provides auditability of slice creation, monitors orchestration operations and data access of clients to the data centre. In such a decentralized virtual network, smart contracts can be very useful to provide automation and transparency in a distributed way instead of trusting a particular node or an authority process transactions. The solution of using blockchain and smart contracts can be an ideal solution to create secure end-to-end network slices for supporting virtual services with diverse requirements and resiliency [109].

Meanwhile, the work in [108] proposes blockchain to secure virtual machine orchestration operations in cloud-based virtualization systems. The main objective is to protect and secure virtual machines and make virtual machine managers well resistant to be compromised by threats. In fact, the complexity of virtual networks with multiple physical machines and virtual machines raises security concerns to be solved. For instance, a virtual machine can be created virtually by an external attacker to run in a server and used to perform external DDOS attacks, and internal attacks can act as legitimate entities to perform unauthorized data access which can impair the

data integrity and confidentiality of the network. Therefore, the proposed work considers the authentication issues in virtualization using a blockchain system shared between the virtualization server, the orchestrator and VMM agents. The orchestration requests (create, destroy, resize, copy, migrate) to a virtualization server are recorded as a transaction which is then authenticated by smart contracts to grant permission for the orchestration command, avoid malicious access to the data centre.

Moreover, in order to prevent from double-spending of same RF resources (frequency slices), the work in [167] leverages a distributed blockchain based scheme to sublease the frequency slice to MVNOs through wireless network virtualization. The proposed wireless virtualization architecture contains three main entities: wireless service providers who participate in sharing or subleasing their wireless resources to MVNOs; data sharing services for wireless resources; and block managers that are trusted devices working to maintain the blockchain. Each transaction in blockchain for wireless virtualization includes the information of bandwidth allocation, allocated channel power, data rates which are utilized by the MVNOs while serving their users through virtual networks. Specially, the work pays special attention to addressing the double-spending issue which is the allocation of same wireless resources to multiple MVNOs with a hope that all MVNOs would not use their leased spectrum at the same time for obtain maximum revenues. Compared to traditional approaches which mainly rely on centralized trusted authorities to perform resource sharing, blockchain is much more efficient in verifying each transaction to ensure that the wireless resources are scheduled to a given MVNO, which not only solves double-spending problems but provides fairness and transparency for network virtualization.

In an effort to secure management, configuration and migration of virtual networks services, the work in [112] presents a blockchain-based architecture for network function virtualization (NFV) and service function chaining (SFC). The blockchain module designed mainly performs three main functions: verify the format of the transaction, validate the accuracy of the signature of the transaction, and check the duplication of transactions. The service requests sent from NFV clients would be verified by blockchain via VNF key pairs and blockchain module key pairs for authentication through a consensus mechanism. In the same direction, the authors of [107] also analyse on how blockchain can support secure configuration and migration of NFVs. The consensus of Practical Byzantine Fault Tolerance (PBFT) is implemented on the Open Platform for Network Function Virtualization (OPNFV) to monitor and schedule the orchestration operations in virtualized networks. Furthermore, the security for network virtualization is analysed in [111], and that is based on blockchain to enable privacy of spectrum resources.

4.4. Resource management

In 5G networks, mobile resource (i.e. computation, memory, bandwidth, channel and storage) is one of the most popular services. The growing variety of 5G services leads to unprecedented levels of complexity in mobile resource management [168]. Edge/cloud computing in 5G needs to allocate its computation capacity to ensure efficient data execution while maintaining resources to serve the increasing demands of mobile users in the long term. In virtualized networks, the VNFs of a single slice may have heterogeneous resource requirements, i.e., CPU, memory, bandwidth and storage, depending on their functions and user requirements. The resource demands of slices of the same function type may be also different since they are serving different number of mobile users. For instance, a provider might run multiple Internet of Things (IoT) slices each one dedicated for a specific application. In such contexts, with heterogeneous resource capacities and heterogeneous resource requirements, implementing an optimal resource allocation to the mobile 5G network is a critical challenge. Importantly, the current resource management architectures mainly rely on a

central authority to perform resource allocation and verification of user resource access, but such models obviously remain single point failure risks and security from the third party. Moreover, the traceability of the current resource sharing schemes is very weak, which makes shared resources being compromised by attacks or used illegally by malicious users. All of these issues need to be solved effectively before deploying 5G services in practical scenarios.

Blockchains can be a highly efficient approach to solve the above remaining issues and improve the resource management. The use of blockchain enables the distributed resource allocation schemes as a strong alternative which is more preferable for both the service providers (edge/cloud, slice providers) and also mobile users/equipments. Blockchain would simplify the resource management concept, while remaining the important features of the core network and ensure strong security. For example, blockchain has been applied in VNFs in [110] to implement reliable resource allocation corresponding to user requests from different aspects such as user demand, cost. More interesting, smart contracts are also integrated to build an auction scheme which enables to allocate optimally to the network of users in a transparent manner (due to the transparency and immutability of smart contracts) in dynamic mobile environments.

Spurred by the power of blockchain, a resource management model is introduced in [169] which proposes a new concept of blockchain radio access network (B-RAN). The main goal is to achieve a spectrum resource balance in the network of user equipment (UE), access points (AP), spectrum bands and blockchain. The resource access services between UE and AP can be implemented by a smart contract-enabled protocol which defines access rules in conjunction with certain resource constraints such as service time, service demand, and service fee. The service requestor, i.e. mobile user, can undertake resource trading with AP by triggering the smart contract so that spectrum access is authenticated and resource is released via blockchain.

In the 5G networks, edge computing plays a significant role in improving QoS of mobile services thanks to its low latency and fast computing capabilities. Resource allocation for edge computing is of significant importance in edge-based mobile networks, such as IoT for better QoS and robustness of the system. A study in [170] employs blockchain to develop a decentralized resource allocation scheme which overcomes the limitation of previous centralized schemes in terms of latency and service provision speed. To provide adaptive computation services for IoT data, resource allocation should be dynamically adjusted without any centralized controller to maintain the high QoS. Blockchain is well suitable for such scenarios by offering a distributed ledgers to update resource information in an automatic and trustworthy manner [171]. In the case of resource scarcity in the network, a cooperative edge computing model can be necessary to support low-capability edge devices [172]. In this regard, blockchain would be useful to provide a reliable resource sharing between edge nodes. Resource requests can be verified strictly by intelligent contracts with access policies without passing a centralized authority, which also reduces resource sharing latency. Another blockchain-based resource allocation architecture for edge computing is presented in [173]. In this work, blockchain is responsible to monitor resource trading and user payment between miners and edge servers. The experimental results also show that the blockchain-based solution is truthful, individual rational and computationally efficient, compared to the conventional approaches.

In the multi-user network, a critical challenge is to allocate fairly the wireless resources among users with respect to their priorities (i.e., emergency levels). For example, a user who needs more resources for his service demand should be allocated more resources from the provider. Without authenticating the users priorities can lead to insufficient wireless resources to the users who are actually in high priorities. To provide a dynamic resource allocation solution for optimal resource usage, the work in [174] presents a blockchain consensus protocol to check the authenticity of priorities. Each mobile user can take the role of a blockchain node to perform authenticity for a

new message or request. The resource level is decided by an asynchronous Byzantine agreement among nodes, which guarantees trustworthiness and fairness for resource sharing.

Moreover, in optical networks, how to implement resource management while ensuring high security is also highly important. The authors in [175] employ blockchain to enforce security policies for 5G optical networks, namely Software Defined Optical Network (SDON). In fact, security for SDON is ensured by using traditional firewall flow tables that may be easy to modify and conflict with firewall policies. Once the attack causes a single point of failure, malicious traffic enters the SDON network for data theft and malicious modification. Blockchain with its anonymity, persistence, and auditability hence supports the trustworthiness of distributed resource communications and storage.

4.5. Interference management

The problem of interference management in the 5G infrastructural wireless networks is expected to become critical due to the unexpected data content traffic and numbers of 5G IoT devices. Although the telecom operators provide mobile services with the implementation of small size networks which can deliver various advantages such as high data rate and low signal delay, it is likely to suffer from various issues such as inter-cell, intra-cell, and inter-user interferences [176]. In the data-intensive service scenarios where a huge amount of mobile data is required to be transmitted in cellular networks, D2D communication can be a good choice to implement low-latency data transmission. However, the coexistence of D2D devices and cellular users in the same spectrum for communication and the short distance between D2D devices and users in small cells can result in cross-tier interference (CTI). The possibility of collaborating communication and sharing service benefits between mobile devices can be infeasible in practice due to the interest conflict between them. Building a fair and trusted economic scheme can be a solution to this problem, and thus mitigate the network interference. Currently, electronic money transactions have received extensive attention in small cell deployments, but the transaction consensus is often reached by passing a central authority [177]. This approach not only incurs additional costs of latency and transmission energy, but also raises security concerns from third parties. Distributed interference management with blockchain would be a feasible approach to cope with such challenges and facilitate interference management.

For example, the authors in [178] present a first example of using distributed blockchain to support a linear interference network. The main objective is to build a monetary mechanism using blockchain for optimal interference management. More precisely, a network model for a pair of two nodes including a transmitter and receiver is considered, wherein the transmitter (payer) may cause interference at the receiver (payee). A distributed interference avoidance transmission strategy is proposed so that a node has to pay in order to be active and then maximizes its monetary credit. The blockchain implementation realizes the monetary policies for cooperative interference management using a greedy algorithm. The proposed strategy also relieved that blockchain can help allocate economic benefits among users for interference avoidance [179].

In the D2D networks, interference may incur from the unfair resource allocation from the service providers to different user types. For example, users with higher spectral resource demands should be prioritized during resource scheduling. Motivated by this, a blockchain consensus method is proposed in [130] to evaluate the amount of cross-tier interference (CTI) caused by each user. The authors pay special attention to building an access control mechanism using blockchain for the authenticity of channel state information (CSI) with a dynamic resource allocation. A user with higher CSI can be allocated a larger amount of wireless resource. A simulation implementation

with an optimal user access algorithm is also presented, showing that the proposed scheme can improve the spectral efficiency for D2D users without interference effects.

The study in [180] utilizes power control with blockchain to support Quality-of-Service (QoS) provisioning for enabling efficient transmission of a macrocell user (MUE) and the time delay of femtocell users (FUEs) in blockchain-based femtocell networks. The macrocell base station (MBS) shares its spectrum resource to FUEs and the co-channel interference can be caused by the FUEs. Blockchain is essential to build a decentralized femtocell network so that payment can be done in a reliable way without the involvement of a middle party.

In another scenario, the interference between IoT transaction nodes (TNs) in the blockchain-enabled IoT network is also analysed in [181]. In this work, the authors focus on investigating the performance of blockchain transaction throughput and communication throughput by deriving the probability density function (PDF) with respect to the interference of TNs, for a transmission from an IoT node to a blockchain full function node. The blockchain-based solution is able to ensure high successful rate and overall communication throughput and preserve the IoT network against security threats.

Despite great research efforts in the field, the use of blockchain for interference management in 5G mobile networks is still in its infancy with few investigated works. The preliminary findings from the literature works are expected to open the door for exploring blockchain in overcoming the challenges in network interference management in terms of network throughput and security.

4.6. Federated learning

Recent years, federated learning has emerged as a promising machine learning technique for large-scale mobile network scenarios [182]. Federated learning enables distributed model training using local datasets from distributed nodes such as IoT devices, edge servers but shares only model updates without revealing raw training data. More specific, it employs the on-device processing power and untapped private data by implementing the model training in a decentralized manner and keeping the data where it is generated. This emerging approach provides an ability to protect privacy of mobile devices while ensuring high learning performance and thus promises to play a significant role in supporting privacy-sensitive 5G mobile applications such as edge computing and catching, networking, and spectrum management. In particular, the cooperation of blockchain and federated learning has been considered in recent works to solve complex issues in mobile 5G wireless networks. The authors in [183] introduce a blockchained federated learning (BlockFL) architecture which enables on-device machine learning without any centralized training data or coordination by employing a consensus mechanism in blockchain. By relying on the decentralized blockchain ledger, the proposed model overcomes the single point of failure problem and enhances the network federation to untrustworthy devices in a public network due to federated validation on the local training results. Besides, the blockchain also accelerate the training process by a reward mechanism, which in return promotes the collaboration of ubiquitous devices.

The study in [184] considers a reputation scheme which selects reliable mobile devices (workers) for federated learning to defend against unreliable model updates in mobile networks. To ensure accurate reputation calculation, a consortium blockchain with the properties of non-repudiation and tamper-resistance is leveraged to create a secure decentralized model update network of edge servers and mobile devices, leading to the reliability of federated learning on mobile edge computing. Importantly, blockchain associated with contract theory enables an incentive mechanism, which stimulates high-reputation workers with high-quality data to join the model training for preventing the poisoning attacks in federated learning [185].

Meanwhile, the authors in [186] incorporate blockchain with federated learning in the determination of data relevance in mobile device networks. This can be done by encourage mobile users to aggregate relevant information belonging to a specific topic that they are seeking during the interaction process with other users. They also introduced a decentralized way of storing data which reduces the risk from centralized data storage. A consensus mechanism called the Proof of Common Interest is considered that provides data verification services to ensure that data that is added to the blockchain ledger is relevant.

To provide a parallel computing architecture for big data analysis, especially for the precision medicine which data sets are owned by healthcare data users, an integrated blockchain-federated learning model is proposed in [187]. Federated learning assists training large medical data sets from various distributed data sources owned and hosted by different hospitals, patients, and health service providers, while blockchain-empowered smart contract is used to enable a distributed parallel computing environment for distributed deep learning using heterogeneous and distributed data. Moreover, the blockchain adoption enables secure, transparent, and auditable data sharing to promote international collaboration.

The work in [188] considers a blockchain empowered secure data sharing architecture for distributed devices in Industrial Internet of Things (IIoT). The key focus is on building a data sharing with privacy preservation by incorporating in federated learning. By using the power of federation of IoT devices, the data privacy is ensured via the federated learning model which allows to share the data model without revealing the actual data.

4.7. Privacy

In addition to smart emerging services that 5G can provide to mobile users and stakeholders, the complex 5G mobile environments also raise many privacy issues to be investigated carefully. According to a survey work in [53], the privacy challenges in 5G come from various aspects, such as end-to-end data privacy, data sharing privacy, trust issues in information flows, and trust issues in centralized mobile data architectures with third parties. Blockchain with its decentralization, traceability, availability and trust capabilities has been demonstrated widely its great potential in solving privacy issues in 5G networks and services [19]. As an example, blockchain is feasible to protect user data for decentralized personal data management [189], which enables to provide personalized services. Laws and regulations for data protection could be programmed into the blockchain so that they are enforced automatically. Interestingly, the blockchain is capable of providing full control of monitoring personal data when sharing on the network, which is unique from all traditional approaches which hinder users from tracking their data [11].

To provide decentralized and trusted data provenance services on cloud computing, the work in [190] uses blockchains to provide tamper-proof records and enable the data transparency. The blockchain can support in three steps, namely provenance data collection, provenance data storage, and provenance data validation. Data provenance record is stored on the blockchain, where blockchain nodes (i.e. mobile users, data owners, and service providers) can participate in consensus for confirmation of every block. During the data sharing between users and service providers, transmitted data can be highly vulnerable to malicious threats, i.e. data attacks, then privacy for shared data should be considered carefully. In this context, the authors in [191] presented a blockchain-based solution for secure data exchange. Data can be recorded in blocks and signed by miners so that sharing is securely implemented. An automated access-control and audit mechanism is considered wherein the blockchain enforces user data privacy policies when sharing their data across third parties for privacy preservation [192].

In current IoT applications, the private information management often relies on centralized databases owned by third-party organizations for data services such as data processing, data storage, data sharing. However, it is easy to find that this architecture remains weaknesses in terms of data leakage coming from curious third parties and high communication latency due to such centralized models. A privacy architecture using blockchain for smart cities is presented in [193], focusing on solving the above issues. Blockchain has the potential to help mitigate privacy exposure while allowing users to benefit from trusted transactions and better data control. The records of data access are added to a transparent ledger so that blockchain with consensus mechanism can verify and validate the data requests from all users to detect any potential threats in a decentralized manner without the involvement of any third parties. In another research effort, the work in [194] investigates how blockchain can support secure data storage and data availability in IoT health networks. Blockchain potentially empowers a decentralized and openly extendable network while protecting data on the network.

A privacy-preserved scheme empowered by blockchain is also considered and discussed in [195]. In this work, a consortium blockchain-based approach is designed to mitigate privacy leakages. Both energy users and suppliers are verified by a trading smart contract so that all trading transactions are authenticated for trustworthiness. Moreover, to achieve good privacy in industrial IoT, the study [196] introduces a decentralized blockchain architecture in conjunction with a hash algorithm and an asymmetric encryption algorithm. IoT data are still stored by the offline database (i.e. cloud storage), and the access record (storage, reading, and control) of each entity is stored in the block for tracking. Therefore, data storage on blockchain can be solved efficiently, and each operation will be strictly supervised via blocks.

In dealing with privacy issues in vehicular networks, the authors of [197] present a privacy-preserving authentication framework. The main goal of the proposed system is to preserve the identity privacy of the vehicles in the vehicular ad hoc networks. All the certificates and transactions are recorded immutably and securely in the blockchain to make the activities of vehicles (i.e. data sharing, energy trading) transparent and verifiable. In a similar direction, a model called CreditCoin for a novel privacy-preserving incentive announcement solution is presented in [198]. On the one hand, by offering incentives to users, CreditCoin can promote data sharing for network expansion, and the transactions and account information of blockchain are also immutable and resistant to be modified by attacks. On the other hand, with a strongly linked ledger, the blockchain controller can be easy to trace user activities, including malicious behaviours, for data protection.

In addition, the work in [199] proposes to use private smart contracts to design a privacy-preserving business protocol in e-commerce. In the contract, the interaction policy is defined via a business logic that determines types of trade, counterparties, underlying assets, and price information of the online shopping. The transactions between the seller and the buyer can be implemented securely and transparently via the contract without the disclosure of private information. Recently, the blockchain benefit to privacy of machine learning algorithm implementation is investigated in [200]. A privacy-preserving and secure decentralized Stochastic Gradient Descent (SGD) algorithm is established on blockchain, which enables computation in a decentralized manner in computing nodes. Computation parameters and information are kept in the block without revealing their own data and being compromised by data attacks. Obviously, the blockchain technology is promising to privacy preservation in the modern mobile networks and services, especially in 5G IoT systems, where data protection is becoming more important in the context of exponential mobile data growth in the 5G era [201].

4.8. Security services

The rapid increase of the 5G traffic and the explosive growth of valuable data produced by user equipment have led to strong demands for security mechanisms to protect mobile data against threats and attacks. With the important security properties, blockchain can provide a number of security services for 5G to improve the overall performance of future mobile systems. Considering the state of the art literature [19], blockchain mainly offers three main security services, including access control, data integrity and authentication, which will be summarized as follows.

4.8.1. Access Control

Access control refers to the ability of preventing the malicious use of network resource. Access control mechanisms guarantee that only legitimate users, devices or machines are granted permissions (e.g., read, write, etc.) the resources in a network, database, services and applications. Blockchain, especially smart contracts can offer access control capability to protect the involved system against any threats. As an example, a trustworthy access control scheme leveraging smart contracts is introduced in [202] to implement access right validation for IoT networks. The access policy is predefined and stored in the contract, which runs on blockchain. The contract can verify the user request using such a policy in a dynamic and decentralized manner. Different from traditional access control architectures which always use external authority for verification, the blockchain-based approach can perform direct access control between the requestor and the data centre so that the access latency can be reduced and security is improved.

To achieve access control for user requests to data resources in fog cloud-based IoT networks, a privacy-oriented distributed key management scheme using blockchain is proposed in [203] to achieve hierarchical access control. To receive a permission grant for data access, a subject needs to send a request with access information (i.e. identification, user address) to the security manager which checks the access and broadcast this request to other entities for verification via blockchain. The access is granted only when a consensus is achieved among all entities, which enhances reliability of the access control architecture.

To overcome the challenges caused by complicated access management and the lack of credibility due to centralization of traditional access control models, the authors in [204] introduce an attribute-based access control scheme. The ultimate goal is to simplify the access management by a distributed blockchain ledger while providing efficient access control ability to safeguard IoT data resources. Moreover, the work in [205] introduces a combination of Ethereum blockchain and ciphertext-policy attribute-based encryption (CP-ABE) to realize fine-grained access control for cloud storage. An access control policy is programmed in a smart contract which verifies the request based on the access period time and the attributes of data users. All information of control functionality results is stored on the blockchain, so the access control is visible to all users.

Meanwhile, a transaction-based access control scheme based on blockchain is proposed in [206]. The access verification follows a four-step procedure: subject registration, object escrowing and publication, access request and grant. Each request of the subject is registered as a transaction that is then submitted to blockchain to be validated by the data owner on blockchain by suing a Bitcoin-type cryptographic script. The works in [207], [208] also investigate the capability of blockchain for realizing access control services with Ethereum and Hyperledger Fabric platforms. To perform access control in the large-scale IoT networks, a platform called BlendCAC is considered in [209] as a promising solution for securing data sharing and resource trading among devices, users and service providers.

4.8.2. Data integrity

The integrity property ensures that the data is not modified in the transit or data is intact from its source to the destination. In recent years, distributed blockchain ledgers are starting to be used to verify data integrity for mobile services and networks, such as data management services or IoT applications, to overcome the limitations of the traditional models, which often rely on a third party auditor for integrity validation [210]. A blockchain-based framework for data integrity service is also presented in [211] which performs integrity verification based on blockchain for both data owners and data customers. To operate the data integrity service, a smart contract living on the blockchain is employed to audit transactions from all users. The information of data history and database stored in blockchain is strongly resistant to modifications, which improves data integrity.

To provide data integrity services on resource-limited IoT devices, the authors in [212] introduce a lightweight integrity verification model in Cyber-Physical Systems (CPS) by taking advantage of blockchain features. The key concept of the proposal is enabled by a three-level design, including the first level for running the Proof-of-Trust (PoT) mechanism among IoT devices, and two upper levels for data persistence and integrity verification by cloud. The implementation results reveal the efficiency of the blockchain-empowered model with good confidentiality, availability, integrity, and authenticity for IoT communication.

In an effort to deal with challenges caused by centralized traditional data integrity schemes such as symmetric key approaches and public key infrastructure (PKI), a decentralized stochastic blockchain-enabled data integrity framework is analysed and discussed in [213]. The proposed stochastic blockchain design includes the chain structure and the consensus mechanism for the data integrity checking procedures.

At present, with the popularity of cloud storage, how to guarantee data integrity on the cloud has become a challenging problem. The authors of [214] describe a framework for data integrity verification in P2P cloud storage via blockchain which makes the verification process more open, transparent, and auditable to all data users. Moreover, a new solution for improving integrity on cloud is introduced in [215]. In the system, blockchain constructs a semi-finished block on a candidate block arranged by data packages that is broadcast to all entities, while the consensus mechanism in blockchain, i.e Proof of Work, is able to generate tamper-resistant metadata associated with policy-based encryption method, leading to better data integrity. Besides, to tackle the issue of verification delay caused by procrastinating third-party auditors, the study [216] implements a solution for cloud storage using blockchain which enables the auditors to record each verification result into a blockchain as a transaction with a stringent time requirement. The time stamp in conjunction with signature and hash values can provide a time-sensitive data integrity service with a high degree of system security.

4.8.3. Authentication

Recent years, blockchain has been also investigated to realize the authentication capability to improve the overall security levels of 5G networks [69]. Mobile user access needs to be authenticated to detect and prevent any potential malicious behaviours to network resources (i.e. database, computing resources), which preserves the involved system and enhances the network robustness. In [217], a privacy-enhancing protocol is proposed by using the blockchain technology. The approach provides an ability to identify users by the evaluation on personal information which is extracted from the user request package. The smart contract is also integrated to perform authentication, aiming to prevent unauthorized access from attacks.

The authors in [218] consider an authentication scheme using blockchain for fog computing.

The fog nodes running on Ethereum blockchain employ smart contracts to authenticate access from IoT users. The proposed scheme facilitates managing and accessing IoT devices on a large scale fog network while providing security features such as decentralization, privacy and authentication without the need of a trusted third party.

In order to achieve authentication in vehicular networks, a strategy working on the blockchain platform is proposed in [219] which can undertake vehicle authentication and privacy preservation with seamless access control for vehicles. Blockchain can bring more advantages than conventional approaches using third party auditors in terms of high trust degree and transparency. Another blockchain application for privacy-awareness authentication is shown in [220], which allows both the server and the user to authenticate each other through this credential or certificate in a decentralized manner. All entities in the network achieve a consensus on an authentication task, and any potential threats can be detected and reflected on decentralized ledgers for necessary prevention.

In summary, we list the key blockchain use cases for 5G services in the taxonomy Table 5 to summarize the key contributions of each reference work.

5. Blockchain for 5G IoT applications

Nowadays, Internet of Things (IoT) have developed rapidly to provide ubiquitous services for almost all industrial applications. The evolution of the 5G networks would be the key enabler of the advancement of the IoT. A number of key enabling 5G technologies such as edge/cloud computing, NFV, D2D communication are developed to facilitate future IoT, giving birth to a new model as 5G IoT, which is expected to disrupt the global industry [221], [222]. Especially, in recent years, blockchain has been investigated and integrated with 5G IoT networks to open up new opportunities to empower IoT services and applications [223]. Reviewing the literature works, we find that blockchains mainly support some key IoT applications, namely smart healthcare, smart city, smart transportation, smart grid and UAVs, which will be highlighted as follows.

5.1. Smart healthcare

Healthcare is an industrial sector where organizations and medical institutions provide healthcare services, medical equipment, health insurance to facilitate healthcare delivery to patients. The emerging 5G technologies are potential to support smart healthcare applications, which fulfill the new requirements for healthcare such as improved QoS, better density and ultra-high reliability [224]. The integration of blockchain with 5G technologies can advance current healthcare systems and provide more performance benefits in terms of better decentralization, security, privacy [225], service efficiency and system simplification for lower operational costs [161]. Blockchain can incorporate with 5G technologies such as softwarization, cloud/edge computing for new smart healthcare services [226] as depicted in Fig. 9. The softwarized infrastructure can perform network functions through NFVs, which promote IoT communication, while cloud computing can support fast healthcare delivery services for early detection of patient health conditions. In such a 5G healthcare scenario, blockchain is employed to build a peer-to-peer database system which can validate and record all transactions (i.e. healthcare request, patient data) and store immutably them in decentralized ledgers. All transaction blocks are also visible to healthcare network members, including doctors, clinicians, and patients to accelerate data sharing during medications and treatment processes.

Blockchain is also integrated with healthcare networks [227] for healthcare networking and computing. A software-defined infrastructure is designed to facilitate the specification of home-based healthcare services, and a cloud edge model is considered to provide a flexible heterogeneous

41

Table 5: Taxonomy of Blockchain applications for key 5G services.

| 5G service	Ref.	Use case	Main contributions	Limitations
Spectrum management	[143]	Blockchain for secure spectrum sharing	A blockchain solution for securing spectrum sharing in cognitive radio networks.	Scalability of blockchain system has not been evaluated.
	[145]	Blockchain for secure spectrum sensing	A spectrum sensing platform empowered by blockchain.	Blockchain risks, i.e malicious consensus have not been considered.
	[147]	Blockchain for secure spectrum sharing	A new unlicensed spectrum sharing among MNOs on blockchain.	Data privacy should be considered.
	[149]	Blockchain for spectrum incentive network	A blockchain scheme for secure spectrum pricing-based incentive mechanism.	Only conceptual analysis is provided and simulation to evaluate the proposal is lacked.
Data sharing	[155]	Blockchain for data sharing privacy	A data storage and sharing scheme for decentralized storage systems.	The feasibility of the proposed model has not been investigated on real world cloud platforms.
	[159]	Blockchain for IoT data sharing	A secure sharing scheme for industrial IoT.	Implementation to investigate the system efficiency is lacked.
	[161]	Blockchain for fog-based data sharing	A sharing concept empowered by blockchain and fog computing.	Privacy issues in blockchain transactions has not been taken into consideration.
Network virtualization	[108]	Blockchain for secure virtualization	A blockchain scheme for secure virtual machine orchestration operations in cloud-based virtualization systems.	Only conceptual analysis is provided while simulation to evaluate the proposal is lacked.
	[167]	Blockchain for wireless virtualization	A blockchain scheme for supporting MVNOs through wireless network virtualization.	Data privacy has not been investigated.
	[112]	Blockchain for function virtualization	A blockchain-based architecture for network function virtualization.	Data privacy has not been investigated.
Resource management	[169]	Blockchain for spectrum resource allocation	A new concept of blockchain radio access network (B-RAN) for resource management.	Experiments on the proposed security scheme has not been done.
	[170]	Blockchain for IoT resource allocation	A decentralized resource allocation scheme for IoT with blockchain.	Investigations on blockchain prototype has not been done.
	[173]	Blockchain for edge resource management	A blockchain-based resource allocation architecture for edge computing.	Access control for IoT storage has not been considered.
Interference management	[178]	Blockchain for interference mitigation	A distributed blockchain to support a linear interference network.	Privacy issues in blockchain transactions has not been taken into consideration.
	[181]	Blockchain for controlling interference	A solution for interference control between IoT transaction nodes (TNs) in the blockchain-enabled IoT network.	The feasibility of the proposed model has not been investigated on real world cloud platforms.
Federated learning	[183]	Blockchain for network federation	A blockchained federated learning (BlockFL) architecture for network federation.	Access control for data storage has not been considered.
	[184]	Blockchain for secure FL	Consortium blockchain for non-repudiation and tamper-resistance of FL.	Real experiments on the proposed security scheme has not been done.

42
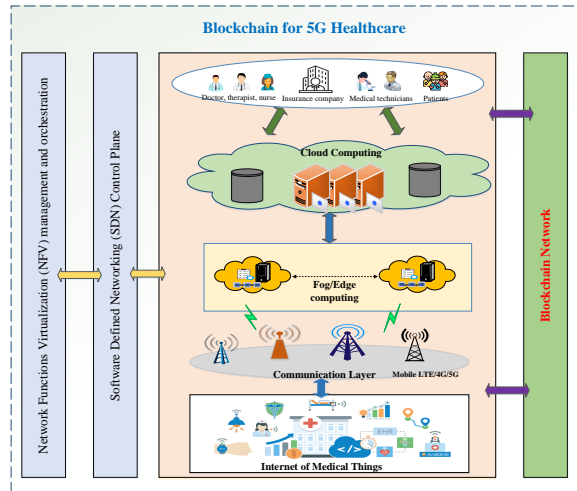
Figure 9: Blockchain for 5G healthcare [226].

health computation services. The role of blockchain in this work is to deal with health data interoperability and security issues, such as enabling effective authorized interactions between patients and healthcare providers (doctors, insurance companies), and delivering patient data securely to a variety of organizations and devices. Also, an access control mechanism empowered by smart contracts is integrated to support secure data sharing through user access verification, aiming to prohibit unauthorized users or threats from malicious access to health data resources.

A healthcare architecture based on D2D communications can a notable solution for efficient information sharing and large-scale data sharing, but it also exists critical privacy issues due to un-trusted sharing environments. An example is presented in [228] wherein blockchain is incorporated with the D2D technology for large scale feature extraction applications on cloud. In healthcare, for example, image features extracted from health data collection contain important information of patients and thus need to be secured. Blockchain would ensure secure data storage by shifting the information to decentralized ledgers which are maintained by all participants. All stored data on blockchain is signed digitally and identified by hash values, which also solve privacy leaking issues from tampering or forging.

Recently, blockchain is also considered and investigated in mobile edge computing (MEC)-empowered healthcare applications. The authors in [174] consider an edge blockchain for telemedicine applications, with the main objective of providing secure transmission and computation of health data. The MEC-based cellular health network contains a base station and a set of mobile users. Here, mobile users can access the Internet via the cellular network, and they share the computation resources of a MEC server linked with a base station in a small cell. Blockchain provides a consensus protocol to verify the patient priority which is defined as the level of wireless resources that a user needs for their computation. As a result, the optimal resource allocation can be achieved to ensure the quality of data transmission of the whole network, and user information is secured due to storing on blockchain ledgers. Another blockchain approach in edge-based mass screening applications for disease detections is presented in [229]. Due to a massive amount of captured multimedia IoT test data, an offline storage solution is considered and integrated with blockchain, which keeps cryptographic hashes of health data. This approach allows patients to take control of their information when performing clinical tests, visiting doctors or moving to other hospitals thanks to the transparency and availability of the blockchain protocol.

Meanwhile, cloud computing, a key enabling technology of 5G networks, has also provided

43

many notable solutions for healthcare services [223]. Many research works have dedicated to use blockchain for cloud-based healthcare networks, such as [230]. In this work, blockchain has proven its efficiency in improving the security of electronic health records (EHRs) sharing in cloud-assisted healthcare. The cloud computing is employed to store EHR ciphertext while the consortium blockchain keeps records of keyword ciphertext for data searching and sharing. In addition, to achieve secure data exchange between IoT health devices and cloud servers, a blockchain-enabled communication protocol is described in [231]. All sensitive patient information and medical test results can be stored and managed by blockchain where a consensus mechanism is necessary for user verification when a medical test is performed.

Very recently, we have also investigated and designed a blockchain architecture for cloud-based health management systems [232]. We have built a cloud platform where blockchain is used to create a secure data sharing network among healthcare providers and patients. All EHRs records are stored in a decentralized storage IPFS storage on cloud, where smart contracts are also integrated to provide authentication services for data sharing. The user without passing a verification phase will not have the right to access the data on cloud, while data retrieval for authorized users is accelerated by the decentralized data storage mechanism using IPFS.

5.2. Smart city

The evolution of 5G technologies has enabled enormous business opportunities and digital transformation initiatives for new smart city models, proving a wide range of services for city citizens [233]. Smart cities involve a variety of components, including ubiquitous IoT devices, heterogeneous networks, largescale data storage, and service provisions. Despite the potential vision of smart cities, how to provide smart city services with high security remains unsolved. In this scenario, blockchain can be a promising candidate to solve critical security issues and empower smart city services [234], [235]. To simplify the management of smart city services on a large scale, a city can be divided into small blocks called smart blocks. Each smart block consists of a variety of IoT devices, such as sensors, cameras, etc. of a certain area under the control of a block admin. A private blockchain using a ledger database is important to securely store all information generated from IoT devices during data exchange, data offloading and computation services.

Another research in [91] analyses a sustainable IoT architecture empowered by blockchain for a secure sharing economy services in mega smart cities. The proposed system employs cognitive fog nodes at the edge to gather and process offloaded multimedia payload and transactions from a mobile edge node and IoT devices. To extract significant information from the outsourced data, machine learning is used during the data analytic, and such results are then put in blockchain for secure sharing and storage. Furthermore, to solve data security issues in IoT for smart cities, blockchain is considered in [236] to secure communication between the smart city and home devices and sensors. IoT data can be executed and computed at the edge layer for latency reduction, while user access information is recorded by blockchain, which works as a universal ledger. The key benefits of the proposed scheme include system transparency as well as the permissionless property which allows adding any new IoT devices without involving any authorities.

In 5G smart cities, a prohibitively large amount of surveillance data will be generated continuously from ubiquitous video sensors. It is very challenging to immediately identify the objects of interest or detect malicious actions from thousands of video frames on the large scale. In such a context, building a distributed edge computing networks is highly efficient to achieve scalable data computation [237], [238]. From the security perspective, blockchain would be a natural choice to establish decentralized security solutions by interconnecting edge nodes, IoT devices and city users, where data sharing, computation and business transactions can be performed on the blockchain

44

ledger platform. It is also demonstrated that the use of distributed blockchain provides more benefits than the centralized architectures with a central cloud server in terms of lower latency, energy consumption, better service delivery, faster user response with security and privacy guarantees [239].

Currently, most Mobility-as-a-Service (MaaS) which monitors the connections between transportation providers and passengers in smart cities is controlled by a central MaaS manager, which potentially introduces privacy leakage and system disruptions if this entity is attacked. By integrating with the blockchain, the MaaS model can be operated in a much more secure and decentralized manner [240]. In this work, blockchain can help improve trust and transparency for all stakeholders and eliminate the need of centralized entity to make commercial agreements on MaaS. The mobility services, such as ticket purchase or payments for using transports, can be programmed by smart contracts, which enable automatic and reliable service trading and payment.

Cloud computing is also a promising technology which can be incorporated to support strong computation and storage capabilities for smart city data, i.e big data from ubiquitous IoT devices. A cloud-smart city architecture is introduced in [241], wherein big data processing can be performed by cloud servers, while data auditing can be achieved by using the blockchain without third party auditors (TPAs). The proposed scheme focuses on building an optimized blockchain instantiation called data auditing blockchain (DAB) that collects auditing proofs and employs a consensus algorithm using a Practical Byzantine Fault Tolerance (PBFT) protocol. The simulation results reveal the potential of the blockchain adoption for big data in smart city with lower communication costs and better security. Furthermore, blockchain can enable interconnection cloud service providers to achieve a larger scale computation service [242]. Any cloud server can be regarded as a blockchain node and cloud computing events are recorded on the ledgers, which effectively improves the system robustness and avoids the risks of single points of failures once the cloud server is compromised or attacked.

5.3. Smart transportation

With the rapid development of modern 5G communication and computation technologies, recent years have witnessed a tremendous growth in intelligent transportation systems (ITS), which create significant impacts on various aspects of our lives with smarter transport facilities and vehicles as well as better transport services [243], [244]. Smart transportation is regarded as a key IoT application which is the integrated architectures of communication technologies and vehicular services. One critical issue in smart transportation is security risks caused by dynamic vehicle-to-vehicle (V2V) communications in untrusted vehicular environments and reliance on centralized network authorities. Blockchain shed lights on several inherent features to implement distributed data storage, peer-to-peer communication, and transparently anonymous user systems, which envisions to build secure, decentralized ITS systems to facilitate customer transportations [240]. One of the most significant services to realize intelligent transportation is data transmission among vehicles. How to provide efficient data exchange services in terms of low latency and increased network throughput while still ensure high degrees of security is a critical challenge. Blockchain would enhance QoS of the current ITS system by offering a decentralized management platform, wherein all vehicles and road side units (RSU) can perform data transmission and sharing on a peer-to-peer model to reduce end-to-end delay without using a vehicular authority [245].

In order to adapt the large volumes of electric vehicle (EV) charging/discharging demand during transportation, the blockchain concept is introduced in [246] that enables peer-to-peer transaction and decentralized storage to record all transaction data of EVs. In fact, EVs can be considered as a mobile power backup device to support the smart grid for load flattening, peak

shaving and frequency regulation. This new energy trading paradigm is known as vehicle-to-grid (V2G), which is essential to build a safer and more sustainable energy platform for both EVs and the main power grid. Consumer power loads from smart city are all connected to the public blockchain power exchanging platform, where the electricity supply and user demand information are transmitted, encrypted and recorded in the blockchain platform. In such a context, the EV can publish and transmit the charging or discharging orders (for buying and selling) to the power blockchain platform which executes the EV request, performs energy trading and payment, and saves the transaction to the distributed ledger, which is also visible to every vehicle in the vehicular network.

In the line of discussion, the authors in [247] also analyse a V2G energy trading model with a combination of blockchain and edge computing. EVs can buy energy from local energy aggregators (LEAGs) via trading. The vehicular communication is secured by a consortium blockchain, in which all the transactions are created, propagated, and verified by authorized LEAGs. To further reduce latency and processing posing on burden blockchain, edge computing servers are employed to undertake block creation and mining. LEAGs can buy computation services from edge computing providers to finalize this process, and store mined blocks to the nearby edge nodes. The blockchain technology envisions a trustless network to eliminate the operation cost of the intermediary participation, which will realize a quicker, safer and cheaper way in ITS systems. Moreover, authentication for vehicle access is of paramount importance for vehicular networks. In this regard, smart contract would be a notable approach which can authenticate and verify vehicular transactions by triggering the programmed logic functions [248]. This enables direct authentication for registered vehicles without revealing device privacy and effectively prevents potential attacks from malicious vehicles.

Recently, blockchain has been used to build secured and controlled vehicular ad hoc networks (VANETs) [249]. With the increasing scale of the current VANETs, traditional VANET frameworks with centralized control mechanisms obviously cannot match the diversification of VANET traffic requirements. Decentralizing controller can be an efficient solution to localize decision making to an individual controller, which thus minimizes the control plane response time to data plane requests. To achieve secure communications between controllers as well as between controllers and EVs, blockchain is leveraged to achieve agreement among different nodes in terms of traffic information and energy demands without using centralized trust management.

Another aspect in VANETs is the security of power trading between EVs and V2G networks. In fact, it is very important to design a safe, efficient, transparent, information symmetrical trading model for VANETs to provide ubiquitous vehicular services (i.e. traffic transmission, vehicle cooperation, energy payment). Blockchain is introduced in [250] for a reliable decentralized power trading platform where a V2G EV trading smart contract is integrated for trading authentication and a decentralized energy ledger is for data storage and sharing without relying on a trusted third party, eliminating the need for trusted third parties to address the high cost, inefficiency, and insecure data storage of traditional centralized organizations.

5.4. Smart grid

The continuously growing power demand in modern society has been a critical challenge that needs significant attention in the present day of the smart grid era. The energy industry has witnessed a paradigm shift in power delivery from a centralized production and distribution energy system into a dynamic mode of decentralized operation thanks to the support of ubiquitous 5G technologies such as IoT, edge/cloud computing, network slice and D2D communication [251], [252]. In this regard, blockchain, a decentralized database platform, enables completely new technological

systems and business models for energy management with added features such as decentralization, security, privacy and transparency [122]. In the 5G energy network slice, the electricity can be allocated to each power user in the housing society through a distributed blockchain platform where all users are interlinked with energy providers on secured and distributed ledgers.

In smart grid, in order to monitor the electricity distribution and power usage of customers, a smart meter can be installed at each home to collect the real-time electricity consumption data for better smart home services. However, a critical drawback is that private user information such as home address, personal information may be disposed and adversaries can track users to obtain electricity consumption profile. To overcome this challenge, blockchain has been introduced in [253] for a privacy-preserving and efficient data aggregation network. The power network has been divided into small groups, each group is controlled by a private blockchain. Instead of relying on a third party for data aggregation, a certain user is chosen to aggregate all user data within his network and record them to the blockchain for storage and monitoring. Such an aggregator only collects data and all other users share the equal right to verify and validate transactions to achieve consensus, which eliminates the risks of single points of failure and improves system trust accordingly.

In order to achieve traceability of power delivery in smart grid, blockchain can be applied to provide transparency and provenance services [254]. The customer can register their information on blockchain and perform energy trading and payment by uploading a transaction to blockchain. By creating an immutable data structure, data recorded and transferred onto the system cannot be altered. Smart contracts are also very useful to provide a transparent and fair energy trading between consumers and utility companies through an energy policy which defines all trading rules. Once the energy billing payment is completed, for example, both the user and the service provider receive a copy of the transaction, which allows users to keep track of their energy usage.

At present, the sophistication of cyberattacks has posed a challenge to the current smart power systems. In recent years, cyber-attacks have caused power systems blackout due to data vulnerability, malicious events or market data manipulation [255]. Therefore, the introduction of blockchain, a strong security mechanism, can help overcome such challenges. The interactions between the electricity market agent and the customer are reflected via transactions which contain electricity demands, electricity price, user information. All such transactions are signed by the private key of the sender (i.e. energy user) to perform energy trading with the agent. In such a context, an attacker can threaten the communication link between users and the agent, but it may be impossible to break the transaction due to the lack of user private key and such malicious access is detected and discarded by consensus mining. Additionally, the authors in [256] also present a research effort in using blockchain to mitigate cyber-attacks on a smart grid. Every prosumer, consumer and substation are connected through a block chain based application under the control of a smart contract, which perform transaction verification when energy transmission occurs. The consensus is maintained by the computing power of all distributed energy servers and users, which also make the energy system well resistant to cyber-attacks [257].

In a similar direction, the work in [258] proposes a smart and scalable ledger framework for secure peer to peer energy trading in smart grid ecosystems. The energy network considered consists of a set of EVs which can participate in three operations, namely charging, discharging and staying idle, EV aggregator which works as an energy broker and provides access points to EVs for both charging and discharging operation, and energy cash as the currency for energy payment. To avoid the issue of spanning and Sybil attacks, instead of using PoW which remains high block generation latency, the authors suggest a proof of time concept. A client must collect a random token, i.e., random messages from neighbours, which makes the process costly for an attacker to

achieve the throughput of honest transactions as each transaction contains associated timestamp with it. For security of energy transactions, another work in [259] also builds a fully decentralised blockchain-based peer-to-peer trading scheme, which realises a more secure transaction and reduced storage burden of distributed prosumers.

Recently, mobile edge computing (MEC), a significant 5G enabling technology, is also cooperated with smart grid. Although MEC can offer promising benefits such as low-latency computation, reduced network congestion for better energy delivery, the characteristics inherent of the MEC architecture such as heterogeneity, mobility can be exploited by attackers to perform nefarious activities. Thus, how to ensure security for MEC-based smart grid system is important. In the work [260], a permissioned blockchain edge model is introduced with the main objectives of privacy protections and energy security. At the layer of distributed edge devices and power supply, smart devices and power supply facilities compose smart grid generating electricity trading transactions. Meanwhile, the smart contract running on blockchain assigns tasks to edge devices and records transaction on blockchain, which enables a secure and trustworthy trading environment. By integrating with distributed edge computing, blockchain can offer a larger number of services, such as device configuration and governance, sensor data storage and management, and trading payments.

Blockchain for edge-empowered smart grid has been considered in [261], in which a blockchain based mutual authentication and key agreement protocol is proposed. The smart grid network model used consists of registration authority (RA), end users (EUs), edge servers (ESs) and blockchain. ESs are responsible to supply timely data analysis and service delivery, and each ES is linked with blockchain to prevent web spoofing attacks and guarantee smooth energy trading and user interactions. The authors in [262] also present a blockchain implementation for smart grid to guarantee information privacy of energy user and energy trading. MEC servers act as active blockchain nodes with strong computation capabilities to enable fast data analytic services, i.e. processing large transaction graphs of energy trading, within the energy trading system among EVs.

5.5. Unmanned Aerial Vehicles (UAVs)

The rapid development of drones or Unmanned Aerial Vehicles (UAVs) [263] is creating numerous new business opportunities for service providers. UAVs can be considered as flying IoT devices and have been used for various purposes, such as military, vehicular networks to smart city. In the era of 5G networks, the rapid growth of IoT data traffic poses critical challenges on current network infrastructure with static base stations (i.e. access point, router) to support data demands of billions of IoT devices for large-scale services. Therefore, using UAV for supporting IoT networks is a natural choice. Indeed, UAV can act as a flying base station to provide unprecedented IoT services, i.e. dynamic traffic offloading, object monitoring due to its mobility and flexibility. However, the operation of UAVs in the sky is highly vulnerable to several privacy and security risks that target data accountability, data integrity, data authorization, and reliability [264].

Recent years have also witnessed a new research trend on the combination of blockchain and UAVs for solving critical challenges in UAV networks and empowering new 5G IoT applications. For instance, the work in [265] takes advantage of consortium blockchain for a spectrum sharing platform between the aerial and terrestrial communication systems for UAV-based cellular networks. The key idea is to establish the distributed shared database to perform secure spectrum trading and sharing between the mobile network operators (MNOs) and the UAV operators. The proposed model possibly addresses two key issues: security risks of UAV-based spectrum trading

due to the unauthorized spectrum exploitations of malicious UAVs, and privacy leakages caused by the centralized sharing architecture with third parties.

To support the security of UAV communication in ad hoc networks (UAANETs), permissioned blockchain has been adopted in [266] to provide decentralized content storage services and detect internal attackers during efficient content dissemination. The key reason behind the blockchain adoption for UAANETs is the ability of blockchain to securely maintain a consistent and tamper-resistant ledger to record all the transactions of content sharing and storage in a decentralized environment without the need for any central authority, which is applicable to the complex and vulnerable network. Besides, to overcome the limitations of traditional blockchain models with low throughput and high resource consumption, an efficient and scalable Adaptive Delegate Consensus Algorithm (ADCA) is integrated to perform consensus without the mining procedures. Similarly, the work [267] also proposes to use blockchain for secure data dissemination in UAV networks. Data collected from UAVs can be recorded and stored in decentralized database ledgers to mitigate the storage burden on UAVs. The use of blockchain allows any of the users in the UAVs network to participate in consensus processes and implement verification without any external authorities, such as cloud servers. The proposed model has the potential to solve various security issues, including spoofing, Denial-of-service (DoS), eavesdropping and data tampering.

The authors in [268] consider an autonomous economic system with UAVs where blockchain acts as a protocol of autonomous business activities in modern industrial and business processes. IoT devices, robots, UAVs in the multi-agent systems can exchange data each other to perform automatic collaborative works (i.e. in smart factory) and share collected data to users via a peer-to-peer ledger. Blockchain link all agents together to create a distributed network where any agent can join and perform block verification to maintain the correct operation and security of the system. To avoid the issues of data leakage or data loss during the transmission among UAVs, blockchain is also considered in [269]. The data transfer process occurs within the blockchain which allows storing all user information and exchange records for security management.

More interesting, blockchain has been considered and incorporated with cloud/edge computing for enabling emerging UAV-based applications. The authors in [270], [271] analyse a blockchain-enabled secure data acquisition scheme for UAV swarm networks in which data are collected from IoT devices employing UAV swarms. Each of the UAVs maintains its own shared key to expedite communication with IoT devices when implementing the security mechanism (i.e., sign, verify, encrypt, and decrypt). A smart contract is also employed in order to handle the IoT devices and missions in data acquisition. The study in [272] also explores a Hyperledger Fabric blockchain design for UAV swarm networks. Each communication request among UAVs is recorded as a transaction which is validated and verified by the mining process enabled by the computing power of all entities in the UAV network for maintaining the blockchain.

In an effort to enhance the security of edge-based UAV networks, the work in [273] proposes a neural blockchain-based transport model as Fig. 10 to ensure ultra-reliability for UAV communication and enable intelligent transport during UAV caching through user equipment (UE) via MEC. The blockchain acts as a distributed database ledger which is shared among all the involved entities (UAVs, MEC servers, and users) identified by their public keys (IDs). The smart contract is responsible to monitor user access and perform verification, while blockchain provides a secure data sharing environment to facilitate content sharing and data delivery between the UEs and the caching servers.

In addition, the authors in [274] integrate blockchain in a cloud-assisted UAV network for surveillance services to investigate the safety condition of the dam infrastructure in real-time. Two blockchains are designed, a public bitcoin blockchain for payment trading, and a private
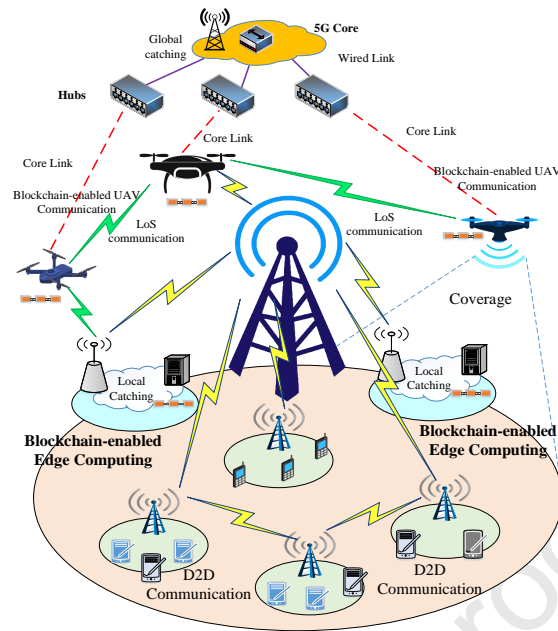
Figure 10: Blockchain for secure 5G UAV networks [273].

blockchain for data storage on the network of UAV providers, users, and cloud providers. To join the blockchain, each entity, i.e. IoT sensor users should have certificates obtained from a certificate authority. Data gathered from cloud providers is considered as an object which is then hashed and anchored by the UAV provider into the blockchain network. The solution using blockchain bring various benefits, including reduced latency due to direct communication without passing a third party, and high data integrity and tampering resistance thanks to the hash function and consensus process.

In summary, we list the key blockchain use cases for 5G IoT in the taxonomy Table 6 to summarize the key contributions of each reference work.

6. Main findings, Challenges and Future research directions

Integrating blockchain in the 5G mobile networks is a hot research topic now. Many research efforts have been devoted to the development of blockchain technology for 5G mobile networks. In the previous sections, we have presented a state of the art review on the current achievements in the blockchain adoption in 5G networks. Specially, we have provided an extensive discussion on the convergence of blockchain into key 5G enabling technologies, namely cloud computing, edge computing, Network Function Virtualization, Network Slicing, and D2D communication. The survey has also covered and highlighted the benefits of blockchain to empower fundamental 5G services such as spectrum management, data sharing, network virtualization, resource management, interference management, privacy and security services. We also analyse the integration of blockchain in a wide range of 5G IoT applications, ranging from smart healthcare, smart city, smart transportation to smart grid and UAVs. Based on the current great research efforts in the literature, in this section, we will summarize the key findings inherited from the integration of blockchain in 5G networks and services. We also identify possible research challenges and open issues in the field along with the future research directions that should be considered and investigated to encourage more innovative solutions and studies in this promising area.

Table 6: Taxonomy of Blockchain applications for key 5G services.

5G IoT application	Ref.	Use case	Main contributions	Limitations
Smart healthcare	[227]	Blockchain for healthcare	A blockchain solution for healthcare networks.	Implementation to investigate the system efficiency is lacked.
	[228]	Blockchain for D2D-based mobile networks	A blockchain scheme for secure D2D in large scale feature extraction in mobile networks.	Only conceptual analysis is provided and simulation to evaluate the proposal is lacked.
	[174]	Blockchain for MEC-based health-care	A blockchain model for mobile edge computing (MEC)-empowered health-care applications.	The performance of the proposed framework has not been simulated.
	[230]	Blockchain for cloud-based health-care	A blockchain scheme for cloud-based healthcare networks.	Privacy issues in blockchain transactions has not been taken into consideration.
Smart city	[246]	Blockchain for secure vehicular data storage	A peer-to-peer transaction and decentralized storage model for secure records of transaction data of EVs.	Data privacy has not been investigated.
	[247]	Blockchain for energy trading in V2G	A V2G energy trading model with a combination of blockchain and edge computing.	The feasibility of the proposed model has not been investigated on real world energy platforms.
	[249]	Blockchain for controlled vehicular networks	A blockchain network for building secured and controlled vehicular ad hoc networks.	The performance of the proposed framework has not been investigated.
Smart grid	[253]	Blockchain for private smart grid	A blockchain model for privacy-preserving and efficient data aggregation network.	Data privacy should be taken into consideration.
	[254]	Blockchain for traced power delivery	A blockchain scheme for traceability of power delivery in smart grid.	Implementation to investigate the system efficiency is lacked.
	[256]	Blockchain for detecting cyber-attacks	A model with blockchain to mitigate cyber-attacks on a smart grid.	The effectiveness of the proposed framework has not been simulated.
Unmanned Aerial Vehicles	[265]	Blockchain for UAV spectrum sharing	A blockchain model for secure spectrum sharing platform between the aerial and terrestrial communication.	Only conceptual analysis is provided and simulation to evaluate the proposal is lacked.
	[266]	Blockchain for secure UAV data services	A blockchain model for decentralized content storage services and detect internal attackers in UAV.	The feasibility of the proposed model has not been evaluated on real world IoT platforms.
	[268]	Blockchain for economic model in UAV	A blockchain scheme for an autonomous economic system with UAVs.	Data privacy has not been investigated.

6.1. Main findings

The comprehensive literature review on the integration of blockchain in 5G technologies, 5G services and IoT applications reveals many important findings, which would enable to open up numerous opportunities for the newly emerging 5G scenarios. This sub-section will highlight the key findings inherited from the convergence of these promising technologies.

6.1.1. Blockchain for 5G technologies

Blockchain can offer many promising technical properties such as decentralization, privacy, immutability, traceability, and transparency to empower 5G technologies. Reviewing the literature works, we find that blockchain can support well 5G technologies mainly from three key aspects, including security, system performance, and resource management. The current 5G technology infrastructure is mainly enabled by the centralized network settings, such as edge/cloud computing which obviously show security vulnerabilities due to the reliance of third parties. Blockchain can arrive to build decentralized network architectures for 5G technology platforms. For example, the concept of blockchain-based cloud computing enables decentralization of cloud/edge 5G networks [68], [83] which gets rid of centralized control at the core network and offers a decentralized fair agreement with blockchain consensus platform. Even when an entity is compromised by malicious attacks or threats, the overall operation of the involved network is still maintained via consensus on distributed ledgers. More interesting, blockchain can help establish secure peer-to-peer communication among users (i.e. in D2D communication) using the computing power of all participants to operate the network instead of passing a third-party intermediary. This would potentially reduce communication latency, transaction costs, and provide the global accessibility for all users, all of which will enhance the overall system performance.

However, there are still some natural limitations on the blockchain adoption in 5G technologies. For example, communication latency is a critical issue when integrating blockchain in 5G platforms. The authors in [66], [69] indicate that if edge/cloud servers have to process multiple requests in parallel, including network user requests and blockchain requests for block data migration, which involves much synchronization overhead. Further, the high latency of blockchain due to transaction processing makes it challenging to its implementation for managing the authentication of virtual machine orchestration commands in network function virtualization systems [113] and network slicing [127]. Developing optimized blockchain platforms may be needed for meeting requirements of low latency performance and smart contracts features in virtualized 5G technologies.

6.1.2. Blockchain for 5G services

Blockchain is expected to facilitate the 5G services by adding security properties and simplification of service management. Blockchain is particularly useful to create secure sharing environments for spectrum or data exchange in the 5G mobile networks. Blockchain is regarded as a middle layer to perform spectrum trading, verify sharing transactions and lease securely the spectrum provided by spectrum resource providers, i.e. license holders. Different from the conventional database management systems which often use a centralized server to perform access authentication, blockchain with smart contracts can implement decentralized user access validation by using the computing power of all legitimate network participants. This makes the sharing system strongly resistant to data modifications. Many research studies on blockchain [143], [144], [145], [146] demonstrate that the blockchain adoption is beneficial to spectrum management in terms of better scalability, power efficiency in spectrum usage, improved accessibility with high degree of security and better system protection capability against DoS attacks and threats.

Besides, blockchain can simplify the network virtualization in 5G networks with high degrees of security [111], [112]. The blockchain technology can provide the required characteristics of nonrepudiation and immutability to overcome the shortcomings of the previous centralized configuration settings in virtual networks. More precisely, blockchain is capable of creating secure virtual wireless networks (VWNs) so that wireless resource-owners sublease their wireless resources (e.g., slice of RF spectrum, infrastructure) to mobile virtual network operators (MVNOs). In such a decentralized virtual network, smart contracts can be very useful to provide automation and transparency in a distributed way instead of trusting a particular node or an authority process transactions, which also enhances the trustworthiness of the resource management services. The building of a fair and trusted economic scheme empowered by blockchain can be a notable solution for network interference control, especially in small cell deployments [178].

Also, we should admit that blockchain-based approaches would have its natural limitation in 5G services. The complexity of blockchain operations, including blockchain mining and block generation, makes 5G services less efficient. For instance, blockchain mining can cause unnecessary offloading latency in the mobile data offloading process [171], which also raises the question of using blockchain for 5G [175]. How to use blockchain to protect data privacy while minimizing its impact on the involved 5G services is worth to be considered. More importantly, the use of public blockchain which always allows to broadcast data to everyone on the network that raises privacy issues [177]. Network resource information including QoS demands, user data can be exposed to the attacks and hence damage data integrity [182]. Therefore, further investigations on blockchain adoption in 5G services should be considered.

6.1.3. Blockchain for 5G IoT applications

Blockchain has been investigated and integrated into a number of key 5G IoT applications, such as smart healthcare, smart city, smart transportation, smart grid and UAVs. The integration of blockchain with 5G technologies can advance current IoT systems and provide more performance benefits in terms of better decentralization, security, privacy, service efficiency and system simplification for lower operational costs [161]. For example, blockchain has been demonstrated its high efficiency in healthcare and smart city scenarios. By implementing a direct and secure interconnection in a network of users, service providers (i.e. hospital in healthcare or traffic control units in smart transportation) and network operators, the data sharing, resource sharing and cooperative communication can be achieved in a secure and low-latency manner. Importantly, the sharing of data over the untrusted environments is highly vulnerable to cyber-attacks, which can monitor and obtain the user information profile (patient information in healthcare of customer data in smart grid). Blockchain comes as a notable solution to address such challenges by securing the transaction and verifying the user access.

Recent years have also witnessed a new research trend on the combination of blockchain and UAVs for solving critical challenges in UAV networks and empowering new 5G IoT applications. UAV with its high mobility and flexibility can be a promising transmission solution for aerial and terrestrial communication systems, but it also remains critical challenges in terms of security due to adversaries and short battery life. Blockchain would be notable to solve such challenges. Recent studies show the feasibility of blockchain in UAV networks [265], [266], [267]. UAV can collect data from the IoT devices and offload data to the blockchain, where data is hashed and recorded securely on the ledger. This would not only preserve IoT data against threats but also reduce the data storage burden on UAV, which is promising to prolong the duration of UAV operations for better service delivery.

However, the deployment of blockchain on IoT networks shows some potential challenges. Due

to the resource constraints of IoT devices, it is challenging to run blockchain on IoT networks. Further, IoT devices might not be capable of storing large databases due to blockchain implementation [251]. In IoT-based applications such as smart health that urgently needs low-latency communication to meet QoS and QoE requirements, the limitations of blockchain in terms of overhead can prohibit the adoption of blockchain in such 5G services [239]. Recently, blockchain has been incorporated with UAVs, but their mobility and complex communications over the sky, the ability of blockchain to securely maintain a consistent and tamper-resistant ledger to record all the transactions of UAV communications is challenged [278]. Designing a flexible aerial-ground blockchain model can be useful in such complex systems.

6.2. Challenges and Open issues

At present, the amalgamation of blockchain and 5G networks has been received widespread research interests from academics and industries. The blockchain technology is promising to revolutionize 5G networks and services by offering the newly emerging features such as decentralization, privacy, and security. The arrival of this emerging technology is potential to change the current shape of 5G infrastructure and transform industrial network architectures with advanced blockchain-5G paradigms. However, the throughout survey on the use of blockchain for 5G networks also reveals several critical research challenges and open issues that should be considered carefully during the system design. We analyse them from four main aspects: integration challenge, blockchain scalability, blockchain security, and QoS limitations, which will be analysed in details as follows.

6.2.1. Challenges of the blockchain and 5G integration

The blockchain and 5G integration currently face some critical challenges that need to be considered before deployment. First, there is a lack of infrastructure in existing 5G systems for blockchain integration. Most of 5G wireless operators set up their systems to target popular network services such as smart city, smart health, supply chain without giving necessary infrastructure such as decentralized network architectures, smart contract software for blockchain integration in 5G [275]. Furthermore, the lack of standardization and regulations also pose critical challenges for the blockchain and 5G integration [276]. The current operations of blockchain are de-standardized and de-regulated due to the lack of collaboration of blockchain companies and governments. Without having standardization, it is very challenging to adopt blockchain in real-world 5G networks which need to be solved before blockchain realization in 5G.

6.2.2. Blockchain performance and scalability

Despite the benefits of blockchain, scalability and performance issues of are major challenges in the integrated blockchain-5G ecosystems. Here, we analyse the scalability issues of blockchain from the perspectives of throughput, storage and networking.

- *Throughput:* In fact, blockchain has much lower throughput in comparison to non-blockchain applications. For instance, Bitcoin processes a maximum of only 4 transactions/seconds, and the number for Ethereum is 20 transactions/seconds, while Visa processes 1667 transactions/second [277]. Obviously, the current blockchain systems have serious scalability bottlenecks in tems of the number of replicas and the performance concerns such as constrained throughput (number of transactions/second) and transaction latency [278]. Many blockchains suffer from a long queueing time for transactions to be added to the chain due to the block size restriction. Therefore, when the block generation time increases rapidly, the overall system throughput can reduce.

54

- *Storage:* When using blockchain in 5G networks, a huge quantity of data generated by ubiquitous IoT devices is processed by the blockchain for 5G services such as data sharing, resource management and user transaction monitoring. In the conventional blockchain systems, each blockchain node must process and store a copy of the complete transaction data. This can pose a storage and computation burden on resource-constrained IoT devices to participate in the blockchain network. [279].

- *Networking:* Blockchain networking is another issue that also affects the scalability of blockchain systems. Blockchain is computationally expensive and requires significant bandwidth resources to perform computational mining puzzle. However, in the 5G scenarios, such as ultra-dense networks where resource is very limited due to the demands from IoT devices and service operators, it may be impossible to meet resource requirement for blockchain to achieve large scale transaction processing. Further, stemming from the property of blockchain consensus mechanisms which require multiple transaction transmissions among nodes to validate a block, the blockchain operation needs to consume much network resources (i.e. bandwidth, mining power, and transmission power), which also results in high network latency [280].

The increasing complexity in 5G IoT network makes blockchain platforms difficult to process high data volumes. The end-to-end latency in 5G networks is expected to achieve less than 1 millisecond [2] for payload and data transmissions. This vision requires careful considerations in designing blockchain platforms before integrating into 5G systems. Many research efforts have been dedicated to improving the performance and scalability in blockchain from different design perspectives such as mining hardware design [281], hybrid consensus protocols [282], on-chain and off-chain solutions [283], [284]. Very recently, a solution using 5G network virtualization is also considered [285] to solve scalability of blockchain by decoupling the blockchain management from the transaction processing to improve QoS of blockchain operations. The preliminary results are expected to shed light on the blockchain research for solving scalability issues and improving the system performance in integrated blockchain 5G networks.

6.2.3. Blockchain security and privacy

Blockchain is considered as secure database platform to ensure safety and privacy for involved 5G networks. However, recent researches have revealed inherent security weaknesses in blockchain which are mostly related to 5G systems [286]. A critical security issue is 51% attack which means a group of blockchain miners manages more than 50% of the network computation power, which thereby hinder from transacting successfully the block and mining it on blockchain. More importantly, adversaries can exploit this weakness to gain dominance on the blockchain to modify or alter the content of transactions [286]. In addition to that, the operations of smart contracts also show some security concerns, such as privacy leakage or system logic modifications [287], [288]. All of these issues would add more security concerns to blockchain-involved 5G networks [289].

Security problems in blockchain in 5G networks can be solved by recent security improvements. For example, a mining pool system called SmartPool [290] was proposed to improve the validation performance for transaction in blockchain mining, which potentially mitigates security bottlenecks, such as 51% vulnerability. Especially, recent works [291], [292] introduced some powerful security analysis tools to investigate and evaluate threat potential for ensuring security of smart contracts. These efforts would improve security of blockchain 5G environments and enhance the overall performance of the system.

6.2.4. QoS limitations

With the advances of mobile 5G technologies, blockchain now can be implemented in mobile devices to provide more flexible blockchain-based solutions for 5G IoT applications. The foundation of the efficient and secure operation of blockchain is a computation process known as mining. In order to append a new transaction to the blockchain, a blockchain user, or a miner, needs to run a mining puzzle, i.e. Proof of Work (PoW) or Proof of Stake (PoS) which is generally complicated and requires vast computing and storage resources. Further, blockchain also requires network bandwidth resources to perform its consensus process. Without a careful design, the blockchain implementation to operate involved IoT applications may lead to Quality of Service (QoS) degradation with long latency, high energy consumption, high bandwidth demands, and high network congestion. Obviously, the integration of blockchain can introduce new QoS challenges that would negatively impact the overall performance of blockchain-5G networks. It is noting that one of the most important goals of future 5G is to provide user-centric values with high QoS to satisfy the growing demands of user traffic and emerging services [2]. Therefore, it is vitally important to develop efficient solutions that can enhance service qualities of blockchain ecosystems to empower the future blockchain-5G networks.

Recently, some strategies have been proposed to solve the above issues from different perspectives. On the one hand, the design of lightweight blockchain platforms can be a notable solution to enhance the QoS, by eliminating computation consensus mechanisms of blockchain [293], compressing consensus storage [294], or designing lightweight block validation techniques [295], [296], [297]. These solutions potentially simplify the blockchain mining process for lower energy consumption and better latency efficiency, which make greats contributions to the QoS improvements in blockchain-5G applications. On the other hand, computation offloading is also another feasible approach to solve the low QoS issues of blockchain . With the development of 5G technologies such as edge/cloud computing, D2D communication, blockchain computation tasks (i.e. consensus puzzle) can be offloaded to resourceful servers such as edge/cloud servers [298], [299] by combining defined networks [300] and D2D communication [131] to bridge the gap between constrained resources of local mobile devices and growing demands of executing the computation tasks. By using offloading solutions, the performance of blockchain-5G systems would be improved significantly, such as saving system energy, reducing computation latency and improving the quality of computation experience for mobile devices. As a result, the system QoS will be enhanced while blockchain features are ensured for high level network security. The offloading optimization solutions should be explored further to balance both blockchain and the core 5G networks for future mobile blockchain-5G applications.

6.3. Future research directions

Motivated by our detailed survey on research studies on the convergence of blockchain and 5G networks, we point out possible research directions which should be considered in the future works.

6.3.1. From simulation to implementation

Reviewing the literature, most of the blockchain platforms conceived for 5G networks are in their simulation stages. Thus, the researchers and practitioners need to further improve blockchain architectures before they are realized in real-world 5G networks. We here propose some solutions that can be considered in practical blockchain-5G systems. First, the 5G wireless operators can incorporate with blockchain companies for large-scale blockchain deployment on the existing 5G platforms. For example, Ethereum blockchain has been integrated with 5G cloud platform on Amazon [301], which facilitates the business operations (i.e. 5G supply chain, IoT applications) of

enterprises for production efficiency and security enhancement. Moreover, regulatory rules should be provided so that blockchain implementation can be realized [302]. Many 5G network operators and businesses are slow to adopt blockchain-based systems because they fear potential government regulations might require them to make expensive or difficult changes in their network architectures in the future. Once the legal issues are solved, the integration of blockchain in 5G networks can be accelerated to create newly emerging network services.

6.3.2. Integrating machine learning with blockchain for 5G

The revolution of machine learning (ML) technology transforms current 5G services by providing a learning ability to provide data-driven insights for supporting decision-making tasks or data predictions. The advances of ML would facilitate blockchain-5G services in the future networks. For instance, ML can provide a solution for facilitating resource management and user communication. ML also exhibits great potential on data feature discovery to predict data usage behaviour for developing control algorithms, such as data traffic estimation for network congestion avoidance or user access tracking for privacy preservation. Recent years, there is an increasing trend of combining machine learning with blockchain for 5G use case domains. For example, deep reinforcement learning (DRL) [21] has been investigated and combined with blockchain to enable secure and intelligent resource management and orchestration in 5G networks. An advanced DRL algorithm is proposed to design the algorithms of optimizing channel association, interference control and resource management. Other significant works also propose the integrated blockchain-DRL architectures for flexible and secure computation offloading, reliable network channel selection [303], and networking optimization [304].

6.3.3. Blockchain for big data in 5G

In the age of data explosion, big data has become a hot research topic in 5G [305]. A large amount of ubiquitous data generated from 5G IoT devices can be used for giving birth to data-related applications, for example, data analytics, data extraction empowered by artificial intelligence solutions [306]. Currently, big data technologies have suffered from security vulnerabilities, such as data privacy breach, data integrity and big data processing security risks [307]. Further, big data analytics on cloud/edge computing are also highly vulnerable to cyberattacks in the complex operational and business environments.

Blockchain can be a promising solution to cope with security challenges in big data [308]. More specifically, blockchain can ensure immutability and transparency for big data processing and analytics. Recently, some big data models enabled by blockchain are proposed, such as data sharing with smart contracts [309], access control for big data security [310], or privacy preservation for big data analytics [311]. These results demonstrate the efficiency of the use of blockchain for security and performance enhancement to big data applications in the age of 5G.

In summary, blockchain has provided enormous opportunities to 5G mobile networks thanks to its exceptional security properties. The convergence of blockchain and 5G technologies has reshaped and transformed the current 5G service provisions with security guarantees. This detailed survey is expected to pave a way for new innovative researches and solutions for empowering the future blockchain-5G networks.

7. Conclusions and discussions

Blockchain is an emerging technology that has drawn significant attention recently and is recognized as one of the key enablers for 5G networks thanks to its unique role to security assurance

and network performance improvements. In this paper, we have explored the opportunities brought by blockchain to empower the 5G systems and services through a state-of-the-art survey and extensive discussions based on the existing literature in the field. This work is motivated by the lack of a comprehensive review on the integration of blockchain and 5G networks. In this article, we have presented a comprehensive survey focusing on the current state-of-the-art achievements in the integration of blockchain into 5G wireless networks. Particularly, we have first provided a brief overview on the background knowledge of blockchain and 5G networks and highlighted the motivation of the integration. We have then explored and analysed in detail the potential of blockchain for enabling key 5G technologies, such as cloud computing, edge computing, Network Function Virtualization, Network Slicing, and D2D communication. A comprehensive discussion on the use of blockchain in a wide range of popular 5G services has been provided, with a prime focus on spectrum management, data sharing, network virtualization, resource management, interference management, federated learning, privacy and security services. Our survey has also covered a holistic investigation on the applications of blockchain in 5G IoT networks and reviews the latest developments of the cooperated blockchain-5G IoT services in various significant use-case domains, ranging from smart healthcare, smart city, smart transportation to smart grid and UAVs. Through the comprehensive survey on the related articles, we have summarized the main findings derived from the integrations of blockchain in 5G networks and services. Finally, we have pointed out several research challenges and outlined potential research directions.

Through the state-of-the-art survey, we have found that the blockchain and 5G integration are mainly implemented via simulations, testbeds, and experiments. The research results from recent efforts demonstrate the great potential of blockchain in various practical 5G areas, ranging from 5G technology improvement (i.e. blockchain-cloud combination, blockchain-SDN adoption) to 5G services (such as blockchain-based data offloading, blockchain-empowered spectrum sharing) and 5G IoT (such as blockchain-based smart city). The main lessons acquired from the review of the use of blockchain in 5G networks are highlighted as follows.

- First, blockchain promises to enhance the security and privacy of 5G ecosystems, by offering many promising technical properties such as decentralization, privacy, immutability, traceability, and transparency. Blockchain can eliminate the centralized network management concept by decentralizing the network infrastructure where there are no third party authorities needed.

- Second, the use of blockchain also potentially improves the performances of 5G systems. In comparison to traditional database platforms such as SQL, blockchain can provide better data storage and management services with low latency data retrieval. In fact, resource requests (i.e. data access) can be verified by decentralized blockchain nodes with the support of intelligent smart contracts without passing a centralized authority, which is promising to reduce network latency. Moreover, motivated by the removal of decentralization, blockchain is able to establish direct communications between 5G service providers and mobile users so that the management cost can be significantly reduced.

- Finally, blockchain can simplify the 5G network deployments thanks to its decentralized architectures. Indeed, by leveraging blockchain, the mobile operators now can have no worries about the establishment of centralized control servers. The 5G service delivery can be achieved by the blockchain network where user access, service responses and service trading (i.e. resource trading and payment) can be implemented on the decentralized ledgers

among network participants including service providers and mobile users without the need for additional management infrastructure.

Research on blockchain for 5G wireless networks is still in its infancy. But it is obvious that blockchain will significantly uplift the shape and experience of future mobile services and applications. We believe our timely study will shed valuable light on the research of the blockchain-5G integration topics as well as motivate the interested researchers and practitioners to put more research efforts into this promising area.

References

[1] M. Agiwal, A. Roy, N. Saxena, Next generation 5G wireless networks: A comprehensive survey, IEEE Communications Surveys & Tutorials 18 (3) (2016) 1617–1655.

[2] N. Panwar, S. Sharma, A. K. Singh, A survey on 5G : The next generation of mobile communication, Physical Communication 18 (2016) 64–84.

[3] A. Gupta, R. K. Jha, A survey of 5G network: Architecture and emerging technologies, IEEE access 3 (2015) 1206–1232.

[4] E. Hossain, M. Hasan, 5G cellular: key enabling technologies and research challenges, IEEE Instrumentation & Measurement Magazine 18 (3) (2015) 11–21.

[5] K. Christidis, M. DevetsikIoTis, Blockchains and smart contracts for the internet of things, Ieee Access 4 (2016) 2292–2303.

[6] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in: 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557–564.

[7] S. Nakamoto, et al., Bitcoin: A peer-to-peer electronic cash system (2008).

[8] F. Tschorsch, B. Scheuermann, Bitcoin and beyond: A technical survey on decentralized digital currencies, IEEE Communications Surveys & Tutorials 18 (3) (2016) 2084–2123.

[9] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M. H. Rehmani, Applications of blockchains in the internet of things: A comprehensive survey, IEEE Communications Surveys & Tutorials 21 (2) (2018) 1676–1717.

[10] R. Yang, F. R. Yu, P. Si, Z. Yang, Y. Zhang, Integrated blockchain and edge computing systems: A survey, some research issues and challenges, IEEE Communications Surveys & Tutorials 21 (2) (2019) 1508–1532.

[11] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, Y. Liu, A survey of blockchain technology applied to smart cities: Research issues and challenges, IEEE Communications Surveys & Tutorials (2019).

[12] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, Where is current research on blockchain technology?a systematic review, PloS one 11 (10) (2016) e0163477.

[13] K. Rabah, Overview of blockchain as the engine of the 4th industrial revolution, Mara Research Journal of Business & Management-ISSN: 2519-1381 1 (1) (2017) 125–135.

[14] Mwc barcelona 2020: https://www.mwcbarcelona.com/, accessed october, 2019.

[15] Blockchain: A key enabler for 5G . [online]. available: https://www.standardsuniversity.org/e-magazine/may-2019-volume-9- issue-1-blockchain-standards/blockchain-a-key-enabler-for-5G /.

[16] The road to the next wave of tech: 5G +blockchain. [online]. available: https://www.asiablockchainreview.com/the-road to-the-next-wave-of-tech-5G blockchain/.

[17] Internet of things 2016. [online]. available: https://www.cisco.com/c/dam/en/us/ products/collateral/se/ internetof-things/at-a-glance-c45-731471.pdf.

[18] Internet of things (IoT). [online]. available: https://www.cisco.com/c/en/us/ solutions/internet-of-things/.

[19] T. Salman, M. Zolanvari, A. Erbad, R. Jain, M. Samaka, Security services using blockchains: A state of the art survey, IEEE Communications Surveys & Tutorials 21 (1) (2018) 858–880.

[20] M. Chaudhry, Joint ieee spectrum and comsoc talk, test and measurement virtualization and blockchain: Enablers for 5G networks (Nov 13, 2018.).

[21] 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.

[22] I. Jovović, S. Husnjak, I. Forenbacher, S. Maček, Innovative application of 5G and blockchain technology in industry 4.0, EAI Endorsed Transactions on Industrial Networks and Intelligent Systems 6 (18) (2019).

[23] I. Mistry, S. Tanwar, S. Tyagi, N. Kumar, Blockchain for 5G -enabled IoT for industrial automation: A systematic review, solutions, and challenges, Mechanical Systems and Signal Processing 135 (2020) 106382.

[24] I. Jovović, S. Husnjak, I. Forenbacher, S. Maček, 5G , blockchain and ipfs: A general survey with possible innovative applications in industry 4.0, in: 3rd EAI International Conference on Management of Manufacturing Systems-MMS 2018, 2018.

[25] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K. R. Choo, A. Y. Zomaya, Blockchain for smart communities: Applications, challenges and opportunities, Journal of Network and Computer Applications (2019).

[26] I. Makhdoom, M. Abolhasan, H. Abbas, W. Ni, Blockchain's adoption in iot: The challenges, and a way forward, Journal of Network and Computer Applications 125 (2019) 251–279.

[27] P. Mehta, R. Gupta, S. Tanwar, Blockchain envisioned uav networks: Challenges, solutions, and comparisons, Computer Communications (2020).

[28] D. Prerna, R. Tekchandani, N. Kumar, Device-to-device content caching techniques in 5g: A taxonomy, solutions, and challenges, Computer Communications (2020).

[29] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, D. I. Kim, A survey on consensus mechanisms and mining strategy management in blockchain networks, IEEE Access 7 (2019) 22328–22370.

[30] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, J. Wang, Untangling blockchain: A data processing view of blockchain systems, IEEE Transactions on Knowledge and Data Engineering 30 (7) (2018) 1366–1385.

[31] S. Zhang, J.-H. Lee, Double-spending with a sybil attack in the bitcoin decentralized network, IEEE Transactions on Industrial Informatics (2019).

[32] J. Liu, Z. Liu, A survey on security verification of blockchain smart contracts, IEEE Access (2019).

[33] S. Rouhani, R. Deters, Security, performance, and applications of smart contracts: A systematic survey, IEEE Access 7 (2019) 50759–50779.

[34] Y. Yu, Y. Li, J. Tian, J. Liu, Blockchain-based solutions to security and privacy issues in the internet of things, IEEE Wireless Communications 25 (6) (2018) 12–18.

[35] (Chinese Telecom Giants Cite Blockchain as the Enabler for the Roll Out of 5G [Online]. Available: https://blockchain.news/news/chinese-telecom-giants-cite-blockchain-as-the-enabler-for-the-roll-out-of-5g).

[36] (Korea Telecom announces secure IoT, 5G blockchain projects [Online]. Available: https://www.ledgerinsights.com/korea-telecom-kt-blockchain/).

[37] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong, J. C. Zhang, What will 5G be?, IEEE Journal on selected areas in communications 32 (6) (2014) 1065–1082.

[38] A. Costanzo, D. Masotti, Energizing 5G : Near-and far-field wireless energy and data trantransfer as an enabling technology for the 5G IoT, IEEE Microwave Magazine 18 (3) (2017) 125–136.

[39] G. A. Akpakwu, B. J. Silva, et al., A survey on 5G networks for the internet of things: Communication technologies and challenges, IEEE Access 6 (2017) 3619–3647.

[40] A. Ahad, M. Tahir, K.-L. A. Yau, 5G -based smart healthcare network: Architecture, taxonomy, challenges and future research directions, IEEE Access 7 (2019) 100747–100762.

[41] D. Garcia-Roger, S. Roger, D. Martín-Sacristán, J. F. Monserrat, A. Kousaridas, P. Spapis, C. Zhou, 5G functional architecture and signaling enhancements to support path management for ev2x, IEEE Access 7 (2019) 20484–20498.

[42] T. Dragičević, P. Siano, S. Prabaharan, et al., Future generation 5G wireless networks for smart grid: A comprehensive review, Energies 12 (11) (2019) 2140.

[43] M. Usman, M. R. Asghar, F. Granelli, 5G and d2d communications at the service of smart cities, Transportation and Power Grid in Smart Cities: Communication Networks and Services (2018) 147–169.

[44] (Feasibility study on new services and markets technology enablers. 3GPP, Tech. Rep. 22.891, Jun. 2016.).

[45] (ITU - RM.2083-0, IMT Vision Framework and Overall Objectives of the Future Development of IMT for 2020 and beyond, Sep. 2015.).

[46] A. N. Khan, M. M. Kiah, S. U. Khan, S. A. Madani, Towards secure mobile cloud computing: A survey, Future Generation Computer Systems 29 (5) (2013) 1278–1299.

[47] U. N. Kar, D. K. Sanyal, An overview of device-to-device communication in cellular networks, ICT express (2017).

[48] X. Wang, L. Kong, F. Kong, F. Qiu, M. Xia, S. Arnon, G. Chen, Millimeter wave communication: A comprehensive survey, IEEE Communications Surveys & Tutorials 20 (3) (2018) 1616–1653.

[49] (NGMN Alliance, NGMN 5G WHITE PAPER, Feb. 2015).

[50] P. K. Agyapong, M. Iwamura, D. Staehle, W. Kiess, A. Benjebbour, Design considerations for a 5G network architecture., IEEE Communications Magazine 52 (11) (2014) 65–75.

[51] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, M. Ylianttila, Security for 5G and beyond, IEEE Communications Surveys & Tutorials (2019).

[52] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, X. Gao, A survey of physical layer security techniques for 5g wireless networks and challenges ahead, IEEE Journal on Selected Areas in Communications 36 (4) (2018) 679–695.

[53] R. Khan, P. Kumar, D. N. K. Jayakody, M. Liyanage, A survey on security and privacy of 5G technologies: Potential solutions, recent advancements and future directions, IEEE Communications Surveys & Tutorials (2019).

[54] V. W. Wong, Key technologies for 5G wireless systems, Cambridge university press, 2017.

[55] D. Wübben, P. Rost, J. Bartelt, M. Lalam, V. Savin, M. Gorgoglione, A. Dekorsy, G. Fettweis, Benefits and impact of cloud computing on 5G signal processing, IEEE Signal Processing Magazine 31 (6) (2014) 35–44.

[56] M. Chen, Y. Zhang, Y. Li, S. Mao, V. C. Leung, Emc: Emotion-aware mobile cloud computing in 5G, IEEE Network 29 (2) (2015) 32–38.

[57] G. H. Carvalho, I. Woungang, A. Anpalagan, M. Jaseemuddin, Analysis of joint parallelism in wireless and cloud domains on mobile edge computing over 5G systems, Journal of Communications and Networks 20 (6) (2018) 565–577.

[58] B. Feng, L. Jiang, G. Feng, S. Qin, Y. Guo, Network coding based content caching in hierarchical cloud service network for 5G, in: 2016 IEEE Global Communications Conference (GLOBECOM), 2016, pp. 1–6.

[59] R. Siddavaatam, I. Woungang, A. Anpalagan, Joint optimisation of radio and infrastructure resources for energy-efficient massive data storage in the mobile cloud over 5G hetnet, IET Wireless Sensor Systems 9 (5) (2019) 323–332.

[60] P. Paglierani, I. Neokosmidis, T. Rokkas, C. Meani, K. M. Nasr, K. Moessner, P. Sayyad Khodashenas, Techno-economic analysis of 5G immersive media services in cloud-enabled small cell networks: The neutral host business model: Providing techno-economic guidelines for the successful provision of 5G innovative services in small cell networks, Transactions on Emerging Telecommunications Technologies (2019) e3746.

[61] J. Wu, Z. Zhang, Y. Hong, Y. Wen, Cloud radio access network (c-ran): a primer, IEEE Network 29 (1) (2015) 35–41.

[62] X. Wang, C. Cavdar, L. Wang, M. Tornatore, H. S. Chung, H. H. Lee, S. M. Park, B. Mukherjee, Virtualized cloud radio access network for 5G transport, IEEE Communications Magazine 55 (9) (2017) 202–209.

[63] L. Ferdouse, A. Anpalagan, S. Erkucuk, Joint communication and computing resource allocation in 5G cloud radio access networks, IEEE Transactions on Vehicular Technology 68 (9) (2019) 9122–9135.

[64] J. Zhou, Z. Cao, X. Dong, A. V. Vasilakos, Security and privacy for cloud-based IoT: Challenges, IEEE Communications Magazine 55 (1) (2017) 26–33.

[65] J. Li, J. Wu, L. Chen, Block-secure: Blockchain based scheme for secure p2p cloud storage, Information Sciences 465 (2018) 219–231.

[66] M. Yang, A. Margheri, R. Hu, V. Sassone, Differentially private data sharing in a cloud federation with blockchain, IEEE Cloud Computing 5 (6) (2018) 69–79.

[67] Y. Zhang, C. Xu, X. Lin, X. S. Shen, Blockchain-based public integrity verification for cloud storage against procrastinating auditors, IEEE Transactions on Cloud Computing (2019).

[68] H. Yang, Y. Wu, J. Zhang, H. Zheng, Y. Ji, Y. Lee, Blockonet: blockchain-based trusted cloud radio over optical fiber network for 5G fronthaul, in: Optical Fiber Communication Conference, Optical Society of America, 2018, pp. W2A–25.

[69] H. Yang, H. Zheng, J. Zhang, Y. Wu, Y. Lee, Y. Ji, Blockchain-based trusted authentication in cloud radio over fiber network for 5G, in: 2017 16th International Conference on Optical Communications and Networks (ICOCN), 2017, pp. 1–3.

[70] S. Ali, G. Wang, M. Z. A. Bhuiyan, H. Jiang, Secure data provenance in cloud-centric internet of things via blockchain smart contracts, in: 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 2018, pp. 991–998.

[71] Y. Zhang, D. He, K.-K. R. Choo, Bads: Blockchain-based architecture for data sharing with abs and cp-abe in IoT, Wireless Communications and Mobile Computing 2018 (2018).

[72] M. Ma, G. Shi, F. Li, Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario, IEEE Access 7 (2019) 34045–34059.

[73] M. Hossain, Y. Karim, R. Hasan, Fif-IoT: A forensic investigation framework for IoT using a public digital ledger, in: 2018 IEEE International Congress on Internet of Things (ICIoT), 2018, pp. 33–40.

[74] W. Chen, M. Ma, Y. Ye, Z. Zheng, Y. Zhou, IoT service based on jointcloud blockchain: The case study of smart traveling, in: 2018 IEEE Symposium on Service-Oriented System Engineering (SOSE), 2018, pp. 216–221.

[75] O. O. Malomo, D. B. Rawat, M. Garuba, Next-generation cybersecurity through a blockchain-enabled federated cloud framework, The Journal of Supercomputing 74 (10) (2018) 5099–5126.

[76] F. Freitag, On the collaborative governance of decentralized edge microclouds with blockchain-based distributed ledgers, in: 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), 2018, pp. 709–712.

[77] H. Yang, J. Yuan, H. Yao, Q. Yao, A. Yu, J. Zhang, Blockchain-based hierarchical trust networking for jointcloud, IEEE Internet of Things Journal (2019).

[78] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, D. Sabella, On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration, IEEE Communications Surveys & Tutorials 19 (3) (2017) 1657–1681.

[79] Q.-V. Pham, F. Fang, V. N. Ha, M. Le, Z. Ding, L. B. Le, W.-J. Hwang, A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art, arXiv preprint arXiv:1906.08452 (2019).

[80] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, V. Kumar, Security and privacy in fog computing: Challenges, IEEE Access 5 (2017) 19293–19304.

[81] J. Zhang, B. Chen, Y. Zhao, X. Cheng, F. Hu, Data security and privacy-preserving in edge computing paradigm: Survey and open issues, IEEE Access 6 (2018) 18209–18237.

[82] A. Stanciu, Blockchain based distributed control system for edge computing, in: 2017 21st International Conference on Control Systems and Computer Science (CSCS), 2017, pp. 667–671.

[83] S. Guo, X. Hu, S. Guo, X. Qiu, F. Qi, Blockchain meets edge computing: A distributed and trusted authentication system, IEEE Transactions on Industrial Informatics (2019).

[84] H. Liu, Y. Zhang, T. Yang, Blockchain-enabled security in electric vehicles cloud and edge computing, IEEE Network 32 (3) (2018) 78–83.

[85] M. Li, L. Zhu, X. Lin, Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing, IEEE Internet of Things Journal (2018).

[86] K. Gai, Y. Wu, L. Zhu, L. Xu, Y. Zhang, Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks, IEEE Internet of Things Journal (2019).

[87] J. Wang, L. Wu, K.-K. R. Choo, D. He, Blockchain based anonymous authentication with key management for smart grid edge computing infrastructure, IEEE Transactions on Industrial Informatics (2019).

[88] G. Qiao, S. Leng, H. Chai, A. Asadi, Y. Zhang, Blockchain empowered resource trading in mobile edge computing and networks, in: ICC 2019-2019 IEEE International Conference on Communications (ICC), 2019, pp. 1–6.

[89] X. Zheng, R. R. Mukkamala, R. Vatrapu, J. Ordieres-Mere, Blockchain-based personal health data sharing system using cloud storage, in: 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), 2018, pp. 1–6.

[90] C. Xia, H. Chen, X. Liu, J. Wu, L. Chen, Etra: Efficient three-stage resource allocation auction for mobile blockchain in edge computing, in: 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), 2018, pp. 701–705.

[91] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, M. Guizani, Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city, IEEE Access 7 (2019) 18611–18621.

[92] K. Kotobi, M. Sartipi, Efficient and secure communications in smart cities using edge, caching, and blockchain, in: 2018 IEEE International Smart Cities Conference (ISC2), 2018, pp. 1–6.

[93] U. Jayasinghe, G. M. Lee, Á. MacDermott, W. S. Rhee, Trustchain: A privacy preserving blockchain with edge computing, Wireless Communications and Mobile Computing 2019 (2019).

[94] B. Confais, A. Lebre, B. Parrein, An object store service for a fog/edge computing infrastructure based on ipfs and a scale-out nas, in: 2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC), 2017, pp. 41–50.

[95] H. Yang, Y. Liang, J. Yuan, Q. Yao, A. Yu, J. Zhang, Distributed blockchain-based trusted multi-domain collaboration for mobile edge computing in 5g and beyond, IEEE Transactions on Industrial Informatics (2020).

[96] W. Tang, X. Zhao, W. Rafique, W. Dou, A blockchain-based offloading approach in fog computing environment, in: 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom), 2018, pp. 308–315.

[97] Y. Liu, R. Yu, X. Li, H. Ji, V. C. Leung, Decentralized resource allocation for video transcoding and delivery in blockchain-based system with mobile edge computing, IEEE Transactions on Vehicular Technology (2019).

[98] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, Z. Han, When mobile blockchain meets edge computing, IEEE Communications Magazine 56 (8) (2018) 33–39.

[99] F. Z. Yousaf, M. Bredel, S. Schaller, F. Schneider, Nfv and sdnkey technology enablers for 5G networks, IEEE Journal on Selected Areas in Communications 35 (11) (2017) 2468–2478.

[100] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. De Turck, R. Boutaba, Network function virtualization: State-of-the-art and research challenges, IEEE Communications Surveys & Tutorials 18 (1) (2015) 236–262.

[101] S. Abdelwahab, B. Hamdaoui, M. Guizani, T. Znati, Network function virtualization in 5G, IEEE Communications Magazine 54 (4) (2016) 84–91.

[102] I. Farris, T. Taleb, Y. Khettab, J. Song, A survey on emerging sdn and nfv security mechanisms for IoT systems, IEEE Communications Surveys & Tutorials 21 (1) (2018) 812–837.

[103] A. M. Alwakeel, A. K. Alnaim, E. B. Fernandez, A survey of network function virtualization security, in: SoutheastCon 2018, 2018, pp. 1–8.

[104] F. Reynaud, F.-X. Aguessy, O. Bettan, M. Bouet, V. Conan, Attacks against network functions virtualization and software-defined networking: State-of-the-art, in: 2016 IEEE NetSoft Conference and Workshops (NetSoft), 2016, pp. 471–476.

[105] E. Ak, B. Canberk, Bcdn: A proof of concept model for blockchain-aided cdn orchestration and routing, Computer Networks (2019).

[106] (Providing a Sliced, Secure, and Isolated Software Infrastructure of Virtual Functions Through Blockchain Technology. [Online]. Available: https://files.ifi.uzh.ch/CSG/teaching/FS18/ComSys/Talk9.pdf).

[107] G. A. F. Rebello, I. D. Alvarenga, I. J. Sanz, O. C. M. Duarte, Bsec-nfvo: A blockchain-based security for network function virtualization orchestration, in: ICC 2019-2019 IEEE International Conference on Communications (ICC), 2019, pp. 1–6.

[108] N. Bozic, G. Pujolle, S. Secci, Securing virtual machine orchestration with blockchains, in: 2017 1st Cyber Security in Networking Conference (CSNet), 2017, pp. 1–8.

[109] G. A. F. Rebello, G. F. Camilo, L. G. Silva, L. C. Guimarães, L. A. C. de Souza, I. D. Alvarenga, O. C. M. Duarte, Providing a sliced, secure, and isolated software infrastructure of virtual functions through blockchain technology, in: 2019 IEEE 20th International Conference on High Performance Switching and Routing (HPSR), 2019, pp. 1–6.

[110] M. F. Franco, E. J. Scheid, L. Z. Granville, B. Stiller, Brain: Blockchain-based reverse auction for infrastructure supply in virtual network functions-as-a-service, in: 2019 IFIP Networking Conference (IFIP Networking), 2019, pp. 1–9.

[111] D. B. Rawat, Fusion of software defined networking, edge computing, and blockchain technology for wireless network virtualization, IEEE Communications Magazine 57 (10) (2019) 50–55.

[112] I. D. Alvarenga, G. A. Rebello, O. C. M. Duarte, Securing configuration management and migration of virtual network functions using blockchain, in: NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium, 2018, pp. 1–9.

[113] R. Rosa, C. E. Rothenberg, Blockchain-based decentralized applications for multiple administrative domain networking, IEEE Communications Standards Magazine 2 (3) (2018) 29–37.

[114] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, H. Flinck, Network slicing and softwarization: A survey on principles, enabling technologies, and solutions, IEEE Communications Surveys & Tutorials 20 (3) (2018) 2429–2453.

[115] S. Zhang, An overview of network slicing for 5G, IEEE Wireless Communications (2019).

[116] A. Kaloxylos, A survey and an analysis of network slicing in 5G networks, IEEE Communications Standards Magazine 2 (1) (2018) 60–65.

[117] X. Foukas, G. Patounas, A. Elmokashfi, M. K. Marina, Network slicing in 5G : Survey and challenges, IEEE Communications Magazine 55 (5) (2017) 94–100.

[118] V. Ortega, F. Bouchmal, J. F. Monserrat, Trusted 5G vehicular networks: Blockchains and content-centric networking, IEEE Vehicular Technology Magazine 13 (2) (2018) 121–127.

[119] B. Nour, A. Ksentini, N. Herbaut, P. A. Frangoudis, H. Moungla, A blockchain-based network slice broker for 5G services, IEEE Networking Letters (2019).

[120] J. Backman, S. Yrjölä, K. Valtanen, O. Mämmelä, Blockchain network slice broker in 5G : Slice leasing in factory of the future use case, in: 2017 Internet of Things Business Models, Users, and Networks, 2017, pp. 1–8.

[121] K. Valtanen, J. Backman, S. Yrjölä, Creating value through blockchain powered resource configurations: Analysis of 5G network slice brokering case, in: 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), 2018, pp. 185–190.

[122] K. Valtanen, et al., Blockchain-powered value creation in the 5G and smart grid use cases, IEEE Access 7 (2019) 25690–25707.

[123] D. B. Rawat, A. Alshaikhi, Leveraging distributed blockchain-based scheme for wireless network virtualization with security and qos constraints, in: 2018 International Conference on Computing, Networking and Communications (ICNC), 2018, pp. 332–336.

[124] A. Adhikari, D. B. Rawat, M. Song, Wireless network virtualization by leveraging blockchain technology and machine learning, in: Proceedings of the ACM Workshop on Wireless Security and Machine Learning, ACM, 2019, pp. 61–66.

[125] F. Jameel, Z. Hamid, F. Jabeen, S. Zeadally, M. A. Javed, A survey of device-to-device communications: Research issues and challenges, IEEE Communications Surveys & Tutorials 20 (3) (2018) 2133–2168.

[126] R. I. Ansari, C. Chrysostomou, S. A. Hassan, M. Guizani, S. Mumtaz, J. Rodriguez, J. J. Rodrigues, 5G d2d networks: Techniques, challenges, and future prospects, IEEE Systems Journal 12 (4) (2017) 3970–3984.

[127] O. N. Hamoud, T. Kenaza, Y. Challal, Security in device-to-device communications: a survey, IET Networks 7 (1) (2017) 14–22.

[128] M. Wang, Z. Yan, Security in d2d communications: A review, in: 2015 IEEE Trustcom/BigDataSE/ISPA, Vol. 1, 2015, pp. 1199–1204.

[129] H. Cui, Z. Chen, N. Liu, B. Xia, Blockchain-driven contents sharing strategy for wireless cache-enabled d2d networks, in: 2019 IEEE International Conference on Communications Workshops (ICC Workshops), 2019, pp. 1–5.

[130] D. Lin, Y. Tang, Blockchain consensus based user access strategies in d2d networks for data-intensive applications, IEEE Access 6 (2018) 72683–72690.

[131] S. Seng, X. Li, C. Luo, H. Ji, H. Zhang, A d2d-assisted mec computation offloading in the blockchain-based framework for udns, in: ICC 2019-2019 IEEE International Conference on Communications (ICC), 2019, pp. 1–6.

[132] V. A. Siris, D. Dimopoulos, N. Fotiou, S. Voulgaris, G. C. Polyzos, Trusted d2d-based IoT resource access using smart contracts, in: 2019 IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM), 2019, pp. 1–9.

[133] M. Liu, F. R. Yu, Y. Teng, V. C. Leung, M. Song, Joint computation offloading and content caching for wireless blockchain networks, in: IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2018, pp. 517–522.

[134] M. Liu, F. R. Yu, et al., Distributed resource allocation in blockchain-based video streaming systems with mobile edge computing, IEEE Transactions on Wireless Communications 18 (1) (2018) 695–708.

[135] X. Feng, J. Ma, T. Feng, Y. Miao, X. Liu, Consortium blockchain-based sift: Outsourcing encrypted feature extraction in the d2d network, IEEE Access 6 (2018) 52248–52260.

[136] S. R. Niya, F. Shüpfer, T. Bocek, B. Stiller, Setting up flexible and light weight trading with enhanced user privacy using smart contracts, in: NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium, 2018, pp. 1–2.

[137] G. Yang, X. Wu, Y. Wu, C. Chen, A distributed secure monitoring system based on blockchain., International Journal of Performability Engineering 14 (10) (2018).

[138] S. K. Sharma, T. E. Bogale, L. B. Le, S. Chatzinotas, X. Wang, B. Ottersten, Dynamic spectrum sharing in 5G wireless networks with full-duplex technology: Recent advances and research challenges, IEEE Communications Surveys & Tutorials 20 (1) (2017) 674–707.

[139] L. Zhang, M. Xiao, G. Wu, M. Alam, Y.-C. Liang, S. Li, A survey of advanced techniques for spectrum sharing in 5G networks, IEEE Wireless Communications 24 (5) (2017) 44–51.

[140] F. Hu, B. Chen, K. Zhu, Full spectrum sharing in cognitive radio networks toward 5G : A survey, IEEE Access 6 (2018) 15754–15776.

[141] M. B. Weiss, K. Werbach, D. C. Sicker, C. Caicedo, On the application of blockchains to spectrum management, IEEE Transactions on Cognitive Communications and Networking (2019).

[142] K. Kotobi, S. G. Bilen, Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access, IEEE vehicular technology magazine 13 (1) (2018) 32–39.

[143] K. Kotobi, S. G. Bilén, Blockchain-enabled spectrum access in cognitive radio networks, in: 2017 Wireless Telecommunications Symposium (WTS), 2017, pp. 1–6.

[144] M. Grissa, A. A. Yavuz, B. Hamdaoui, Trustsas: A trustworthy spectrum access system for the 3.5 ghz cbrs band, in: IEEE INFOCOM 2019-IEEE Conference on Computer Communications, 2019, pp. 1495–1503.

[145] S. Bayhan, A. Zubow, P. Gawłowicz, A. Wolisz, Smart contracts for spectrum sensing as a service, IEEE Transactions on Cognitive Communications and Networking 5 (3) (2019) 648–660.

[146] S. Bayhan, A. Zubow, A. Wolisz, Spass: Spectrum sensing as a service via smart contracts, in: 2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), 2018, pp. 1–10.

[147] T. Maksymyuk, J. Gazda, L. Han, M. Jo, Blockchain-based intelligent network management for 5G and beyond, in: 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), 2019, pp. 36–39.

[148] F. den Hartog, F. Bouhafs, Q. Shi, Toward secure trading of unlicensed spectrum in cyber-physical systems, in: 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2019, pp. 1–4.

[149] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, D. Sabella, On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration, IEEE Communications Surveys & Tutorials 19 (3) (2017) 1657–1681.

[150] (Cisco Visual Networking Index: Forecast and Trends, 20172022 White Paper. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/ visual-networking-index-vni/white-paper-c11-741490.html).

[151] M. B. Mollah, M. A. K. Azad, A. Vasilakos, Secure data sharing and searching at the edge of cloud-assisted internet of things, IEEE Cloud Computing 4 (1) (2017) 34–42.

[152] R. Mahmoud, T. Yousuf, F. Aloul, I. Zualkernan, Internet of things (IoT) security: Current status, challenges and prospective measures, in: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), 2015, pp. 336–341.

[153] K. Fan, Y. Ren, Y. Wang, H. Li, Y. Yang, Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G, IET Communications 12 (5) (2017) 527–532.

[154] D. Li, R. Du, Y. Fu, M. H. Au, Meta-key: A secure data-sharing protocol under blockchain-based decentralized storage architecture, IEEE Networking Letters 1 (1) (2019) 30–33.

[155] S. Wang, Y. Zhang, Y. Zhang, A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems, IEEE Access 6 (2018) 38437–38450.

[156] X. Zheng, R. R. Mukkamala, R. Vatrapu, J. Ordieres-Mere, Blockchain-based personal health data sharing system using cloud storage, in: 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), 2018, pp. 1–6.

[157] M. Yang, A. Margheri, R. Hu, V. Sassone, Differentially private data sharing in a cloud federation with blockchain, IEEE Cloud Computing 5 (6) (2018) 69–79.

[158] W. Liang, M. Tang, J. Long, X. Peng, J. Xu, K.-C. Li, A secure fabric blockchain-based data transmission technique for industrial internet-of-things, IEEE Transactions on Industrial Informatics (2019).

[159] C. H. Liu, Q. Lin, S. Wen, Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning, IEEE Transactions on Industrial Informatics (2018).

[160] Y. Lu, X. Huang, Y. Dai, S. Maharjan, Y. Zhang, Blockchain and federated learning for privacy-preserved data sharing in industrial IoT, IEEE Transactions on Industrial Informatics (2019).

[161] H. L. Cech, M. Großmann, U. R. Krieger, A fog computing architecture to share sensor data by means of blockchain functionality, in: 2019 IEEE International Conference on Fog Computing (ICFC), 2019, pp. 31–40.

[162] Y. Qian, Z. Liu, J. Yang, Q. Wang, A method of exchanging data in smart city by blockchain, in: 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2018, pp. 1344–1349.

[163] X. Zhang, X. Chen, Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network, IEEE Access 7 (2019) 58241–58254.

[164] K. Bhaskaran, P. Ilfrich, D. Liffman, C. Vecchiola, P. Jayachandran, A. Kumar, F. Lim, K. Nandakumar, Z. Qin, V. Ramakrishna, et al., Double-blind consent-driven data sharing on blockchain, in: 2018 IEEE International Conference on Cloud Engineering (IC2E), 2018, pp. 385–391.

[165] M. Condoluci, T. Mahmoodi, Softwarization and virtualization in 5G mobile networks: Benefits, trends and challenges, Computer Networks 146 (2018) 65–84.

[166] E. J. Kitindi, S. Fu, Y. Jia, A. Kabir, Y. Wang, Wireless network virtualization with sdn and c-ran for 5G networks: Requirements, opportunities, and challenges, IEEE Access 5 (2017) 19099–19115.

[167] D. B. Rawat, M. S. Parwez, A. Alshammari, Edge computing enabled resilient wireless network virtualization for internet of things, in: 2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC), 2017, pp. 155–162.

[168] F. D. Calabrese, L. Wang, E. Ghadimi, G. Peters, L. Hanzo, P. Soldati, Learning radio resource management in rans: Framework, opportunities, and challenges, IEEE Communications Magazine 56 (9) (2018) 138–145.

[169] Y. Le, X. Ling, J. Wang, Z. Ding, Prototype design and test of blockchain radio access network, in: 2019 IEEE International Conference on Communications Workshops (ICC Workshops), 2019, pp. 1–6.

[170] Y. Liu, F. R. Yu, X. Li, H. Ji, V. C. Leung, Resource allocation for video transcoding and delivery based on mobile edge computing and blockchain, in: 2018 IEEE Global Communications Conference (GLOBECOM), 2018, pp. 1–6.

[171] Y. Liu, R. Yu, X. Li, H. Ji, V. C. Leung, Decentralized resource allocation for video transcoding and delivery in blockchain-based system with mobile edge computing, IEEE Transactions on Vehicular Technology (2019).

[172] C. Xu, K. Wang, G. Xu, P. Li, S. Guo, J. Luo, Making big data open in collaborative edges: A blockchain-based framework with reduced resource requirements, in: 2018 IEEE International Conference on Communications (ICC), 2018, pp. 1–6.

[173] C. Xia, H. Chen, X. Liu, J. Wu, L. Chen, Etra: Efficient three-stage resource allocation auction for mobile blockchain in edge computing, in: 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), 2018, pp. 701–705.

[174] D. Lin, S. Hu, Y. Gao, Y. Tang, Optimizing mec networks for healthcare applications in 5G communications with the authenticity of users priorities, IEEE Access 7 (2019) 88592–88600.

[175] H. Yang, L. Guan, J. Nan, X. Zhao, Y. Liang, Q. Yao, A. Yu, J. Zhang, Intelligent optical network with ai and blockchain, in: 2019 18th International Conference on Optical Communications and Networks (ICOCN), IEEE, 2019, pp. 1–3.

[176] W. Nam, D. Bai, J. Lee, I. Kang, Advanced interference management for 5G cellular networks., IEEE Communications Magazine 52 (5) (2014) 52–60.

[177] F. Qamar, M. N. Hindia, K. Dimyati, K. A. Noordin, I. S. Amiri, Interference management issues for the future 5G network: a review, Telecommunication Systems (2019) 1–17.

[178] A. El Gamal, H. El Gamal, A single coin monetary mechanism for distributed cooperative interference management, IEEE Wireless Communications Letters (2019).

[179] A. E. Gamal, H. E. Gamal, A blockchain example for cooperative interference management, arXiv preprint arXiv:1808.01538 (2018).

[180] Z. Liu, L. Gao, Y. Liu, X. Guan, K. Ma, Y. Wang, Efficient qos support for robust resource allocation in blockchain-based femtocell networks, IEEE Transactions on Industrial Informatics (2019).

[181] 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 (2019).

[182] T. Li, A. K. Sahu, A. Talwalkar, V. Smith, Federated learning: Challenges, methods, and future directions, arXiv preprint arXiv:1908.07873 (2019).

[183] H. Kim, J. Park, M. Bennis, S.-L. Kim, Blockchained on-device federated learning, IEEE Communications Letters (2019).

[184] J. Kang, Z. Xiong, D. Niyato, S. Xie, J. Zhang, Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory, IEEE Internet of Things Journal (2019).

[185] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, C. Miao, Federated learning in mobile edge networks: A comprehensive survey, arXiv preprint arXiv:1909.11875 (2019).

[186] R. Doku, D. B. Rawat, C. Liu, Towards federated learning approach to determine data relevance in big data, in: 2019 IEEE 20th International Conference on Information Reuse and Integration for Data Science (IRI), 2019, pp. 184–192.

[187] Z. Shae, J. Tsai, Transform blockchain into distributed parallel computing architecture for precision medicine, in: 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), 2018, pp. 1290–1299.

71

[188] Y. Lu, X. Huang, Y. Dai, S. Maharjan, Y. Zhang, Blockchain and federated learning for privacy-preserved data sharing in industrial IoT, IEEE Transactions on Industrial Informatics (2019).

[189] G. Zyskind, O. Nathan, et al., Decentralizing privacy: Using blockchain to protect personal data, in: 2015 IEEE Security and Privacy Workshops, 2015, pp. 180–184.

[190] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, L. Njilla, Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability, in: Proceedings of the 17th IEEE/ACM international symposium on cluster, cloud and grid computing, IEEE Press, 2017, pp. 468–477.

[191] A. Banerjee, K. P. Joshi, Link before you share: Managing privacy policies through blockchain, in: 2017 IEEE International Conference on Big Data (Big Data), 2017, pp. 4438–4447.

[192] T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily, Y. Jararweh, Privacy management in social internet of vehicles: Review, challenges and blockchain based solutions, IEEE Access 7 (2019) 79694–79713.

[193] O. B. Mora, R. Rivera, V. M. Larios, J. R. Beltrán-Ramírez, R. Maciel, A. Ochoa, A use case in cybersecurity based in blockchain to deal with the security and privacy of citizens and smart cities cyberinfrastructures, in: 2018 IEEE International Smart Cities Conference (ISC2), 2018, pp. 1–4.

[194] G. Magyar, Blockchain: Solving the privacy and research availability tradeoff for ehr data: A new disruptive technology in health data management, in: 2017 IEEE 30th Neumann Colloquium (NC), 2017, pp. 000135–000140.

[195] K. Gai, Y. Wu, L. Zhu, M. Qiu, M. Shen, Privacy-preserving energy trading using consortium blockchain in smart grid, IEEE Transactions on Industrial Informatics (2019).

[196] J. Wan, J. Li, M. Imran, D. Li, et al., A blockchain-based solution for enhancing security and privacy in smart factory, IEEE Transactions on Industrial Informatics (2019).

[197] Z. Lu, Q. Wang, G. Qu, H. Zhang, Z. Liu, A blockchain-based privacy-preserving authentication scheme for vanets, IEEE Transactions on Very Large Scale Integration (VLSI) Systems (2019).

[198] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, Z. Zhang, Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles, IEEE Transactions on Intelligent Transportation Systems 19 (7) (2018) 2204–2220.

[199] Y. Jiang, C. Wang, Y. Wang, L. Gao, A privacy-preserving e-commerce system based on the blockchain technology, in: 2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), 2019, pp. 50–55.

[200] X. Chen, J. Ji, C. Luo, W. Liao, P. Li, When machine learning meets blockchain: A decentralized, privacy-preserving and secure design, in: 2018 IEEE International Conference on Big Data (Big Data), 2018, pp. 1178–1187.

72

[201] M. U. Hassan, M. H. Rehmani, J. Chen, Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions, Future Generation Computer Systems 97 (2019) 512–529.

[202] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, J. Wan, Smart contract-based access control for the internet of things, IEEE Internet of Things Journal 6 (2) (2018) 1594–1605.

[203] M. Ma, G. Shi, F. Li, Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario, IEEE Access 7 (2019) 34045–34059.

[204] S. Ding, J. Cao, C. Li, K. Fan, H. Li, A novel attribute-based access control scheme using blockchain for IoT, IEEE Access 7 (2019) 38431–38441.

[205] S. Wang, X. Wang, Y. Zhang, A secure cloud storage framework with access control based on blockchain, IEEE Access 7 (2019) 112713–112725.

[206] Y. Zhu, Y. Qin, G. Gan, Y. Shuai, W. C.-C. Chu, Tbac: transaction-based access control on blockchain for resource sharing with cryptographically decentralized authorization, in: 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Vol. 1, 2018, pp. 535–544.

[207] S. Rouhani, V. Pourheidari, R. Deters, Physical access control management system based on permissioned blockchain, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1078–1083.

[208] A. Ouaddah, A. Abou Elkalam, A. Ait Ouahman, Fairaccess: a new blockchain-based access control framework for the internet of things, Security and Communication Networks 9 (18) (2016) 5943–5964.

[209] R. Xu, Y. Chen, E. Blasch, G. Chen, Blendcac: A blockchain-enabled decentralized capability-based access control for IoTs, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1027–1034.

[210] I. Zikratov, A. Kuzmin, V. Akimenko, V. Niculichev, L. Yalansky, Ensuring data integrity using blockchain technology, in: 2017 20th Conference of Open Innovations Association (FRUCT), 2017, pp. 534–539.

[211] B. Liu, X. L. Yu, S. Chen, X. Xu, L. Zhu, Blockchain based data integrity service framework for IoT data, in: 2017 IEEE International Conference on Web Services (ICWS), 2017, pp. 468–475.

[212] C. Machado, A. A. M. Fröhlich, IoT data integrity verification for cyber-physical systems using blockchain, in: 2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC), 2018, pp. 83–90.

[213] Y.-J. Chen, L.-C. Wang, S. Wang, Stochastic blockchain for IoT data integrity, IEEE Transactions on Network Science and Engineering (2018).

[214] D. Yue, R. Li, Y. Zhang, W. Tian, C. Peng, Blockchain based data integrity verification in p2p cloud storage, in: 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), 2018, pp. 561–568.

[215] B. Zhao, P. Fan, M. Ni, Mchain: a blockchain-based vm measurements secure storage approach in iaas cloud with enhanced integrity and controllability, IEEE Access 6 (2018) 43758–43769.

[216] Y. Zhang, C. Xu, X. Lin, X. S. Shen, Blockchain-based public integrity verification for cloud storage against procrastinating auditors, IEEE Transactions on Cloud Computing (2019).

[217] S. Raju, S. Boddepalli, S. Gampa, Q. Yan, J. S. Deogun, Identity management using blockchain for cognitive cellular networks, in: 2017 IEEE International Conference on Communications (ICC), 2017, pp. 1–6.

[218] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, K. Salah, A user authentication scheme of IoT devices using blockchain-enabled fog nodes, in: 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), 2018, pp. 1–8.

[219] R. Sharma, S. Chakraborty, Blockapp: Using blockchain for authentication and privacy preservation in iov, in: 2018 IEEE Globecom Workshops (GC Wkshps), 2018, pp. 1–6.

[220] L. Xiong, L. et al., A blockchain-based privacy-awareness authentication scheme with efficient revocation for multi-server architectures, IEEE Access 7 (2019) 125840–125853.

[221] S. Li, L. Da Xu, S. Zhao, 5G internet of things: A survey, Journal of Industrial Information Integration 10 (2018) 1–9.

[222] W. Ejaz, A. Anpalagan, M. A. Imran, M. Jo, M. Naeem, S. B. Qaisar, W. Wang, Internet of things (IoT) in 5G wireless communications, IEEE Access 4 (2016) 10310–10314.

[223] D. C. Nguyen, P. N. Pathirana, M. Ding, A. Seneviratne, Integration of blockchain and cloud of things: Architecture, applications and challenges, arXiv preprint arXiv:1908.09058 (2019).

[224] A. Ahad, M. Tahir, K.-L. A. Yau, 5G -based smart healthcare network: Architecture, taxonomy, challenges and future research directions, IEEE Access 7 (2019) 100747–100762.

[225] C. Thuemmler, C. Rolffs, A. Bollmann, G. Hindricks, W. Buchanan, Requirements for 5G based telemetric cardiac monitoring, in: 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2018, pp. 1–4.

[226] M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib, F. Sallabi, Softwarization of internet of things infrastructure for secure and smart healthcare, arXiv preprint arXiv:1805.11011 (2018).

[227] P. Li, C. Xu, et al., Chainsdi: A software-defined infrastructure for regulation-compliant home-based healthcare services secured by blockchains, IEEE Systems Journal (2019).

[228] X. Feng, J. Ma, T. Feng, Y. Miao, X. Liu, Consortium blockchain-based sift: Outsourcing encrypted feature extraction in the d2d network, IEEE Access 6 (2018) 52248–52260.

[229] M. A. Rahman, E. Hassanain, et al., Spatial blockchain-based secure mass screening framework for children with dyslexia, IEEE Access 6 (2018) 61876–61885.

[230] Y. Wang, A. Zhang, P. Zhang, H. Wang, Cloud-assisted ehr sharing with security and privacy preservation via consortium blockchain, IEEE Access 7 (2019) 136704–136719.

[231] A. K. Talukder, M. Chaitanya, D. Arnold, K. Sakurai, Proof of disease: A blockchain consensus protocol for accurate medical decisions and reducing the disease burden, in: 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 2018, pp. 257–262.

[232] D. C. Nguyen, P. N. Pathirana, M. Ding, A. Seneviratne, Blockchain for secure ehrs sharing of mobile cloud based e-health systems, IEEE Access (2019).

[233] K. E. Skouby, P. Lynggaard, Smart home and smart city solutions enabled by 5G , IoT, aai and cot services, in: 2014 International Conference on Contemporary Computing and Informatics (IC3I), 2014, pp. 874–878.

[234] J.-h. Noh, H.-y. Kwon, A study on smart city security policy based on blockchain in 5G age, in: 2019 International Conference on Platform Technology and Service (PlatCon), 2019, pp. 1–4.

[235] R. Paul, P. Baidya, S. Sau, K. Maity, S. Maity, S. B. Mandal, IoT based secure smart city architecture using blockchain, in: 2018 2nd International Conference on Data Science and Business Analytics (ICDSBA), 2018, pp. 215–220.

[236] K. Kotobi, M. Sartipi, Efficient and secure communications in smart cities using edge, caching, and blockchain, in: 2018 IEEE International Smart Cities Conference (ISC2), 2018, pp. 1–6.

[237] S. Y. Nikouei, R. Xu, D. Nagothu, Y. Chen, A. Aved, E. Blasch, Real-time index authentication for event-oriented surveillance video query using blockchain, in: 2018 IEEE International Smart Cities Conference (ISC2), 2018, pp. 1–8.

[238] R. Wang, W.-T. Tsai, J. He, C. Liu, Q. Li, E. Deng, A video surveillance system based on permissioned blockchains and edge computing, in: 2019 IEEE International Conference on Big Data and Smart Computing (BigComp), 2019, pp. 1–6.

[239] A. Damianou, C. M. Angelopoulos, V. Katos, An architecture for blockchain over edge-enabled IoT for smart circular cities, in: 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), 2019, pp. 465–472.

[240] T. H. Nguyen, J. Partala, S. Pirttikangas, Blockchain-based mobility-as-a-service, in: 2019 28th International Conference on Computer Communication and Networks (ICCCN), 2019, pp. 1–6.

[241] H. Yu, Z. Yang, R. O. Sinnott, Decentralized big data auditing for smart city environments leveraging blockchain technology, IEEE Access 7 (2018) 6288–6296.

[242] M.-H. R. Tseng, S. E. Chang, T.-Y. Kuo, Using blockchain to access cloud services: A case of financial service application, in: 2019 Federated Conference on Computer Science and Information Systems (FedCSIS), 2019, pp. 565–568.

[243] S. A. A. Shah, E. Ahmed, M. Imran, S. Zeadally, 5G for vehicular communications, IEEE Communications Magazine 56 (1) (2018) 111–117.

[244] P. Dong, T. Zheng, S. Yu, H. Zhang, X. Yan, Enhancing vehicular communication using 5G -enabled smart collaborative networking, IEEE Wireless Communications 24 (6) (2017) 72–79.

[245] Q. Ren, et al., Using blockchain to enhance and optimize IoT-based intelligent traffic system, in: 2019 International Conference on Platform Technology and Service (PlatCon), 2019, pp. 1–4.

[246] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, Y. Chen, Adaptive blockchain-based electric vehicle participation scheme in smart grid platform, IEEE Access 6 (2018) 25657–25665.

[247] Z. Zhou, B. Wang, M. Dong, K. Ota, Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing, IEEE Transactions on Systems, Man, and Cybernetics: Systems (2019).

[248] S. Guo, X. Hu, Z. Zhou, X. Wang, F. Qi, L. Gao, Trust access authentication in vehicular network based on blockchain, China Communications 16 (6) (2019) 18–30.

[249] D. Zhang, F. R. Yu, R. Yang, Blockchain-based distributed software-defined vehicular networks: A dueling deep q-learning approach, IEEE Transactions on Cognitive Communications and Networking (2019).

[250] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, K. Ren, A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks, IEEE Network 32 (6) (2018) 184–192.

[251] S. De Dutta, R. Prasad, Security for smart grid in 5G and beyond networks, Wireless Personal Communications 106 (1) (2019) 261–273.

[252] T. Dragičević, P. Siano, S. Prabaharan, et al., Future generation 5G wireless networks for smart grid: A comprehensive review, Energies 12 (11) (2019) 2140.

[253] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, Y. Ma, Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities, IEEE Communications Magazine 56 (7) (2018) 82–88.

[254] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, G. Dong, Grid-monitoring: Secured sovereign blockchain based monitoring on smart grid, IEEE Access 6 (2018) 9917–9925.

[255] M. M. Esfahani, O. A. Mohammed, Secure blockchain-based energy transaction framework in smart power systems, in: IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society, 2018, pp. 260–264.

[256] K. Singh, S. Choube, Using blockchain against cyber attacks on smart grids, in: 2018 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), 2018, pp. 1–4.

[257] X. Lu, Z. Guan, X. Zhou, X. Du, L. Wu, M. Guizani, A secure and efficient renewable energy trading scheme based on blockchain in smart grid, in: 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2019, pp. 1839–1844.

[258] G. Bansal, A. Dua, G. S. Aujla, M. Singh, N. Kumar, Smartchain: a smart and scalable blockchain consortium for smart grid systems, in: 2019 IEEE International Conference on Communications Workshops (ICC Workshops), 2019, pp. 1–6.

[259] W. Hua, H. Sun, A blockchain-based peer-to-peer trading scheme coupling energy and carbon markets, in: 2019 International Conference on Smart Energy Systems and Technologies (SEST), 2019, pp. 1–6.

[260] K. Gai, Y. Wu, L. Zhu, L. Xu, Y. Zhang, Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks, IEEE Internet of Things Journal (2019).

[261] J. Wang, L. Wu, K.-K. R. Choo, D. He, Blockchain based anonymous authentication with key management for smart grid edge computing infrastructure, IEEE Transactions on Industrial Informatics (2019).

[262] A. Choubey, S. Behera, Y. S. Patel, K. Mahidhar, R. Misra, Energytradingrank algorithm for truthful auctions among evs via blockchain analytics of large scale transaction graphs, in: 2019 11th International Conference on Communication Systems & Networks (COMSNETS), 2019, pp. 1–6.

[263] D. Chi-Nguyen, P. N. Pathirana, M. Ding, A. Seneviratne, Secrecy performance of the UAV enabled cognitive relay network, in: 2018 IEEE 3rd International Conference on Communication and Information Systems (ICCIS), 2018, pp. 117–121.

[264] L. Gupta, R. Jain, G. Vaszkun, Survey of important issues in UAV communication networks, IEEE Communications Surveys & Tutorials 18 (2) (2015) 1123–1152.

[265] J. Qiu, D. Grace, G. Ding, J. Yao, Q. Wu, Blockchain-based secure spectrum trading for unmanned aerial vehicle assisted cellular networks: An operators perspective, IEEE Internet of Things Journal (2019).

[266] K. Lei, Q. Zhang, J. Lou, B. Bai, K. Xu, Securing icn-based UAV ad hoc networks with blockchain, IEEE Communications Magazine 57 (6) (2019) 26–32.

[267] S. Aggarwal, M. Shojafar, N. Kumar, M. Conti, A new secure data dissemination model in internet of drones, in: ICC 2019-2019 IEEE International Conference on Communications (ICC), 2019, pp. 1–6.

[268] A. Kapitonov, et al., Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of uavs, in: 2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS), 2017, pp. 84–89.

[269] T. Rana, A. Shankar, et al., An intelligent approach for UAV and drone privacy security using blockchain methodology, in: 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 2019, pp. 162–167.

[270] A. Islam, S. Y. Shin, Bus: A blockchain-enabled data acquisition scheme with the assistance of UAV swarm in internet of things, IEEE Access 7 (2019) 103231–103249.

[271] A. Islam, et al., BHMUS: Blockchain based secure outdoor health monitoring scheme using UAV in smart city, in: 2019 7th International Conference on Information and Communication Technology (ICoICT), 2019, pp. 1–6.

[272] I. J. Jensen, D. F. Selvaraj, P. Ranganathan, Blockchain technology for networked swarms of unmanned aerial vehicles (uavs), in: 2019 IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM), 2019, pp. 1–7.

[273] V. Sharma, I. You, D. N. K. Jayakody, D. G. Reina, K.-K. R. Choo, Neural-blockchain-based ultrareliable caching for edge-enabled UAV networks, IEEE Transactions on Industrial Informatics 15 (10) (2019) 5723–5736.

[274] S. B. H. Youssef, S. Rekhis, N. Boudriga, A blockchain based secure IoT solution for the dam surveillance, in: 2019 IEEE Wireless Communications and Networking Conference (WCNC), 2019, pp. 1–6.

[275] (Blockchain Transforms 5G: Opportunities and Challenges [Online]. Available: https://www.blockchain-council.org/blockchain/blockchain-transforms-5g-opportunities-and-challenges/).

[276] A. Anjum, M. Sporny, A. Sill, Blockchain standards for compliance and trust, IEEE Cloud Computing 4 (4) (2017) 84–90.

[277] A. A. Monrat, O. Schelén, K. Andersson, A survey of blockchain from the perspectives of applications, challenges, and opportunities, IEEE Access 7 (2019) 117134–117151.

[278] S. Kim, Y. Kwon, S. Cho, A survey of scalability solutions on blockchain, in: 2018 International Conference on Information and Communication Technology Convergence (ICTC), 2018, pp. 1204–1207.

[279] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, D. I. Kim, A survey on consensus mechanisms and mining strategy management in blockchain networks, IEEE Access 7 (2019) 22328–22370.

[280] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, Y. Liu, A survey on the scalability of blockchain systems, IEEE Network 33 (5) (2019) 166–173.

[281] A. I. Sanka, R. C. Cheung, Efficient high performance fpga based nosql caching system for blockchain scalability and throughput improvement, in: 2018 26th International Conference on Systems Engineering (ICSEng), 2018, pp. 1–8.

[282] S. S. Hazari, Q. H. Mahmoud, A parallel proof of work to improve transaction speed and scalability in blockchain systems, in: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019, pp. 0916–0921.

78

[283] S. Ali, G. Wang, B. White, R. L. Cottrell, A blockchain-based decentralized data storage and access framework for pinger, in: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), 2018, pp. 1303–1308.

[284] W. Xiong, L. Xiong, Smart contract based data trading mode using blockchain and machine learning, IEEE Access 7 (2019) 102331–102344.

[285] F. R. Yu, vdlt: A service-oriented blockchain system with virtualization and decoupled management/control and execution, arXiv preprint arXiv:1809.00290 (2018).

[286] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Generation Computer Systems (2017).

[287] S. Rouhani, R. Deters, Security, performance, and applications of smart contracts: A systematic survey, IEEE Access 7 (2019) 50759–50779.

[288] M. Wohrer, U. Zdun, Smart contracts: security patterns in the ethereum ecosystem and solidity, in: 2018 International Workshop on Blockchain Oriented Software Engineering (IW-BOSE), 2018, pp. 2–8.

[289] A. Miller, M. Möser, K. Lee, A. Narayanan, An empirical analysis of linkability in the monero blockchain.(2017) (2017).

[290] L. Luu, Y. Velner, J. Teutsch, P. Saxena, Smartpool: Practical decentralized pooled mining, in: 26th {USENIX} Security Symposium ({USENIX} Security 17), 2017, pp. 1409–1426.

[291] R. Cheng, F. Zhang, J. Kos, W. He, N. Hynes, N. Johnson, A. Juels, A. Miller, D. Song, Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts, in: 2019 IEEE European Symposium on Security and Privacy (EuroS&P), 2019, pp. 185–200.

[292] P. Tsankov, A. Dan, D. Drachsler-Cohen, A. Gervais, F. Buenzli, M. Vechev, Securify: Practical security analysis of smart contracts, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2018, pp. 67–82.

[293] A. Dorri, S. S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: The case study of a smart home, in: 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), 2017, pp. 618–623.

[294] T. Kim, J. Noh, S. Cho, Scc: Storage compression consensus for blockchain in lightweight IoT network, in: 2019 IEEE International Conference on Consumer Electronics (ICCE), 2019, pp. 1–4.

[295] Y. Liu, K. Wang, Y. Lin, W. Xu, Lightchain: A lightweight blockchain system for industrial internet of things, IEEE Trans. Ind. Informat. (2019).

[296] M. U. Zaman, T. Shen, M. Min, Proof of sincerity: A new lightweight consensus approach for mobile blockchains, in: 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2019, pp. 1–4.

[297] T. Le, M. W. Mutka, A lightweight block validation method for resource-constrained IoT devices in blockchain-based applications, in: 2019 IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM), 2019, pp. 1–9.

[298] Z. Xiong, S. Feng, et al., Optimal pricing-based edge computing resource management in mobile blockchain, in: 2018 IEEE International Conference on Communications (ICC), 2018, pp. 1–6.

[299] C. Qiu, H. Yao, C. Jiang, S. Guo, F. Xu, Cloud computing assisted blockchain-enabled internet of things, IEEE Transactions on Cloud Computing (2019).

[300] P. K. Sharma, S. Singh, Y.-S. Jeong, J. H. Park, Distblocknet: A distributed blockchains-based secure sdn architecture for IoT networks, IEEE Communications Magazine 55 (9) (2017) 78–85.

[301] (Amazon Partners On New Ethereum Marketplace For Enterprises [Online]. Available: https://www.forbes.com/sites/sarahhansen/2018/11/08/consensys-kaleido-launches-full-stack-marketplace-platform-for-enterprise-blockchains/).

[302] D. Unal, M. Hammoudeh, M. S. Kiraz, Policy specification and verification for blockchain and smart contracts in 5g networks, ICT Express 6 (1) (2020) 43–47.

[303] N. C. Luong, T. T. Anh, H. T. T. Binh, D. Niyato, D. I. Kim, Y.-C. Liang, Joint transaction transmission and channel selection in cognitive radio based blockchain networks: A deep reinforcement learning approach, in: ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2019, pp. 8409–8413.

[304] M. Liu, Y. Teng, F. R. Yu, V. C. Leung, M. Song, Deep reinforcement learning based performance optimization in blockchain-enabled internet of vehicle, in: ICC 2019-2019 IEEE International Conference on Communications (ICC), 2019, pp. 1–6.

[305] M. G. Kibria, K. Nguyen, G. P. Villardi, O. Zhao, K. Ishizu, F. Kojima, Big data analytics, machine learning, and artificial intelligence in next-generation wireless networks, IEEE access 6 (2018) 32328–32338.

[306] A. A. Cárdenas, P. K. Manadhata, S. P. Rajan, Big data analytics for security, IEEE Security & Privacy 11 (6) (2013) 74–76.

[307] K. Sultan, H. Ali, Z. Zhang, Big data perspective and challenges in next generation networks, Future Internet 10 (7) (2018) 56.

[308] E. Karafiloski, A. Mishev, Blockchain solutions for big data challenges: A literature review, in: IEEE EUROCON 2017-17th International Conference on Smart Technologies, 2017, pp. 763–768.

[309] L. Yue, H. Junqin, Q. Shengzhi, W. Ruijin, Big data model of security sharing based on blockchain, in: 2017 3rd International Conference on Big Data Computing and Communications (BIGCOM), 2017, pp. 117–121.

[310] U. U. Uchibeke, K. A. Schneider, S. H. Kassani, R. Deters, Blockchain access control ecosystem for big data security, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1373–1378.

[311] K. Lampropoulos, G. Georgakakos, S. Ioannidis, Using blockchains to enable big data analysis of private information, in: 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2019, pp. 1–6.

Author Biography

	Dinh C. Nguyen received the B.S. degree (first class honors) in electrical and electronic engineering from Ho Chi Minh City University of Technology, Vietnam, in 2015. Currently, he is a Ph.D. scholar in the School of Engineering, Deakin University, Victoria, Australia. His research interests focus on security and privacy of Internet of Things, mobile cloud computing, and smart e-healthcare. He is currently working on adopting blockchain for secure communication networks including clouds, IoTs, and healthcare. He is a recipient of the Data61 PhD scholarship, CSIRO, Australia.
	Pubudu N. Pathirana (SMIEEE) was born in 1970 in Matara, Sri Lanka, and was educated at Royal College Colombo. He received the B.E. degree (first class honors) in electrical engineering and the B.Sc. degree in mathematics in 1996, and the Ph.D. degree in electrical engineering in 2000 from the University of Western Australia, all sponsored by the government of Australia on EMSS and IPRS scholarships, respectively. He was a Postdoctoral Research Fellow at Oxford University, Oxford, a Research Fellow at the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia, and a Consultant to the Defence Science and Technology Organization (DSTO), Australia, in 2002. He was a visiting associate professor at Yale University in 2009. Currently, he is an Associate Professor with the School of Engineering, Deakin University, Geelong, Australia and his current research interests include Bio-Medical assistive device design, human motion capture, mobile/wireless networks, rehabilitation robotics and radar array signal processing.
	Ming Ding (M'12-SM'17) is a Senior Research Scientist at Data61 (previously known as NICTA), CSIRO, Australia. He has authored over 80 papers in IEEE journals and conferences, all in recognized venues, and about 20 3GPP standardization contributions, as well as a Springer book "Multi-point Cooperative Communication Systems: Theory and Applications". Currently he holds 14 US patents and co-invented another 100+ patents on 4G/5G technologies in CN, JP, EU, etc. Currently, he is an editor of IEEE Transactions on Wireless Communications. He was the lead speaker of the industrial presentation on unmanned aerial vehicles in IEEE Globecom 2017, which was awarded as the Most Attended Industry Program in the conference. Also, he was awarded in 2017 as the Exemplary Reviewer for IEEE Transactions on Wireless Communications.

Aruna Seneviratne is the foundation Chair in Telecommunications and holds the Mahanakorn Chair of Telecommunications, and the leader of the Mobile Systems Research Group at NICTA. His current research interests are in mobile content distributions and preservation of privacy. He received his PhD in electrical engineering from the University of Bath, UK. He has held academic appointments at the University of Bradford, UK, Curtin University, and UTS.

The authors report no conflicts of interest. The authors alone are responsible for the content and writing of this article.