IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 19 January 2023, accepted 1 February 2023, date of publication 10 February 2023, date of current version 24 February 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3243985

SURVEY

Blockchain for Dynamic Spectrum Access and Network Slicing: A Review

SIDRA TUL MUNTAHA[1], (Graduate Student Member, IEEE), PAVLOS I. LAZARIDIS[1], (Senior Member, IEEE), MARYAM HAFEEZ[1], (Member, IEEE), QASIM Z. AHMED[1], (Member, IEEE), FAHEEM A. KHAN[1], (Member, IEEE), AND ZAHARIAS D. ZAHARIS[2], (Senior Member, IEEE)

[1]School of Computing and Engineering, University of Huddersfield, HD1 3DH Huddersfield, U.K.
[2]School of Electrical and Computer Engineering, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece

Corresponding author: Pavlos I. Lazaridis (p.lazaridis@hud.ac.uk)

This work was supported by the European Union through the Horizon 2020 Marie Skł odowska-Curie Innovative Training Networks Program "Mobility and Training for Beyond 5G Ecosystems (MOTOR5G)" under Grant 861219.

ABSTRACT Dynamic spectrum access (DSA) and network slicing are some of the principal concepts to realize the emerging applications in Beyond 5th Generation (B5G) and 6th Generation (6G) networks. The frequency spectrum remains scarce and underutilized, while the performance requirements in terms of data throughput and latency of the network tenants have diversified. DSA allows for the efficient utilization of spectrum resources, while network slicing aims to serve network users with highly distinctive service needs. Lack of incentivization, sharing of spectrum resources among multiple operators, and lack of trust between operators are some of the challenges faced by centralized DSA approaches. Similarly, secure network slice orchestration, slice-isolation, secure access to network resources, privacy of user sensitive data, assuring the provision of Service Level Agreements (SLAs), are some of the challenges in existing network slicing techniques. Blockchain due to its innate capabilities can be a promising technology to solve the key issues pertaining to current DSA and network slicing approaches. Blockchain through smart contracts, provides traceability of network resources, auditability and accountability of network operators and service providers. Smart contracts facilitate the automation of resource sharing and network slice orchestration, while ensuring that SLAs are met, and network operators are compensated. This paper first provides a comprehensive overview of the DSA concept, the existing DSA techniques, and the challenges posed by these techniques. This is followed by a detailed description of network slicing, its key elements and architecture, various network slicing parameters, existing network slicing techniques and their challenges. Then an in-depth review on blockchain, its working principle, factors that affect blockchain implementation, and a comparison of various open-source blockchain platforms that support smart contracts is presented. This discussion is summarized by presenting the state-of-the-art in the blockchain-enabled DSA and network slicing, challenges and trade-offs of these techniques, and the gaps and future directions in this research area. Finally, we conclude by providing some future research directions.

INDEX TERMS 6G, blockchain, dynamic spectrum access (DSA), network slicing, smart contract.

I. INTRODUCTION

Spectrum is a limited and vital resource, and most of our electronic communications rely on it. Spectrum usage is increasing exponentially and thus the spectrum is becoming scarce. As per the Cisco Annual Internet Report (2018-2023) [1], the total number of internet users will increase from 3.9 billion in 2018 to 5.3 billion internet users in 2023. This is an increase of 35% in internet users in only five years. Furthermore, there will be a massive increase of 59% in networked devices from 18.4 billion in 2018 to 29.3 billion in 2023, which is almost three times the predicted global population

The associate editor coordinating the review of this manuscript and approving it for publication was Mehdi Sookhak.

in 2023 [1]. Similarly, as per the International Telecommunication Union Radio-communication (ITU-R) report on traffic estimates from 2020 to 2030, the global mobile traffic is estimated to increase from 62 Exabytes (EB)/month to 607 EB/month by 2025 and reach 5016 EB/month by 2030 [2]. This immense growth in data requirements and the number of connected devices have resulted in a demand for higher bandwidth availability and new network resources. Therefore, spectrum scarcity and decentralized management of network resources have emerged as crucial challenges in this current era of hyper-connectivity with enhanced data and latency requirements [3]. Fixed spectrum allocation is the least efficient resource sharing method, as the spectrum becomes insufficient to serve all the users due to it being underutilized. For instance, to deploy and provide connectivity to billions of Internet-of-Things (IoT) devices, we need 76 GHz of spectrum resources for exclusive frequency allocation [4], [5], [6]. To increase spectrum utilization, the concept of Dynamic Spectrum Access (DSA) networks was introduced [7]. With DSA, the spectrum required to provide connectivity to billions of IoT devices, reduces from 76 GHz to just 19 GHz [4], [5]. In 4th Generation (4G) Long-Term Evolution (LTE), centrally managed DSA techniques, such as Cognitive Radios (CRs), Licensed Shared Access (LSA), Spectrum Access System (SAS) for Citizens Broadband Radio Service (CBRS), and TV White Spaces (TVWS) were proposed [5], [8], [9], [10], [11], and [12]. All these DSA techniques rely on a central control authority to gain access to the spectrum and thus introduce issues, such as bias, single-point-of-failure, lack-of-incentive-based sharing, breach of security, and additional signaling overhead in DSA networks. Therefore, the need for more decentralized approaches has gained attention in 5th Generation New Radio (5GNR) and Beyond 5th Generation (B5G). The issues related to centralized DSA techniques can be mitigated by introducing a decentralized and distributed solution for spectrum sharing.

Recently, blockchain has gained massive popularity in this context due to its inherent capabilities such as immutability, decentralization, transparency, traceability, and no single point-of-failure. Blockchain-based DSA provides several advantages over the centralized DSA techniques, such as incentivization of the spectrum sharing mechanism, sharing of spectrum among multiple trustless entities, privacy protection of users and the sensitive data of users, fairness of the sharing mechanism, etc. [5], [8], [9], [10], [11], [13].

The development of B5G technologies and the emerging data-driven applications that 6th Generation (6G) aims to support, have also contributed to this increase in traffic volume [14]. Global 5th Generation (5G) rollout is currently underway where the focus of 5G networks is to achieve services such as enhanced Mobile Broadband (eMBB), Ultra-Reliable and Low Latency Communication (URLLC), and massive Machine Type Communication (mMTC) or massive Internet-of-Things (mIoTs). These 5GNR services demand varying performance requirements, such as peak data rates of 10 Gbps in eMBB, URLLC with a latency of less than 1 ms in the Radio Access Network (RAN), while mMTC aims to have as many as 1 million connected devices per square kilometer [15]. 5GNR relies on key enabling technologies such as End-to-End (E2E) network slicing, Network Function Virtualization (NFV), and Software Defined Networking (SDN) to realize these diverse services with varying data and latency requirements [16]. E2E Network slicing enables the network providers to provide the required services to these emerging applications and network tenants through the creation of multiple logical networks over the common physical infrastructure which span over multiple technical domains such as RAN, Transport Network (TN), Core Network (CN), and Network Management System [17], [18]. The security of network slice orchestration and the efficiency and transparency of resource allocation are prominent challenges in network slicing. Continuous monitoring of customer-devised Service Level Agreements (SLAs) is required to coordinate the service requirements and network capabilities [16]. This necessitates the need for a more decentralized slice orchestration mechanism. To this extent, blockchain-enabled network slicing has become increasingly popular. Blockchain enhances the security of network slice creation, safeguards the sensitive information of network tenants, reduces operational costs, and provides secure access to the services [19]. Fig. 1 presents a typical depiction of blockchain-based DSA and network slicing scenario. It shows the different 5GNR services with distinct Quality-of-Service (QoS) requirements, such as high data throughput for eMBB slice users, high reliability and low latency for URLLC slice users, and massive connectivity for mMTC slice users. It depicts how blockchain through smart contracts can be deployed in slice manager to ensure the SLAs. It also depicts a blockchain-based DSA scenario.

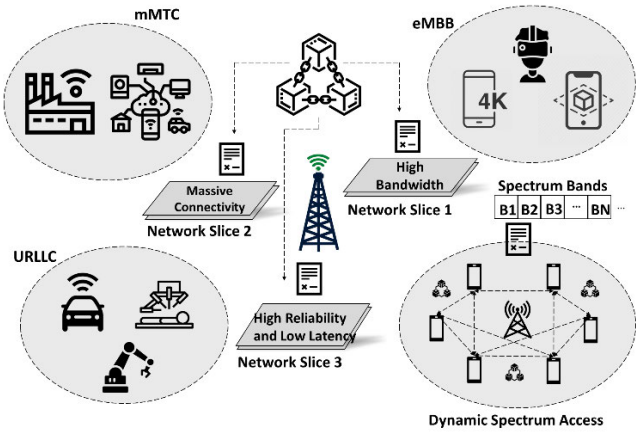


FIGURE 1. Typical depiction of a blockchain-based DSA and network slicing architecture.

6G networks are expected to be more intelligent, secure, energy and spectrum efficient, scalable, reliable, and supporting a multitude of emerging applications [20]. 6G is envisioned to support peak data rates as high as 1 Tbps, an E2E latency of less than 1 ms, the E2E network reliability

TABLE 1. Summary of related surveys and their scope.

Contributions	Luka et al. [13] [2021]	Chahbar et al. [26] [2021]	Yue et al. [27] [2021]	Khan et al. [28] [2021]	Javed et al. [29] [2022]	Our work [2022]
DSA techniques	×	×	×	×	×	✓
DSA Challenges	✓	×	×	×	×	✓
Network slicing architecture and key attributes	×	✓	×	×	✓	✓
Network slicing parameters and existing techniques	×	×	×	×	✓	✓
Network slicing challenges	×	✓	✓	×	×	✓
Blockchain overview	×	×	✓	×	✓	✓
Blockchain architecture, working principle, and types of blockchains	×	×	✓	✓	✓	✓
Factors affecting blockchain implementation	×	×	×	×	×	✓
Open-source blockchain platforms supporting smart contract	×	×	×	✓	✓	✓
Blockchain applications	✓	×	✓	×	✓	✓
Review of state-of-the-art in blockchain-enabled DSA, challenges, and future directions	×	×	×	×	×	✓
Review of state-of-the-art in blockchain-enabled network slicing, challenges, and future directions	×	×	×	×	✓	✓

to be near 99.99999%, and to have as many as 10 million connected devices per square kilometer to support Internet-of-Everything (IoE). 6G is envisioned to support newer applications and use cases, a few of which are discussed as follows [8], [20], [21], [22], [23]:

1) *Mobile Broadband Reliable Low Latency Communication (MBRLLC):* Emerging applications, such as Extended Reality (XR), encompassing Virtual Reality VR) and Augmented Reality (AR), Brain-Computer Interactions (BCI), and Connected Robotics and Autonomous Systems (CRAS), not only require low latency and reliable communication, but also high data rates. Thus, for the above-mentioned mainstream 6G applications, eMBB and URLLC can be combined as MBRLLC to deliver high speed, reliability, and data rates [8], [20], [21].
2) *Massive URLLC (MURLLC):* To satisfy the newer applications, 6G envisions combining mMTC with URLLC and thus making a reliable, latency conscious, and scalable network for entertaining services such as IoE [8], [20], [21].
3) *Human-Centric Services (HCS):* For applications such as wireless BCI, HCS is envisioned which aims to define a new performance metric, Quality-of-Physical-Experience (QoPE), which determines the network performance based on human users [8], [20], [21].
4) *Multi-Purpose Services (MPS):* MPS envision the convergence of multiple functions of wireless communication as one, such as Communications, Computing, Control, Localization, and Sensing (3CLS) [8], [20], [21].

The above discussed ambitious use cases which are envisioned for 6G will be challenging to realize without the presence of efficient spectrum access and resource management mechanisms. To this extent, some potential schemes such as blockchain-based DSA and network slicing will be discussed, as well as the implementation challenges of 6G networks with respect to these schemes in Section V and VI of this paper.

A. EXISTING WORK

In the recent research efforts, blockchain has been considered as an efficient solution for many emerging wireless network applications, such as improving security, enhancing automation, and reducing issues pertaining to the centralized control of the application processes [24], [25]. Current surveys in the domain of blockchain-based solutions for decentralized applications, lack an in-depth discussion on the application of blockchain through smart contracts for enhancing the performance of DSA and network slicing, as well as in addressing the issues that arise with the centralized control of these applications. In [26], authors have provided a detailed survey on E2E network slicing, which encompasses the network slicing modelling for RAN, CN, and TN. This survey [26], also provides a general structure of network slicing modelling as suggested by the ETSI NGP workgroup and how a network slice is ordered through the service graph, as well as the in-depth network slicing models for RAN, CN, and TN are provided. Furthermore, the authors in [26] have identified key issues pertaining to the conventional network slicing orchestration methods, such as security and isolation. But this survey lacks the discussion on other potential 6G schemes like DSA and blockchain.

In [27], various use-cases of blockchain as a solution for decentralized applications in 5GNR and beyond such as network coding, authentication, infrastructure sharing, spectrum sharing, and network slicing are described.

Furthermore, a detailed overview of blockchain technology and its characteristics that results in blockchain being an effective solution for decentralized applications is provided. But this survey does not provide any discussion on other spectrum management schemes like DSA.

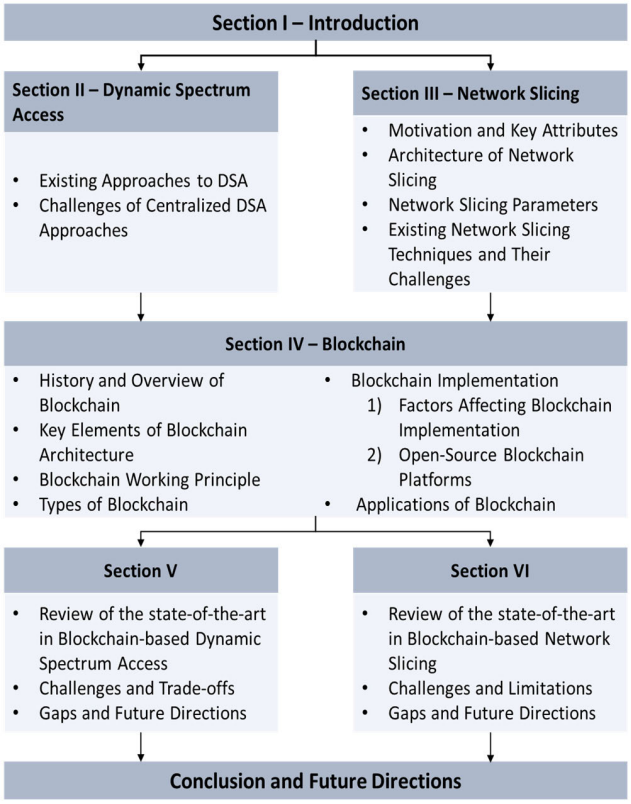


FIGURE 2. Organization of the review paper.

In [28], numerous solutions for Blockchains interoperability are surveyed which are based on smart contracts. This survey aims to provide a detailed discussion on how different Blockchains can achieve interoperability by employing smart contracts. However, it did not discuss the application of blockchain for many decentralized applications.

In [29], the application of blockchain as a Distributed Ledger Technology (DLT) for network slicing is presented. The authors provide an overview of blockchain and network slicing. They have also shown how blockchain can be implemented for network slicing. But they have not discussed any other use-case of blockchain in 5GNR and beyond.

In [13], the blockchain implementation for spectrum sensing and spectrum sharing is presented. However, the work in [13] lacks a discussion on different blockchain platforms that are available and how to use them for spectrum sharing, including the use of smart contract based blockchain platforms. Table 1 highlights the contributions and scope of the related surveys and our work.

B. OUR CONTRIBUTION

As evident from the discussion provided above, the existing research lacks a comprehensive overview of the key-enabling technologies DSA and network slicing for B5G and 6G networks, as well as their integration with blockchain. Blockchain when deployed in these applications, can enhance the spectrum utilization and ensure the provision of the required QoS. The recent surveys also lack a discussion about different open-source blockchain platforms that provide a smart contract development environment. Furthermore, there lacks a discussion about the various implementation features of blockchain that facilitate in its implementation for applications like network slicing and DSA.

In summary, the prominent contributions of this survey article are as follows:

- To provide a comprehensive overview and state-of-the-art research in DSA and network slicing, along with their challenges and research gaps.
- To provide an in-depth overview and various implementation features of blockchain and compare several open-source blockchain platforms that enable smart contract development environment.

C. ORGANIZATION OF THE PAPER

This paper is organized as follows and as depicted in Fig. 2. In Section II, we discuss DSA, the existing DSA approaches, and the challenges faced in centralized DSA techniques. In Section III, we provide a comprehensive discussion on network slicing, its key attributes and architecture, the various parameters of network slicing that can be enhanced through more decentralized approaches, existing network slicing techniques and their challenges. In Section IV, we provide an in-depth review of blockchain technology which encompasses the history of blockchain, key elements of blockchain architecture, its working principle, different types of blockchain, factors affecting blockchain implementation, and various open-source blockchain platforms that support smart contract development environments, and applications of blockchain in B5G and 6G networks. In Sections V, we review the state-of-the-art research in blockchain-enabled DSA, followed the challenges and trade-offs of these techniques, and gaps and future directions of this research area. In Section VI, we first provide the review of the state-of-the-art in blockchain-enabled network slicing, followed by the challenges and limitations of these techniques, and lastly the gaps and future research directions. Finally, we conclude the paper with a discussion of some future research directions.

II. DYNAMIC SPECTRUM ACCESS

The spectrum is divided into two distinctive frequency groups for the deployment of 5GNR and B5G networks. One group comprises of frequencies lower than 7.225 GHz, and the other group is composed of frequencies ranging between 24.25–52.6 GHz. The higher frequencies band can offer high data rates as supported in millimeter wave

communication, but its transmission range is short. This poses other challenges, such as interference management and mitigation. For most, long-distance communications, the lower frequency group is the one that is preferred, but it is underutilized due to fixed spectrum allocations. To resolve the spectrum under-utilization problem, DSA has been proposed as an effective way to enhance the spectrum usability [30]. DSA is the process that enables the use of spectrum holes through spectrum sensing and real-time management of network resources. The aim here is to enhance the resource utilization efficiency and support the opportunistic access of spectrum resources without the need for additional bandwidth [31]. In this section, we will discuss several different techniques for DSA that have been proposed in the past, their drawbacks, and what could be a better solution for the challenges posed by DSA in 6G networks.

A. EXISTING APPROACHES TO DSA

Various DSA techniques have evolved to enhance spectrum utilization. From opportunistic access approaches, such as a few different schemes in CRs, and LSA, to cooperative sharing schemes which are based on databases, such as TVWS and CBRS [32]. For instance, service-based incentives were exploited for spectrum sharing between incumbent and secondary users in [33], [34], [35]. Whereas [36] presents an analytical case study based on game theoretic analysis of LSA to demonstrate the energy and spectral efficiency of the scheme. A game theory-based DSA technique for enhancing spectrum utilization is proposed in [37]. Firstly, the network is trained using the Long Short-Term Memory (LSTM)-based deep Q-network with a fairness incentive mechanism for optimal DSA. Then based on the trained model, spectrum is allocated to user for maximum utilization of resources. Similarly in [38], a deep reinforcement learning based distributed DSA mechanism is proposed. A spectrum access system is designed which aims to maximize network utility while limiting message exchange among users. The design parameters are established through a game-theoretic analysis of the system attributes. In [39], various auction-based mechanisms for DSA in cognitive radio networks have been proposed. Several auction-based methods for spectrum sharing have been discussed such as:

- One-sided spectrum auctions in which there is one spectrum seller and multiple buyers.
- Double-sided spectrum auctions in which there are multiple sellers and buyers with an intermediate operator playing the role of the auctioneer.
- Online spectrum auctions where the bids are placed continuously, and the auctioneer must take a decision about allocation and payment instantly.
- Dynamic spectrum auctions in which the auction mechanism is dynamically modified to enhance the performance of the mechanism.

These methods enhance the spectrum utilization in CRs networks. Similarly, other DSA techniques, such as In-Band Full-Duplex (IBFD) scheme for Dynamic Spectrum Sharing (DSS) in the CBRS band have been examined in [10]. In this CBRS Mobile Broadband Network (MBN), a Multiple Input Multiple Output (MIMO) radar system represents the Incumbent Access (IA) users, while the Priority Access License (PAL) and General Authorized Access (GAA) users are specified in terms of IBFD-based MIMO MBN. A joint beamformer is designed with constraints on transmit and detection probability of IA users to satisfy the QoS requirement of the PAL and GAA users and reduce the interference caused by the radar system towards the MBN. It enhances the conventional SAS for CBRS three-tier spectrum sharing regime. It also improves the QoS requirements and performance of PAL and GAA users while limiting the interference incurred on IA users. However, the IBFD-CBRS scheme introduces new challenges, such as security of the sensitive information shared by the IA users, such as for military communication, and new MAC layer protocols are required for adaptation of the IBFD scheme. Recognizing and classifying interfering signals is another open issue. The most advanced DSA techniques utilize blockchain as a solution, but these are discussed later in Section V of this paper.

B. CHALLENGES OF CENTRALIZED DSA APPROACHES

The centralized DSA techniques present certain challenges as these approaches demand a central management system to ensure QoS of the incumbent user. Few of these challenges are mentioned as follows [40], [41], [42]:

- centralized control requires additional signaling overhead;
- addition of new infrastructure;
- sharing of sensitive user data such as identity and geo-locations;
- interference management;
- centralized control of access leads to bias and untrustworthiness of the network administrators;
- risk of exposure of sensitive user information;
- single-point-of-failure, among other challenges.

In this section, we discussed one of the key-enabling techniques for realizing the emerging B5G and 6G applications, that is DSA. We further mentioned some existing DSA approaches, followed by the drawbacks of centralized DSA techniques. In the following section, we will provide an overview of another 5GNR key enabling technology, which is network slicing.

III. NETWORK SLICING

A. MOTIVATION

A multitude of applications with varying data, latency, and QoS requirements are emerging with the advent of 6G. Spectrum resources are limited and the 6G use case scenarios such as e-health, vehicle-to-everything communication, smart cities, smart factories, and mIoTs connectivity, have different QoS requirements [43]. Network slicing is a mechanism in 5GNR that enables the service providers to meet the diverse service requirements of a broad range of Network Service Customers (NSC). In network slicing the end-to-end

network is divided into multiple logical networks called network slices. A network slice consists of multiple Virtual Network Functions (VNFs). These VNFs consist of resource blocks from different layers such as access, transport, and core layer. Furthermore, these VNFs must be managed and isolated from the other VNFs of slices, while ensuring security, QoS, and other aspects of the network slice [29], [44]. Each VNF performs a specific network task from Access Network (AN) to the CN to fulfil the agreed-upon SLAs between the network tenant and the service provider. Each network slice configures the E2E network resources to deliver the required service in terms of throughput, latency, QoS, and reliability [45]. E2E network slicing offers numerous advantages to network operators and allows them to serve the commercial users as per their diverse data and latency demands, but at a low cost with better flexibility and swiftness [18], [46]. For instance, high data throughput would concern some commercial users. While for others, low latency and seamless communication would be desirable, and for some users, massive device connectivity might be crucial for their operation [18]. Hence by further optimizing and automating the network slice creation, modification, and management process, additional gains in terms of QoS and performance can be achieved. Network slice management can allow the network operators to fully utilize their physical resources through efficient management and allocation of their spare resources to the network slice instances. Automation along with resource management can maximize profits while maintaining or lowering the cost of deployment [18].

B. KEY ATTRIBUTES

In this subsection, we will discuss the key attributes of network slicing. Network slicing relies on two enabling technologies: NFV and SDN [47]. We first define NFV and SDN, followed by brief definitions of the key attributes of network slicing.

1) NFV

Traditional networks comprise Network Functions (NFs) that are implemented on vendor specific software and hardware and are also known as network elements or nodes. NFV decouples software from the hardware, thus making the software network nodes independent of the hardware network nodes. This assists in modifying both nodes separately. Due to this decoupling, the infrastructure resources can be shared and reassigned, thus enabling both the software and hardware to perform distinct functions at different times. This further facilitates the network operators to deploy latest services over the common physical infrastructure [48].

2) SDN

SDN is a network architecture that allows the network to be controlled centrally through software applications such as Application Programming Interfaces (APIs), regardless of the underlying technologies. Thus, network operators can manage and control the whole network consistently. SDN achieves this by separating the control plane from the data plane. By decoupling the control plane and data plane, the network switches become mere forwarding devices, and network control is implemented in a logically centralized controller. This separation between SDN controller and network switches is achieved by programming interfaces such as OpenFlow [49].

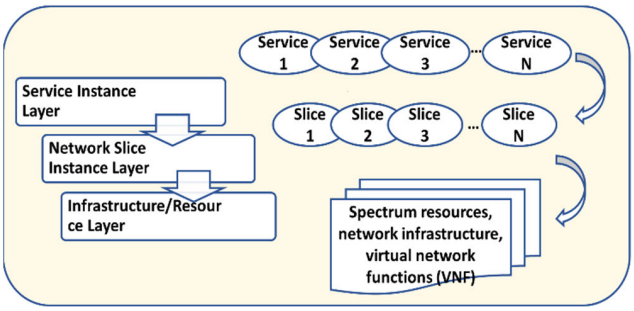


FIGURE 3. Network slicing operational layers [55].

3) E2E SERVICE

The E2E service provision attribute of network slicing ensures that the requested E2E performance by the slice customer should be provided, and if a specific Network Service Provider (NSP) does not have the control over the required E2E network resources, then multiple NSPs must reach to an agreement and stitch together the required network resources in order to fulfil the agreed upon SLAs [29], [44].

4) NETWORK RESOURCES

The network slice consists of VNFs comprising network resources spanned over multiple technical domains, from access, to transport, and to the core layer of the network. These resources could comprise of virtual resource blocks, computing resources, storage, and other network components [29], [44].

5) PROGRAMMABILITY

SDN and NFV can simplify network management and service provision and enable integration and operability of multiple networks to support communication services. They facilitate real-time service customization, and they control the allotted network slice resources through open APIs [50].

6) AUTOMATION

Automation allows the dynamic and on-demand configuration of network slices without manual intervention. The automation process relies on a signaling-based technique, which enables the third parties to put in network slice requests and mention the main performance requirements in the SLAs. Through automation techniques, network slice creation, deployment, and management processes are automated [47].

7) ISOLATION

For E2E network slicing, it is crucial to keep the network resources allocated to one slice isolated from the other slices. Isolation ensures the QoS and performance agreement, as multiple logical slices are created over the same shared network resources and each network tenant can have variable capacity and latency requirements. However, achieving slice isolation is a critical task and it introduces performance degradations, such as reduction in multiplexing gain and inefficient use of network resources to achieve explicit resource separation [51].

8) CUSTOMIZATION

The network resources allotted to the network slice instances must be able to adapt to the varying needs of a wide range of services. The allocated resources can be scaled up or down as per the diverse requirements of the network tenants. This kind of resource customization ensures that the SLA requirements are met [52].

C. ARCHITECTURE OF NETWORK SLICING

To support a multitude of applications and provide particular services to the end users, NFV and SDN are used to create, partition, and manage the physical infrastructure elements comprising software and hardware network components such as computational, storage, and communication resources [53]. Each slice has unique properties such as its design, packet capacity, and signal processing capabilities to serve particular users with variable performance, functionality, and isolation demands [54]. Let us now briefly discuss the operational layers of network slicing architecture.

1) LAYERS OF NETWORK SLICING ARCHITECTURE

According to Next Generation Mobile Networks (NGMN) [55], the network slicing architecture consists of three layers. These operational layers of network slicing are discussed below and shown in Fig. 3 [46], [54], [55].

- *Resource/Infrastructure Layer:* This layer is responsible for providing the required physical and VNF resources for creating the service instance to serve the end users as per their demands. These resources comprise of communication and computational resources, storage etc. [46], [53].
- *Network Slice/Partition Instance Layer:* This layer runs on top of the resource/infrastructure layer. It provides the necessary network capabilities for the service instance layer. A network operator creates a network slice instance, and it is shared by multiple service instances. Network slice instances combine to form E2E logical network slices [46], [53].
- *Service Instance Layer:* This layer is composed of end-users and other services that are required to be served by the network operator or by a third party. There is a service instance for each service and the service instance layer runs on top of the network slice instance layer and resource layer [46], [53].

D. NETWORK SLICING PARAMETERS

E2E network slicing involves the virtualization of network resources which spans over multiple network elements, from RAN to CN, and TN to User Equipment and network operators [18], [46]. The network parameters that may be configured as SLAs for network slicing implementation as per the GSMA white paper [18] are:

- the maximum data throughput that can be achieved,
- the minimum signal latency,
- the highest number of users that can be served,
- the availability of resources, in cases of any limits on time and place utilization, and
- the availability of support for voice and mobility capabilities.

For the creation of a network slice through the virtualization techniques, a logical network is created consisting of either dedicated or shared NFs of the 5G Stand-Alone (SA) network and the network resources such as computational and storage resources, signal propagation resources, and bandwidth allocation in transport network [18].

E. EXISTING NETWORK SLICING TECHNIQUES

In this subsection, we present some of the existing network slicing techniques, from deep learning and Artificial Intelligence (AI) based techniques to opportunistic resource allocation-based network slicing. For enhanced resource utilization while satisfying user's QoS requirements, a deep learning based Deep-Q-Network (DQN) algorithm for dynamic network slice creation for users with heterogeneous service demands is proposed in [56], [57]. Similarly, a Deep Reinforcement Learning (DRL) based network slicing mechanism for Vehicle-to-Vehicle (V2V) communication is proposed in [58]. An AI-based approach for RAN slicing is proposed in [59], for the Next Generation Wireless Networks (NGWNs). A DRL-based network slicing solution for resource allocation for smart grids is proposed in [60]. A network slicing technique based on opportunistic access of a shared channel is proposed in [61], to simultaneously enhance the spectrum utilization. The most recent network slicing approaches are based on a blockchain implementation, but these are discussed later in Section VI of this paper.

F. CHALLENGES OF EXISTING NETWORK SLICING TECHNIQUES

A centralized control-based slice manager can introduce certain challenges pertaining to the provision of required SLAs and security of the slice orchestration process. With regards to E2E network slice creation, there exist two major challenges; isolation and security. Slice isolation is a multi-dimension challenge. Firstly, performance isolation requires that the SLAs per slice are ensured, regardless of the network load of other slices. Secondly, there must exist isolation between network resources which are allocated to various slices. And

lastly, isolation of slice security, which requires that any attack on one network slice does not affect the security of other slices [18], [51].

In the next section, we will provide an in-depth review of blockchain technology, which is the key enabler for achieving decentralization in the emerging B5G and 6G applications. In Section V and VI we will discuss how blockchain can be a potential solution to resolve the issues pertaining to centralized approaches for DSA and network slicing.

IV. BLOCKCHAIN

In this section, we will provide a detailed overview of blockchain technology. We begin by defining the key aspects and elements of blockchain architecture, its working principle, and different types of blockchain. We then discuss various factors that affect the blockchain implementation, and a comparison of various open-source blockchain platforms. We conclude this section with a brief discussion on various applications of blockchain in 6G networks.

A. HISTORY AND OVERVIEW OF BLOCKCHAIN

The term blockchain has been in use since 2008 when it was first revealed by Satoshi Nakamoto in his paper ''Bitcoin: A Peer-to-Peer Electronic Cash System'' [62]. However, the concept of creating a secure chain of digital blocks has been in existence since 1991, when it was proposed by Stuart Haber et al. with the primary aim to digitally time stamp the electronic documents in a distributed manner to protect them against any kind of tampering [63], [64], [65]. Blockchain technology started to gain massive popularity in the last decade [66]. In the earlier years, blockchain had just been used as a DLT to store digital transactions without requiring a trusted third party or central control. However, blockchain is being used in a variety of different applications beyond cryptocurrency, such as for resource sharing, eHealth services, IoTs, security, network slicing [25], [67]. Blockchain has been identified and considered as a key-enabler for 6G communication networks [9]. Blockchain, due to its inherent capabilities such as decentralization, auditability, immutability, traceability, and transparency, has been integrated with 5GNR and B5G networks by providing E2E services to the users. The potential use cases of blockchain in B5G and 6G networks are resource management, spectrum sharing, network slicing, authentication, tracking, record keeping, infrastructure sharing, and secure control of access [68]. Blockchain gives an additional advantage over traditional spectrum sharing by providing a secure and incentive-based sharing mechanism. The transactions are monitored and tracked, and a distributed ledger is maintained to ensure fairness in the system [69], [70], [71]. Furthermore, to deal with the challenges posed by a multitude of different applications with diverse performance, security, and mobility requirements, network slicing enables a division of the physical infrastructure into multiple virtual networks [72]. Blockchain-enabled network slicing ensures the security of network slice orchestration and provides secure admission control. These network slices provide a customized user experience with specific requirements [27].

1) WHAT IS BLOCKCHAIN?

Blockchain is a decentralized, unchangeable, distributed ledger that can record a transaction and keep track of the resources in a business network [73]. These transaction records are stored on time-stamped, unchangeable, digital blocks. These digital blocks of data are connected to form a chain, which is called blockchain. Blockchain is maintained by the network nodes. Each node has a copy of the blockchain, thus enabling tracking and maintaining a record of transactions [74].

In the following sub-section, we will discuss in detail the key elements of blockchain architecture, and its operating principle.

B. KEY ELEMENTS OF BLOCKCHAIN ARCHITECTURE

To fully understand how blockchain works, we need to review the key elements of its architecture, which are:

1) PEER-TO-PEER NETWORK

A Peer-to-Peer (P2P) network consists of a distributed network of connected computing devices. P2P devices do not have a central controlling node or a server where data is stored. Each node acts as a server and a client by sharing its data with other nodes in the P2P network. Each node stores its data in its storage and does not rely on a server for storing data. Each node in a P2P network possesses equal capabilities in terms of sharing, receiving, and transferring of data and thus is less prone to cyberattacks and single-point-of-failure [64], [75].

2) NODE

A node can be a computer system in a P2P network where all nodes are linked to each other in a distributed manner having equal capabilities. The main task of a node is to verify and process all the transactions [25].

3) HASH

A hash function calculates a fixed length cryptographic string called hash from any kind of data, which can either be a sentence or a whole file. Hash chains the digital blocks of data together and prevents tampering with the data. Even if a single transaction is tampered with, the resulting hash will change indicating that the data integrity is lost [74], [76].

4) TRANSACTIONS

This is the most basic element of blockchain. Blockchain technology's purpose is to be able to access and verify transactions which happened in the past. A transaction can be a payment record containing critical information about the sender and the receiver, the time stamp marking the completion of transaction [25]. A transaction is approved through a

method called consensus, and there are different algorithms to reach a consensus to approve and validate a transaction [77]. These consensus algorithms will be discussed later in detail.

5) MINERS

Adding a transaction to the block consumes substantial amount of computing power and resources. Miners are the network nodes/individuals who process blocks. The process of solving for the verification of a block is called mining [78], [79].

6) BLOCK

Blocks are the units that are linked together to form a blockchain. Each block has two main components, a block header and its data that comprises numerous transactions. Each block contains the following information:

- A block version number, containing the policies used for block validation.
- Timestamp, indicating the creation time of that particular block.
- nBits or target hash, the threshold target for a valid block hash.
- Nonce, is the abbreviation for ''number only used once''. The nonce is the number that the blockchain miners/nodes are trying to solve. Before any block is verified, a nonce is calculated, and the node which calculates the nonce first receives the reward. Miners go through several solutions to obtain the correct nonce, and this process is called Proof-of-Work (PoW).
- Merkle tree root hash, which is calculated from all the transactions in a particular block. If any transaction is modified, the Merkle tree root hash will get modified as well.
- Previous block hash field, which contains the hash of the previous already verified block, hence forming a chain which provides security and integrity.
- Current block hash, which is calculated from all the transactions present in the block as well as the hash of the previous block [25], [78], [79].

7) CONSENSUS ALGORITHM

Consensus algorithm or consensus protocol is a procedure that takes place when a new block is added to the blockchain. The addition of a new block requires a consensus from all the participating nodes in the P2P network to reach an agreement. Consensus in blockchain is majority-based, so when at least 51% of the network nodes agree to the verification and addition of a new block, the block is verified and then added to the blockchain. Various types of consensus algorithms are present which are implemented based on the specific type and performance requirements of a blockchain framework, such as PoW, Proof-of-Stake (PoS), Proof-of-Authority (PoA), Practical Byzantine Fault Tolerance (PBFT), LibraBFT, etc. PoW is the basis of Bitcoin cryptocurrency blockchain. PoW is highly decentralized and secure, but it is not scalable, as it requires a huge amount of computational power and storage capacity. Recently new algorithms such as PoS have been implemented which focus on reducing energy consumption and decreasing the computations required to add a new block to the chain [9], [27].

8) SMART CONTRACT

A smart contract is an executable computer code stored on blockchain, and it runs autonomously once some predefined conditions are satisfied. Nick Szabo created Smart Contracts in 1994 and they allows the participating nodes in a blockchain to make transactions without the control of a central entity. Smart contracts promote automated decentralization while also ensuring that the terms of the agreement, also known as SLAs, between trustless parties are met. When a smart contract is stored in blockchain, it ensures its authenticity and integrity [9], [27], [74], [80].

9) ORACLE

An oracle is a device or entity that provides services for connecting blockchain and real-world data. For the smart contract to execute based on some off-chain real-time data, oracle provides the required data inputs and outputs from the real-world to meet the specific conditions of a smart contract, and thus enable the smart contract to execute [74], [81].

C. BLOCKCHAIN WORKING PRINCIPLE

After defining the key elements that constitute a blockchain, we will discuss how to create a block and how these elements are chained together to form a blockchain. Fig. 4 depicts the working principle of blockchain [68]. A blockchain is a distributed database, shared among all the participating connected nodes forming a P2P network as shown in Fig. 4. Each node possesses the same copy of that database. Therefore, it is impossible to alter an added block since all the nodes can verify if any record is altered. The first block in the blockchain is called the Genesis block, and it does not contain the hash of the previous block. But for adding the next block to the chain, multiple nodes/miners compete against each other to find the nonce. The winner is selected through a consensus algorithm, such as PoW. The winner is rewarded with some predefined incentive, and the block is added to the blockchain. The new block contains the hash of the previous block; hence any kind of alteration can be detected and thus it makes it immutable. Fig. 4 shows that every new block that is created holds the hash of the previous block in its header. Furthermore, all the nodes are connected in a P2P network, thus each node stores a copy of the blockchain, which makes it immutable [82].

D. TYPES OF BLOCKCHAIN

There are different types of blockchains which are implemented based on their application. These are briefly discussed in this sub-section.

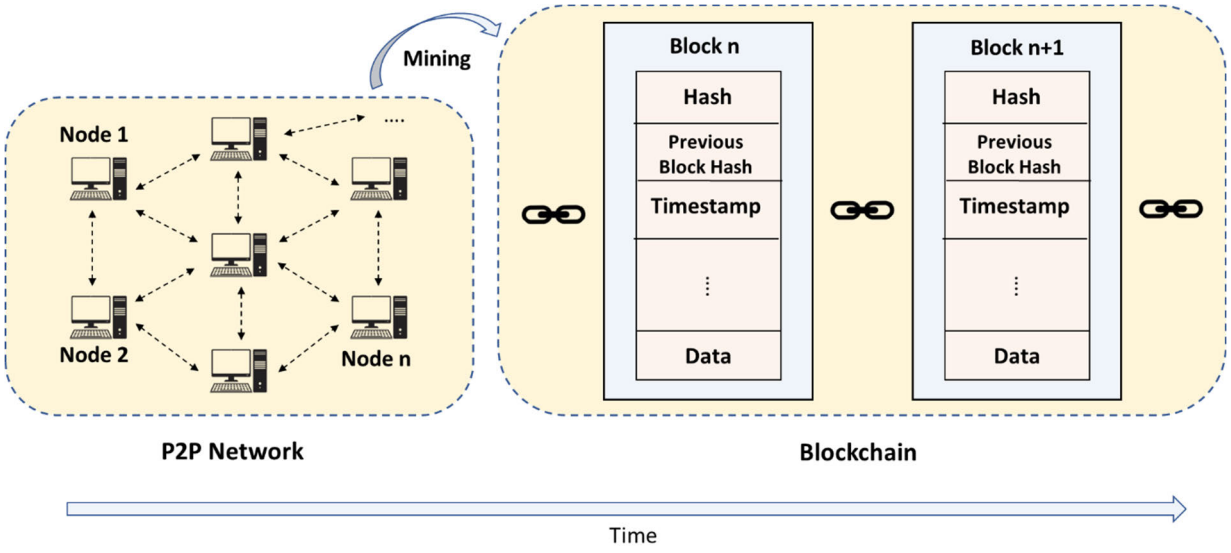


FIGURE 4. Blockchain working principle depicting the creation of chain of blocks.

1) PUBLIC BLOCKCHAIN

In a public blockchain or "permissionless" blockchain, anyone can join, view the ledger, and write to the blockchain. A public blockchain can be adopted for network slicing and spectrum sharing to service the users within the service domain of a single operator. It can also find its application in smart cities, smart energy, etc. to develop trust among connected communities [83].

2) PRIVATE BLOCKCHAIN

This is also called as "permissioned" blockchain, and it is managed by a "trusted" intermediary node, allowing only the invited nodes from a specific organization to join. Private blockchains can be implemented for services that are limited to a specific organization, with particular requirements and regulations, such as e-health services, etc. [84].

3) CONSORTIUM BLOCKCHAIN

This is also known as "federated" blockchain, and it is a combination of both public and private blockchains. Instead of a single organization, multiple organizations join this blockchain through permission and are governed by a single trusted node. The consortium blockchain is the solution when spectrum is shared among multiple operators, where each operator runs a public blockchain for its own users and a private blockchain is implemented among multiple operators for regulatory purposes and to build trust among the operators [64], [74], [85].

E. BLOCKCHAIN IMPLEMENTATION

The fundamental goal behind blockchain implementation is to attain three basic properties that are: scalability, decentralization, and security. However, attaining all these three properties in a single blockchain implementation is challenging, and this challenge in blockchain implementation is also termed "Vitalik's blockchain scalability trilemma" which is shown in Fig. 5 (Vitalik is the co-founder of Ethereum) [85], [86]. According to Vitalik, usually, only two out of these three properties can be achieved in a blockchain implementation, through simple methods [85]. In this sub-section, we will discuss the factors that impact blockchain implementation, followed by an overview of various open-source blockchain platforms that are available.

1) FACTORS AFFECTING BLOCKCHAIN IMPLEMENTATION

Applications which have their back-end code running on a decentralized network, are called Decentralized Applications (DApps) [87]. In recent years, multiple blockchain open-source platforms have been developed, which can be employed based on their specific applications requirements. Each blockchain has distinct characteristics, and based on those characteristics, we decide which implementation is best suited for our specific DApp. The factors that impact the decision while choosing which blockchain implementation is suitable for a specific application are discussed below, and they are depicted in Fig. 6:

1) ***Type of Blockchain:*** The first thing when choosing a specific blockchain is its type, such as a public, private, or consortium blockchain. Many applications require a permissionless blockchain, where any user/node can join and read/write on the blockchain. While some applications require a permissioned blockchain solution, such as for enterprise applications where only a few trusted users/nodes are allowed to join the blockchain. Many inter-company applications demand hybrid solutions, where a federated blockchain implementation is the most suitable, such as e-Health systems [88].

2) ***Scalability, Security, and Decentralization:*** The next factor that impacts the blockchain implementation is the attainment of these three capabilities. As discussed earlier, through simpler solutions, only two of these three capabilities are usually attainable. There are already available open-source blockchain platforms, but most of them lack at least one of these three attributes. Most public blockchain platforms are highly secure and decentralized, but they are not scalable, since storing and processing public Blockchains requires huge storage and computational resources. In a similar way, private blockchain platforms are scalable and secure, but they lack the decentralized aspect of the blockchain. In a private blockchain, there is a central controlling node which decides which nodes can stay and participate in the blockchain, thus it is compromised on decentralization. Some of these open-source platforms will be discussed in detail later in this section [89], [90].

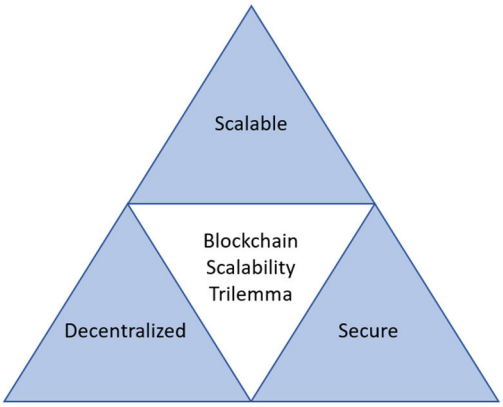


FIGURE 5. Vitalik's blockchain scalability trilemma [85].

3) ***Smart Contract Development Environment:*** Smart contracts are self-executable computer programs that employ blockchain to store the terms of the contracts. Once the predefined conditions in the smart contract are met, the program executes itself, thus removing the need for a third party or central control to enforce the terms [91]. Several blockchain open-source platforms are available, each with different characteristics, some are private, some are public, and many of these platforms support a smart contract development environment, but there are quite a few which do not support smart contracts. Thus, this becomes a crucial factor when deciding which blockchain implementation will be compatible with a specific DApp [92], [93].
4) ***Transactions per Second (TPS):*** Another key factor is the TPS rate of the blockchain platform. In this context, TPS means how many transactions is a blockchain platform able to process in one second. Many of the public and highly decentralized blockchain platforms have a lower TPS rate, which means that the time to process a single transaction is high. For time-sensitive DApps, such a platform with low TPS might not be suitable [94].
5) ***Transaction Cost:*** Transaction cost or transaction fees were introduced to speed up the transaction validation process. The transaction fee depends upon the size of the data block, as well as the time required to validate the transaction. Therefore, if a block's data size is large, and it needs to be validated in a shorter time, then the transaction fee will be higher. Transaction fees facilitate transaction processing, help to pay the miners, and reduce the number of spam transactions [95], [96]. The transaction fee in the Ethereum platform is calculated in terms of 'Gas.' Gas is the computing power required to complete a specific transaction. Each gas unit has a price that can be measured in gwei. For the case of Bitcoin, the pricing is calculated in terms of Satoshis. While deciding which blockchain platform would be suitable for a specific application, we need to analyze how many times the app will need to interact with the blockchain, and what will be the cost burden per transaction [27], [97].
6) ***Confirmation Time:*** The time between when a transaction is submitted to the blockchain network and the moment it is recorded on a validated block is called confirmation time. This is the time which a user will have to wait after submitting the transaction until a miner validates the transaction and adds it to the block. A user can expedite the confirmation time by paying a higher transaction fee [98].
7) ***Consensus Algorithm:*** The purpose of the consensus algorithm is to reach to an agreement regarding the addition of a new block in the blockchain, and which consensus algorithm is employed greatly impacts the performance of a blockchain platform. Different platforms deploy different consensus algorithms, such as PoW, PoS, Delegated Proof-of-Stake (DPoS), etc. and each consensus algorithm has varying computational and storage requirements, thus impacting the performance of a blockchain platform [99], [100].

2) OPEN-SOURCE BLOCKCHAIN PLATFORMS

There are various open-source blockchain platforms that are available and choosing which blockchain platform to use depends upon its characteristics. Traditional chains such as blockchain (Bitcoin) and Ethereum are highly decentralized and secure, but they are not scalable. There are also some high-TPS chains such as those which deploy DPoS. These are scalable and secure, but not decentralized. Multi-chain ecosystems are scalable and decentralized, but they are not secure [9], [27]. Here we will only discuss a few open-source blockchain platforms which support the smart contract development environment. The comparison of these platforms is depicted in Table 2, and these are discussed in detail below.

1) ***Ethereum:*** is a public blockchain, and it uses PoW as the consensus algorithm. Ethereum is the most

renowned blockchain platform for creating smart contracts, and it uses Solidity and Vyper scripting languages for the implementation of smart contracts. With the PoW consensus mechanism, Ethereum can support 15 TPS. The base transaction fee for Ethereum is 21,000 Gas units, and the confirmation time ranges between 12 to 14 seconds [101].

2) ***Hyperledger Fabric:*** is a private blockchain, and it utilizes the PBFT algorithm as a consensus mechanism. Hyperledger Fabric can support more than 3,500 TPS with a lower than one second confirmation time. It supports smart contract development with scripting languages Go and Java [102].
3) ***Polygon (Matic):*** Polygon or previously known as Matic, is a scalable version of Ethereum, which aims to increase the TPS exponentially with lower transaction costs. It is a public blockchain platform and it uses PoS as the consensus mechanism, thus enabling higher TPS of more than 7,200. Polygon supports smart contract development, and it uses the Solidity language for scripting the smart contracts [103].

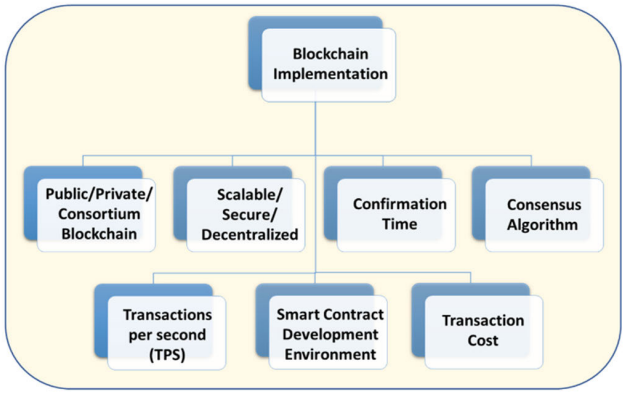


FIGURE 6. Factors affecting Blockchain implementation.

4) ***Algorand:*** is a public blockchain, which uses Pure PoS as a consensus mechanism. It supports smart contract implementation using the Java and Go languages. It has a very low transaction fee and supports more than 1,000 TPS with a confirmation time of less than 40 seconds [104], [105].
5) ***Energy Web Chain:*** is a hybrid blockchain platform. Anyone can join, but only selected few remain on the blockchain. It utilizes PoA as the consensus algorithm. With lower Gas fees as compared to Ethereum, it gives a high throughput of more than 76 TPS, with a confirmation time of less than 5 seconds. It supports smart contract deployment and utilizes Solidity as the scripting language for smart contracts [106], [107].

F. APPLICATIONS OF BLOCKCHAIN

Blockchain technology evolved from cryptocurrency and found its application in various key challenges posed by B5G and 6G networks. The following sub-section discusses various applications of blockchain in B5G and 6G networks.

1) SPECTRUM MANAGEMENT

The current spectrum sharing methods rely on a central entity for verifying all the spectrum access transactions, which may lead to biasness, single-point-of-failure, and privacy issues. There is still a lack of E2E dynamic spectrum management and sharing techniques. To create a more flexible and efficient spectrum sharing process, blockchain can be deployed to enhance the security, access fairness, and automate and incentivize the sharing mechanism [27], [81].

2) NETWORK SLICING

B5G and 6G enables multiple applications with varying QoS, mobility, and security requirements. The one-size-fits-all philosophy does not apply to these emerging applications, therefore new mechanisms are being proposed to cater for such diversified user requirements. Network slicing has been proposed as a prominent solution, which divides the physical network resources into multiple logical networks with varying QoS requirements. Blockchain can be deployed to create and manage the network slices in a decentralized and automated way, while safeguarding the privacy of the users. Network slicing aims towards a more efficient resource management and utilization, while minimizing the administration related costs and the delays caused by negotiations [9], [19], [27].

3) SECURE ACCESS CONTROL

With the massive increase in the number of connected devices, the security risks pertaining to access of the wireless communication systems have also increased. The traditional access mechanisms are based on centralized access control, which may create challenges such as single-point-of-failure. Blockchain can be employed to provide a secure access control mechanism for wireless networks, due to its decentralized nature and capabilities such as traceability and auditability [108], [109].

4) PRIVACY PROTECTION

The merging 6G applications involve sharing of sensitive user data such as identity information, location, and other confidential data. For gaining access to certain services like DSA and network slicing, sensitive data needs to be shared. Therefore, to preserve the security and privacy of the network users, blockchain can be employed to safeguard user sensitive information, and provide a secure access to services [27], [110].

V. BLOCKCHAIN-BASED DYNAMIC SPECTRUM ACCESS

DSA techniques mostly rely on a centralized control system for spectrum sensing, spectrum sharing, and spectrum management. The centralized control of access poses challenges such as, biasness and untrustworthiness of the network administrators, risk of exposure of sensitive user-related data, additional communication overhead between user and

TABLE 2. Comparison of open-source blockchain platforms that support smart contract development environment.

Characteristics	Ethereum	Hyperledger Fabric	Polygon (Matic)	Algorand	Energy Web Chain
Type of blockchain	Public	Private	Public	Public	Hybrid
Consensus algorithm	PoW	PBFT	PoS	PPoS	PoA
Smart contract	Yes	Yes	Yes	Yes	Yes
Transaction per Second (TPS)	> 15	> 3,500	> 7,200	> 1,000	> 76
Transaction cost	21,000 Gas	None	Low transaction fees	1,000 microAlgos	Lower Gas fees
Confirmation time	12-14 sec	< 1 sec	Not known	< 40 sec	< 5 sec
Contract scripting language	Solidity, Vyper	Go, Java	Solidity	Java, Go	Solidity

network operators, and interference management. Blockchain provides a potential solution to cater for these problems by providing a decentralized solution for DSA. Blockchain-based DSA solution can provide numerous benefits, such as automation of resource sharing process, incentivization and compensation mechanisms for network operators, fair resource trading, and unbiased access to spectrum resources. In this section, we will first provide review of the State-of-the-Art (SOTA) research in blockchain-based DSA, followed by the challenges and limitations of blockchain-based DSA techniques, and lastly the gaps in this research area with some future research directions.

A. REVIEW OF THE STATE-OF-THE-ART RESEARCH

In this subsection we present the SOTA research which has been done in the field of blockchain-based DSA. We outline the primary focus, the consensus algorithms used, DSA techniques and the results obtained, and the limitation and/or future direction of these works. The review has been summarized in Table 3.

A novel blockchain-based spectrum trading mechanism Spectrum Trading Blockchain (STBC) is proposed in [111]. STBC aims to enhance the efficiency, provide better security, increase simplicity of the trading process, and improve energy usage. As opposed to the Nakamoto consensus algorithm, STBC is based on a new consensus algorithm with prompt transaction confirmation and a better fault-tolerance. STBC also safeguards against the Distributed Denial of Service (DDoS) attack and protects the identity of the nodes through temporarily anonymous transactions. Moreover, STBC considerably reduces the power consumption, improves the spectrum utilization by 30%, and reduces the transaction confirmation delay by 12.5 times. STBC is majorly focused on consensus of transaction information of spectrum, and it lacks the auction and management of spectrum. Furthermore, the security considerations of the proposed mechanism are limited.

In [112], for dynamic and opportunistic access to the CBRS band, a blockchain-based secure SAS framework called TrustSAS is proposed. TrustSAS aims to safeguard the privacy of secondary access users lying under the category of PAL and GAA users by providing anonymous access to SAS. The major drawback of this work is the communication and computational overhead incurred by the blockchain operations.

The authors in [113], propose a blockchain-enabled interference-based consensus algorithm for spectrum sharing. This mechanism aims to reduce the system overhead and improve the efficiency of transactions. The node which suffers the most combined interference in the last transaction will obtain as a compensation, the accounting rights for the next block to be added to the blockchain. When this new block is verified by the participating nodes, it will be added to the blockchain, and the node with accounting rights will be rewarded with spectrum coins. These spectrum coins can then be traded with other nodes for the use of spectrum. An interference-based transaction validation mechanism is devised to circumvent the interference caused by spectrum traders, by validating the stored spectrum transactions in the block. The proposed solution not only reduces the system overhead, but also improves the system fairness and the Signal to Interference and Noise Ratio (SINR) of the nodes. In order to test the proposed blockchain-based architecture, various mechanisms are required to be developed, such as block generation, pricing, and incentive mechanisms.

A blockchain-enabled multi-operator spectrum sharing mechanism is proposed in [114], with intra and inter spectrum sharing management. Blockchain-based smart contracts are employed for serving a primary user of one operator through spectrum resources of secondary operators. Extensive simulations show that the blockchain-based spectrum management system is not only scalable but provides ample security as well. In [114], the trust on operators and security of the regional telecommunications network is still an open issue.

A blockchain and AI based Dynamic Resource Sharing (DRS) mechanism is proposed in [115], for 6G and beyond networks. The authors in [115], present a two-layer hierarchical solution for overcoming the challenges of storage and computation for blockchain-based DRS strategies. Blockchain is employed to obtain DRS functionalities, while AI aims to enhance the performance of pattern recognition and decision making, as well as improve the profit margins of the users. The future direction includes the setting of criteria for choosing the type for blockchain such as private or public

for different scenarios. And the formulation of a consensus algorithm with reduced computational complexity and cost.

In [116], a new distributed blockchain-based dynamic access model for CBRS band sharing is proposed, which aims to reduce the high administrative costs and privacy concerns. For spectrum allocation, a new consensus algorithm named Proof-of-Strategy is devised, as well as a privacy protection method based on ring signature techniques. These mechanisms protect the spectrum access system from single-point-of-failure, protection of legal users from malicious users, and enhance the spectrum utilization. The future direction of this work is to predict the usage behavior of incumbent users, thus enabling PAL users to continually utilize the spectrum.

The authors in [117], propose a blockchain and smart contracts based dynamic spectrum access management of unlicensed spectrum for transmission of non-real-time data in Cyber-Physical-Social Systems (CPSS). Users gain access to spectrum licenses through PoW mining, and they can also sell/lease the spectrum access license through an auction when they no longer need to utilize the spectrum. Just like digital currency in blockchain, such as bitcoin (BTC) or ether coin (ETH), a new virtual currency called Xcoin is introduced for spectrum trading which is used in the auction process as an incentive for spectrum sharing. Xcoin may refer to spectrum, or paid edge computing services, or digital currency etc. They also outline some future extensions of their work, such as development of blockchain-based spectrum auction mechanisms, blockchain-based cooperative transmission and cloud-fog-edge computing schemes, and other consensus algorithms to replace resource-hungry PoW algorithm.

The authors in [118], envision blockchain-enabled services for 6G networks such as spectrum sharing and resource management, computing and energy trading, network slice management, and hardware virtualization. Blockchain will enable the sharing of resources between devices, such as data, spectrum lease, energy, and computing power. They also present some motivations for the use of blockchain in future use-cases, such as IoT, network slicing, Device-to-Device (D2D) communication, and network virtualization. Due to its application as a trusted database, blockchain has opened new opportunities for DSM. Blockchain helps to reduce the DSM related administrative costs, and it also improves the traditional spectrum management techniques such as spectrum auction. We can securely record sensitive information such as spectrum sensing, spectrum auction results and leasing mappings, data mining outcomes, and information about idle spectrum on the blockchain. The future direction of this work is the creating a lightweight blockchain solution while considering the privacy and security concerns of a wireless communication system.

The authors in [119], propose a blockchain-enabled spectrum sharing mechanism for 5G heterogeneous networks. Primary User (PU) agree to share its spectrum with the Secondary User (SU) in return for some incentives. Matching theory is employed to match the PU spectrum with the SU. PU and SU detail their spectrum preferences in their respective preference lists and utilize the Gale-Shapley algorithm to get matched. In [119], there are certain limitations, such as multi-operator spectrum sharing is not considered, as well as a PU can receive varying contracts from multiple base stations with overlapped coverage.

A cooperation-based contract needs to be devised in such scenarios.

The authors in [120], propose another blockchain-based spectrum sharing mechanism. They implement auction and spectrum sensing based sharing techniques for opportunistic use by the secondary user. Blockchain is deployed to ensure that spectrum use is validated, tracked, and compensated. Proof-of-Concept (PoC) is implemented in Ethereum for the purpose of demonstrating the usefulness of the proposed scheme. The drawback of this scheme is the increased latency introduced by blockchain mining, but this can be deployed for those cases of spectrum sharing where the spectrum share is for longer durations, such as CBRS, IEEE 802.22 WRAN, and Small-Cell as a Service.

In this subsection, we reviewed the SOTA research in blockchain-based DSA, along with the limitations of these works. In the following subsection, we will discuss the challenges faced by the blockchain-based DSA and few future directions.

B. IMPLEMENTATION CHALLENGES AND TRADE-OFFS

In this subsection, we will discuss the challenges of implementing blockchain for DSA and the trade-offs that must be made, considering the B5G and 6G network requirements. 6G networks are envisioned to support peak data rate of 1 Tbps, latency of 25 μs to 1 ms, and a connection density of 10 million devices/km^2 [8]. Keeping in view these network requirements, we will discuss the various challenges and the trade-offs that need to be made for blockchain-based solutions.

1) SUITABILITY

Considering the performance requirements of B5G and 6G networks, the foremost challenge is to categorize the areas where blockchain will be suitable as a solution. Blockchain provides certain benefits like decentralization of network management system, auditability and accountability of network resources, but these advantages come at a cost of higher implementation expenses. For a multi-operator resource sharing scenario, where different operators are willing to share their resources, a decentralized resource sharing scheme outweighs the cost and system overhead incurred by the blockchain. Due to the stringent QoS requirements of users in 6G networks, the implications of blockchain on the service delivery must be considered before it is employed as a solution for resource sharing and management. However, with proper incentive mechanisms, the performance of blockchain can be optimized for its applicability in 6G networks.

TABLE 3. Summary of related work with their main contributions.

Reference	Primary Focus	Consensus Algorithm	DSA Technique and Results	Limitations and/or Future Directions
Xue et al. [111] [2021]	Dynamic Spectrum Sharing and Management, Distributed Consensus Algorithm	Spectrum Trading Blockchain (STBC) Consensus Protocol	• Novel blockchain-based spectrum trading mechanism STBC • Consumes less power, enhances security and scalability of spectrum sharing • Improves spectrum utilization by 30%, reduces transaction confirmation delay by 12.5 times over the SOTA blockchain-based spectrum sharing solution	*Limitation:* STBC algorithm does not consider the consensus of spectrum auction and management. Furthermore, it requires better security considerations.
Grissa et al. [112] [2021]	CBRS, Privacy Safeguarding, Spectrum Access System	Byzantine Fault Tolerant (BFT)	• Blockchain-based secure SAS for secondary access users (SAUs) in CBRS band called TrustSAS • Protects the privacy of SAUs through the provision of anonymous access to SAS	*Limitation:* Communication and computational overhead incurred by the blockchain operation.
Liang et al. [113] [2021]	Dynamic Spectrum Management, Transaction Validation	Interference-based Consensus Mechanism	• Blockchain-enabled interference-based spectrum sharing method as well as transaction validation mechanism • Improves system overhead, fairness of operation, and SINR of nodes	*Future direction:* To test the proposed blockchain-based architecture, various mechanisms are required to be developed, such as block generation, pricing, and incentive mechanisms.
Gorla et al. [114] [2021]	Multi-Operator Spectrum Sharing, Smart Contracts	Proof of Authority (PoA)	• Blockchain-enabled Smart Contracts for multi-operator spectrum sharing • Licensed user of one operator is served through spectrum resources of secondary operators • Blockchain-based DSM methods are scalable as well as secure	*Limitation:* Trust on operators and security of regional telecommunications network.
Hu et al. [115] [2021]	Artificial Intelligence, Dynamic Resource Sharing	Proof of Work (PoW) or Proof-of-Stake (PoS)	• Two-layer hierarchical blockchain and AI based Dynamic Resource Sharing (DRS) mechanism • Blockchain is employed to obtain DRS functionalities • AI enhances the performance of pattern recognition and decision making	*Future direction:* Design of a computationally less complex consensus algorithm, and blockchain type selection criteria.
Zhang et al. [116] [2020]	CBRS, Consensus Algorithm, Spectrum Management	Proof-of-Strategy (PoS)	• Novel blockchain-based consensus algorithm called Proof-of-Strategy for dynamic access to the CBRS band • Reduces the administrative cost of DSM, prevents single-point-of-failure, and provides consensus mechanism	*Future direction:* Predict the usage behavior of incumbent users, thus enabling PAL users to continually utilize the spectrum.
Fan et al. [117] [2020]	Smart Contracts, DSA of unlicensed spectrum	Proof of Work (PoW)	• Blockchain-based smart contracts for DSA management of unlicensed spectrum • PoW based consensus algorithm for spectrum sharing in return for incentives in the form of spectrum, edge computing services, or digital currency	*Future direction:* Development of blockchain-based spectrum auction mechanisms, cooperative transmission, and cloud-fog-edge computing schemes. Design of consensus algorithm to replace resource hungry PoW.
Xu et al. [118] [2020]	6G, Spectrum Management, Network Slicing, Wireless Blockchain	Comparison of Multiple Consensus Algorithms	• Blockchain-enabled services for 6G networks are envisioned • For instance, spectrum sharing and resource management, computing and energy trading, network slice management, and hardware virtualization	*Future direction:* Creating a lightweight blockchain solution while considering the privacy and security concerns of a wireless communication system.
Zhou et al. [119] [2020]	Spectrum Sharing, Heterogeneous Networks, Matching Theory	Proof of Work (PoW)	• Blockchain-enabled spectrum sharing mechanism for 5G heterogeneous networks • Primary users share their spectrum with secondary users in return for some incentives	*Limitation:* Multi-operator spectrum sharing is not considered, as well as cooperation-based contract needs to be devised.
Ariyarathna et al. [120] [2019]	Smart Contracts, Spectrum Sharing, Cognitive radio	Proof of Concept (PoC)	• Blockchain-based spectrum sharing mechanism • Auction and spectrum sensing based sharing techniques for opportunistic access by SU • Blockchain ensures that spectrum use is validated, tracked, and compensated	*Limitation:* Increased latency introduced by blockchain mining.

2) STORAGE OVERHEAD VS. LEVEL OF CENTRALIZATION

For blockchain-based DSA solutions, a highly decentralized public blockchain is a better solution, but that increases the storage overhead of the network, since all the participating nodes in blockchain have access to the same copy of blockchain and it is saved on each node. For a public blockchain, as the number of nodes increases, the storage overhead also increases exponentially. While for a private or consortium blockchain implementation, the storage overhead is lower, but we lose the degree of decentralization. Thus, there exists a trade-off between the level of decentralization and the storage overhead, which poses an implementation challenge for 6G networks [115].

3) LATENCY REQUIREMENTS VS. SCALABILITY

B5G and 6G use-cases like URLLC and MURLLC demand a latency of less than 1 ms. Due to high spectrum demand in 6G networks, the resource requests will be more frequent, which will induce a high transaction confirmation delay in blockchain-based DSA. For a highly decentralized blockchain solution, the transaction confirmation time also increases as the number of transactions increases, which makes it less scalable. Public blockchain with reduced scalability poses an implementation challenge for blockchain-based DSA solutions in 6G networks with stringent delay requirements [115].

4) COMPUTATION COMPLEXITY VS. SECURITY

Computation complexity of a blockchain consensus algorithm is an essential implementation challenge for blockchain-based DSA solutions. For future 6G networks, to enhance resource utilization, more users will be involved in the resource sharing process. With high number of nodes involved in the consensus process, the computation complexity of consensus algorithms elevates, but this brings more security in the network. Therefore, we have a trade-off between computational complexity and the level of security for a particular 6G application [121].

5) ENERGY CONSUMPTION

A public blockchain consumes a massive amount of energy. Even private or consortium blockchains consume more energy than a traditional centralized management system. In 6G networks, DSA system will need to accommodate a large number of users, therefore the energy consumption will pose a great challenge and will affect the Operational Expenditures (OPEX) of the network operators [122].

C. GAPS AND FUTURE DIRECTIONS

There is immense potential for blockchain implementation for the evolving B5G and 6G applications. Firstly, a computationally less complex consensus algorithm needs to be developed, which can reduce the transaction confirmation delay and hence improve the system latency. This will improve the TPS rate and make the blockchain solution more scalable for 6G applications. Secondly, to reduce the system overheads, the researchers are focusing on creating *off-chain* and *on-chain* blockchains. This will help reduce the storage overhead as well as the computation complexity. Most of the transactions will be stored on the *off-chain* part of the blockchain, while only the final transaction will be mined on the *on-chain* part of blockchain. The second most popular concept for reducing the blockchain overheads is *Sharding*. Where the transactions are divided among different branches and are only validated by the nodes associated with that branch [115]. Since DSA needs a public blockchain platform, so that maximum number of users can participate in the resource sharing process, therefore, it is required to create lightweight blockchain solutions. Furthermore, combining Machine Learning (ML) as well as AI with blockchain can further assist in optimizing blockchain solutions for B5G and 6G network applications and services [102]. With ML and AI, user request and usage can be predicted, which can help in better management of resources, thus improving the performance of blockchain [103].

VI. BLOCKCHAIN-ENABLED NETWORK SLICING

Network slicing techniques face certain challenges as outlined in Section III-F. Blockchain with its inherent capabilities, can be a potential solution to cater for these challenges. Blockchain can enable secure network slice orchestration process, safeguarding of user-sensitive data such as identity and geo-locations, secure access to network resources, slice isolation, and ensuring SLAs. In this section, we first present the SOTA research in blockchain-enabled network slicing, followed by the challenges and limitations posed by these techniques, and lastly the gaps and future research directions in blockchain-enabled network slicing.

A. REVIEW OF THE STATE-OF-THE-ART RESEARCH

This subsection presents a review of SOTA research which has been carried out in the domain of blockchain-enabled network slicing. We outline the network slicing parameter which has been optimized, the consensus algorithm used, the presented network slicing technique and the obtained results. The review is summarized in Table 4.

An experimental testbed for blockchain-enabled state-based allocation of network slice to User Equipment (UE) has been implemented in [123]. This allocation is based on the UE's state and the user's QoS demand. Blockchain-enabled network slice allocation achieves transparency, security, fairness, and makes the slice allocation process cost-efficient. A smart contract is implemented for achieving these goals. Furthermore, the blockchain-enabled state-based network slice allocation mechanism enhances the network resource handling as well as improves the security and transparency of the system.

A secure E2E network slice creation mechanism called NetChain is proposed in [124], which is based on blockchain and the Trusted Execution Environment (TEE). NetChain aims to eradicate the challenges and risks which arise from

the disclosure of sensitive information, from single point-of-failure, and having no guarantee of providing the agreed upon QoS to the users. Furthermore, to complement the privacy and scalability of NetChain, the authors have developed a novel protocol for consensus called CoNet. In order to prevent any malicious activities and guarantee QoS and fairness during the multi-domain slice creation process, a game theoretic based bilateral evaluation method is devised. The viability of the proposed scheme is evaluated on Microsoft Azure Cloud, and the results show that NetChain and CoNet provide better security during slice orchestration than current blockchain-based solutions.

A blockchain-based information management system for network slice creation is proposed in [125]. The goal is to allow the users to securely access and manage the services, while also allowing the network and service providers to monitor the transactions. Blockchain provides a distributed ledger, which maintains the security, privacy, and integrity of delicate information.

The authors in [126], propose a novel blockchain-based architecture for the implementation of network slicing and NFV. Blockchain-based distributed ledger provides secure direct interaction between any end user with any virtualized network instance of any Mobile Network Operator (MNO), which enhances the flexibility of network deployment. By means of AI-predicted traffic demand of each network slice and through the potential of blockchain, network slicing performance in terms of overall throughput of the physical network infrastructure is improved by almost two times during peak traffic load.

A blockchain-based network slicing brokerage solution called NSBchain is proposed in [127], to cater for the needs of new network tenants such as automotive industry, e-health, smart factories etc. NSBchain comprises of Intermediate Brokers (IBs) who acquire network resources from Infrastructure Providers (InPs) through the implementation of smart contracts. IBs then reallocate these resources among the network tenants who are willing to pay for gaining access to the network slices and computational resources. NSBchain is proposed as a secure and cost effective solution, which is scalable and automated. By making use of the open-source Hyperledger platform and through a PoC implementation, the viability of the proposed solution is verified.

A blockchain-based distributed network slicing framework is proposed in [128], which enables the dynamic leasing of resources to the service tenants by the resource providers to enhance the performance and QoS provision. The prominent aspect of this framework is the Global Service Positioning (GSP) system, which allows the new users to make a service request and control their admission through a blockchain-based auction type bidding system for dynamic resource allocation. The main purpose of this work is to improve the performance of users having varying service requirements, and to minimize the monetary burden of operation and service provision of the network provider.

A blockchain-based brokerage mechanism is devised for network slice provision in 5G [129]. The network slice provider will lease the network resources from multiple providers while maintaining the security and anonymity of the transactions, to create E2E network slices. PoC based implementation is used to observe the performance of a blockchain-based network slice broker. The results demonstrate that the enhanced security provided by blockchain does not impact the performance of the network slice broker.

The authors in [130], propose a blockchain-based mechanism to ensure that network slice orchestration is secure, to identify any malicious and failed VNFs, and to prevent the degradation of QoS of valid network users. Each slice has different requirements, which initiates the need for the use of various blockchains each with different characteristics. Various blockchain characteristics come into play here, such as the number of participating nodes, throughput and type of transaction, different consensus algorithms, and kinds of networks involved, etc. Through PoC implementation, the viability of blockchain-based network slice creation is studied, where the security of slice orchestration and network virtualization is assessed.

In [131], a blockchain-based slice leasing mechanism is proposed for network slice creation for factory equipment. It allows the equipment for mechanical operations to dynamically and autonomously request and acquire the needed resources for efficient slice creation. Blockchain provides the trust and accountability for sharing of resources among resource providers. In [131], authors have presented a use case scenario for the blockchain-enabled network slice brokerage. In order to fully automate the factory operations, they have automated the slice request and creation process for the mechanical equipment based on their resource requirements through the use of blockchain.

In this subsection, we reviewed the SOTA research in blockchain-enabled network slicing. In the following subsection, we will discuss the challenges faced by the blockchain-enabled network slicing and some future directions.

B. IMPLEMENTATION CHALLENGES AND TRADE-OFFS

In this subsection, we will discuss the challenges of implementing blockchain for a network slicing system with stringent QoS requirements in B5G and 6G networks.

1) COMPUTATION COMPLEXITY OF CONSENSUS ALGORITHM

In B5G and 6G networks, for multi-operator resource sharing, a consortium or private blockchain is the appropriate solution. When only few permitted stakeholders are allowed in the blockchain network, the computation complexity of consensus algorithm will be lower. But if the nodes involved in network slice orchestration process increase, the need for a public blockchain might arise, which can lead to the challenge of higher computation complexity of the consensus algorithm for time-sensitive 6G applications [123], [132].

TABLE 4. Summary of related work with their main contributions.

Reference	Network Slicing Parameter	Consensus Algorithm	Network Slicing Technique and Results
Gorla et al. [123] [2021]	Number of Users Connected, Bandwidth Usage, Total Bandwidth Usage	Proof-of-Authority (PoA)	• Experimental testbed for blockchain-enabled state-based allocation of network slice to User Equipment (UE) • This allocation is based on the UE's state and the user's QoS demand • Blockchain-enabled network slice allocation achieves transparency, security, fairness, and also makes the slice allocation process cost-efficient
He et al. [124] [2021]	Security of slice orchestration process	Novel consensus protocol CoNet	• Blockchain and Trusted Execution Environment (TEE) based secure E2E network slice creation mechanism called NetChain • Prevent disclosure of sensitive information, malicious activities during slice creation, and single point-of-failure • Ensure provision of agreed upon QoS/QoE to the users
Gebraselase et al. [125] [2021]	Secure access to services	Unspecified	• Blockchain-based information management system for network slice creation • Allowing the users to securely access and manage the services • Blockchain helps maintain the privacy and integrity of the delicate information
Maksymyuk et al. [126] [2020]	Overall Throughput	Delegated Proof-of-Stake (DPoS)	• Blockchain-based NS and NFV enhances flexibility of network deployment • Through AI-prediction of network slice traffic demand and blockchain implementation, overall throughput of physical infrastructure almost doubles
Zanzi et al. [127] [2020]	Slice Request Throughput	Proof-of-Concept (PoC), Byzantine Fault Tolerant (BFT)	• NSBchain – a network slicing brokerage solution is proposed • IBs acquire network resources from InPs through smart contracts • IBs reallocate these resources to the users who are willing to pay to get access to the network slices and computational resources • NSBchain is secure, cost-effective, scalable, and automated solution
Togou et al. [128] [2020]	Improve user's performance, reduce operational cost of provider	Multiple consensus algorithms	• Blockchain-based distributed network slicing framework • Enables dynamic leasing of resources to the service tenants by the resource providers • Enhance the performance and QoS provision • Blockchain-based auction type bidding system for dynamic resource allocation
Nour et al. [129] [2019]	Security and Anonymity	Proof-of-Concept (PoC), Hashcash PoW	• Blockchain-based brokerage system for the creation of E2E network slices • This mechanism enhances the security and anonymity of the transactions
Rebello et al. [130] [2019]	Security of network slice orchestration and virtualization	Proof-of-Concept, Hyperledger Fabric	• Blockchain-based mechanism to ensure the security of network slice orchestration • To identify any malicious and failed virtual network functions (VNF) • To prevent the degradation of QoS of valid network users
Backman et al. [131] [2017]	Automation of network slice orchestration process	Unspecified	• Blockchain-based network slice brokerage mechanism • Use case scenario: factory of the future • Equipment can dynamically and autonomously request and acquire network slices as per the requirements

2) ENERGY CONSUMPTION

The energy consumption will be comparatively less for a network slice broker with fewer nodes running on the blockchain. But if the number of nodes in the network slice management system increases, the OPEX will increase significantly, which poses a challenge. But these expenses outweighs the benefits received by blockchain-enabled network slicing system for the network operators in 6G networks. Since it enables the secure access to network resources and proper incentivization when resources are shared among multiple operators [29].

3) SCALABILITY AND STORAGE OVERHEAD

The future 6G networks will depend on high spectrum availability for users with high mobility. The scalability does not pose a bigger concern when it comes to network slicing until the number of operators are limited. But even if the blockchain nodes are lower, when the blockchain starts

recording transactions, the storage overhead starts increasing exponentially, which poses a challenge for service providers in 6G networks [29], [132].

C. GAPS AND FUTURE DIRECTIONS

Blockchain-enabled network slicing is of paramount importance in realizing the future wireless networks. There are still many areas which need to be investigated in this domain. Since the future networks depend upon even lower latency in service provision, blockchain-based network slicing can be combined with edge computing to bring the service provision closer to the end users. Furthermore, blockchain-enabled network slicing and machine learning can be combined to learn the user usage patterns, so that the resources can be managed more efficiently [123], [132].

VII. CONCLUSION AND FUTURE DIRECTIONS

A. CONCLUSION

DSA and network slicing are the key-enabling technologies for the realization of envisioned B5G and 6G applications. In this article, we have provided a comprehensive overview of DSA and network slicing, as well as the challenges posed by their existing schemes. We have provided an extensive overview of blockchain, its architecture, and smart contracts, in a manner that gives the reader a complete yet precise tutorial of blockchain. We have reviewed the state-of-the-art in blockchain-enabled DSA and network slicing, their implementation challenges related to B5G and 6G network requirements, and some future research directions. Considering the stringent QoS requirements of B5G and 6G networks, blockchain can be viewed as a promising solution for ensuring the SLAs where multiple entities participate in the resource sharing process.

B. FUTURE RESEARCH DIRECTIONS

The research on blockchain integration with DSA and network slicing is still in its initial stages, and there are many challenges which are yet to be investigated. Trust between operators is still an open issue while sharing the resources among multiple operators. Slice-isolation and secure network slice orchestration is a challenge faced by current network slicing techniques. Preserving the privacy of user sensitive data such as identity and geo-location is a challenge faced by both DSA and network slicing. Blockchain pose a great storage overhead as well as high energy consumption. Ways to reduce the system overheads in blockchain-based solutions and making it more energy efficient is of prime importance. A use-case scenario for blockchain-based DSA and network slicing is to integrate DSA and network slicing together, so that the focus is to primarily use the underutilized spectrum resources while creating the user-specific network slices. This way, we not only enhance spectrum utilization, but also satisfy users with stringent QoS requirements. Blockchain will provide the functionality of ensuring SLAs of users and fair incentivization for the network operators. Nonetheless, the transaction confirmation time in blockchain-based solutions pose a challenge for time-sensitive applications like URLLC and MURLLC, as well as the highly mobile users in B5G and 6G networks.

TABLE 5. Technical abbreviations.

Acronym	Definition
3CLS	Communications, Computing, Control, Localization, and Sensing
4G	4th Generation
5G	5th Generation
5GNR	5th Generation New Radio
6G	6th Generation
AI	Artificial Intelligence
AN	Access Network
API	Application Programming Interfaces
AR	Augmented Reality
B5G	Beyond 5th Generation
BCI	Brain-Computer Interactions
CBRS	Citizens Broadband Radio Service
CN	Core Network
CPSS	Cyber Physical Social Systems
CRs	Cognitive Radios
CRAS	Connected Robotics and Autonomous Systems
D2D	Device-to-Device
DApps	Decentralized Applications
DDoS	Distributed Denial of Service
DLT	Distributed Ledger Technology
DPoS	Delegated Proof-of-Stake
DQN	Deep-Q-Network
DRL	Deep Reinforcement Learning
DRS	Dynamic Resource Sharing
DSA	Dynamic Spectrum Access
DSS	Dynamic Spectrum Sharing
E2E	End-to-End
eMBB	enhanced Mobile Broadband
GAA	General Authorized Access
HCS	Human-Centric Services
IA	Incumbent Access
IBs	Intermediate Brokers
IBFD	In-Band Full-Duplex
InPs	Infrastructure Providers
IoE	Internet-of-Everything
IoT	Internet-of-Things
LSA	Licensed Shared Access
LSTM	Long Short-Term Memory
LTE	Long-Term Evolution
MBN	Mobile Broadband Network
MBRLLC	Mobile Broadband Reliable Low Latency Communication
MMTC	massive Machine Type Communication
MNO	Mobile Network Operator
MPS	Multi-Purpose Services
MURLLC	Massive URLLC
NFs	Network Functions
NFV	Network Function Virtualization
NGWN	Next Generation Wireless Networks
NSP	Network Service Provider
P2P	Peer-to-Peer
PAL	Priority Access License
PBFT	Practical Byzantine Fault Tolerance
PoA	Proof-of-Authority
PoC	Proof-of-Concept
PoS	Proof-of-Stake
PoW	Proof-of-Work
PU	Primary User
QoPE	Quality-of-Physical-Experience
QoS	Quality-of-Service
RAN	Radio Access Network
SAS	Spectrum Access System
SDN	Software Defined Networking
SINR	Signal to Interference and Noise Ratio
SLA	Service Level Agreements
SU	Secondary User
TEE	Trusted Execution Environment
TN	Transport Network
TPS	Transactions Per Second
TVWS	TV White Spaces
UE	User Equipment
URLLC	Ultra-Reliable and Low Latency Communication
VNF	Virtual Network Functions
VR	Virtual Reality
XR	Extended Reality

APPENDIX

In the appendix, we tabulate the technical abbreviations used in the paper and their corresponding definitions in Table 5.

ACKNOWLEDGMENT

This work was supported by the European Union through the Horizon 2020 Marie Skłodowska-Curie Innovative Training Networks Program "Mobility and Training for Beyond 5G Ecosystems (MOTOR5G)" under Grant 861219.

REFERENCES

[1] Cisco. *Cisco Annual Internet Report (2018–2023) White Paper*. Accessed: Mar. 3, 2022. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[2] *IMT Traffic Estimates for the Years 2020 to 2030*. ITU-R. Accessed: Mar. 3, 2022. [Online]. Available: https://www.itu.int/dms-pub/itu-r/opb/rep/R-REP-M.2370-2015-PDF-E.pdf

[3] P. Vamvakas, E. E. Tsiropoulou, and S. Papavassiliou, "Dynamic spectrum management in 5G wireless networks: A real-life modeling approach," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2019, pp. 2134–2142.

[4] *Identification and Quantification of Key Socio-Economic Data to Support Strategic Planning for the Introduction of 5G in Europe*, European Commission, Brussels, Belgium, 2016.

[5] Y. C. Liang, *Dynamic Spectrum Management: From Cognitive Radio to Blockchain and Artificial Intelligence*. Berlin, Germany: Nature, 2020.

[6] V. A. Memos, K. E. Psannis, and Z. Lv, "A secure network model against bot attacks in edge-enabled industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 18, no. 11, pp. 7998–8006, Nov. 2022.

[7] B. Wang and K. J. R. Liu, "Advances in cognitive radio networks: A survey," *IEEE J. Sel. Topics Signal Process.*, vol. 5, no. 1, pp. 5–23, Feb. 2011.

[8] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, "6G wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 28–41, Sep. 2019.

[9] M. Tahir, M. H. Habaebi, M. Dabbagh, A. Mughees, A. Ahad, and K. I. Ahmed, "A review on application of blockchain in 5G and beyond networks: Taxonomy, field-trials, challenges and opportunities," *IEEE Access*, vol. 8, pp. 115876–115904, 2020.

[10] S. Biswas, A. Bishnu, F. A. Khan, and T. Ratnarajah, "In-band full-duplex dynamic spectrum sharing in beyond 5G networks," *IEEE Commun. Mag.*, vol. 59, no. 7, pp. 54–60, Jul. 2021.

[11] M. Hassan, M. Singh, and K. Hamid, "Survey on NOMA and spectrum sharing techniques in 5G," in *Proc. IEEE Int. Conf. Smart Inf. Syst. Technol. (SIST)*, Apr. 2021, pp. 1–4.

[12] A. Ahmed, Z. Elsaraf, F. A. Khan, and Q. Z. Ahmed, "Cooperative non-orthogonal multiple access for beyond 5G networks," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 990–999, 2021.

[13] M. K. Luka, O. U. Okereke, E. E. Omizegba, and E. C. Anene, "Blockchains for spectrum management in wireless networks: A survey," 2021, *arXiv:2107.01005*.

[14] S. Iyer, A. Patil, S. Bhairanatti, S. Halagatti, and R. J. Pandya, "A survey on technological trends to enhance spectrum efficiency in 6G communications," 2022, *arXiv:2202.11493*.

[15] K. Husenovic, I. Bedi, S. Maddens, I. Bozsoki, D. Daryabwite, N. Sundberg, and M. Maniewicz, "Setting the scene for 5G: Opportunities & challenges," ITU, Geneva, Switzerland, Tech. Rep., 56, 2019.

[16] *View on 5G Architecture: Version 2.0*, 5GPPP Architecture Working Group, 5GPPP Association, Brussels, Belgium, 2017.

[17] L. U. Khan, I. Yaqoob, N. H. Tran, Z. Han, and C. S. Hong, "Network slicing: Recent advances, taxonomy, requirements, and open research challenges," *IEEE Access*, vol. 8, pp. 36009–36028, 2020.

[18] *E2E Network Slicing Architecture*, document NG.127, GSMA, Jun. 2021.

[19] Z. S. Bojkovic and B. M. Bakmaz, "Blockchain-enabled network slicing," in *Proc. 15th Int. Conf. Adv. Technol., Syst. Services Telecommun. (TELSIKS)*, Oct. 2021, pp. 203–208.

[20] C. D. Alwis, A. Kalla, Q.-V. Pham, P. Kumar, K. Dev, W.-J. Hwang, and M. Liyanage, "Survey on 6G frontiers: Trends, applications, requirements, technologies and future research," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 836–886, 2021.

[21] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May 2019.

[22] V. A. Memos and K. E. Psannis, "NFV-based scheme for effective protection against bot attacks in AI-enabled IoT," *IEEE Internet Things Mag.*, vol. 5, no. 1, pp. 91–95, Mar. 2022.

[23] C. L. Stergiou, K. E. Psannis, and B. B. Gupta, "IoT-based big data secure management in the fog over a 6G wireless network," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5164–5171, Apr. 2021.

[24] Y. Gupta, A. Shrivastava, K. Kunal, and N. Sadashiv, "Survey paper on blockchain based cloud computing applications," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jan. 2021, pp. 1–6.

[25] V. Sharma and L. K. Awasthi, "Divergent applications of blockchain security: A survey," in *Proc. 2nd Int. Conf. Secure Cyber Comput. Commun. (ICSCCC)*, May 2021, pp. 212–217.

[26] M. Chahbar, G. Diaz, A. Dandoush, C. Cerin, and K. Ghoumid, "A comprehensive survey on the E2E 5G network slicing model," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 1, pp. 49–62, Mar. 2021.

[27] K. Yue, Y. Zhang, Y. Chen, Y. Li, L. Zhao, C. Rong, and L. Chen, "A survey of decentralizing applications via blockchain: The 5G and beyond perspective," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2191–2217, 4th Quart., 2021.

[28] S. Khan, M. B. Amin, A. T. Azar, and S. Aslam, "Towards interoperable blockchains: A survey on the role of smart contracts in blockchain interoperability," *IEEE Access*, vol. 9, pp. 116672–116691, 2021.

[29] F. Javed, K. Antevski, J. Mangues-Bafalluy, L. Giupponi, and C. J. Bernardos, "Distributed ledger technologies for network slicing: A survey," *IEEE Access*, vol. 10, pp. 19412–19442, 2022.

[30] C. B. Papadias, T. Ratnarajah, and D. T. M. Slock, *Spectrum Sharing: The Next Frontier in Wireless Networks*. Hoboken, NJ, USA: Wiley, 2020.

[31] K. C. Chen and R. Prasad, *Cognitive Radio Networks*. Hoboken, NJ, USA: Wiley, 2009.

[32] M. B. H. Weiss, K. Werbach, D. C. Sicker, and C. E. C. Bastidas, "On the application of blockchains to spectrum management," *IEEE Trans. Cogn. Commun. Netw.*, vol. 5, no. 2, pp. 193–205, Jun. 2019.

[33] M. Hafeez and J. M. H. Elmirghani, "Analysis of dynamic spectrum leasing for coded bi-directional communication," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1500–1512, Sep. 2012.

[34] M. Hafeez and J. M. H. Elmirghani, "Dynamic spectrum leasing for bi-directional communication: Impact of selfishness," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2427–2437, Jun. 2016.

[35] M. Hafeez and J. M. H. Elmirghani, "Dynamic spectrum leasing for beamforming cognitive radio networks using network coding," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2013, pp. 2840–2845.

[36] M. Hafeez and J. M. H. Elmirghani, "Green licensed-shared access," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 12, pp. 2579–2595, Dec. 2015.

[37] C. Qu, C. Fan, Y. Wang, M. Liu, and Y. Zhang, "A game theory based approach for distributed dynamic spectrum access," *Evol. Intell.*, vol. 2022, pp. 1–8, Apr. 2022.

[38] O. Naparstek and K. Cohen, "Deep multi-user reinforcement learning for distributed dynamic spectrum access," *IEEE Trans. Wireless Commun.*, vol. 18, no. 1, pp. 310–323, Nov. 2019.

[39] F. Benedetto, L. Mastroeni, and G. Quaresima, "Auction-based theory for dynamic spectrum access: A review," in *Proc. 44th Int. Conf. Telecommun. Signal Process. (TSP)*, Jul. 2021, pp. 146–151.

[40] R. H. Tehrani, S. Vahid, D. Triantafyllopoulou, H. Lee, and K. Moessner, "Licensed spectrum sharing schemes for mobile operators: A survey and outlook," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2591–2623, 4th Quart., 2016.

[41] Y. Xiao, S. Shi, W. Lou, C. Wang, X. Li, N. Zhang, Y. T. Hou, and J. H. Reed, "Decentralized spectrum access system: Vision, challenges, and a blockchain solution," *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 220–228, Feb. 2022.

[42] J. Ye, X. Kang, Y.-C. Liang, and S. Sun, "A trust-centric privacy-preserving blockchain for dynamic spectrum management in IoT networks," *IEEE Internet Things J.*, vol. 9, no. 15, pp. 13263–13278, Aug. 2022.

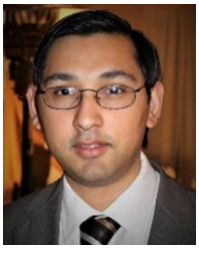
[43] K. David and H. Berndt, "6G vision and requirements: Is there any need for beyond 5G?" *IEEE Veh. Technol. Mag.*, vol. 13, no. 3, pp. 72–80, Sep. 2018.
[44] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," *Comput. Netw.*, vol. 167, Feb. 2020, Art. no. 106984.
[45] Ericcson. *Network Slicing Made Easy*. Accessed: Mar. 1, 2022. [Online]. Available: https://www.ericsson.com/en/network-slicing?
[46] S. Wijethilaka and M. Liyanage, "Survey on network slicing for Internet of Things realization in 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 957–994, 2nd Quart., 2021.
[47] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2429–2453, 3rd Quart., 2018.
[48] ETSI. *Network Functions Virtualisation (NFV); Architectural Framework*. Accessed: Mar. 1, 2022. [Online]. Available: https://www.etsi.org/deliver/etsi-gs/nfv/001-099/002/01.02.01-60/gs-nfv002v010201p.pdf
[49] D. Kreutz, F. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proc. IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2015.
[50] I. Afolabi, A. Ksentini, M. Bagaa, T. Taleb, M. Corici, and A. Nakao, "Towards 5G network slicing over multiple-domains," *IEICE Trans. Commun.*, vol. 100, no. 11, pp. 1992–2006, 2017.
[51] X. Li, M. Samaka, H. A. Chan, D. Bhamare, L. Gupta, C. Guo, and R. Jain, "Network slicing for 5G: Challenges and opportunities," *IEEE Internet Comput.*, vol. 21, no. 5, pp. 20–27, Sep. 2017.
[52] P. Caballero, A. Banchs, G. De Veciana, and X. Costa-Perez, "Network slicing games: Enabling customization in multi-tenant mobile networks," *IEEE/ACM Trans. Netw.*, vol. 27, no. 2, pp. 662–675, Apr. 2019.
[53] Q. Li, G. Wu, A. Papathanassiou, and U. Mukherjee, "An end-to-end network slicing framework for 5G wireless communication systems," 2016, *arXiv:1608.00572*.
[54] M. A. Habibi, B. Han, and H. D. Schotten, "Network slicing in 5G mobile communication architecture, profit modeling, and challenges," 2017, *arXiv:1707.00852*.
[55] *Description of Network Slicing Concept*, Northern Alliance, Taloqan, Afghanistan, 2016.
[56] G. Sun, K. Xiong, G. O. Boateng, D. Ayepah-Mensah, G. Liu, and W. Jiang, "Autonomous resource provisioning and resource customization for mixed traffics in virtualized radio access network," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2454–2465, Sep. 2019.
[57] G. O. Boateng, D. Ayepah-Mensah, D. M. Doe, A. Mohammed, G. Sun, and G. Liu, "Blockchain-enabled resource trading and deep reinforcement learning-based autonomous RAN slicing in 5G," *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 1, pp. 216–227, Mar. 2022.
[58] G. Sun, G. O. Boateng, D. Ayepah-Mensah, G. Liu, and J. Wei, "Autonomous resource slicing for virtualized vehicular networks with D2D communications based on deep reinforcement learning," *IEEE Syst. J.*, vol. 14, no. 4, pp. 4694–4705, Dec. 2020.
[59] X. Shen, J. Gao, W. Wu, K. Lyu, M. Li, W. Zhuang, X. Li, and J. Rao, "AI-assisted network-slicing based next-generation wireless networks," *IEEE Open J. Veh. Technol.*, vol. 1, pp. 45–66, 2020.
[60] Y. Chi, Y. Zhang, Y. Liu, H. Zhu, Z. Zheng, R. Liu, and P. Zhang, "Deep reinforcement learning based edge computing network aided resource allocation algorithm for smart grid," *IEEE Access*, vol. 11, pp. 6541–6550, 2023.
[61] J. Huang, F. Yang, C. Chakraborty, Z. Guo, H. Zhang, L. Zhen, and K. Yu, "Opportunistic capacity based resource allocation for 6G wireless systems with network slicing," *Future Gener. Comput. Syst.*, vol. 140, pp. 390–401, Mar. 2023.
[62] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Feb. 16, 2022. [Online]. Available: https://blockchair.com/bitcoin/whitepaper/bitcoin.pdf
[63] M. D. Pierro, "What is the blockchain?" *Comput. Sci. Eng.*, vol. 19, no. 5, pp. 92–95, 2017.
[64] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari, and Y. Cao, "A survey on blockchain technology: Evolution, architecture and security," *IEEE Access*, vol. 9, pp. 61048–61073, 2021.
[65] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," in *Proc. Conf. Theory Appl. Cryptogr.* Cham, Switzerland: Springer, 1990, pp. 437–455.
[66] V. Gupta. *A Brief History of Blockchain*. Accessed: Feb. 17, 2022. [Online]. Available: https://hbr.org/2017/02/a-brief-history-of-blockchain
[67] M. H. Miraz and M. Ali, "Applications of blockchain technology beyond cryptocurrency," 2018, *arXiv:1801.03528*.
[68] J. Wang, X. Ling, Y. Le, Y. Huang, and X. You, "Blockchain-enabled wireless communications: A new paradigm towards 6G," *Nat. Sci. Rev.*, vol. 8, no. 9, Sep. 2021, Art. no. nwab069.
[69] W. Y. B. Lim, J. S. Ng, Z. Xiong, D. Niyato, C. Leung, C. Miao, and Q. Yang, "Incentive mechanism design for resource sharing in collaborative edge learning," 2020, *arXiv:2006.00511*.
[70] T. Maksymyuk, J. Gazda, M. Volosin, G. Bugar, D. Horvath, M. Klymash, and M. Dohler, "Blockchain-empowered framework for decentralized network management in 6G," *IEEE Commun. Mag.*, vol. 58, no. 9, pp. 86–92, Sep. 2020.
[71] J. Gao, L. Zhao, and X. Shen, "Network utility maximization based on an incentive mechanism for truthful reporting of local information," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7523–7537, Aug. 2018.
[72] S. Zhang, "An overview of network slicing for 5G," *IEEE Wireless Commun.*, vol. 26, no. 3, pp. 111–117, Jun. 2019.
[73] IBM. *What is Blockchain Technology?*. Accessed: Feb. 17, 2022. [Online]. Available: https://www.ibm.com/uk-en/topics/what-is-blockchain
[74] V. Gatteschi. (Jun. 2019). *Foundation and Basics of Blockchain and Smart Contracts*. Ireland Blockchain Group. [Online]. Available: https://www.ieee-ukandireland.org/future-directions/blockchain
[75] W. Vermaak. *What Are Peer-to-Peer (P2P) Networks?*. Accessed: Feb. 17, 2022. [Online]. Available: https://coinmarketcap.com/alexandria/article/what-is-peer-to-peer-p2p
[76] Bitpanda. *What is a Hash Function in a Blockchain Transaction?*. Accessed: Feb. 17, 2022. [Online]. Available: https://www.bitpanda.com/academy/en/lessons/what-is-a-hash-function-in-a-blockchain-transaction/
[77] D. Hamilton. *What is a Blockchain Transaction Anyway?*. Accessed: Feb. 17, 2022. [Online]. Available: https://coincentral.com/what-is-a-blockchain-transaction-anyway/
[78] D. Cosset. *Blockchain: What is in a Block?*. Accessed: Feb. 18, 2022. [Online]. Available: https://dev.to/damcosset/blockchain-what-is-in-a-block-48jo
[79] J. Frankenfield. *Nonce*. Accessed: Apr. 12, 2022. [Online]. Available: https://www.investopedia.com/terms/n/nonce.asp
[80] IBM. *What Are Smart Contracts on Blockchain?*. Accessed: Feb. 17, 2022. [Online]. Available: https://www.ibm.com/topics/smart-contracts
[81] Chainlink. *What is a Blockchain Oracle?*. Accessed: Feb. 17, 2022. [Online]. Available: https://chain.link/education/blockchain-oracles
[82] L. Madaan, A. Kumar, and B. Bhushan, "Working principle, application areas and challenges for blockchain technology," in *Proc. IEEE 9th Int. Conf. Commun. Syst. Netw. Technol. (CSNT)*, Apr. 2020, pp. 254–259.
[83] M. Niranjanamurthy, B. N. Nithya, and S. Jagannatha, "Analysis of blockchain technology: Pros, cons and SWOT," *Cluster Comput.*, vol. 22, no. S6, pp. 14743–14757, Nov. 2019.
[84] M. Liu, K. Wu, and J. J. Xu, "How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain," *Current Issues Auditing*, vol. 13, no. 2, pp. A19–A29, Sep. 2019.
[85] N. Afraz. (Jul. 2021). *Scaling Blockchain for Telecom Networks: An Impossible Trinity*. Ireland Blockchain Group. [Online]. Available: https://www.ieee-ukandireland.org/future-directions/blockchain
[86] V. Buterin. *Why Sharding is Great: Demystifying the Technical Properties*. Accessed: Feb. 20, 2022. [Online]. Available: https://vitalik.ca/general/2021/04/07/sharding.html
[87] Ethereum. *Introduction to DApps*. Accessed: Feb. 22, 2022. [Online]. Available: https://ethereum.org/en/developers/docs/dapps/
[88] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *J. Med. Syst.*, vol. 42, no. 140, pp. 1–18, 2018.
[89] G. D. Monte, D. Pennino, and M. Pizzonia, "Scaling blockchains without giving up decentralization and security," in *Proc. 3rd Workshop Cryptocurrencies Blockchains Distrib. Syst.*, Sep. 2020, pp. 71–76.
[90] P. Febrero and J. Pereira, "Cryptocurrency constellations across the three-dimensional space: Governance decentralization, security, and scalability," *IEEE Trans. Eng. Manag.*, vol. 69, no. 6, pp. 3127–3138, Dec. 2022.

[91] A. Makarov. *Top 6 Smart Contract Platforms: A Deep Dive*. Accessed: Feb. 21, 2022. [Online]. Available: https://www.itransition.com/blog/smart-contract-platforms
[92] P. Das, L. Eckey, T. Frassetto, D. Gens, K. Hostáková, P. Jauernig, S. Faust, and A.-R. Sadeghi, "FastKitten: Practical smart contracts on Bitcoin," in *Proc. USENIX Secur. Symp.*, 2019, pp. 801–818.
[93] Polkadot. *Smart Contracts*. Accessed: Feb. 21, 2022. [Online]. Available: https://wiki.polkadot.network/docs/build-smart-contracts
[94] Binance Academy. *Transactions Per Second (TPS)*. Accessed: Feb. 22, 2022. [Online]. Available: https://academy.binance.com/en/glossary/transactions-per-second-tps
[95] Bybit Learn. *Blockchain Transaction Fees: Why Do They Matter?*. Accessed: Feb. 22, 2022. [Online]. Available: https://learn.bybit.com/blockchain/blockchain-transaction-fees-explained/
[96] Wirex. *What is the Blockchain Fee?*. Accessed: Feb. 22, 2022. [Online]. Available: https://wirexapp.com/help/article/what-is-the-blockchain-fee-0078
[97] Binance Academy. *What are Blockchain Transaction Fees?*. Accessed: Feb. 22, 2022. [Online]. Available: https://academy.binance.com/en/articles/what-are-blockchain-transaction-fees
[98] Binance Academy. *Confirmation Time*. Accessed: Feb. 22, 2022. [Online]. Available: https://academy.binance.com/en/glossary/confirmation-time
[99] W. Gu, J. Li, and Z. Tang, "A survey on consensus mechanisms for blockchain technology," in *Proc. Int. Conf. Artif. Intell., Big Data Algorithms (CAIBDA)*, May 2021, pp. 46–49.
[100] GeeksforGeeks. *Consensus Algorithms in Blockchain*. Accessed: Feb. 22, 2022. [Online]. Available: https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/
[101] Ethereum. *Ethereum Development Documentation*. Accessed: Feb. 22, 2022. [Online]. Available: https://ethereum.org/en/developers/docs/
[102] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, and D. Enyeart, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, 2018, pp. 1–15.
[103] Polygon. *The Polygon Blog*. Accessed: Feb. 23, 2022. [Online]. Available: https://blog.polygon.technology/category/ecosystem/infrastructure/
[104] Algorand Developer Portal. *Algorand Developer Docs*. Accessed: Feb. 23, 2022. [Online]. Available: https://developer.algorand.org/docs/
[105] J. Chen and S. Micali, "Algorand," 2016, *arXiv:1607.01341*.
[106] S. Hartnett, C. Henly, E. Hesse, T. Hildebrandt, C. Jentzch, K. Krämer, G. MacDonald, J. Morris, H. Touati, and A. Trbovich, "The energy web chain-accelerating the energy transition with an open-source, decentralized blockchain platform," Energy Web Found., Berlin, Germany, Tech. Rep., Oct. 2018.
[107] "EW-DOS: The energy web decentralized operating system," Energy Web Found., Berlin, Germany, Tech. Rep., Jun. 2020.
[108] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1594–1605, Apr. 2019.
[109] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019.
[110] C. Benzaid and T. Taleb, "AI for beyond 5G networks: A cyber-security defense or offense enabler?" *IEEE Netw.*, vol. 34, no. 6, pp. 140–147, Nov. 2020.
[111] L. Xue, W. Yang, W. Chen, and L. Huang, "STBC: A novel blockchain-based spectrum trading solution," *IEEE Trans. Cognit. Commun. Netw.*, vol. 8, no. 1, pp. 13–30, Mar. 2022.
[112] M. Grissa, A. A. Yavuz, B. Hamdaoui, and C. Tirupathi, "Anonymous dynamic spectrum access and sharing mechanisms for the CBRS band," *IEEE Access*, vol. 9, pp. 33860–33879, 2021.
[113] Y. Liang, C. Lu, Y. Zhao, and C. Sun, "Interference-based consensus and transaction validation mechanisms for blockchain-based spectrum management," *IEEE Access*, vol. 9, pp. 90757–90766, 2021.
[114] P. Gorla, V. Chamola, V. Hassija, and N. Ansari, "Blockchain based framework for modeling and evaluating 5G spectrum sharing," *IEEE Netw.*, vol. 35, no. 2, pp. 229–235, Mar. 2021.
[115] S. Hu, Y.-C. Liang, Z. Xiong, and D. Niyato, "Blockchain and artificial intelligence for dynamic resource sharing in 6G and beyond," *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 145–151, Aug. 2021.
[116] H. Zhang, S. Leng, and H. Chai, "A blockchain enhanced dynamic spectrum sharing model based on proof-of-strategy," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6.
[117] X. Fan and Y. Huo, "Blockchain based dynamic spectrum access of non-real-time data in cyber-physical-social systems," *IEEE Access*, vol. 8, pp. 64486–64498, 2020.
[118] H. Xu, P. V. Klaine, O. Onireti, B. Cao, M. Imran, and L. Zhang, "Blockchain-enabled resource management and sharing for 6G communications," *Digit. Commun. Netw.*, vol. 6, no. 3, pp. 261–269, Aug. 2020.
[119] Z. Zhou, X. Chen, Y. Zhang, and S. Mumtaz, "Blockchain-empowered secure spectrum sharing for 5G heterogeneous networks," *IEEE Netw.*, vol. 34, no. 1, pp. 24–31, Jan./Feb. 2020.
[120] T. Ariyarathna, P. Harankahadeniya, S. Isthikar, N. Pathirana, H. M. N. D. Bandara, and A. Madanayake, "Dynamic spectrum access via smart contracts on blockchain," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–6.
[121] G. Bansal, A. Dua, G. S. Aujla, M. Singh, and N. Kumar, "SmartChain: A smart and scalable blockchain consortium for smart grid systems," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2019, pp. 1–6.
[122] J. Sedlmeir, H. U. Buhl, G. Fridgen, and R. Keller, "The energy consumption of blockchain technology: Beyond myth," *Bus. Inf. Syst. Eng.*, vol. 62, no. 6, pp. 599–608, Jun. 2020.
[123] P. Gorla, V. Chamola, V. Hassija, and D. Niyato, "Network slicing for 5G with UE state based allocation and blockchain approach," *IEEE Netw.*, vol. 35, no. 3, pp. 184–190, May 2021.
[124] G. He, W. Su, S. Gao, N. Liu, and S. K. Das, "NetChain: A blockchain-enabled privacy-preserving multi-domain network slice orchestration architecture," *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 1, pp. 188–202, Mar. 2022.
[125] B. G. Gebraselase, "Blockchain-based information management for network slicing," in *Proc. Int. Conf. Comput. Intell. Knowl. Economy (ICCIKE)*, Mar. 2021, pp. 555–559.
[126] T. Maksymyuk, V. Andrushchak, S. Dumych, B. Shubyn, B. Gabriel, and J. Gazda, "Blockchain-based network functions virtualization for 5G network slicing," *Acta Electrotechnica Inf.*, vol. 20, no. 4, pp. 54–59, 2020.
[127] L. Zanzi, A. Albanese, V. Sciancalepore, and X. Costa-Perez, "NSBchain: A secure blockchain framework for network slicing brokerage," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–7.
[128] M. A. Togou, T. Bi, K. Dev, K. McDonnell, A. Milenovic, H. Tewari, and G.-M. Muntean, "DBNS: A distributed blockchain-enabled network slicing framework for 5G networks," *IEEE Commun. Mag.*, vol. 58, no. 11, pp. 90–96, Nov. 2020.
[129] B. Nour, A. Ksentini, N. Herbaut, P. A. Frangoudis, and H. Moungla, "A blockchain-based network slice broker for 5G services," *IEEE Netw. Lett.*, vol. 1, no. 3, pp. 99–102, Sep. 2019.
[130] G. A. F. Rebello, G. F. Camilo, L. G. C. Silva, L. C. B. Guimaraes, L. A. C. de Souza, I. D. Alvarenga, and O. C. M. B. Duarte, "Providing a sliced, secure, and isolated software infrastructure of virtual functions through blockchain technology," in *Proc. IEEE 20th Int. Conf. High Perform. Switching Routing (HPSR)*, May 2019, pp. 1–6.
[131] J. Backman, S. Yrjola, K. Valtanen, and O. Mammela, "Blockchain network slice broker in 5G: Slice leasing in factory of the future use case," in *Proc. Internet Things Bus. Models, Users, Netw.*, Nov. 2017, pp. 1–8.
[132] G. O. Boateng, G. Sun, D. A. Mensah, D. M. Doe, R. Ou, and G. Liu, "Consortium blockchain-based spectrum trading for network slicing in 5G RAN: A multi-agent deep reinforcement learning approach," *IEEE Trans. Mobile Comput.*, early access, Jul. 19, 2022, doi: 10.1109/TMC.2022.3190449.

SIDRA TUL MUNTAHA (Graduate Student Member, IEEE) received the B.Sc. degree (Hons.) in electrical engineering from the National University of Computer and Emerging Sciences (NUCES-FAST), Islamabad, Pakistan, in 2015, and the M.Sc. degree (Hons.) in electrical engineering from the National University of Sciences and Technology (NUST), Islamabad, in 2019. She is currently pursuing the Ph.D. degree in electrical engineering with the University of Huddersfield (UoH), U.K. She worked as a Research Assistant with the Lahore University of Management Sciences (LUMS), Lahore, Pakistan, from December 2020 to June 2021. Her current research interests include 6G wireless communication, network slicing, software-defined networking, and blockchain. She was a recipient of MSCA ITN H2020 Grant at UoH.

PAVLOS I. LAZARIDIS (Senior Member, IEEE) received the Diploma degree in electrical engineering from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 1990, the M.Sc. degree in electronics from Université Pierre and Marie Curie (Paris 6), Paris, France, in 1992, and the joint Ph.D. degree from the École Nationale Supérieure des Télécommunications (ENST) Paris and Université Paris 6, in 1996. From 1991 to 1996, he was involved in research with France Télécom and teaching with ENST Paris. In 1997, he became the Head of the Antennas and Propagation Laboratory, Télédiffusion de France/the France Télécom Research Center (TDF—C2R Metz). From 1998 to 2002, he was a Senior Examiner with the European Patent Office (EPO), The Hague, The Netherlands. From 2002 to 2014, he was involved in teaching and research with the ATEI of Thessaloniki, Thessaloniki, and Brunel University, London, U.K. He is currently a Professor in electronics and telecommunications with the University of Huddersfield, U.K. He has been involved in several international research projects, such as EU Horizon 2020 MOTOR5G and RECOMBINE and NATO-SfP ORCA. He has published over 150 research articles and several national and European patents. He is a member of IET (MIET), a Senior Member of URSI, and a fellow of the Higher Education Academy (FHEA). He is serving as an Associate Editor for IEEE Access.

MARYAM HAFEEZ (Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Leeds, U.K., in 2015. From 2015 to 2018, she was a Research Fellow with the Institute of Robotics, Autonomous Systems and Sensing (IRASS), University of Leeds, U.K. Since 2018, she has been a Senior Lecturer with the Department of Engineering and Technology, University of Huddersfield. Her current research is funded by the EU Horizon 2020 Programme. Her research interests include the design and analysis of protocols for next generation green intelligent wireless networks by employing tools from game theory and stochastic geometry along with the Internet of Things (IoT) and industry 4.0 related research. She has worked in the area of dynamic spectrum access had received the Best Paper Award at the IEEE International Conference on Communications (ICC), in 2013. She is also serving as a member of the Editorial Board for *Frontiers in Communications and Networks* journal.



QASIM Z. AHMED (Member, IEEE) received the Ph.D. degree from the University of Southampton, Southampton, U.K., in 2009. He worked as an Assistant Professor with the National University of Computer and Emerging Sciences (NUCES-FAST), Islamabad, Pakistan, from November 2009 to June 2011. He has been a Postdoctoral Fellow with the Computer, Electrical and Mathematical Sciences and Engineering Division, King Abdullah University of Science and Technology, Thuwal, Saudi Arabia, from June 2011 to June 2014. He joined the University of Kent, U.K., as a Lecturer, from January 2015 to January 2017. He was a Lecturer, then a Senior Lecturer, in 2017, 2018. He is currently a Reader with the University of Huddersfield since 2020. His research interests include mainly ultrawide bandwidth systems, millimeter waves, device to device, digital health, and cooperative communications. He is currently a Principal Investigator, U.K. for Erasmus + DigiHealth-Asia Project, and the MSCA Staff Exchanges EVOLVE Project. He is also a Co-Investigator of EU H2020 ETN Research MOTOR5G Project and EU H2020 RISE Research RECOMBINE Project. He is a fellow of HEA.

FAHEEM A. KHAN (Member, IEEE) received the bachelor's degree in electronics engineering from Aligarh Muslim University, India, the master's degree in communication and radar engineering from the Indian Institute of Technology, Delhi, India, and the Ph.D. degree in electrical and electronic engineering from Queen's University Belfast, in 2012. He is currently a Senior Lecturer in electronic engineering with the School of Computing and Engineering, University of Huddersfield. He has more than 15 years of teaching and research experience at academic and research institutions in the U.K., Sultanate of Oman, United Arab Emirates, and India. Prior to joining as a Lecturer with the University of Huddersfield, in 2016, he worked as a Research Associate in wireless communications and signal processing with the Institute for Digital Communications, University of Edinburgh, where he contributed to research and project management in several EU/EPSRC research projects. His current research interests include spectrum sharing/spectrum management for beyond 5G wireless networks, licensed shared access and cognitive radio, non-orthogonal multiple access, machine learning and deep learning in wireless communications, full-duplex communications, MIMO and millimeter wave communications, and the Internet of Things (IoT) networks. His research is currently funded by the following research grants: Proof of Commercial Concept (PoCC) research grant on "Non-orthogonal multiple access techniques in beyond 5G networks," EU H2020 ETN Research Project MOTOR5G, and EU H2020 RISE Research Project. He is a fellow of HEA.

ZAHARIAS D. ZAHARIS (Senior Member, IEEE) received the B.Sc. degree in physics, the M.Sc. degree in electronics, the Ph.D. degree in antennas and propagation modeling for mobile communications, and the Diploma degree in electrical and computer engineering from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 1987, 1994, 2000, and 2011, respectively. From 2002 to 2013, he was with the Administration of the Telecommunications Network, Aristotle University of Thessaloniki, where he has been with the School of Electrical and Computer Engineering, since 2013. He has been involved in several international research projects, such as EU Horizon 2020 MOTOR5G and RECOMBINE. He is the author of 78 scientific journal articles, 62 international conference papers, one national patent, five book chapters, and one textbook. His current research interests include design and optimization of antennas and microwave circuits, signal processing on smart antennas, development of evolutionary optimization algorithms, and neural networks. He is a member of the Technical Chamber of Greece. Recently, he was the elected Chair of the Electron Devices/Microwave Theory and Techniques/Antennas and Propagation Joint Chapter of the IEEE Greece Section. He is currently serving as an Associate Editor for IEEE Access.