Received 5 January 2024; revised 14 February 2024; accepted 1 March 2024. Date of publication 14 March 2024; date of current version 1 April 2024.

Digital Object Identifier 10.1109/OJCOMS.2024.3376233

A Survey on Blockchain for Dynamic Spectrum Sharing

LAVAN PERERA (Student Member, IEEE), PASIKA RANAWEERA (Member, IEEE), SACHITHA KUSALADHARMA (Member, IEEE), SHEN WANG (Senior Member, IEEE), AND MADHUSANKA LIYANAGE (Senior Member, IEEE)

School of Computer Science, University College Dublin, Dublin 4, D04 V1W8 Ireland

CORRESPONDING AUTHORS: L. PERERA AND M. LIYANAGE (e-mail: lavan.perera@UCDconnect.ie; madhusanka@ucd.ie)

This work was supported in part by the European Union in the CONFIDENTIAL-6G Project under Grant 101096435.

ABSTRACT The rapid increase in mobile users, the IoT, and data-hungry applications have brought forth unprecedented demand on the spectrum, which is scarce; on top of that, the existing static spectrum allocation schemes have resulted in a heavily underutilized spectrum which can be mitigated with a Dynamic Spectrum Access (DSA) scheme with unlicensed users gaining access to the idle spectrum bands of licensed spectrum users opportunistically. Such a DSA and Dynamic Spectrum Management (DSM) scheme would significantly increase spectral efficiency while facilitating new services and applications beyond 5G (B5G) networks. Even with access to new spectrum bands like terahertz (THz) and Visible light communication and enabling technologies such as Software Defined Networks (SDN) and Cognitive Radio (CR), implementing a fully realized DSM requires rapid sensing, coordination, and management, and sharing of idle spectrum bands in a fair manner while preserving the security and privacy aspects, limiting interferences. With their decentralized, immutable nature, blockchains promise the execution of spectrum access and sharing in a fully transparent, fair manner while preserving privacy and security. Furthermore, blockchain-based Smart Contracts (SCs) allow automation of DSM, cryptocurrencies, and tokens to facilitate the trading of spectrum and related resources. In addition to that, blockchains act as an interface for integrating AI and Machine Learning (ML) techniques into DSM, which provides a certain level of intelligence to the underlying architecture. Although several attempts have been carried out to analyze the research gaps in DSM, a comprehensive analysis addressing the blockchains as the primary solution to address DSM has not been carried out. In this survey, we address the potential of a blockchain-based approach toward realizing a decentralized DSM while presenting future directives to improve the use of blockchains for DSM.

INDEX TERMS 6G, Blockchain, Dynamic Spectrum Management, privacy, security, and Internet of Things

I. INTRODUCTION

THE EVOLUTION of mobile generations has driven an escalating demand for spectrum resources. In the 1G era, analog communication with voice-centric support operated within a 40MHz bandwidth, despite limitations. Transitioning to 2G, the adoption of digital modulation in Global System for Mobile Communication (GSM), using Time Division Multiple Access (TDMA), allowed multiplexing up to 8 calls per channel in the 900 and 1800 MHz bands, with spectrum resources proving more than sufficient. The shift to 2.5G, represented by General Packet Radio Service (GPRS), saw increased data rates to 384 Kbps and the introduction of Internet access, marking a shift to data-driven services.

Moving to 3G, a 2Mbps data rate and Internet access supported multimedia applications, fostering exponential mobile user growth. However, portions of the spectrum remained underutilized, prompting the need for co-sharing

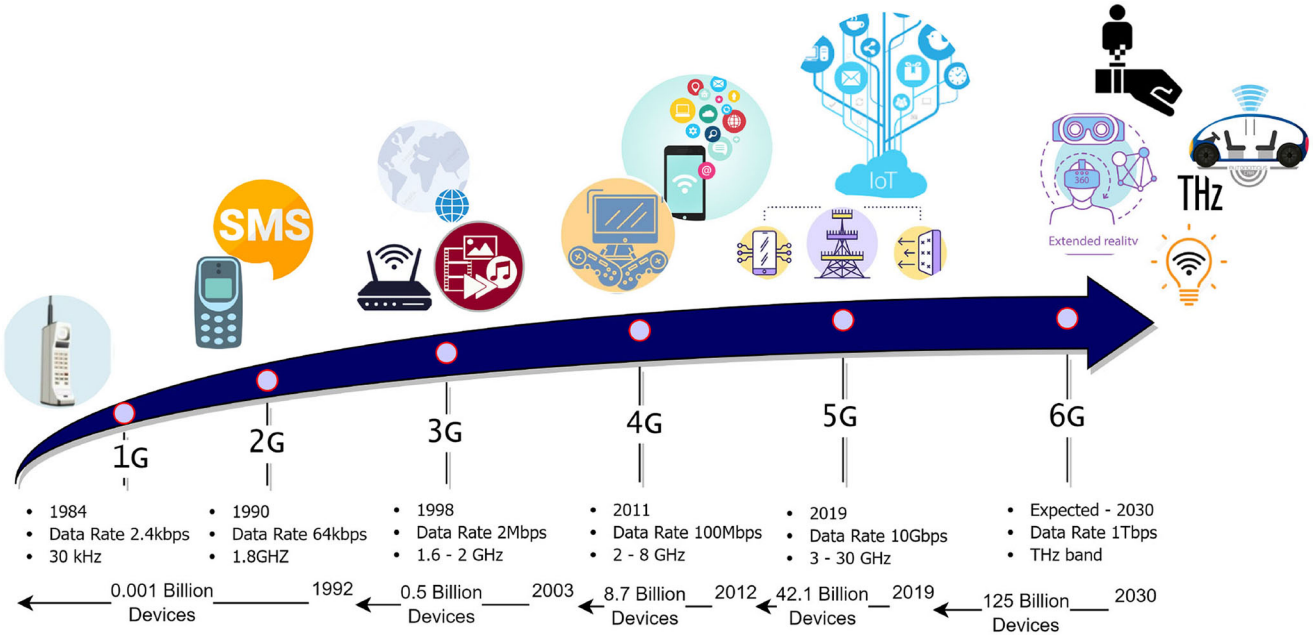

FIGURE 1. Increase in Spectrum Demand with each Mobile Generation.

mechanisms. 4G introduced an all-IP-based system, offering high-speed, high-quality, and high-capacity services. Despite advancements, static spectrum management of these architectures, hindered the optimal utilization of spectrum.

5G addressed IoT demands and diverse applications with a flexible architecture, utilizing sub-6-GHz spectrum, millimeter waves, and unlicensed spectrum. Cloud-based architecture and dynamic Radio Access Network (dyRAN) supported new verticals and data-intensive applications. 5G achieved data rates up to 10 Gbps with low latency, utilizing technologies like Massive MIMO and beamforming. B5G aims for even higher data rates, up to 1 Tbps, and promises five times the spectrum efficiency of 5G. Emerging technologies like AI, FL, BC, and access to new spectrum bands are expected to contribute to a dynamic spectrum-sharing platform, optimizing utilization [1]. (Figure 1)

Spectrum sensing emerges as the optimal solution to tackle the dual challenges of scarcity and underutilization in spectrum bands. It effectively manages the escalating data traffic and ensures the availability of essential spectrum resources for delivering broadband services. Despite technological advancements, accessing entirely new spectrum bands demands in-depth research. Spectrum sharing assumes a pivotal role in optimizing spectrum utilization by granting access to additional bands during idle periods, thereby efficiently utilizing resources originally designated for predefined services. Moreover, the implementation of a transparent spectrum sharing and allocation scheme becomes imperative for fostering trust among all stakeholders involved in the process [2].

Recognizing the spectrum as a finite and crucial resource, its management must evolve to meet the escalating demands posed by growing applications. Traditional static spectrum management, while essential, faces limitations in addressing the dynamic nature of spectrum users, particularly SUs in unlicensed spectrum bands. The rigidity of static architectures hampers their ability to support applications with higher data rates and low latency requirements [3], [4]. The absence of dynamic spectrum allocation, utilization, and management techniques poses a potential bottleneck for future mobile network developments. Moreover, these approaches encounter challenges in terms of security for users' data, imposing high infrastructure and maintenance costs, and lacking effective incentive mechanisms. Security, privacy, and trustworthiness issues often plague static spectrum management approaches, rendering them susceptible to attacks [5]. Additionally, traditional centralized electromagnetic spectrum monitoring platforms grapple with data redundancy issues across time, frequency, and space dimensions, significantly complicating the monitoring process [6]. In essence, the conventional static spectrum sharing and management, relying on centralized databases, proves inflexible, lacks scalability, and is vulnerable to a single point of failure [7], [8]. Recognizing these challenges, there is a pressing need to transition from static spectrum sharing to dynamic approaches that can adapt to the evolving demands of modern wireless communication, ensuring flexibility, scalability, and enhanced resilience against potential failures.

Even though existing DSM platforms are far from being optimum with automation, flexibility, transparency security, and privacy, in general, they have some degree of adaptability to the dynamic environment. Within these DSM approaches, CR stands out as an early pioneer, introducing a degree of control over the dynamic communication environment.

In essence, CR possesses the ability to adjust its transmitter parameters based on environmental feedback and interactions, aiming to acquire the most optimal available spectrum [9]. The cognitive capability empowers the radio to sense and capture information in dynamic environments, while reconfigurability allows for parameter adjustments, adapting the radio network accordingly. Despite its flexibility, CR faces challenges in automation and is susceptible to security issues. Alternatively, the Spectrum Access System (SAS) presents a DSM framework tailored for the Citizen Broadband Radio Service (CBRS). This system allocates frequencies dynamically, managing interference effectively [10]. However, it necessitates strict adherence to regulations imposed by the Federal Communication Commission (FCC), with spectrum allocation carried out through SAS based on a priority scheme.

While DSM has long been proposed as a solution to spectrum scarcity and under-utilization, the realization of a DSM system remains incomplete. A fully-fledged DSM platform has the potential to provide DSA to Secondary Users (SUs) without requiring a dedicated spectrum resource, ensuring availability for Primary Users (PUs) when needed [11], [12]. The application of DSM can enhance spectrum allocation and utilization efficiency, alleviate the burden on spectrum management systems, and bolster security. Without a robust DSM platform, spectrum transactions, including auctions, could encounter issues such as rights violations for PUs, data leaks, and unauthorized resource allocation by malicious users [13]. While methods like wireless network virtualization show promise in improving spectral efficiency, dynamic spectrum acquisition schemes lacking energy considerations pose sustainability challenges [14]. Efforts to advance toward a comprehensive DSM platform are critical for addressing these limitations and optimizing spectrum utilization.

Furthermore, the existing DSM suffers from several formidable challenges that hinder its seamless operation. Security and privacy concerns loom large in networks utilizing DSA, as the presence of multiple unlicensed users exacerbates the severity of threats. The cognitive capability and reconfigurability inherent in DSM introduce additional vulnerabilities to users in both primary and secondary networks [15], [16]. Maintaining privacy becomes a significant challenge, particularly in DSM approaches where SUs transmit operational attributes to databases for spectrum availability information, potentially exposing them to privacy threats in untrustworthy systems [15]. Spectrum access coordination and sharing present intricate challenges, demanding effective schemes for fairness and dynamic Medium Access Control (MAC) strategies to balance spectrum-aware sensing and access control [17]. Reliable sensing data is elusive, as most SUs must remain silent during sensing periods, introducing interference and compromising the reliability of spectrum-aware decisions [18]. Moreover, the lack of methods for detecting and addressing spectrum violations poses a significant obstacle, impacting both PUs and SUs [19]. The existing spectrum marketplace is plagued by trust issues, with fraudulent activities stemming from a centralized architecture and selfish trading parties, hindering transparency and automation [20]. Additionally, the absence of a direct mechanism for SUs to verify spectrum ownership leads to conflicts and interference issues, posing challenges to shared spectrum bands and degrading Quality of Service (QoS) for exclusive spectrum users [19], [21].

The concept of blockchains emerged alongside the advent of Bitcoin [22], gaining popularity due to its core attributes of decentralization and immutability. Decentralization eliminates the need for trust in central authorities, distributing data across the network to prevent single-point failures. Immutability ensures that the distributed data remains

TABLE 1. Summary of important acronyms.

Acronym	Definition
BC	Blockchain
CBRS	Citizen Broadband Radio Service
CDMA	Code Division Multiple Access
CRN	Cognitive Radio Network
DAG	Directed Acrylic Graphs
DLT	Distributed Ledger Technologies
DRL	Deep Reinforcement Learning
DSA	DSA
DSM	Dynamic Spectrum Management
DSS	Dynamic Spectrum Sharing
EON	Elastic Optical Network
FL	Federated Learning
FCC	Federal Communication Commission
IoT	Internet of Things
L5GOs	Local 5G Operators
LAG	Local Aggregator
ML	Machine Learning
MNO	Mobile Network Operators
NFT	Non Fungible Tokens
NFV	Network Function Virtualization
NS	Network Slicing
PLOs	Primary Licensed Operators
PoA	Proof of Authority
PoS	Proof of Stake
PoT	Proof of Trust
PUs	Primary Users
RAN	Radio Access Network
RL	Reinforcement Learning
SAS	Spectrum Access System
SC	Smart Contract
SDN	Software-defined Networks
SE	Stackelberg Equilibrium
SLA	Service Level Agreement
SSMs	Secondary Spectrum Markets
SUs	Secondary Users
SVM	Support Vector Machine
UIoT	Ubiquitous Internet of Things
VM	Virtual Machine
VNO	Virtual Network Operators

unaltered and resistant to unauthorized modifications. Additionally, all information within a blockchain is visible to every node in the network through a consensus mechanism, where agreement among nodes determines the blockchain's status. Other features include persistence, ensuring verified data within the blockchain, auditability for tracing and verification, and robust security and privacy through asymmetric cryptography.

The intrinsic features of blockchain position it as an immutable distributed ledger, offering a promising solution to overcome limitations in existing DSM approaches. Integrating blockchain into spectrum management yields numerous advantages, including secure and distributed handling of spectrum rights and enhanced transparency for auditing processes. Blockchain-based services, such as reputation management and smart contract automation, augment the system's adaptability to dynamic scenarios, while tokenization facilitates efficient sharing of spectrum and infrastructure. The immutability and transparency, coupled with innovations like Non-Fungible Tokens (NFTs), provide an excellent means of authenticating ownership of spectrum bands, fostering a more trustworthy and efficient spectrum marketplace. Furthermore, the automation facilitated by blockchains, coupled with its capacity to integrate AI and ML techniques, lays the groundwork for a more intelligent DSM scheme with a decentralized architecture.

A. MOTIVATION

DSM stands as the widely acknowledged solution to tackle the scarcity and underutilization of spectrum resources. Despite its conceptual existence for some time and the recognized advantages it brings in terms of enhanced spectrum efficiency and the enablement of novel services, the progress in DSM has been hindered by inflexible architectures that impede automation. Furthermore, existing DSM implementations suffer from:

- Security and Privacy Issues: Networks with DSM face unique security challenges, escalating in the presence of multiple unlicensed users, Cognitive capability and reconfigurability introduce additional threats to users in both primary and secondary networks, Privacy preservation is a major concern in DSM, where SUs transmitting operational attributes to databases may face threats to their privacy.
- Spectrum Access Coordination and Sharing Issues: Effective spectrum-sharing schemes are crucial in CR networks to ensure fairness when different SUs attempt to access PUs' spectrum simultaneously, Dynamic MAC strategies are needed to balance time spent on spectrum-aware sensing and access control, Sharing agreements between primary and SUsin dynamic settings require further research.
- Lack of Reliable Sensing Data: Reliable channel status diagnosis during sensing periods is hindered as most SUs must remain silent, causing low SNIR, Any SU transmission during the sensing period introduces interference, resulting in unreliable sensing process decisions.
- Lack of Spectrum Violation Detection Methods: Open spectrum access makes unauthorized access inevitable, requiring enforcement policies for fair and lawful access, Spectrum patrolling and punitive approaches aim to detect and prevent unauthorized behaviors, rogue transmissions, and violations, Lack of reliable monitoring and enforcement mechanisms challenges the identification and address of spectrum violations.
- Lack of Trustworthy Spectrum Marketplace: Scarcity of spectrum resources leads to fraudulent activities in the existing spectrum trading marketplace, Centralized architecture, and selfish trading parties contribute to untrustworthiness, Lack of transparency in spectrum transactions, and private information leakage during auctions create challenges.
- No Direct Mechanism to Verify Spectrum Ownership: Spectrum, considered exclusive property, undergoes ownership transitions through a bidding process, Lack of direct mechanisms for SUs to verify spectrum ownership leads to conflicts, interference, and degradation of QoS for exclusive spectrum users.

Blockchain emerges as a promising solution to overcome challenges and transition towards a more decentralized, autonomous, and transparent DSM scheme infused with intelligence. The distinct attributes of Blockchain, particularly the implementation of SCs, empower the establishment of intricate Service Level Agreements (SLAs) among operators. Furthermore, the integration of tokens within BC ensures a reliable and trustworthy environment for spectrum trading. BC's seamless compatibility with Artificial Intelligence (AI) and related ML techniques opens avenues for automating and enhancing the adaptability of DSM frameworks. BC offers a means to address the limitations of existing DSM approaches, improving coordination, collision prevention, and transparency for fairer spectrum access. It decentralizes decision-making through merged sensing results, enabling distributed and secure mining, while tokens act as incentives. BC facilitates the creation of a trustworthy spectrum trading marketplace, characterized by decentralization, automation, immutability, low maintenance costs, enhanced security, and transparency. It eliminates reliance on third parties, employs digital signatures for authentication, and optimizes trading parameters. SCs automate spectrum-related transactions, benefiting operators, subletters, and users, thereby enhancing spectrum utilization rates. Despite its potential, existing research gaps necessitate attention, motivating this paper to conduct a comprehensive analysis of Blockchain as the primary solution to DSM challenges. By addressing these gaps, the survey aims to provide valuable insights and outline future directions for DSM enhancement.

In Table 2, the existing BC-based solutions for addressing various aspects of DSM are presented with each paper's key contribution and highlighting the relevance of each

TABLE 2. Summary of related survey papers.

Ref.	Dynamic Spectrum				BC based DSM Solutions				Key Contribution
	Sensing	Access	Sharing	Management	Technical Aspects	Services	Platforms	Deployment Challenges	
[24]	L	M	H	L	N	N	N	N	Recent spectrum sharing (SS) technologies relevant to 5G networks along with SAS based DSA
[25]	L	H	L	L	N	N	N	N	Various aspects of DSA opportunistic spectrum, spectrum pooling, spectrum underlay versus spectrum overlay has been considered
[8]	L	H	L	M	N	N	N	N	Provide an overview about the importance of moving to dynamic and flexible spectrum management approaches
[26]	L	M	L	L	N	N	N	N	Provide an overview regarding DRL approaches proposed to address emerging issues in communications including network access
[27]	L	L	H	L	L	M	L	L	Explores the application of BC for spectrum management in terms of dynamic spectrum sharing applications and considers the benefits and limitations of blockchain based solutions
[28]	M	L	H	H	L	M	L	L	The use of blockchains as a technology for SS, DSM has been discussed, specifically the use of BC for the aspects of sensing, auctioning, smart contract for the use of SLA has been considered
[29]	L	L	H	L	L	M	L	L	The study highlights the aspects of using decentralizing applications with blockchain for 5G and B5G applications. The study's main focus is on utilizing Dapps for B5G
[20]	H	L	L	M	L	L	L	L	The study considers the rapid integration of UAVs with existing wireless technologies, specifically Spectrum Management for UAV operation
[30]	L	H	L	L	L	M	L	L	An overview of DSA along with DSA techniques, network slicing and its challenges and blockchain-based DSA has been considered
[31]	L	H	L	L	L	M	L	L	Various security and privacy attacks on SAS and possible countermeasures has been considered
[32]	L	L	L	L	M	H	L	L	A comprehensive study of blockchain and AI in wireless communications. The study discusses in depth the integration of AI into blockchain and its application to DSM.
[33]	L	L	H	L	L	L	L	M	An overview of the standardization progress of spectrum sharing and the application of blockchain in wireless communications, addressing key issues and proposing potential solutions.
Ours	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**A comprehensive survey covering all the latest development and aspects of dynamic spectrum sensing, access, sharing and management along with blockchain-based technical aspects and services, platform implementation aspects and highlighting the challenges for DSM**

L Low Impact: consider BC-based approaches in this area briefly

M Medium Impact: consider BC-based approaches in this area partially

N Non: consider only non BC-based Solutions in the area

H High Impact: consider BC-based approaches in this area in high detail

paper towards a BC-based DSM. Spectrum sensing (SS) and monitoring aspects of DSM have been discussed under [19], but the study is limited in the sense that its only focus has been to address the rapid integration of UAVs with existing technologies related to SS and monitoring aspects. Furthermore, BC-based solutions have been considered viable solutions for spectrum management for UAV environments. In terms of DSA, [29] provides an overview of existing DSA approaches while highlighting the importance of network slicing to facilitate the requirements of DSA. In addition to that automation capability of SCs has been explored. A considerable focus has also been placed on Blockchain-based platforms with the added feature of implementing SCs. On the other hand [30] main aim has

been to address the SAS, specifically the security and privacy vulnerabilities under such a system has been considered with a discussion of possible countermeasures. The contribution of BC to addressing security and privacy vulnerabilities has been limited to acting as a secure database while enabling policy enforcement in the secondary spectrum market. The spectrum sharing aspect has been explored under [28] with DApps (Decentralised applications built on Ethereum based BC platform) to enable decentralized applications of Dynamic Spectrum Sharing (DSS) using BC as the main enabler for B5G. Blockchains' contribution towards SC-based automation, tokenization, and obtaining a flexible DSS has been discussed. Finally, spectrum sharing and DSM have been considered under [27] focusing more on using BC for spectrum sensing, spectrum trading and auctioning, SLA, and SCs. However, the study limits the number of BC-based applications.

In terms of non-blockchain-based dynamic spectrum aspects goes, [7] highlights the importance of moving towards dynamic approaches for handling spectrum under-utilization and management while [23] considers the recent developments in terms of the field of the dynamic spectrum towards 5G the focus of the survey has been to explore the DSA and spectrum access systems. Various aspects of DSA such as opportunistic spectrum, spectrum pooling, and spectrum underlays and overlays have been considered under [24]. In terms of novel approaches [25] discusses how deep reinforcement learning approaches can be used to address various aspects of communication networks for facilitating DSA. Although there are several attempts to address the current state of DSM, a comprehensive approach addressing all the aspects of DSM has not been conducted. Furthermore, no in-depth review has been conducted focusing BC based approaches for DSM even though plenty of research is conducted for addressing specific aspects of DSM using BC as their primary solution.

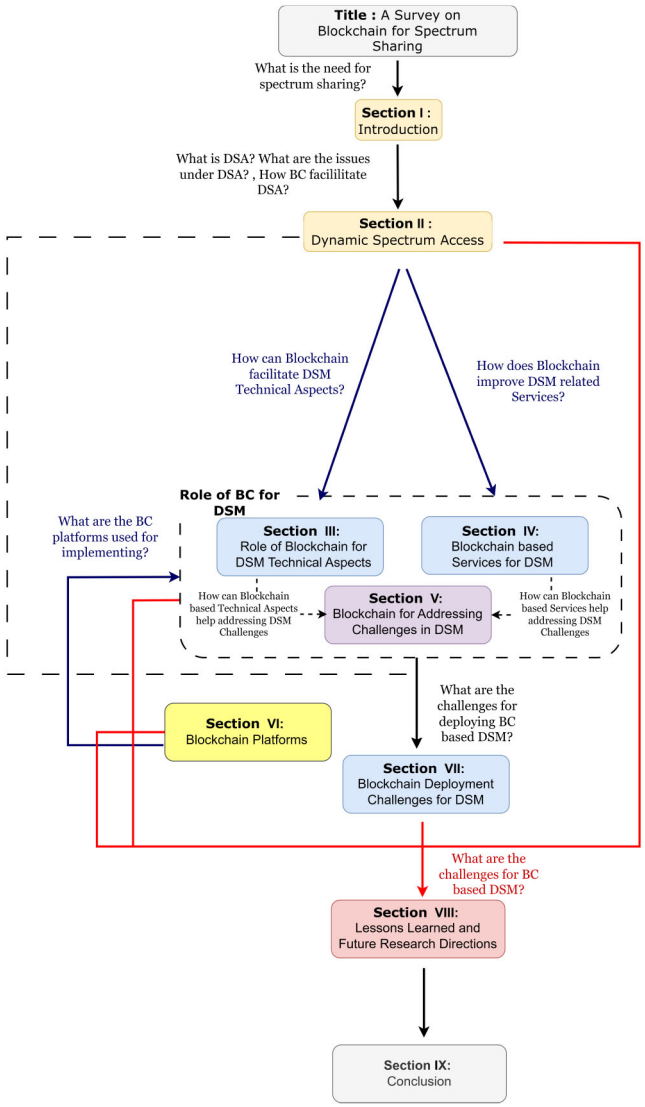

FIGURE 2. Structure and Relationship between the Sections of Paper.

B. OUR CONTRIBUTION

The main contributing factors of this paper are listed below:

- Discuss the current state of DSA and identify the challenges and limitations: the lack of comprehensive analysis might hinder the development and planning in the field
- Identify BC as the primary solution to solve the said issues and bring decentralization to DSM while enhancing fairness and transparency
- Identify the potential research gaps in using BC for facilitating DSM-related technical aspects
- Identify the potential research gaps in using BC-based services for DSM
- Compare and contrast the most frequently used BC platforms for DSM-related implementations and discuss other possible approaches
- Identify BC deployment challenges for DSM
- Discuss the assimilated facts gathered during the research and reflect on future research directions

Moreover, the authors of previous surveys focus have been on a specific aspect of DSM. In contrast, this is the very first paper that covers a broader scope, covering all aspects of DSM while prioritizing Blockchain-based solutions toward addressing the requirements of futuristic networks.

C. OUTLINE

As shown in Figure 2, the rest of the paper is organized as follows. The introduction section highlights the motivation and the overall contribution of this paper, Section II presents the DSA along with the key aspects and challenges for DSA, and the role of blockchains in terms of technical aspects of DSM is elaborated in Section III. Section IV presents blockchain-based services for DSM. Section V Discuss some of the major open research challenges in DSM and shows how blockchains could be used to address those issues. The use of blockchain platforms for DSM is presented under Section VI. Blockchain development challenges have

TABLE 3. Existing frequency assignment for legacy services.

Service	Frequency
E-GSM-900 (Mobile)	880-915, 925-960 MHz
DCS (Mobile)	1710-1785, 1805-1880 MHz
FM radio (Broadcasting)	88-108 MHz
Standard C Band (Satellite Communication)	5.850-6.425, 3.625-4.200 GHz
Non-directional radio beacon (Navigation)	190-1535 kHz

been addressed under Section VII, whereas Section VIII discusses Lessons learned and future research directions. Finally, Section IX concludes the paper.

II. DYNAMIC SPECTRUM ACCESS

The evolution of mobile communication networks brings forth diverse technologies and operators, leading to continuous expansion in demands for capacity, connectivity, coverage, and energy efficiency. However, the available spectrum is finite and cannot be expanded, posing a challenge to meet the growing needs. Higher frequency ranges beyond 6 GHz face increased attenuation and atmospheric absorption, limiting their usability with current mobile hardware. Frequencies below 1 GHz are already allocated for various functions, further restricting the available spectrum. This scarcity acts as a significant impediment to the rapid growth of wireless networks and users (Table 3). In addition to scarcity, the existing spectrum usage is inherently inefficient, with the rate of spectrum efficiency growth declining over successive generations of mobile networks. Addressing this challenge is crucial for breaking the trend of saturation and ensuring continued improvement in spectrum efficiency [17].

Currently, regulatory bodies in various countries and regions statically allocate spectrum, dividing it into smaller blocks licensed to individual users or specific services. Despite this, a significant portion of the licensed spectrum remains idle, with studies indicating an idle range between $15 - 85\%$ [33]. This static spectrum assignment results in substantial underutilization of already scarce spectrum resources. To address this, DSA is crucial, allowing unlicensed users to opportunistically access licensed spectrum. This dynamic access, often termed CR scheme, aims to minimize interference and security issues for licensed users. DSA involves rapid sensing, coordination, and cooperation, with unlicensed users (SUs) identifying underutilized spectrum portions and adjusting their communications while minimizing the impact on licensed users (PUs). The terms DSA and CR are often used interchangeably in the literature.

CR functionalities have been standardized in various IEEE protocols, such as IEEE 802.22 WRAN, IEEE 802.11af, and IEEE 1900.x series [34], [35], [36], enabling DSA. IEEE 802.22 WRAN focuses on the unlicensed use of TV frequency bands to provide wireless broadband access in rural areas without interfering with primary users. Secondary devices utilize GPS-aided geolocation databases and spectrum sensing to identify available spectrum chunks and dynamically switch to alternative blocks when PUsare active. The IEEE 1900.x series encompasses multiple standards for DSA. IEEE 802.11af employs CR techniques to identify white spaces through geolocation databases. In LTE and 5G NR networks, Licensed Shared Access (LSA) is introduced for mobile operators to control network parameters and reduce harmful interference, requiring SUs to obtain licenses [37]. 6G networks envision incorporating CR functionalities for intelligence using game theory and ML [38]. The FCC's citizens' broadband radio service exemplifies practical DSA. Additional standards like IEEE 802.15.4m for Zigbee networks [39], and IEEE 802.19.1 for exploiting spectrum holes in TV service allocations and ensuring coexistence between CR devices have also been developed.

A. KEY BENEFITS OF DSA

The adoption of DSA has multiple benefits to all stakeholders [17], [38].

- *Improved Spectral Efficiency:* DSA allows secondary unlicensed networks to access licensed spectrum which is either unutilized or underutilized. It has been shown that the amount of time on average that a signal is detected within a particular frequency band (duty cycle) is as low as $10 - 40\%$ [38]. Therefore, by accessing this spectrum, other networks will be able to conduct transmissions without requiring to lease additional spectrum for themselves, which improves spectral efficiency.
- *Enabling New Services:* One of the significant bottlenecks and hindrances for establishing new services is the difficulty of obtaining a new dedicated spectrum. The limited available spectrum is also extremely expensive. As such, there is a significant barrier to the establishment of newer services. However, with DSA, new networks will be able to access the spectrum more simply.
- *Reduced Cost:* For a new network, accessing licensed spectrum opportunistically would be significantly cheaper than licensing spectrum outright for itself.
- *Economic Gain for Licensed Networks:* For licensed networks, DSA presents an opportunity to gain extra income by essentially renting their spectrum bands for a portion of the time when they are not used.

B. CLASSIFICATIONS ON DSA

DSA techniques can be classified based on different metrics (Fig. 3). These include the network architecture, the spectrum sensing behavior, and the spectrum access method [23].

1) CLASSIFICATION BASED ON SYSTEM ARCHITECTURE

DSA methods can be broadly classified based on the network architecture, with two main types identified: centralized

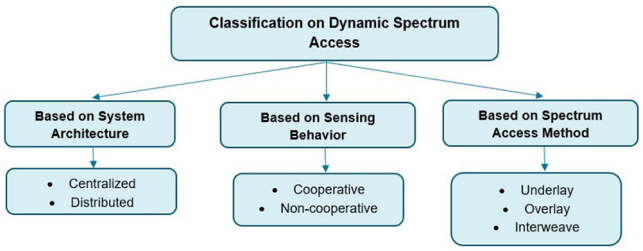

FIGURE 3. Summary of DSA classification.

networks and distributed networks [17]. In a centralized network, a designated controlling entity, often the regulator, manages network access. This entity, equipped with spectrum sensing data from individual devices, oversees most cognitive functionalities, including maintaining records of frequency block usage, granting permission for SUsto access channels, and enforcing penalties for unauthorized access [17]. Despite the advantages of a centralized decision process, such as optimizing network throughput, reducing interference, ensuring fairness among devices, and prioritizing critical devices, this approach comes with drawbacks. Centralization introduces high overhead, necessitates additional network infrastructure, and presents a single point of failure as networks become denser and more congested [17].

Conversely, distributed networks lack a central controller, with individual secondary devices holding all cognitive capabilities and responsibilities [17]. This decentralized approach, suitable for ad-hoc networks without base stations, allows devices to respond in real-time to sudden changes in spectrum activities without waiting for central directives. However, decision optimality for the overall network may be compromised, leading to suboptimal outcomes. Additionally, the absence of a central device managing network access raises concerns about security and the enforcement of penalties for unauthorized access.

Early spectrum-sharing approaches were designed based on distributed and centralized network architectures, each with distinct characteristics and trade-offs [40]. Distributed spectrum sharing involves local coordination among systems on an equivalent basis, offering efficiency compared to centralized techniques that rely on a central unit for coordination without direct interaction [40]. Centralized techniques, exemplified by the geo-location database method and spectrum broker method, present challenges in terms of adaptability to changing environments. Approaches such as the harmonized SDN-enabled approach (HSA) in centralized spectrum sharing aim to minimize incorrect decisions influenced by inconsistent QoS [41]. Various studies explore optimization strategies, including interference graph and game-theoretic approaches for joint optimization of decentralized spectrum sensing, emphasizing the need for adaptability to dynamic environments [42]. While these approaches simplify network management, their limited adaptability to changing conditions remains a significant challenge.

2) CLASSIFICATION BASED ON SPECTRUM SENSING BEHAVIOR

Based on spectrum sensing behavior, DSA can be classified into non-cooperative and cooperative networks [17]. In non-cooperative networks, individual devices or networks make decisions based on their own spectrum sensing results. This has the advantage of reduced overhead as there is no need to share information. Moreover, the decisions will be more timely. However, due to wireless channel impairments, a secondary device may not be able to detect a spectrum hole or a spectrum hole may be detected when none exist [43].

On the other hand, in cooperative spectrum sensing, several secondary devices share their local spectrum sensing results for an overall decision [17]. Thus, a better sensing performance is achieved by exploiting spatial and multiuser diversity [44]. Co-operation techniques can be broadly classified as data fusion and decision fusion [45]. In data fusion, a node shares the sensed information, whereas in decision fusion, the spectrum decision is shared. Co-operation among secondary devices faces issues including added complexity and implementation challenges. Ideally, for sharing data among secondary devices, a separate dedicated control channel is required. Furthermore, different secondary devices may have performed their sensing at different times, making the information asynchronous and not up-to-date.

3) CLASSIFICATION BASED ON THE SPECTRUM ACCESS METHOD

DSA encompasses three main types based on the spectrum access method: interweave networks, overlay networks, and underlay networks. Interweave networks adhere to the principle of utilizing spectrum holes, operating on an interference-free basis. Secondary devices initiate data transmission when a spectrum hole is identified, but transmissions must cease when the primary network reoccupies the frequency block. Overlay networks enable concurrent primary and secondary transmissions, requiring knowledge of primary user transmissions for interference cancellation and relaying primary user messages (Figure 4). Underlay networks allow concurrent transmissions without spectrum hole detection, but secondary devices must maintain interference levels below an acceptable threshold, often achieved by adjusting transmit power or implementing non-transmitting blackout regions around primary devices [15], [46], [47], [48], [49].

The SAS is an emerging spectrum-sharing model gaining attention for its potential to manage uplink interference in massive machine-type Communication (mMTC) scenarios with low overhead. SAS can be utilized by operators to access the 3.5 GHz military radar band for commercial use in the USA. However, database-driven DSA, as promoted by CR technology, raises concerns about location privacy for SUs. To address this, a multi-server Private Information Retrieval (PIR) approach is discussed as a means to enable private access to spectrum databases, protecting the location information of SUs in database-driven spectrum sharing [50].

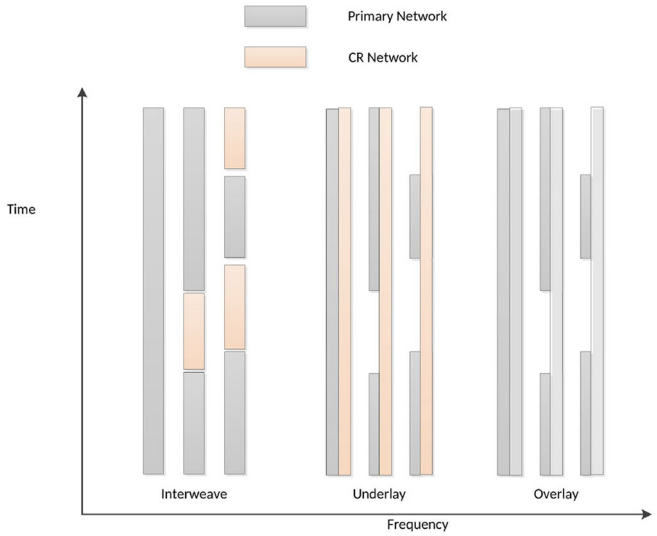

FIGURE 4. Interweave, underlay, and overlay modes of CR for three frequency bands. It can be seen that while there are no concurrent transmissions in interweave networks within the same frequency band, concurrent transmissions occur in both overlay and underlay networks (subject to certain conditions).

Analytic Hierarchy Process (AHP) is applied to spectrum sharing to address interference and enhance performance in 5G New Radio (NR). This method, structured hierarchically with objectives, criteria, and alternatives, calculates user priority for spectrum access, avoiding conflicts among SUs. A two-time-scale hierarchical model for wireless network virtualization resource management focuses on efficient network sharing, considering packet delay, data rate, and IoT throughput for different user types [51], [52].

The Dynamical Advance Access Spectrum Sharing method is introduced for public and dedicated telecommunication operators, ensuring Quality of Experience (QoE) for SUs. The system employs a finite-state Markov chain to model state transitions, demonstrating improved queuing time and architecture compared to alternative access methods. This approach considers variations in channel condition and service state, resulting in superior QoE performance [53].

A novel hybrid spectrum access method is proposed to combine exclusive access and pooled spectrum access. This hybrid design aggregates low-frequency carriers for exclusive access and high-frequency carriers for spectrum pooling. The authors suggest an optimal Power Allocation (PA) strategy to maximize Energy Efficiency (EE) when feasible, offering a versatile solution for spectrum access challenges [54].

C. FUNCTIONALITIES OF A CR DEVICE

A CR device engaging in DSA must satisfy several key functionalities. These include spectrum sensing, spectrum management and decision, and spectrum mobility [17], [46].

1) SPECTRUM SENSING

Devices or networks attempting to access licensed spectrum must first and foremost perform spectrum sensing to identify whether it is already occupied by the licensed primary network [46], [55]. DSA can only occur if the spectrum is found to be vacant through spectrum sensing. The spectrum sensing process should be regular and ongoing to assess whether the primary network has re-started its transmissions. If so, secondary devices should either cease transmissions or reduce transmission power accordingly. Spectrum sensing can be performed in several different ways which will be elaborated later.

2) SPECTRUM MANAGEMENT AND DECISION

When multiple spectrum holes are available, the secondary network must decide on which ones to use [46]. These decisions can be based either on the optimality for a single pair of communicating nodes or for a whole secondary network itself. Spectrum decisions can either be made centrally or in a distributed manner. When a spectrum decision is made, several factors need to be taken into account. These include interference to the primary network, interference among secondary users, holding time (the amount of time SUs have access to a spectrum hole before having to release it back to the primary network), overall channel capacity, and the frequency band (as some bands may be less suitable for different networks) [56].

3) SPECTRUM SHARING

Each block of frequency spectrum within a given geographical area has a dynamic number of spectrum holes that need to be shared between different secondary devices. The sharing process is based on scheduling and may be performed in time, frequency, code, and even space dimensions. It also aims to reduce or remove interference among the SUsthemselves [56]. Spectrum sharing may either be centrally managed or distributed. When centrally managed, a control center manages spectrum access using the sensing results it receives from different devices [56]. This entity conducts all the spectrum decisions and decides on the fair scheme to share available spectrum. In a distributed system, each node makes decisions based on local information. In a more general sense, spectrum sharing may also involve the licensed network, but in such cases, it would always be afforded priority access.

4) SPECTRUM MOBILITY

In a DSA environment, the available frequency slots may be distributed in disparate frequencies [17]. Also, the available frequency blocks may change continuously (this may be due to primary devices re-accessing spectrum and adverse channel conditions. Secondary networks may also require increased bandwidth for their traffic. Spectrum mobility refers to the ability of secondary devices to use different vacant spectrum blocks seamlessly. The movement between different spectrum holes is referred to as a spectrum hand-off [46], and is analogous to traditional cellular hand-offs. However, a hand-off should be performed while not adversely affecting the quality of service, which is challenging in a DSA environment where the availability of spectrum is not guaranteed.

D. SPECTRUM IDENTIFICATION METHODS

In DSA, SUsopportunistically access spectrum holes, which may be present in vacant, under-utilized, or occupied spectrum [17]. Vacant spectrum is where primary user activity is absent within a particular area [15]. On the other hand, when the primary user accesses the spectrum intermittently at certain times, the spectrum is said to be under-utilized. Finally, even the occupied spectrum can be accessed by secondary devices under certain conditions (such as with underlay CR). For example, transmit beamforming allows the signals to focus toward the intended receiver without interfering with other devices. Vacant spectrum identification may be conducted either through geolocation databases or via different spectrum sensing methods. These are elaborated below.

1) GEOLOCATION DATABASES

Geolocation databases store up-to-date information about spectrum usage within different geographical areas [17]. SUsquery a geo-location database for a list of available frequencies at a particular location. The database may also supply additional information such as the associated maximum permitted transmit power levels for each of the available frequencies and the time period to which the data is valid [43], [57]. These databases will be administered by regulatory authorities, who will make the final decision about opportunistic access. As geographical areas are divided into a grid, the size of the grid impacts both the performance and data transfer rates. For example, with a large-scale grid, the spectrum information might be inaccurate whereas a finer grid will be complex to implement. Geolocation databases have several disadvantages. As the exact location of a secondary device may be incorrect, there's a risk of unintended interference. Accurate Global Positioning System (GPS) information will be required [17]. Geolocation databases are not robust, and thus cannot adapt to rapid network changes. While they may be ideal for primary networks such as relatively static digital terrestrial television networks, modern heterogeneous cellular networks present a more complicated situation [56], [58]. Temporal opportunities where some time-frequency slots are available dynamically will also be missed. Furthermore, some spectrum usage information may not be up to date, and implementing a geolocation database will be extremely complex when the grid is fine. Finally, a geolocation database presents a single point of failure which is a severe security issue.

2) ENERGY DETECTION

Energy detection is a form of in-band sensing, which refers to the direct measurement of the primary user spectrum by a secondary device that is trying to access it [59]. While in-band sensing is best suited to be used with distributed systems, it can also be adapted for centralized ones. A major disadvantage is that it relies upon the detection of primary transmitters, but cannot identify primary receivers which are the entities affected by any resulting interference. Therefore, when a secondary user transmits after not detecting a signal, it can still cause interference to nearby primary receivers. This is termed the hidden terminal problem [43].

An energy detector measures the energy level of a signal over a target frequency band and compares it with a threshold [59]. If the energy is below the threshold, the spectrum band is identified as a spectrum vacant, whereas it is identified as occupied otherwise [55]. This detector is optimal under the presence of additive white Gaussian noise (AWGN) and when no prior information is available about the primary user transmissions. Energy detectors aim to reduce the probability of missed detection (the probability that a signal exists when the detection indicates otherwise) and the probability of false alarm (the probability of detecting a signal when one doesn't exist).

Energy detectors are easy to implement, have low computational complexity, and lack the need for primary signal information [46]. However, it lacks resilience against noise uncertainty, which increases both missed detection and false alarm probabilities. Furthermore, it is vulnerable to interference from co-channel transmitters, which could be primary or secondary devices in adjacent areas. Moreover, it cannot identify different primary signals apart [60], and the probability of false alarm can increase due to signals from unknown sources [15]. Finally, it performs poorly in low SNR (signal-to-noise ratio) regimes [61].

3) CYCLOSTATIONARY FEATURE DETECTION

This in-band sensing method exploits the periodicity of signal statistics such as mean and autocorrelation of primary signals [15], [46]. This periodicity arises due to the features of signal modulation, up-conversion, cyclic prefixes, codes, hopping sequences, and other factors of the primary user signals. Consequently, this phenomenon is termed cyclo stationarity. Moreover, as this phenomenon is not present in additive noise signals, this detector will work even in low SNR regimes. Furthermore, if periodic features are deliberately introduced to signals, this detector performs even better. The ability to differentiate between different primary systems due to differing transmit features is another advantage. However, this method has high complexity, a high sampling rate, and requires a large number of samples [46]. Timing and frequency offsets reduce the degree of correlation, which reduces the periodicity of the received signal. Furthermore, when the primary network employs Orthogonal Frequency Division Multiplexing (OFDM), identifying different primary systems is difficult [15]. As such, for simple secondary devices, this method may be unsuitable.

4) EIGENVALUE DETECTION

This is another method of in-band sensing and uses eigenvalues of the covariance matrix of the received signal to obtain the ratio between the maximum and minimum eigenvalues [17]. This is used to detect the presence of primary signals in the presence of noise and without prior knowledge of the signal, channel, or noise power [62]. When

noise is the only component present in the received signal, this ratio tends to one while when primary signals are present, it increases [60]. Eigenvalue-based detection works well under low SNRs, different fading environments, and noise uncertainty. However, the computational complexity is high [63], and this detector may also fail when the samples of primary signals are uncorrelated [59].

5) MATCHED FILTER DETECTION

With this in-band sensing scheme, a matched filter is obtained by correlating a transmit signal with the received signal to detect the presence of the transmit signal [17]. In other words, the received signal is convolved with a conjugated time-reversed version of the transmit signal. The matched filter is optimal in maximizing the received SNR in the presence of additive Gaussian noise. Matched filter detection requires prior information about the transmitted primary signal such as modulation format, pulse shapes, phase, and others [60]. Thus, periodic pilot transmissions from the primary devices are necessary [60]. This detection scheme has a lower sensing time to achieve the required level of performance. However, matched filter detection performs poorly with increased noise and the age of the transmission information [15]. Furthermore, when spectrum holes are dispersed over a wide swath of spectrum, different primary signals over different frequency bands must be correlated, which increases the complexity. However, matched filter detection is among the best ways for spectrum sensing when prior information about the primary user signals is known beforehand [15].

6) BEACON DETECTION

Beacon detection is a method of out-of-band sensing [17]. Unlike in-band sensing, this does not involve directly sensing the spectrum band whose access is required. Instead, a dedicated out-of-band control channel tells whether the frequency band is occupied or not through a beacon signal. The beacons are simple narrowband signals modulated by on-off switching [64]. They do not necessarily have to be continuous and can be transmitted periodically, reducing additional power requirements. The SUsdetect beacon signals and decides on channel occupation. Beacon signals are efficient and relatively simple to implement [65], [66], and beacon detection circuits can be relatively simple. Furthermore, the beacon signals can be used to separate different primary devices. Individual identification of primary devices is not readily possible in most in-band spectrum detection methods. Moreover, beacons provide an added layer of control to the primary network, which can proactively prevent dynamic access through beacons. Beacons may also be transmitted by primary receiver devices where necessary/possible, which prevents the hidden terminal problem of in-band sensing.

Beacon signals can take the form of permission or denial [44], [67]. Permission beacons actively allow secondary user transmissions, whereas denial beacons proactively prevent it [17]. As primary devices can transmit the beacons simultaneously with their data, denial beacons appear more feasible. Denial beacons can become problematic if the primary device goes into sleep mode or turns off temporarily. However, by using dual beacons which combine grant and deny beacons, the reliability of beacon signaling can be further increased. The main drawback of beacon signals and out-of-band sensing, in general, is the use of additional spectral resources and power. Furthermore, beacon signals may not be properly received due to wireless channel effects. While increasing the beacon transmit power is an obvious answer, the energy efficiency of the system will subsequently decrease. Furthermore, the prevention of beacon reception outside its intended coverage area [68] is important to increase the spectrum available to SUs. In addition, when the licensed spectrum has multiple different sub-bands, beacon signaling can become more complex.

7) INTERFERENCE TEMPERATURE

Interference temperature is a receiver-centric concept that aims to quantify the aggregate interference experienced at a primary user receiver [17]. This interference may be from other co-channel licensed users or from SUsopportunistically accessing the spectrum. Interference temperature-based spectrum identification is attractive, especially for the underlay mode of CR whose devices do not actively sense the spectrum. For a given geographic area and frequency band, one can establish an interference temperature, which is the maximum amount of tolerable interference. Any secondary device using this band must guarantee that their transmissions added to the existing interference must not exceed this value at a receiver [69]. The interference experienced at a primary receiver can be thought of as impulses superimposed on the noise floor. These spikes are tolerable up till a threshold beyond which they degrade performance. When different receivers have different interference temperature levels, the level of the device having the lowest threshold must be used. A major drawback is that real-time estimations of the interference temperature are difficult. As a remedy, the primary network may provide feedback to potential secondary devices. Moreover, interference temperature-based spectrum identification may become infeasible in a decentralized network [17]. While the secondary devices can make a probabilistic estimate about the interference temperature at a primary receiver, their locations must be known in advance [15].

E. KEY CHALLENGES IN DSA

DSA holds promise for enhancing spectral efficiency but grapples with several challenges demanding resolution for effective implementation. Notably, interference emerges as a significant concern affecting both primary and secondary networks, where erroneous perceptions of channel vacancy by SUs may lead to concurrent transmissions. The establishment of a reliable common control channel becomes imperative for reporting and negotiating access, requiring full availability and interoperability across diverse protocol

TABLE 4. Summary of spectrum identification methods.

Spectrum Identification Method	Description
Geolocation Databases	Uses a centralized database where users query for available frequencies. Not robust, and not suitable for distributed systems. [44]
Energy Detection	Measures the ambient energy within a frequency band. Simple to implement. Has a high probability of false alarms. [60]
Cyclostationary Feature Detection	Uses the periodicity of signal statistics to identify primary users. Has high complexity. [16]
Eigenvalue Detection	Uses Eigenvalues of the covariance matrix of the received signal to identify primary users. Has high complexity. [16]
Matched-filter Detection	Correlates the transmit signal with the received signal to detect signal presence. Needs prior information about the transmitted signal. [61]
Beacon Detection	An out-of-band scheme. Uses additional resources. High reliability. [65]
Interference Temperature	Aims to quantify the aggregate interference experienced by a primary user. An interference temperature specifies the maximum tolerable interference. [18]

stacks. Security and privacy issues compound due to the presence of multiple unlicensed users and the adaptable nature of CR networks, introducing threats like mimicking primary user behaviors and disseminating false spectrum information. Coordination challenges in spectrum access and sharing schemes, including the necessity for robust medium access control strategies and well-defined payment procedures, add complexity to the landscape. Reliable sensing data becomes a hurdle, with the inefficiency of single users mitigated through cooperative sensing to address fading and shadowing issues. The detection of spectrum violations necessitates stringent enforcement policies and vigilant monitoring mechanisms. Spectrum-sharing strategies confront challenges in defining agreements between primary and SUs and establishing trustworthy marketplaces. The absence of a direct mechanism to verify spectrum ownership raises security concerns, potentially leading to conflicts and interference that compromise the overall Quality of Service. These challenges are discussed in detail in Section V,

F. BLOCKCHAIN FOR DSM

The distinctive features of blockchains position it uniquely as a technology capable of addressing the requirements of DSM and other facets of communication, including edge computing [70]. Essentially, blockchains and their inherent properties offer avenues to reduce costs associated with DSA, enhance overall efficiency, securely store spectrum trading and auction-related transactions, and fortify the security of DSM systems [71]. Beyond conventional blockchains, SCs built atop blockchain frameworks present an opportunity to automate spectrum-related transactions while compelling stakeholders to adhere to predefined SLAs [11]. The multi-faceted role of blockchain in DSM can be delineated across four key sections (refer to Figure 5).

1) SPECTRUM SENSING (SS)

Blockchains can significantly expedite the spectrum sensing process, particularly through SCs tailored to autonomously execute spectrum sensing tasks. However, the challenge arises when SUs contemplate accessing the spectrum, especially in faded conditions, potentially reducing their inclination to participate in spectrum sensing. This hurdle can be mitigated by implementing carefully designed Spectrum Consensus mechanisms, incentivizing nodes to persist in spectrum sensing tasks even under adverse conditions [72]. Moreover, blockchains offer a reliable repository for storing sensing information, facilitating decisions on identifying malicious nodes that generate falsified sensing reports [73]. This enhances the overall trustworthiness of the spectrum sensing process. Additionally, blockchain technology enables the autonomous and immutable supervision of payments among PUs, SUs, and other stakeholders, eliminating the need for central authorities to oversee the entire spectrum payment process. Beyond financial transactions, blockchain-based DSS can efficiently handle advertising spectrum availability and manage reputation scores associated with each node, fostering a more transparent and accountable spectrum management system.

2) SPECTRUM TRADING (ST)

SCs enable tamper-proof transactions, automated contract execution, and seamless payment settlement, contributing to the establishment of a self-organized spectrum market [74]. Additionally, blockchain facilitates reliable identity management, where pseudonymous identities can be employed to safeguard node privacy. In contrast to traditional centralized spectrum trading platforms vulnerable to malicious activities, leveraging blockchain for spectrum trading offers distinct advantages. The decentralization inherent in blockchains enhances the robustness of spectrum trading by mitigating single points of failure and ensuring the immutability of transactions [75]. Blockchain-based platforms also exhibit a higher degree of accessibility, allowing any interested SU to participate in spectrum auctions without the necessity to register with a centralized auctioneer. Digital signatures further strengthen the authentication of PUs and SUs, rendering impersonation impossible and reinforcing the security of the spectrum trading process. Moreover, regulatory bodies can ensure compliance with spectrum policies by embedding relevant policies into SCs, thereby streamlining regulatory oversight and enforcement.

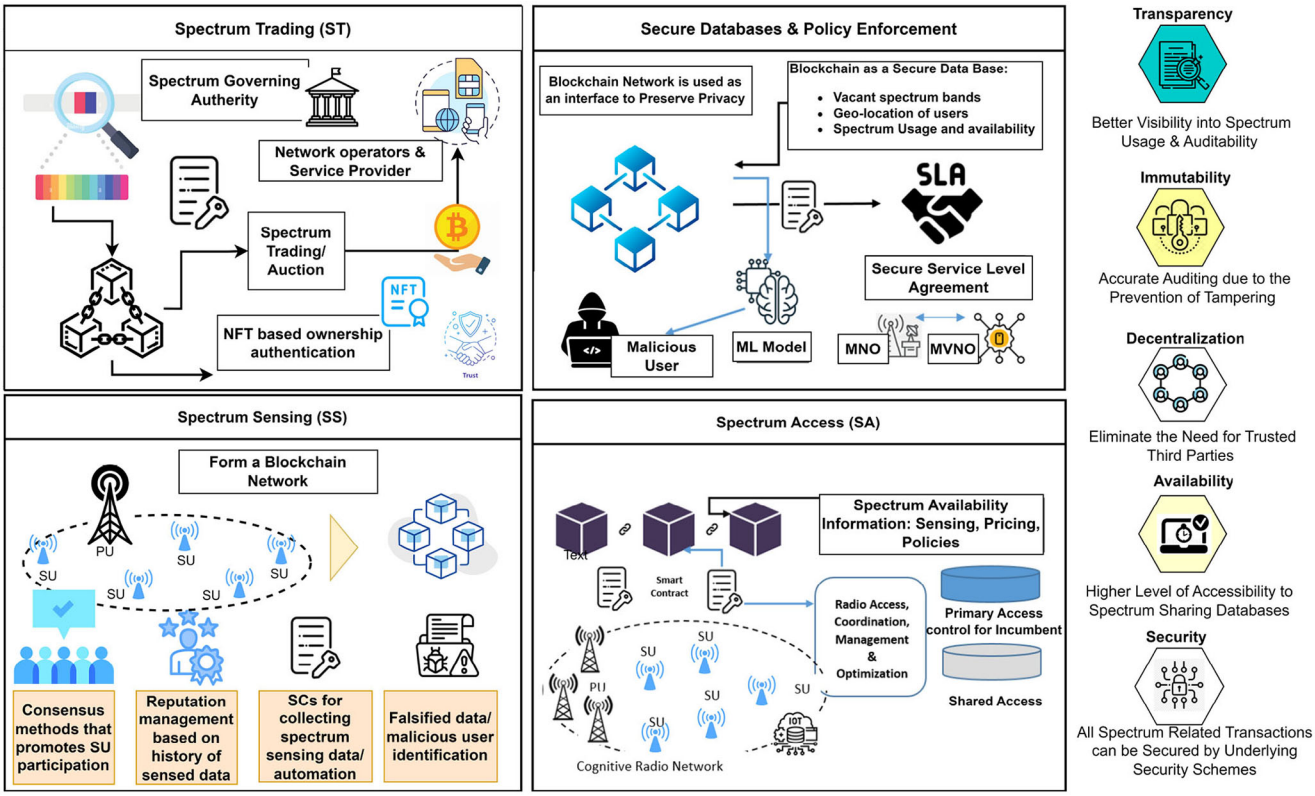

FIGURE 5. Role of Blockchains for DSM.

3) SPECTRUM ACCESS AND COORDINATION (SAC) AND SHARING

Blockchain-based spectrum access streamlines the coordination of spectrum access, effectively preventing collisions. Additionally, utilizing blockchain for spectrum access ensures transparency throughout the entire process, fostering fairness in spectrum allocation. In the context of spectrum auctions, collaborative supervision by all SUs enhances fairness and helps prevent unauthorized access [76]. The comprehensive information on spectrum availability, along with sensing, pricing, and policy details stored in blockchains, allows for the strategic use of well-designed SCs. These SCs, supported by ML and AI techniques that seamlessly integrate with the blockchain architecture [5], facilitate efficient radio access coordination, management, and optimization. This integrated approach enhances the overall effectiveness of spectrum management and utilization.

4) SECURE DATABASE AND POLICY ENFORCEMENT

Blockchain, with its inherent qualities of immutability and verifiability, serves as a secure database for storing DSM information. This utilization prevents fraudulent actions by PUs, as all transactions are transparent, ensuring the integrity of processes like spectrum auctions and related payments [77]. It acts as a safeguard against the access of malicious SUs. By employing a blockchain network as an interface, the privacy of all stakeholders can be effectively secured [78], [79]. The sensing results stored in the blockchain, when combined with ML techniques, enable the recognition of behavioral patterns among nodes, facilitating the identification of malicious entities. This information, being a reliable source, becomes integral in making informed decisions related to spectrum management.

III. ROLE OF BLOCKCHAIN FOR DSM TECHNICAL ASPECTS

Blockchain with its innate features can be used to address the technical requirements of DSM. For instance, the distributed nature of blockchains can be used to improve the scalability of DSM to support a massive number of devices/nodes while not hindering other related tasks such as spectrum sensing data generation and related spectrum rewards and accessing. Technical aspects such as immutable and transparent features would facilitate the enhancement of security and privacy aspects of DSM via its underlying privacy and security protection schemes. Furthermore recognizing such security and privacy violations related to transactions becomes significantly easier with the non-repudiation feature (See Figure 6).

A. OPTIMIZATION

1) INTRODUCTION

Optimizing DSA and DSM is pivotal to addressing the pervasive challenge of spectrum underutilization. A comprehensive approach, encompassing spectrum sensing, access,

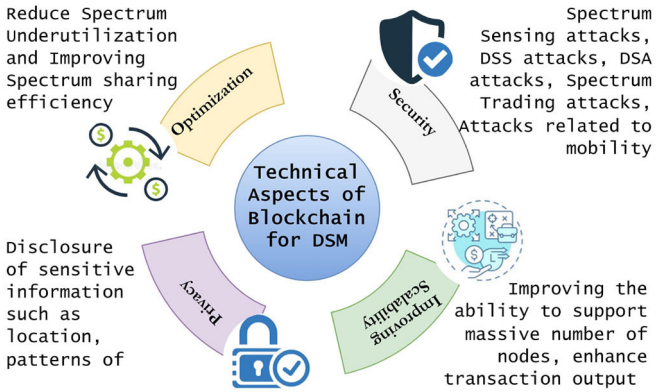

FIGURE 6. Technical Aspects of Blockchain that can be used for DSM.

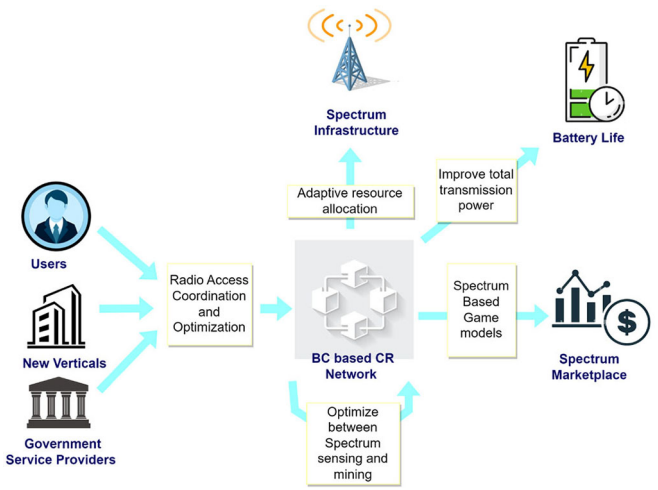

FIGURE 7. BC-based Spectrum Optimization.

trading, and sharing, becomes imperative to unlock the full potential of available resources. Various facets of DSM benefit from optimization, including spectrum trading platforms utilizing game models for efficient allocation and adaptive resource allocation methods for managing spectrum-related infrastructure. CR necessitates meticulous optimization of radio access to support the burgeoning Internet of Things (IoT) ecosystem, emerging business verticals, and data-intensive applications. Energy efficiency is critical, and DSM optimization plays a vital role in mitigating consumption, incorporating elements like energy harvesting within the DSA process. This holistic optimization approach, as illustrated in Figure 7, is central to overcoming spectrum underutilization and fostering a more efficient and sustainable dynamic spectrum ecosystem.

2) HOW BLOCKCHAIN HELPS

In the domain of DSA and management, the persistent presence of malicious spectrum nodes exacerbates the strain on a heavily constrained spectrum, hindering efficient and secure resource allocation. Traditional consensus algorithms, such as Raft, coupled with game theories, navigate the Byzantine complexities of spectrum sharing. However, these approaches often fall short in jointly considering the spectrum occupancy of PUs and Cognitive Users, neglecting factors like primary users' utility and enthusiasm. Praft, a blockchain-based game spectrum model, represents a notable advancement, introducing an optimal strategy that refines the inverse demand function of PUs to encompass the spectrum occupancy of both PUs and SUs [80].

The specter of an underutilized spectrum presents a wasteful oversight that could be mitigated with more strategic approaches. Even within the license-free spectrum, the untapped potential exists, necessitating attention, especially in addressing lower access requirements. A blockchain and smart contract-based framework proposed by Fan and Huo [81] focuses on the Cyber-Physical-Social Systems (CPSS) band, emphasizing edge computing. This framework divides local cell spectrums into multiple blockchain-based channels, leveraging a K-Means algorithm to expedite transactions and adeptly responding to the scarcity of spectrum resources in CPSSs, optimizing spectrum utilization.

Idle spectrum sensing nodes and uncooperative users result in the squandering of valuable resources. To incentivize participation and cooperation, a Tit-For-Tat (TFT) game theory-based blockchain approach [82] for spectrum sharing is proposed. The TFT scheme fosters cooperation among users who may not actively engage in spectrum sharing, indicating a substantial improvement of approximately 55.1 percent in the efficiency of the spectrum-sharing scheme compared to traditional centralized methods, achieved through meticulous optimization in a game-driven environment.

Preserving battery life and ensuring energy efficiency in the B5G era dissuade nodes from active participation in spectrum-related tasks. CR is anticipated to play a pivotal role in optimizing spectrum utilization, particularly through spectrum sensing. Acknowledging the key role of multi-node Cooperative Spectrum Sensing (CSS), [83] introduces a consensus algorithm to strategically select nodes, minimizing energy utilization and maximizing spectrum efficiency. Additionally, wireless network virtualization is explored as [14] proposes a decentralized blockchain-based dynamic spectrum acquisition scheme for wireless mediums with Mobile Virtual Network Operators (MVNOs), minimizing transmission power while ensuring average data transmission rates.

Timely and relevant data extraction is imperative for the optimization of dynamic spectrum processes. Traditional centralized spectrum management platforms tend to accumulate redundant data. Reference [6] advocates for a Minimum Average Distance (MAD) approach to enhance the accuracy of collaborative detection in CR networks, consequently improving the efficiency of the spectrum sensing process. A blockchain-based database, referred to as Blockchain-DSDB, is instrumental in regulating the rational utilization of electromagnetic spectrum resources and determining the priority of SUs for DSA. With redundancies eliminated,

SUs can formulate efficient DSA policies based on BC-DSDB and Source Routing Control (SRC) in distributed CR networks. The versatility of blockchains extends to supporting multi-dimensional management of various resources, including spectrum allocation, and facilitating Multiple-Input Multiple-Output (MIMO) support. Reference [84] introduces a blockchain-based framework for multi-operator inter and intra-spectrum management and service provisioning. By holding records of frequency band usage across multiple operators in the blockchain, the framework successfully reduces spectrum under-utilization.

Efficiency in spectrum-related resource allocation is a linchpin for overall spectrum utilization enhancement. For instance, [85] proposes a blockchain-based Mobile Edge Computing (B-MEC) framework designed for adaptive resource allocation and computation offloading. The model orchestrates optimization through deep Reinforcement Learning (RL) based on Q learning, addressing factors such as resource allocation, block size, and the number of consecutive blocks. Elastic Optical Networks (EONs) coupled with Software-Defined Networking (SDN) architecture present an avenue for increased availability, failure resilience, and efficient resource allocation. However, operational challenges in optimal spectrum assignment impede their widespread use. SpectrumChain (SC) [86] emerges as a blockchain-enhanced, Quality of Service (QoS)-concentrated cross-Internet Service Provider (ISP) spectrum assignment framework for SDONs. By eliminating centralized control and fostering coordination between QoS-based inter-ISP traffic, SpectrumChain increases QoS signaling during ISP routing, thereby enhancing and optimizing operational efficiency.

The correlation between revenue increase and heightened spectrum sensing participation underscores the potential for better-utilized spectrum resources. A multi-operators, multi-access Points (APs) distributed spectrum management scheme [87] for unlicensed spectrum sharing introduces a lightweight consensus mechanism, termed Proof of Strategy (PoS). This mechanism addresses overhead issues associated with spectrum-related blockchain deployment, optimizing the entire spectrum to achieve maximum global revenue. The optimization encourages greater participation from nodes in the spectrum sensing process, subsequently elevating the efficiency of spectrum sensing and allocation.

While combining blockchains for spectrum sensing yields advantages, opportunistic spectrum access schemes often consume substantial time, limiting the available window for sensing and access. To address this, [72] proposes an optimization approach that balances sensing and mining times, maximizing spectrum utilization and achievable throughput. The research demonstrates that the original optimization problem can be decoupled into sub-optimal problems of sensing and mining times, offering a nuanced solution.

In summary, prevailing Blockchain-based DSM optimization approaches meticulously tackle challenges in spectrum sensing by focusing on participation improvement, optimizing sensing and mining times, and boosting global revenue. Energy-aware DSM assumes prominence, recognizing that less energy-efficient methods deter miners from participating in spectrum sensing, consequently yielding suboptimal revenue. In tandem, efforts have been directed towards efficient resource allocation schemes, furthering the cause of spectrum sharing and optimization.

B. SECURITY

1) INTRODUCTION

Addressing security concerns is paramount in the realm of DSA and DSM, as attacks manifest across various dimensions, posing threats to spectrum sensing, DSA, spectrum trading, and mobility. The deceptive behavior of nodes within DSM systems gives rise to a spectrum of attacks, encompassing Denial of Service (DoS), system penetration, repudiation, spoofing, authorization violation, malware infection, and data modification. Integrating blockchain technologies into DSM architectures emerges as a robust solution to mitigate these attacks, particularly in the context of monetary-based transactions in spectrum marketplaces. Security challenges within DSM markets include replay attacks, interference generation in tradable spectrum bands, and collaborative attacks. Spectrum markets, in general, are susceptible to spoofing and DoS attacks, requiring lightweight security protocols tailored for resource-constrained environments. Attacks on SS often target the MAC layer and with the proliferation of opportunistic DSA, the likelihood of attacks increases, necessitating specialized security measures. Notably, data falsification attacks and primary user emulation attacks undermine spectrum management systems, leading to suboptimal decisions and deceptive SUs pretending to be primary users. Additional threats include DoS attacks on spectrum sensing and sharing, message spoofing to identify idle spectrum bands, and service disruption attacks. Greedy resource occupancy attacks pose substantial threats to secondary users, introducing delays in spectrum access. These disruptions can propagate across networks, known as overlapping secondary user attacks [88]. Mitigating these security challenges involves employing frequency hopping techniques, spread spectrum methods, and leveraging ML for data analysis or reputation-based trust models to detect and prevent malicious users, thereby fortifying the resilience of the DSA system.

2) HOW BLOCKCHAIN HELPS

The scarcity of spectrum resources, exacerbated by the proliferation of machine-type devices, necessitates innovative solutions for efficient utilization. Addressing challenges related to privacy and security threats, a blockchain-based framework proposed by [77] emerges as a robust solution for secure spectrum sharing between human-to-human (H2H) and machine-to-machine (M2M) communications. This framework employs SCs and a distributed, immutable blockchain structure to establish secure contracts for

spectrum sharing, enhancing overall security and efficiency in the process.

In the context of DSA, effective spectrum sensing is crucial but faces constraints due to node scarcity, narrow sensing ranges, and security considerations. Lv et al. [89] introduce the Blockchain-Based Spectrum Sensing (BBSS) system, leveraging blockchain to enhance security in spectrum sensing. This system ensures secure and benefit-distributed participation by encrypting transaction information through a public-private encryption scheme, thereby rendering the decryption process virtually impossible. Reference [90] proposes a blockchain-based method for detecting malicious users in CRNs, which can reduce the accuracy of spectrum sensing, especially in cooperative spectrum sensing. The method uses cryptographic keys to distinguish between trustworthy users and MUs, thereby improving the performance of cognitive radios.

Traditional centralized approaches to DSA, reliant on fusion centers, are vulnerable to single-point failures. Pei et al. [71] present a blockchain-based DSA framework that introduces decentralization and built-in protocols for cooperative spectrum sensing. By eliminating the need for a fusion center, this framework protects against single-point failures and ensures secure, distributed updates of sensing and access results.

Security in spectrum trading, a critical aspect given the limited nature of spectrum resources, is often overlooked in auction-based schemes. Zhu et al. [91] propose the Blockchain-based two-stage secure spectrum Intelligent Sensing and sharing Auction mechanism (BISA), emphasizing security aspects in spectrum trading. This cloud-edge corporate method utilizes blockchain for secure spectrum trading, demonstrating its effectiveness in reducing security risks associated with centralized third-party reliance, double-spending attacks, and privacy concerns.

To address the challenges in UAV-based spectrum trading and sharing within non-terrestrial networks, Qiu et al. [97] propose a secure scheme based on blockchains. The blockchain-based framework enhances security, leveraging a Stakelberg game to maximize profits for MNOs and UAV operators while mitigating the risks associated with malicious users.

In CR Networks, effective spectrum sensing is vital for opportunistic spectrum access. Jain et al. [98] introduce blockchain-based SCs to enhance the privacy of participation-related transactions, ensuring users adhere to contracts after being awarded rewards. In CRN-based Internet of Vehicles (IoV), Rathee et al. [99] propose a blockchain framework that addresses security concerns in spectrum sensing. Using the Technique for Order Preference by Similarity to the Ideal Solution (TOPSIS), the framework improves security against various attacks, achieving a substantial improvement in attack detection and report generation.

For CRNs related to the Internet of Battlefield Things (IoBT), ProBLeSS, a proactive blockchain-based spectrum sharing protocol, is introduced by Patnaik et al. [76]. This protocol effectively counters Spectrum Sharing Data Falsification (SSDF) attacks, showcasing its superiority in comparison to traditional protocols. In the context of collusion attacks in CRNs, Zhang [100] propose a novel blockchain-based secure spectrum sensing method that utilizes historical transactions to monitor and identify collusion attacks, enhancing overall security.

In the CBRS system, Qiu et al. [97] introduce a blockchain-assisted DSM model. This model improves security and efficient management, providing enhanced QoS for General Authorized Access (GAA) users without compromising security and privacy.

Blockchain-based solutions contribute significantly to mitigating security challenges in various aspects of DSA Table 5 and DSM. Decentralization, encryption, and SCs play pivotal roles in ensuring the security, integrity, and efficiency of spectrum-related processes, thereby addressing the multifaceted security concerns outlined in the literature. Further research is needed to explore blockchain solutions for specific attacks such as jamming, common control channel attacks, and the integration of AI in DSS.

C. PRIVACY

1) INTRODUCTION

Ensuring privacy in a DSM system, particularly within SAS, presents a critical challenge. SAS mandates the sharing of sensitive information, including real-time locations and identities, among spectrum sensing nodes, raising concerns about potential exploitation by malicious entities for economic, political, and security purposes. The intricate balance between preventing information disclosure and maintaining the operational effectiveness of spectrum management is highlighted. The disclosure of such details, while essential for decision-making, introduces security vulnerabilities, such as the validation of nodes contributing to spectrum sensing [101]. Striking a balance between privacy preservation and effective spectrum management is pivotal for safeguarding individual rights and reinforcing the overall security of the DSM system. Ongoing research endeavors are vital to devise innovative mechanisms that ensure robust spectrum management without compromising participant privacy.

2) HOW BLOCKCHAIN HELPS

Blockchain technology plays a pivotal role in enhancing privacy across various aspects of DSA and DSM. In spectrum sensing, maintaining the confidentiality of sensing nodes' geographical locations is crucial to preserving privacy. The Blockchain-oriented Location Privacy Preserving (BoLPP) framework, proposed by Vuppula and Pradhan [73], specifically designed for CSS in 6G networks, utilizes blockchain and an energy detection technique to fortify the system against malicious attacks. BoLPP demonstrates superior performance compared to other mechanisms, such as Friend

TABLE 5. DSS security vulnerabilities and existing BC-based solutions.

Aspects of Security on DSA	Security Vulnerability	Description	Esixting BC based solution
Attacks on Spectrum Sensing	Overlapping SU attacks	Transmissions from malicious users within a particular network causes DoS to PUs and SUs in another network	Modifying the modulation scheme, Detection and prevention of attacks, Using authentication and trust models can be carried out via BCs [93]
	Single point failures	Inherent to centralized Spectrum sensing schemes, crowd sensing	BC Based Spectrum Sensing (BBSS) [90] in which nodes involved in spectrum sensing and obtain and distribute benefit securely, time slotted-based BC framework all SUs act cooperatively for the spectrum sensing process
Attacks of Spectrum Mobility	Masquerading/ Primary User Emulation	Attacker is pretending to be a PU	Frequency hopping, BC based malicious user detection and reputation schemes [94]
	Jamming	Attacker is jamming the communication link forcing to increase the time required to select a new channel	Broadening the operation range of CR
	Common Control Channel attacks	Attacker gain the control of common control channel	Securing control channels via AAA process, BC based Solutions needed to be explored
Attacks on Spectrum Management	Collusion attacks	Multiple malicious SUs act together to improve the reputation of nearby nodes to their own benefit	BC-based historical transaction identification scheme [95]
	Greedy Resource Occupancy Attacks [96]	SUs keep using the allocated spectrum band without resharing it	BC based approaches have not been considered so far
	Spectrum Sensing Data Falsification (SSDF) / Byzantine Data Falsification Attacks	Type of a DoS attack where the attackers modify the spectrum sensing report in order to compel the cognitive sensor node to take a wrong decision regarding the vacant spectrum band in other's networks	Efficient Filtering / Robust CR performance using BC platform [97]
Attacks against the Learning Engine	Poisoning Attacks	Manipulating an AI model's input data to compromise its training data sets and accuracy	BC based approaches has not been considered so far
	Evasion Attacks	Avoid detection by targeting AI systems security/ anomaly detection scheme	
	Surrogacy	Creates an identical version of the target model - surrogate model	
Attacks on Spectrum Trading	Double Spending Attacks	Making a second transaction with the same data as a previous one that has already been validated on the network.	BC-based temporary anonymous transactions along with BC hierarchical frameworks [92]

or Foe (FoF) and Tidal Trust Algorithm (TTA), emphasizing its effectiveness in safeguarding location privacy (see Figure 8).

In H2H systems aiming to opportunistically allocate underutilized spectrum for M2M communication, privacy concerns pose significant challenges. Zhou et al. [77] propose a blockchain-based framework that prioritizes privacy, incentivizes users through SCs, and ensures spectrum efficiency. Through the use of public and private keys and digital wallets, the framework replaces true addresses with public keys, preserving the privacy of Base Stations (BS) and PUs.

In the realm of the Industrial Internet of Things (IIoT), where spectrum auctioning is a potential solution for addressing secondary user access issues, Liu et al. [74] introduce a blockchain-based spectrum auction method for 6G mobile networks. The privacy of users is guaranteed through SCs, offering a fair and secure auctioning process. Blockchain-based spectrum trading and sharing systems, such as the one proposed by Liu et al. [75], not only protect

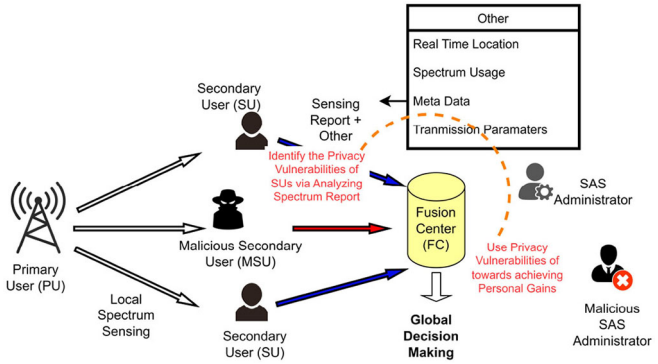

FIGURE 8. Privacy Vulnerabilities of Spectrum Sensing.

user privacy against various attacks but also ensure efficient management by diverting transactions to edge computer nodes for confirmation.

In the realm of spectrum auctions, Yu et al. [79] introduce a secure scheme leveraging blockchain and cryptography to protect bidders' identities and bid privacy, while also safeguarding against collusion attacks. Bidders initially broadcast bids and generate unique blockchain addresses using SHA256 hash functions on their ECDSA public keys, ensuring identity protection by allowing bidders to generate numerous addresses with the same private key. Additionally, a privacy-preserving double auction mechanism based on differential privacy [102] is proposed, enhancing the accuracy of data transactions and minimizing the risk of information leakage in auction environments.

Moving away from centralized database approaches in spectrum sharing, Tu et al. [78] present a blockchain-based dynamic spectrum-sharing framework. This framework incorporates a differential privacy-based, privacy-preserving double auction mechanism using SCs. The specific information required for spectrum bids is stored securely in the blockchain, creating a hash address recorded in an SC. Users access their encrypted public keys stored in the blockchain, ensuring secure bid sharing. To further decentralize and protect spectrum user privacy, Xiao et al. [103] propose BD-SAS, a blockchain-based decentralized SAS architecture. It features a G-Chain for global SAS service state synchronization and L-Chains for local spectrum access management. Privacy is upheld through user information obfuscation, striking a balance between privacy preservation and task functionality.

Addressing challenges in spectrum allocation for large-scale IoT devices, Zhang et al. [104] propose a Directed Acrylic Graph (DAG) blockchain-enhanced user-autonomy spectrum sharing model. This model leverages swarm intelligence and ring signatures to ensure privacy during spectrum sharing. Meanwhile, Ye et al. [105] focus on real-time geo-location privacy of sensor nodes, proposing a trust-centric privacy-preserving blockchain for DSA. This protocol combines ring signatures with a unique commitment scheme

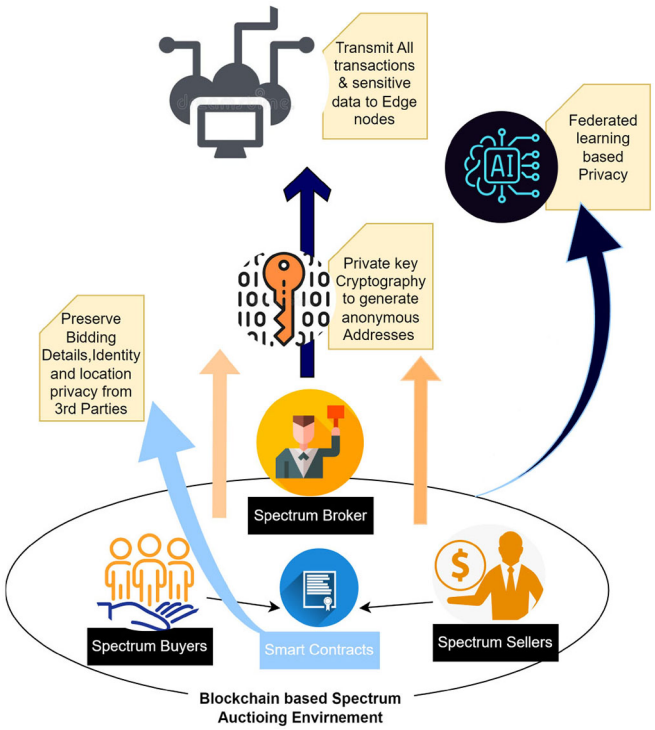

FIGURE 9. Spectrum Auction related Privacy Preservation methods.

to counteract privacy leakage during cooperative spectrum sensing.

For effective and privacy-preserving operations in the CBRS, TrustSAS [106] presents a trustworthy framework based on blockchain. It employs the multi-server PIR protocol to extract data securely without compromising privacy-related information. In a blockchain-assisted DSM mode [107] for the CBRS, the privacy-related information is accessible to a limited group of users, and user registration with the system is mandatory for accessing the spectrum.

Privacy preservation is a common theme across these diverse applications, addressing location and identity privacy concerns. Blockchain-based solutions, incorporating cryptographic techniques and decentralized structures, contribute significantly to ensuring privacy in DSA, management, sharing, and related fields (see Figure 9).

D. IMPROVE SCALABILITY

1) INTRODUCTION

In the realm of DSM, addressing the escalating number of nodes, including IoT devices and diverse stakeholders, presents a formidable challenge. The surge in nodes imposes a substantial burden on DSM systems, necessitating effective strategies for managing millions of nodes efficiently. Furthermore, the proliferation of Local 5G Operators (L5GOs) in the context of 5G and B5G networks compounds scalability concerns, particularly as L5GOs often lack the autonomy to directly purchase spectrum bands, adding complexity to the scalability issue. Blockchain emerges as a

promising solution to confront these scalability challenges in DSM. BC-based solutions exhibit the capability to support an extensive number of nodes, offering a scalable framework to accommodate the growing demands of DSM ecosystems. However, achieving scalability must not compromise timeliness, as the efficiency of managing nodes in real-time is crucial. Overcoming existing bottlenecks in traditional BC architectures, especially ensuring timely processing, is imperative. Enhancing scalability without sacrificing decentralization and security, the foundational principles of BC, requires innovative approaches, including the development of more resource-efficient consensus mechanisms and the exploration of architectural changes within BC frameworks. Striking a delicate balance between scalability, decentralization, and security is crucial for advancing BC's capabilities in the evolving DSM landscape with a growing multitude of nodes and stakeholders.

2) HOW BLOCKCHAIN HELPS

The decentralized nature of blockchains plays a crucial role in improving scalability, particularly in scenarios involving a surge in nodes, such as IoT devices and stakeholders. For instance, SpectrumChain [86], designed for Software Defined Optical Networking (SDON) in EONs, leverages blockchain to enhance QoS-focused spectrum assignment. By incorporating blockchain to share QoS-based information, SpectrumChain significantly reduces the number of messages, enhancing the scalability of SDONs.

Scalability challenges are also addressed in the context of spectrum trading between Virtual Optical Networks (VONs). Ding et al. [108] introduce a blockchain-based spectrum trading platform, allowing VONs to trade spectrum resources without real-time fluctuations affecting capacity assignments. The distributed nature of blockchains is harnessed to scale up the system, providing a robust solution.

Improving processing speed and transaction rates is pivotal for scalability. Ye et al. [105] present a trust-centric privacy-preserving blockchain for DSA in IoT networks, incorporating a Proof-of-Trust (PoT) consensus mechanism for scalable high Transaction Per Second (TPS). This innovation demonstrates a reduction in computation cost, enhancing the scalability of blockchain-based DSA systems.

In the realm of spectrum sharing and energy trading for IoT, Zhang et al. [109] propose the Spectrum-Energy Chain, a secure framework utilizing a consortium blockchain and DAG. This framework efficiently manages the growing number of micro-transactions, addressing scalability concerns and ensuring secure spectrum sharing and energy trading.

The scalability of blockchain networks can also be achieved by modifying the blockchain architecture. Hu et al. [110] introduce a blockchain and AI-empowered Dynamic Resource Sharing (DRS) architecture. The hierarchical structure of blockchains is leveraged to resolve scalability issues, demonstrating an innovative approach to maintaining distribution, security, and automation while enhancing scalability.

In the context of Radio Access Networks (RAN), Blockchain Radio Access Network (B-RAN) [111] strives to unite trustless sub-networks into a large-scale trustworthy cooperative network. The two-tier blockchain structure of B-RAN addresses scalability concerns arising from collaborations among geographically close locations, demonstrating a novel geographical proximity-based approach to enhance scalability.

Architectural changes and innovative methods are combined in various examples. Cheng et al. [112] propose a blockchain-based spectrum trading mechanism for CBRS. Their approach involves a queuing mechanism and a multiple blockchain architecture with cross-chain spectrum trading to improve scalability and efficiency in intra-coexistence group (CxG) trading, showcasing the integration of both architectural enhancements and performance improvements.

In summary, existing blockchain-based scalability solutions encompass performance enhancements, hierarchical network architectures, or a combination of both. Performance improvements include reducing redundant communication through blockchain integration, novel consensus mechanisms, or blockchain-based DAG approaches. Architectural changes involve introducing AI, creating multilateral groups, and employing features like sharding. The most effective solutions often combine these approaches to create a holistic platform that addresses scalability challenges comprehensively.

IV. BLOCKCHAIN BASED SERVICES FOR DSM

Various aspects of DSM such as Spectrum sensing and mining, spectrum trading and auctioning, and spectrum sharing and monitoring can all benefit from BC-based services. For instance, SCs and the ability to integrate AI can be used to automate every aspect of DSM while providing some level of autonomy, and Spectrum marketplace can benefit from enhanced service level agreements, reputation management, tokenization, and violation detection. Furthermore, all these services brought forth by BCs complement each other: spectrum sensing will benefit from reputation management, tokenization, and SCs. (See Figure 10)

A. AUTOMATION VIA SCS

1) INTRODUCTION

SCs, within the context of blockchain technology, represent executable programs stored in a blockchain, enabling the execution of transactions in a trustworthy, traceable, and immutable manner. Their distinctive feature lies in their ability to be initiated by any node within the blockchain, facilitating interaction with others in a distributed fashion. This decentralized nature ensures that the underlying blockchain network upholds security requirements. The popularity of SCs is steadily rising due to their transactional nature, which eliminates the need for a trusted third party. This adoption is particularly evident in novel business entities, showcasing the growing significance of SCs in modern transactions (See Figure 11). The decentralized

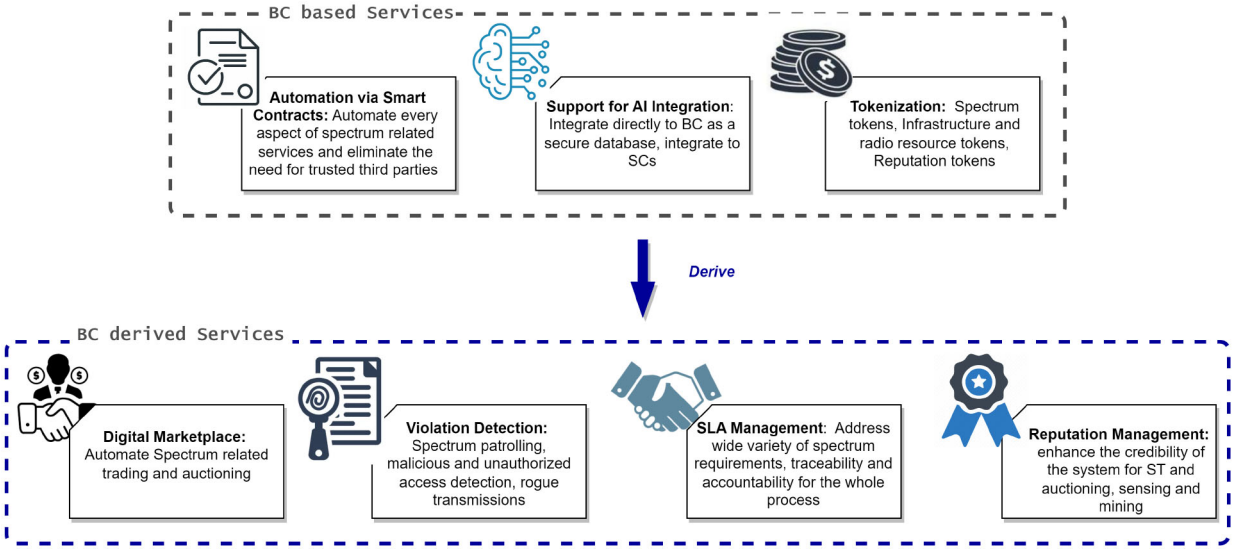

FIGURE 10. Blockchain-based Services for DSM.

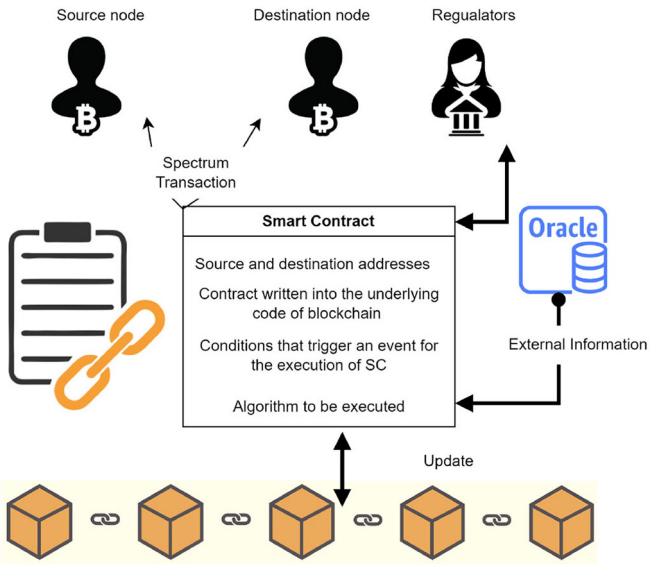

FIGURE 11. Operations of SCs under DSM.

and zero-trust characteristics, coupled with consensus-based security, transparency, and automation capabilities, position blockchain-based SCs as a promising technology. This is especially relevant in the realm of dynamic spectrum sharing for 5G and beyond, aligning with the envisioned scenarios outlined in recent surveys [113]. The transformative potential of SCs lies in their ability to revolutionize DSM, offering a secure, transparent, and automated framework that addresses the evolving needs of advanced communication networks.

2) HOW BLOCKCHAIN HELPS

The integration of SCs in DSM brings forth numerous benefits, transforming the landscape of spectrum access, sharing, and management. As the demand for spectrum increases, particularly in higher frequency bands, DSA becomes essential. Traditional centralized architectures often face challenges such as interference and capacity loss. Leveraging SCs addresses these concerns and ensures the protection of PUs rights. For instance, a smart contract-based DSA scheme proposed by [114] prioritizes the organized execution of DSA, safeguarding PUs' rights and ensuring interference prevention.

The scarcity of sensing nodes and security issues are major hurdles in achieving a fully functional DSA architecture. Reference [89] introduces a Blockchain-Based Spectrum Sensing (BBSS) system, utilizing SCs to enhance spectrum sensing. Through a reward-based sensing time game, this system employs SCs to optimize rewards for both sensing and recruitment nodes, demonstrating increased rewards for both parties involved.

Dynamic spectrum sharing requires efficient spectrum resource management, necessitating easily accessible yet secure databases. Reference [115] proposes a solution using blockchain, SCs, and an intelligent contract database to achieve transparent and secure data-sharing in dynamic resource-sharing scenarios. Additionally, [116] showcases a Distributed Ledger Technology (DLT)-based spectrum authorization system that utilizes SCs for decentralized, automated, and verifiable trust in spectrum sharing and trading.

Spectrum trading, a complex task, benefits significantly from SCs. Reference [14] proposes a decentralized blockchain-based dynamic spectrum acquisition scheme that automates spectrum trading processes, making real-time DSA feasible. SCs, such as those introduced by [114], facilitate advertising and sensing-based spectrum sharing for various leasing scenarios, enhancing the efficiency of spectrum leasing agreements.

SCs prove instrumental in ensuring security, transparency, and efficiency in wireless network virtualization. In [14], a decentralized blockchain-based dynamic spectrum

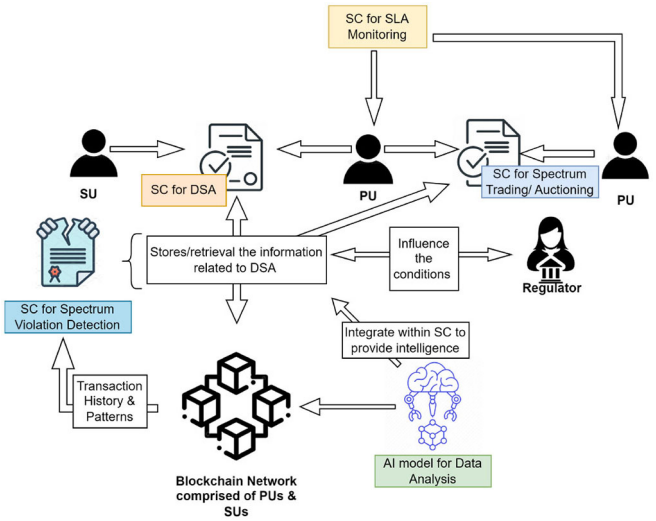

FIGURE 12. Use Cases of SCs for DSM Operations.

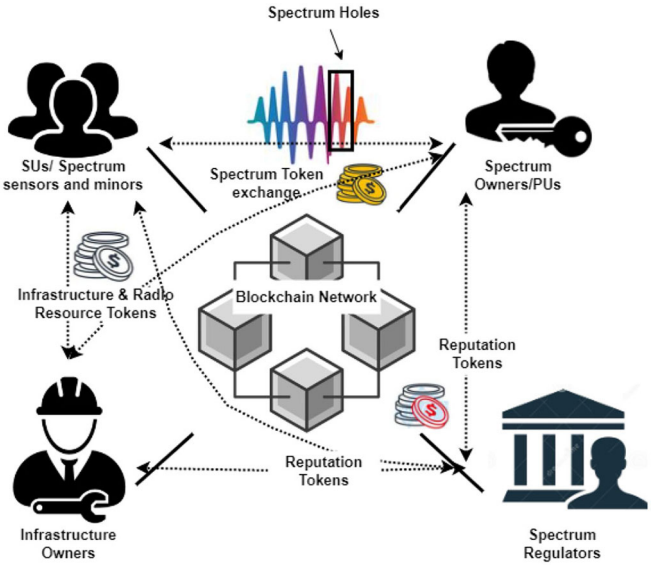

FIGURE 13. DSM Token Exchange.

acquisition scheme minimizes transmit power while satisfying data transmission rate thresholds. Additionally, privacy-preserving double auction mechanisms, based on SCs and differential privacy, [102] enhance user privacy and spectrum resource allocation in an untrusted environment.

In the context of Multi-Operators Spectrum Sharing (MOSS), [117] introduces a permissioned blockchain trust framework that utilizes SCs for automatic spectrum trading and payment transferring among multi-operators. The immutability of SCs enhances security, protecting against malicious activities in DSA.

For CBRS in 6G or B5G networks, [118] proposes a consensus mechanism PoS, utilizing SCs to prevent single-point failures in spectrum allocation. Reference [103] introduces a decentralized SAS architecture using SCs to securely and efficiently provide SAS services without relying on the trust of individual SAS servers.

SCs also address privacy concerns in SAS, as discussed in [106]. They enforce channel usage rules and ensure fair sharing of spectrum resources, mitigating interference among SUs. Overall, the application of SCs proves beneficial across various aspects of DSM, enhancing security, transparency, and efficiency in spectrum access and management (See Figure 12).

B. TOKANIZATION/TOKEN ECONOMY

1) INTRODUCTION

The integration of digital tokens and tokenization processes plays a pivotal role in revolutionizing DSA management and sharing, adding a layer of efficiency, security, and flexibility to the spectrum trading ecosystem. Tokens, generated using SCs, offer superior programmability, allowing for intricate and automated execution of spectrum-related processes. Blockchain-based tokenization serves as a powerful tool to represent ownership of spectrum assets, particularly in terms of space and time, enhancing fluidity in the spectrum market. Various token types, including reward, security, utility, governance, and asset tokens, find utility in the spectrum domain. Spectrum tokens, representing legal ownership of diverse spectrum bands, enable decentralized and transparent trade within the blockchain-based system, ensuring scalability and efficiency in the market. Beyond spectrum rights, utility tokens play a crucial role in managing access to spectrum resources and can be exchanged for asset tokens, signifying ownership or rights to specific spectrum bands. This dynamic exchange process introduces interoperability and financial fluidity to the spectrum market, unlocking new possibilities for precise and accessible spectrum resource management within the blockchain ecosystem (See Figure 13).

2) HOW BLOCKCHAIN HELPS

To implement a blockchain-based DSM system successfully, it is crucial to address key challenges such as evaluating the trustworthiness of nodes' spectrum sensing data, ensuring privacy protection for participating nodes, and developing lightweight consensus algorithms. One notable solution, presented in a study on privacy-preserving blockchain for DSA in IoT networks [105], introduces a trust-centric approach. This includes a specific trust evaluation mechanism and a PoT consensus mechanism, incentivizing nodes to participate actively in spectrum sensing and promoting accurate sensing. Tokens play a central role in this context, with nodes providing accurate sensing data having a higher likelihood of obtaining tokens. The consensus mechanism, by assigning higher trust values to accurate nodes, further increases their chances of obtaining tokens through mining.

Another example in the realm of DSA, as proposed in [71], introduces a cooperative-sensing-based DSA framework. In this model, Spectrum Users act as both sensing and mining nodes in a blockchain network. Tokens are employed to incentivize SUs to participate in spectrum sensing and

mining. The implementation includes a heuristic-based sensing-mining policy, determining optimal bidding based on buffer occupancy and available tokens. Compensating PUs fairly for sharing their licensed spectrum is essential for conflict-free DSA operations. A blockchain-based platform, incorporating a token named Spectrum token [114], has been proposed. This token validates and tracks licensed bands, enforcing sequential access by SUs without interference through SCs.

In the context of 6G networks, precise spectrum sharing is vital to prevent underutilization. A blockchain-based spectrum and infrastructure sharing model [119] among multiple MNOs introduces tokenization. Three SCs facilitate semi-persistent, dynamic, and intelligent spectrum trading. Radio Resource Tokens (RRT) for tradable radio resources and Infrastructure Resource Tokens (IRT) as stable coins with a static price are introduced. Another instance, as outlined in [80], involves blockchain-based spectrum sharing among nodes, incorporating game theory. The proposed Praft consensus algorithm considers malicious nodes, and a reinforcement factor analyzes strategies based on spectrum occupancy, influence of PUs, and enthusiasm. Information obtained by PUs is encrypted, and tokens are sent to SUs along with a digital signature.

Furthermore, a blockchain-based spectrum resource optimization and trading scheme [120] for satellite communication is presented. This scheme aims to maximize satellite system benefits and enhance spectrum utilization. Tokens play a central role, with terrestrials acquiring tokens by acting as trustees or through charging. The survival of the secondary spectrum market (SSMs) depends on licensed spectrum and infrastructure by Primary Licensed Operators (PLOs). A blockchain-based automated pricing model [121], featuring a token called Spectrum Dollar, addresses secondary radio spectrum trade. Spectrum Dollars help eliminate malpractices of PLOs, reducing spectrum reuse costs. Notably, recent efforts have focused on developing blockchain-based token systems between operators and users within multi-operator environments for trading in wireless communication networks [117].

In summary, tokens are pivotal for DSM, incentivizing participation, managing access, promoting fine-grained infrastructure sharing, ensuring fair compensation, and eliminating malpractices. The emerging trend of NFTs holds promise for representing digital assets in DSM, suggesting the need for further research in integrating NFTs into the dynamic spectrum landscape.

C. MONITORING OR SLA MANAGEMENT

1) INTRODUCTION

The realm of mobile networks faces escalating challenges in managing SLAs due to the expansive array of requirements and spectrum use cases. The intricate nature of these challenges has prompted the adoption of blockchain technology, offering inherent capabilities to revolutionize SLA management. Blockchains, through their decentralized architecture,

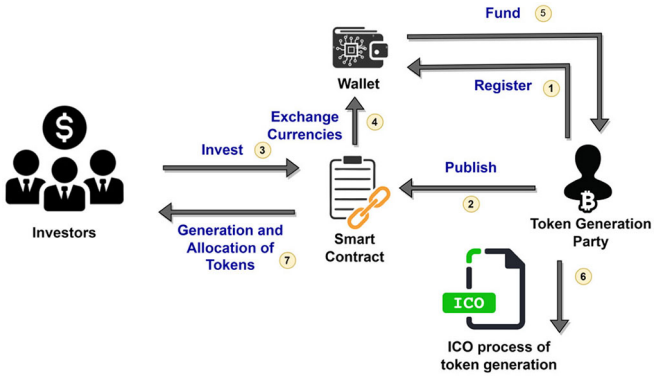

FIGURE 14. Initial Coin Offering Token Generation Process.

provide a secure foundation for SLA management, mitigating the complexities associated with virtualization and network-slicing architectures. SCs within blockchains play a pivotal role by ensuring traceability of network resources, bolstering accountability, and automating the entire SLA process. The transparency and tamper-resistant features of blockchains enhance audibility, maintaining a secure record of actions and transactions in the dynamic mobile network environment. Automation capabilities, facilitated by SCs, streamline SLA execution, reducing errors and disputes. Notably, blockchain-enabled network slicing emerges as a key solution, allowing the creation of isolated, virtualized network instances tailored to specific SLAs. This dynamic adaptation ensures continuous monitoring of customer-devised SLAs, fostering a responsive and adaptable infrastructure. In essence, blockchain technology introduces a decentralized, secure, and automated paradigm to SLA management, addressing the multifaceted challenges of modern mobile networks.

2) HOW BLOCKCHAIN HELPS

In the context of B5G, the evolving spectrum management landscape necessitates a reevaluation of existing architectures to meet heightened performance expectations and accommodate fine-grained spectrum sharing. SLAs have traditionally imposed overhead on networks, forcing trade-offs between factors like price, coverage, and QoS when selecting a MNO and data plan. A transformative solution is offered by a blockchain-based spectrum and infrastructure-sharing platform, as proposed in [119]. This platform leverages three SCs to facilitate quasi-real-time service provisioning between MNOs and users. The trustless MNO environment, often challenging for interoperability, is addressed through a blockchain-enabled SDN approach [122] for managing radio spectrum access over small cell networks. SCs validate transactions between MNOs, ensuring secure and efficient management of spectrum access and business-level agreements. Automation of SLAs' complexities is achieved through SCs, enabling dynamic spectrum negotiations. Another blockchain-based platform, proposed in [123], focuses on secure SLAs among MNOs, Mobile Virtual Network Operators (MVNOs), and regulatory bodies. SCs

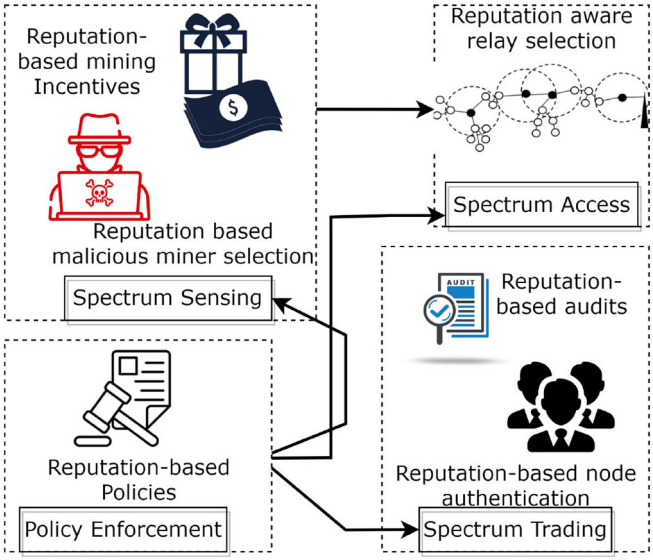

FIGURE 15. Use Cases of Reputation Schemes for DSM.

within this architecture streamline SLAs, enhancing QoS for subscribers compared to opportunistic MVNO approaches. The integration of SDN enhances spectrum management, providing seamless roaming and introducing flexibility and programmability. Challenges in incorporating SLAs into SDN are addressed by a proposed Blockchain and SDN Architecture for Spectrum Management in Cellular Networks [122]. This framework employs SCs to instill trust among MNOs, simplifying billing processes and roaming settlements, thereby streamlining the spectrum management lifecycle. The intersection of blockchain and SDN offers a novel and robust approach to addressing SLA complexities and fostering interoperability in the dynamic landscape of mobile network operators.

D. REPUTATION MANAGEMENT

1) INTRODUCTION

The concept of node reputation emerges as a potent tool with diverse applications, finding utility in various scenarios, particularly in the logical fusion of sensor node results. Calculated based on the transactional and behavioral history of nodes, this reputation serves as a robust metric stored transparently and in a distributed manner within a blockchain network. Beyond enhancing the credibility of the system by employing reputation methods for node selection, this mechanism significantly contributes to the efficacy of spectrum-related trading, spectrum sharing, and the refinement of spectrum sensing and mining accuracy. By incentivizing node participation, reputation methods play a pivotal role in encouraging active engagement. Furthermore, the strategic deployment of reputation mechanisms serves as an effective deterrent against malicious node activities, thereby fortifying the security of the network (Refer to Figure 15).

2) HOW BLOCKCHAIN HELPS

The reputation of nodes involved in spectrum sensing and mining plays a pivotal role in ensuring the reliability of spectrum-related processes. In contexts such as CR-based opportunistic spectrum access, where effective corporate spectrum sensing is crucial, the reputation of participating nodes becomes paramount. To address this, a blockchain-based SCs approach, as outlined in [98], employs a reputation parameter and a money-locking scheme to enhance the efficiency of calculating reputation based on recent sensing accuracy. Similarly, another framework for smart contract-based distributed spectrum sensing [124] incorporates a reputation-based incentive algorithm within SCs to incentivize and reward SUs for spectrum sensing activities. Automating spectrum sensing via SCs, as proposed in [125], introduces an incentive mechanism that encourages sensor nodes to take correct actions while penalizing malicious nodes. Active nodes with higher reputation scores receive rewards, fostering a trustworthy SS environment.

The dynamic nature of CR networks poses challenges in achieving stringent spectrum access requirements. A Reputation-Aware Relay Selection with Opportunistic Spectrum Access method [126] combines relay selection and opportunistic spectrum access using blockchains through a cross-layer method. This involves Secondary Relays (SR) receiving access to the spectrum based on their virtual wallets, representing SRs' secrecy capacity and behavior. Rewarding or penalizing SRs is determined by a mathematical framework that assesses the trustworthiness of nodes, with an offline blockchain storing relay information to detect reputable and non-reputable relay nodes. Reputation values calculated for relay nodes are fed into an ML model to discard non-reputable relays.

In spectrum-sharing scenarios, reputation schemes are integral to ensuring resource sharing is free from malicious nodes. For CR-based Internet of Battlefield Things (IoBT) networks tackling SSDF attacks, the ProBLeSS protocol [76] utilizes blockchain and reputation-based incentives to secure spectrum sensing data integrity. Integrating a game theory-based TFT approach, a blockchain-based spectrum-sharing system [82] incentivizes corporate users to engage more in spectrum sharing. The reputation scheme evaluates spectrum quality, usage information, and security, aiding regulatory authorities in making efficient spectrum resource management.

In spectrum trading, the reputation of nodes becomes crucial for authenticating participants. For instance, a consortium blockchain-enabled secure spectrum trading framework for UAV-assisted cellular networks [97] incorporates a reputation-based miner selection. This ensures that edge computing nodes with higher reputation act as reliable miners, enhancing consensus reliability in spectrum trading. Another decentralized blockchain-enabled spectrum trading framework [127] proposes a reputation scheme where highly reputed nodes can audit and verify transactions and block

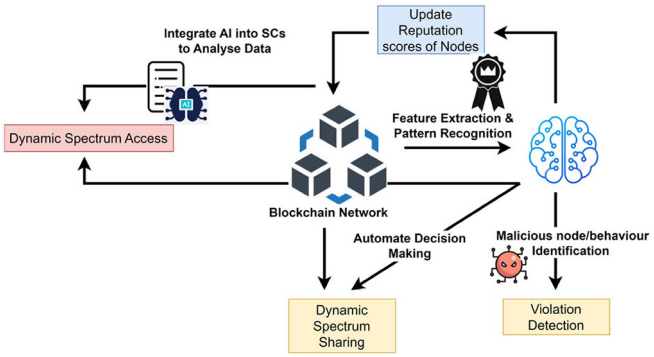

FIGURE 16. Integrating AI into Blockchain-based DSM.

correctness. In a satellite-based spectrum trading framework [128], a blockchain with edge computing employs a reputation-oriented node selection scheme, preventing malicious nodes from entering the spectrum trading process.

Lastly, for enforcing spectrum policies and detecting anomalies, SenseChain [129] utilizes blockchain to access the reputation of sensor nodes. The distributed nature of blockchain, along with its consensus mechanism, helps extract the reputation of sensor nodes, facilitating accurate anomaly detection and identification of malicious nodes. The reputation is established through a financial incentive mechanism that rewards validators and sensors for their contributions.

E. SUPPORT FOR AI INTEGRATION

1) INTRODUCTION

Achieving a decentralized and dynamic spectrum resource management platform necessitates a synergistic integration of blockchains and ML. While blockchains serve as a distributed ledger to record spectrum-related transactions, ML plays a pivotal role in analyzing these transactions and elevating spectrum-related decision-making to new heights of autonomy, fostering increased intelligence within the system. To illustrate, leveraging deep learning-based approaches facilitates automatic feature extraction, reducing operational costs significantly. Additionally, employing deep reinforcement learning methods enables online learning, enhancing efficiency across spectrum sensing, mining, access management, sharing, and trading. This combined approach harnesses the strengths of AI and ML, empowering the entire spectrum management system with enhanced intelligence and operational efficacy (See Figure 16).

2) HOW BLOCKCHAIN HELPS

Spectrum sensing and management are pivotal components of CR Networks, and the convergence of ML and blockchain technologies introduces innovative techniques for efficient spectrum utilization and security. In a groundbreaking approach outlined in [130], a comprehensive ML and blockchain-based spectrum management technique is introduced for CR networks. This model encompasses spectrum sensing, blockchain-enabled spectrum access, and the identification of Malicious Users (MUs). An initial ML-based Extreme Learning Machine (ELM) is employed for spectrum sensing, utilizing the blockchain network to ensure secure spectrum allocation for SUs, while malicious users are identified and blocked from accessing spectrum resources.

Spectrum handoff allows unlicensed users to leave their current channel when a licensed user needs to start another transmission. The SU switches to a different channel to finish the incomplete transmission. The CR system allows unlicensed clients to use channels without licensing, but secondary users must wait for every second. As a solution [131] proposes a hybrid blockchain-based spectrum-sharing algorithm thats based on a Convolution Neural Network (CNN) to automatically extract features.

For spectrum allocation, an advanced multi-layer framework is proposed in [132], decoupling operators and infrastructure planes to enhance flexibility. This model, utilizing a multi-dimensional matrix representation of data flows, facilitates dynamic switching within a multi-operator environment for service provisioning. Additionally, an AI-based workflow for dynamic spectrum allocation among multiple mobile network operators, adapting to various combinations of data flows, is developed. A deep recurrent neural network architecture, specifically Long Short-Term Memory (LSTM), is employed for long and short-term traffic prediction.

Addressing dynamic spectrum allocation, the DeepBlocks scheme [133] introduces a Deep-Q-Network (DQN) to minimize the search state explosion through a reward penalty framework, utilizing blockchain architecture to record transactions related to the dynamic allocation of unallocated spectrum resources to mobile units. SCs are employed to track resource usage and automate spectrum assignments based on DSA profits. Dynamic Resource Sharing (DRS) gains significance for improved resource utilization, and a blockchain-based AI-empowered DRS architecture [110] is proposed. Deep Reinforcement Learning (DRL)-based approaches enhance pattern recognition, improving the decision-making process of DRS and optimizing profit ratios for users.

In the realm of spectrum trading, a decentralized spectrum trading platform is established through Network Slicing (NS) and blockchains for autonomous RAN slicing, as presented in [127]. This hierarchical framework incorporates a three-stage Stackelberg game for incentive maximization and uses a multi-deep reinforcement learning algorithm to achieve Stakelberg Equilibrium (SE). Addressing security concerns in CR-IoT networks, a sophisticated ML model for identifying and clustering malicious CR-IoT users is introduced along with a blockchain-based spectrum sharing framework [5]. Each cognitive user serves as a sensing and mining node, and decision tree algorithms classify them based on spectrum sensing and mining revenue data, enhancing the security of opportunistic spectrum access in CR-IoT networks.

TABLE 6. A Summary of important papers.

Ref.	Technical Aspects				Services					Remarks
	Optimization	Security	Privacy	Scalability	Automation via SC	Tokenization	SLA Management	Reputation Management	Support for AI Integration	
[15]	✓				✓					A decentralized blockchain-based dynamic spectrum acquisition scheme where optimal channel allocation is achieved for minimum energy
[111]				✓					✓	An AI-based DRS architecture is proposed with enhanced security and automation plus DRL has been used for pattern recognition and decision-making in DRS while optimizing the profit ratios for customers
[72]						✓				A DSA framework that utilizes tokens for incentivizing SUs for participating in such energy-consuming sensing and mining, which is based on a sensing-access-mining policy
[82]	✓				✓					A framework for license-free spectrum resource management in CPSSs using SCs with KM algorithm to enhance transaction processing speeds
[85]	✓									A Blockchain-based multi-operator service provisioning with the ability to manage spectrum sharing among multiple operators to minimize spectrum under-utilization
[86]	✓									A BC-based mobile edge computing (B-MEC) framework for adaptive resource allocation and computation offloading where spectrum allocation, size of the blocks, and number of producing blocks for each producer are formulated as a joint optimization problem and optimized via DRL
[78]		✓	✓			✓				A BC based spectrum sharing framework with enhanced privacy, compatibility, and spectrum efficiency
[92]		✓								An intelligent and secure spectrum sensing platform with spectrum auction mechanism (BISA)
[128]		✓						✓	✓	A BC based hierarchical framework for spectrum trading for NS in RAN with a three-stage Stackelberg game framework for joint optimal pricing and demand and a multi-agent deep reinforcement learning (MADRL) method is designed to achieve a Stackelberg equilibrium (SE)
[93]		✓		✓						A BC based spectrum trading protocol STBC (Spectrum Trading Blockchain) with enhanced efficiency and scalability
[98]		✓						✓		A BC privacy-preserving secure spectrum trading and sharing scheme for UAV networks and a Stackelberg game has been used to jointly maximize the profits of the MNO and the UAV operators under both uniform and nonuniform pricing schemes
[100]		✓								Enhanced security scheme for Internet of Vehicle (IoV) using BC is proposed where BC maintains blockchain is used to store every activity and stored information
[77]		✓						✓		A protocol called Proactive Blockchain based Spectrum Sharing (ProBLeSS) is proposed to provide security against SSFD attacks in CR-IoBT networks based on blockchain
[135]		✓								A BC-based platform for security enhancement under spectrum sensing against the malicious user in the CRN using an Adaptive threshold spectrum energy detection algorithm
[104]			✓		✓					A BC-based decentralized SAS architecture to provide services securely and efficiently with smart contract-enabled local blockchains for automating spectrum access assignment
[118]			✓		✓	✓				A permissioned BC trust framework for spectrum sharing in multi-OPs wireless communication networks with the smart contract being used to implement the spectrum trading among multi-OPs

V. BLOCKCHAIN FOR ADDRESSING CHALLENGES IN DSM

DSM confronts a range of complex challenges encompassing interference, security, coordination, reliable sensing data, spectrum violation detection, and spectrum ownership verification. Inaccuracies in channel sensing contribute to interference issues affecting both primary and secondary networks. Security concerns emerge during spectrum sensing

TABLE 6. *(Continued.)* **A Summary of important papers.**

[106]			✓	✓	✓	✓				A trust evaluation mechanism for sensing nodes with a and consensus mechanism-Proof-of-Trust (PoT) to build a scalable blockchain with high transaction-per-second (TPS). Furthermore the framework proposes privacy protection with SCs for automating the process
[107]			✓		✓					A trustworthy framework implemented with BCs to address these privacy issues while adhering to FCC's regulatory design requirements
[109]				✓						A BC-based spectrum trading (ST) platform for trading among VONs in the context of an elastic optical network (EON)
[112]				✓						A BC radio access network (B-RAN) to facilitate trustworthy corporation among massive trustless sub-networks
[120]						✓	✓			A BC based platform for spectrum and infrastructure sharing with a built-in tokenization model for spectrum and infrastructure and feasible consensus algorithms. SCs have been used for service provisioning with semi-persistent, dynamic, and intelligent spectrum trading
[115]					✓	✓				A BC-based spectrum sharing platform with a digital token to validate and track the use of a licensed frequency which enables both advertising and sensing based spectrum sharing under various leasing policies
[119]					✓					A CBRS-Blockchain model with a specialized consensus method called proof-of-strategy that reduce administrative expense of dynamic access system
[130]								✓		A distributed consensus mechanism has been employed to come up with an accurate enforcement system that is capable of detecting anomalies and track reputation of distributed sensors for the enforcement of spectrum policies
[136]	✓			✓						A consortium BC-based DSS framework that enables spectrum trading with assured revenue for each participant
[73]	✓			✓						An algorithm for optimizing spectrum sensing and mining time in a BC-based DSA system
[108]	✓	✓	✓			✓				A novel BC-based DSM in CBRS band to improve spectrum management and QoS for GAA users
[137]				✓						A new BC-enabled spectrum trading framework that also addresses the high energy consumption and latency issues of consensus algorithms
[79]			✓		✓					A BC-based dynamic spectrum sharing framework has been proposed using differential privacy for a privacy-preserving double auction mechanism

and communication phases, necessitating resilient countermeasures. Coordination hurdles persist among SUsvying for simultaneous access to the primary user spectrum. The reliability of sensing data is crucial for the effectiveness of DSA schemes. Spectrum violation detection is pivotal for preserving the integrity of the open spectrum, and verifying spectrum ownership is essential given the limited nature of this resource. Overcoming these challenges is imperative for promoting fairness, efficiency, and smooth operations in DSA scenarios (Figure 17).

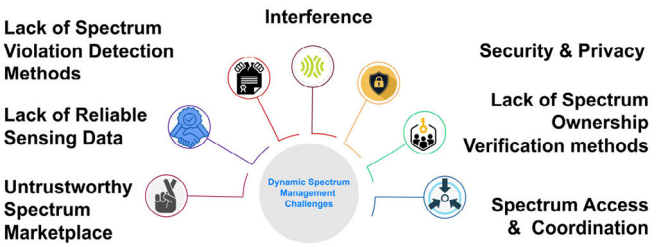

FIGURE 17. Key Challenges in Existing DSM.

A. INTERFERENCE

1) INTRODUCTION TO ISSUE

The issue of interference, both between primary and secondary networks and within secondary networks, constitutes a significant challenge in DSA. Interference to the primary network arises when SUsinaccurately sense the channel as vacant [17]. This leads to concurrent transmissions, causing disruptions for primary users. In the underlay mode of CR networks, interference is intrinsic, demanding that it be maintained at an acceptable level. Several crucial factors influence interference, encompassing the propagation characteristics of the wireless channel (including path loss, fading, and shadowing), the spatial distribution of primary and secondary networks, power control procedures adopted by secondary users, the spectrum sensing schemes in use, and the collaboration between SUsduring spectrum sensing [17]. To mitigate interference, networks can implement policies such as establishing blackout regions where SUs are prohibited from transmitting or imposing a maximum power level for secondary networks. These strategic measures are

vital for ensuring the effective coexistence and optimal performance of DSA systems.

2) POSSIBLE BLOCKCHAIN-BASED SOLUTIONS

Blockchain technology presents a promising avenue for reducing interference in DSA, ensuring fair competition and optimal spectrum utilization. A notable contribution comes from [81], where a license-free spectrum resource management framework for Cyber-Physical Systems of Systems (CPSSs) is proposed. This framework, leveraging blockchain and SCs, divides the local cell spectrum into multiple channels, particularly beneficial for edge computing of non-real-time data. The introduction of blockchain consensus mechanisms, as tailored by the authors, facilitates efficient interference management, preventing collisions and enhancing the overall transaction processing speed without compromising the fundamental attributes of blockchain technology.

An innovative interference-based consensus mechanism is introduced in [137], aiming to enhance transaction efficiency, reduce system overhead, and promote effective spectrum sharing. This mechanism compares aggregated interference experienced by nodes, compensating the most affected node. Additionally, a transaction validation mechanism is designed to prevent harmful interference from spectrum traders, ensuring that validated spectrum transactions stored in blocks contribute to interference reduction.

The use of blockchain-based tokens is explored in [114] as a means to mitigate interference. A spectral token is introduced to validate and track the use of a licensed frequency band, enforcing sequential access by SUs to minimize interference. This token-based access protocol, akin to holding a license for frequency band usage, ensures effective data transmission by limiting interference. With only one user holding the token at a time, this crypto-token-based approach efficiently promotes radio spectrum use while minimizing interference.

In the context of CBRS system proposed by the FCC, [107] proposes a dedicated blockchain-based graph coloring scheme for interference management. The goal is to avoid conflicts among GAA users, addressing limitations in the centralized SAS and central database. This blockchain-based interference management approach provides a scalable solution for efficiently handling large-scale networks and users.

In summary, blockchain applications, such as interference-based consensus mechanisms and token-based access protocols, offer innovative solutions to reduce interference in DSA, fostering fair competition and effective spectrum sharing.

B. SECURITY AND PRIVACY ISSUES

1) INTRODUCTION TO ISSUE

In contrast to traditional wireless networks, DSA and DSM networks face unique security challenges due to the presence of multiple unlicensed users, cognitive capabilities, and reconfigurability [15]. Alongside conventional security concerns, threats such as adversaries mimicking primary user behaviors, transmitting false spectrum information, and selfish actions by secondary user devices pose significant risks during spectrum sensing and communication phases [16], [138]. Privacy preservation, particularly in database-centric DSM approaches, where SUs disclose operational attributes for spectrum availability, becomes a challenge susceptible to exploitation by malicious users [138]. Implementing countermeasures, including transmitter verification, cryptographic signatures, abnormality detection, trusted node-assisted schemes, and blockchain integration for secure spectrum sharing, enhances correctness and security while mitigating potential threats [138]. The centralized fusion center's single point of failure underscores the need for robust security measures in DSA networks. Addressing these security challenges requires adaptive solutions to ensure the privacy and integrity of spectrum-related information, safeguarding against malicious activities in the dynamic spectrum environment.

2) POSSIBLE BLOCKCHAIN-BASED SOLUTIONS

The inherent features of blockchain, including its distributed nature and immutability, play a pivotal role in enhancing overall security. In a spectrum-sharing context, Zhou et al. [77] introduce a blockchain-based framework that significantly amplifies security within the domain. To further fortify security, leveraging the distributed benefits of blockchain involves the implementation of public-private encryption schemes, rendering decryption nearly impossible—an aspect demonstrated in crowd-sensing security by Lv et al. [89].

The absence of a spectrum ownership authentication mechanism introduces a security vulnerability known as primary user emulation, wherein attackers impersonate legitimate PUs, often leading to fraudulent activities. Blockchain's decentralization and consensus mechanisms provide an effective solution through reputation scores. Jain et al. [98] propose a method where malicious activities are identified by analyzing spectrum transactions stored in the blockchain, leading to the assignment of lower reputation scores through consensus. In CRN, identifying malicious users and denying access is essential. Unauthorized access to the spectrum poses challenges, as primary users can share bandwidth with secondary users, but malicious secondary users can access through misusing identity or altering primary signals. Blockchain technology can help improve spectrum management efficiency. Reference [139] proposes a private blockchain-based security scheme to secure spectrum allocation and limit access to only authorized users.

Beyond primary user emulation, collusion among multiple SUs poses a significant threat. Blockchain serves as an interface for integrating ML techniques, facilitating the analysis of data patterns stored in the blockchain to categorize nodes as malicious or non-malicious [5]. This approach, coupled with reputation scores, forms a robust defense

against collusion attacks [94]. Miah et al. [5] introduce an intelligent ML model for identifying and clustering malicious CR-IoT users based on blockchain, providing effective spectrum management.

Automating spectrum transactions through SCs not only reduces the risk of identity exposure but also safeguards private transactions among participants [77]. In summary, the attributes of blockchain, combined with encryption, consensus mechanisms, and ML integration, establish a comprehensive security framework that effectively addresses issues such as primary user emulation and collusion attacks, ensuring secure and trustworthy spectrum transactions.

C. SPECTRUM ACCESS COORDINATION AND SHARING ISSUES

1) INTRODUCTION TO ISSUE

In the realm of CR networks, the coordination and sharing of spectrum access present substantial challenges as multiple SUs strive to access the primary user spectrum simultaneously. Essential for ensuring fairness, spectrum-sharing schemes are imperative, particularly given the dynamic nature of available channels across dimensions like time, frequency, and space. Implementing dynamic MAC strategies is crucial for the proper functioning of the network, with the MAC layer managing spectrum-aware sensing and access control. Various spectrum-sharing methods, including Carrier Sense Multiple Access (CSMA), dynamic frequency hopping, TDMA, and Code Division Multiple Access (CDMA), address challenges such as fluid channel availability and frequency disparities. While significant strides have been made, coordination challenges persist, including establishing sharing agreements between primary and SUsin dynamic settings. Defining proper payment procedures for scenarios involving compensation from secondary to PUs remains an open challenge, emphasizing the importance of resolving these issues for fostering fairness, efficiency, and seamless operations in DSA scenarios within CR networks.

2) POSSIBLE BLOCKCHAIN-BASED SOLUTIONS

Blockchain-based spectrum access represents a substantial advancement in coordination, collision prevention, and transparency, thereby fostering fairer spectrum auctions. Unlike traditional DSA, which relies on a centralized fusion center susceptible to single-point failure, BC decentralizes decision-making by leveraging merged sensing results. Each SU serves as a sensing and verifying node in the BC network, enabling secure and distributed mining and updating of sensing and access outcomes. The introduction of tokens acts as a potent incentive for participation, as proposed by [71]. These tokens serve not only as digital currency rewards but also as spectrum access licenses, creating an auctionable asset that enhances engagement in spectrum sensing and improves access strategies, as emphasized by [81]. The utilization of digital tokens is instrumental in validating and tracking the use of licensed frequency bands, ensuring sequential access by SUs, and mitigating interference. Reference [126] explores the use of blockchain technology for secure relay selection and opportunistic spectrum access in vehicular CR networks. It proposes a cross-layer reliable relay selection scheme, utilizing blockchain as a trustworthy technique to enhance the credibility index of secondary relays and improve network security. SCs play a crucial role in facilitating the seamless transfer of spectral tokens between PUs and SUs, as outlined by [114]. Furthermore, BC significantly bolsters fairness and transparency in spectrum access and allocation through consensus algorithms tailored for DSA, such as the proof-of-strategy method proposed by [118], thereby fortifying the system against single-point failures.

D. LACK OF RELIABLE SENSING DATA

1) INTRODUCTION TO ISSUE

DSS hinges on SUs sensing idle spectrum bands and reporting the data, yet relying on a single SU for spectrum sensing proves inefficient due to the fading effect and shadowing. Cooperative sensing emerges as a solution, presenting numerous advantages over non-cooperative methods [140]. However, spectrum sensing, while valuable for statistical computation, is susceptible to errors in real-world scenarios, potentially leading to inaccurate decision-making [141]. Ensuring reliable channel status diagnosis necessitates most SUs to remain silent during the sensing period, crucial for overcoming challenges related to low Signal-to-Noise-and-Interference Ratio (SNIR) caused by the short distance between transmit and receive antennas. Any SU transmission during sensing introduces significant interference compared to the PU signal, undermining the reliability of the sensing process [18]. The unreliability in spectrum sharing diminishes the efficiency of DSA schemes, resulting in conflicts among participants [142]. Particularly concerning are data falsification attacks, which pose a severe threat to spectrum management systems, leading to sub-optimal decisions and potential Primary User emulation attacks. Thus, ensuring the reliability of sensing data becomes paramount for the robustness and effectiveness of DSA schemes.

2) POSSIBLE BLOCKCHAIN-BASED SOLUTIONS

Blockchain emerges as a pivotal solution to enhance the reliability of spectrum sensing processes, particularly in the face of challenges like potential fading that may discourage SUs from active participation. BC's automated tasks, specialized SCs for spectrum sensing, and robust storage mechanisms prove instrumental in overcoming this challenge. SUs are incentivized to persist in spectrum sensing through thoughtfully designed consensus mechanisms that reward continuous participation, even in challenging environments, fostering a more resilient sensing ecosystem [72]. In a Blockchain-based Distributed spectrum sensing framework, spectrum availability is efficiently advertised, and reputation scores for individual nodes are effectively managed, ensuring the reliability of sensing information. Blockchains' inherent

decentralization and consensus mechanisms enable the identification and rewarding of nodes contributing accurate data while swiftly addressing malicious nodes generating falsified sensing reports [73]. This approach not only streamlines payment processes but also efficiently manages reputation scores in the spectrum-sharing landscape. Unlike traditional DSA relying on a centralized fusion center, which poses vulnerabilities to single points of failure, Blockchain eliminates this issue, significantly enhancing reliability in cooperative sensing settings. In such settings, where SUs function as sensing nodes contributing to the mining process, Blockchain ensures secure operations and prevents the generation of unreliable data [71]. Beyond incentivizing spectrum sensing accuracy, BC-based methodologies, as proposed by [89], collectively contribute to boosting the efficiency, security, and overall reliability of spectrum sensing processes, effectively addressing challenges associated with fading environments and promoting sustained and trustworthy participation.

E. LACK OF SPECTRUM VIOLATION DETECTION METHODS

1) INTRODUCTION TO ISSUE

The detection and prevention of spectrum violations are paramount for maintaining the integrity and lawful utilization of the open spectrum. Given the challenges posed by the open nature of the spectrum, robust enforcement policies are essential to detect and address unauthorized access effectively. Spectrum patrolling, although resource-intensive, emerges as a prominent method, with crowd-sourcing techniques enhancing monitoring and enforcement efforts. Punitive approaches play a vital role in identifying unauthorized behaviors, localizing malicious users, and imposing suitable punishments, as highlighted in [19]. Proactive measures are imperative for preventing unauthorized access, particularly in the context of the spectrum being an open resource. Spectrum management practices must incorporate mechanisms to prohibit interference violations by SUs when PUs are utilizing the spectrum. This ensures that unlicensed SUs can access licensed PUs' spectrum only when it is not in use, as emphasized by [114]. Additionally, addressing SLA violations is crucial, representing a significant form of misconduct. Detecting violations by both PUs and SUs, in breach of stipulated SLA conditions, becomes challenging without robust monitoring and enforcement mechanisms. Effectively addressing these issues is vital to safeguard the integrity of spectrum usage and prevent unauthorized access to these limited and valuable resources.

2) POSSIBLE BLOCKCHAIN-BASED SOLUTIONS

In ensuring a reliable operation of a DSS scheme, safeguarding the individual identities of nodes is crucial to prevent identity violations and misuse of the spectrum. The consortium blockchain-based DSS framework, as presented by [135], not only addresses this concern but also establishes regulators within the blockchain network. These regulators play a key role in regulating and ensuring the secure and robust operation of DSS. The framework utilizes mining and data analysis to synchronize and regulate the DSS process, tracing transaction history for identifying violations. In cases where violations are detected, transactions can be revised or deleted from the block. Additionally, operators undergo certificate authorization before joining the blockchain, and regulators have the authority to remove detected malicious nodes. Violations by Base Stations Operators (BOPs) or Spectrum Operators (SOPs) result in the confiscation of their deposits, ensuring accountability.

A prevalent issue in spectrum management is the occurrence of violations when multiple parties attempt to access the same spectrum band. The blockchain-based system proposed by [143] offers a dynamic channel allocation mechanism to reduce conflicts. This system not only automates communication between SASs among conflicting parties but also achieves consensus through SCs while maintaining the confidentiality of sensitive information. Simultaneous conflicting reports from users, belonging to the same or different organizations, are utilized for the de-confliction process. SCs and SASs work collaboratively to detect channel assignment violations, and SCs are then employed to enforce adherence to underlying channel assignment policies.

The adherence to FCC standards is paramount for access and operations in the CBRS spectrum. TrustSAS, a trustworthy framework proposed by [106], addresses privacy concerns during spectrum sensing processes. This framework utilizes blockchain to ensure privacy protection for SUs and establishes secure channels via SCs for smooth spectrum queries.

To prevent violations of spectrum access, all nodes participating in the spectrum-related marketplace must adhere to underlying regulations and policies. The integration of blockchains into mobile network infrastructure, as proposed by [119], introduces three types of SCs for service provisioning. This scheme supports stakeholders, including end users, spectrum owners, spectrum regulators, and infrastructure owners. Spectrum regulators leverage SCs to enforce high-level policies and constraints, making it challenging to violate these policies.

Furthermore, the combination of blockchains or specifically SCs with 6G hybrid cloud architectures, as explored by [144], is investigated for ensuring stability, security, and energy efficiency in spectrum sharing among Ubiquitous Internet of Things (UIoT) devices. The study demonstrates that SCs can be instrumental in preventing spectrum violations throughout the spectrum transition process.

Monitoring the behavior of nodes is identified as an invaluable method for identifying potential spectrum violations. The framework proposed by [122] utilizes SCs to ensure that all nodes contributing to the spectrum management process adhere to rules issued by a spectrum regulator. This ensures the efficient utilization of the spectrum and enforces penalties against MNOs violating the standards. Suspicious behaviors of nodes are monitored through SCs.

SenseChain, as introduced by [129], is a consensus-employed blockchain-based network designed for reliable and accurate enforcement. This network estimates the reputation of sensors and recognizes falsified sensors through a blockchain-based distributed anomaly detection system. The anomaly detection system is instrumental in detecting violations of spectrum access policies, detecting malicious intent, and separating good actions from bad, assigning a reputation metric to nodes. A novel consensus mechanism, "Proof-of-Sense" is proposed by [145] for a BC-based DSA system. Operating on spectrum sensing procedures rather than cryptographic calculations, this mechanism detects spectrum fraud and prevents unauthorized access by analyzing sensed spectrum data.

In conclusion, the use of SCs plays a pivotal role in detecting and preventing spectrum violations across various aspects of DSM. These mechanisms not only ensure transparency and security but also automate enforcement, addressing challenges related to identity protection, conflicts, privacy, and regulatory adherence. The presented frameworks and systems leverage blockchain and smart contract technologies to create robust, secure, and efficient spectrum-sharing ecosystems.

F. LACK OF TRUSTWORTHY SPECTRUM MARKETPLACE

1) INTRODUCTION TO ISSUE

Due to the scarcity of spectrum as a resource, the existing spectrum trading marketplace has become a highly fraudulent place. One major reason for this issue is the centralized architecture with selfish spectrum trading parties. In addition, the spectrum transactions are not disclosed to parties of interest, while private information related to spectrum auctions and trading leakage can be observed. This creates a highly untrustworthy environment. The current spectrum right transfer takes place as an offline spectrum auction event and most of the [20] spectrum-related trading happens manually. These static contracts due to their low scalability time-consuming nature and high cost are less ideal for automation. All these factors lead to the underutilization of this valuable resource, provisioning overheads, and security issues.

2) POSSIBLE BLOCKCHAIN-BASED SOLUTIONS

Blockchain technology revolutionizes the spectrum marketplace by offering unparalleled features such as immutability, low maintenance costs, security, and transparency. These attributes pave the way for dynamic systems in spectrum management. The decentralized and immutable nature of blockchains enhances the security of spectrum trading systems, enabling transactions without the need for a central trusted party. Automating spectrum trading, auctioning, and related marketplace activities becomes feasible through the integration of blockchain technologies.

Satellite spectrum resource management, particularly in the context of IoT's integration into massive IoT systems, is a pressing issue. A blockchain-based scheme proposed by Wang et al. [120] optimizes spectrum allocation in a satellite system. This scheme employs blockchain to create a novel spectrum trading approach, considering the spectrum's quality and pricing ranges. Differential spectrum pricing, coupled with a pool structure accommodating various quality spectra, effectively addresses the heterogeneity of the Low Earth Orbit (LEO) satellite spectrum.

Blockchain-based solutions extend to spectrum auctioning methods, especially in scenarios where maintaining bidder privacy is crucial. Yu et al. [79] propose a blockchain and cryptography-based auctioning scheme to ensure bidder privacy against collusion attacks in heterogeneous spacecraft networks. The scheme employs a secure spectrum auction framework with a blockchain address based on SHA256 hash functions, enhancing security and privacy during the auctioning process.

To intelligently address the scarcity of spectrum resources due to the proliferation of IoT devices, Blockchain-based Intelligent Spectrum Auctioning (BISA) is introduced. Zhu et al. [91] present BISA, a framework ensuring secure and efficient spectrum auctions with low complexity. The blockchain records all transactions, eliminating self-interested auctioneer traditions from the auctioning process.

In the realm of network virtualization, Zhao et al. [146] propose a blockchain-enabled secure spectrum trading framework. This framework focuses on developing a spectrum trading strategy among operators, subletters, and users using SCs. The blockchain-driven automation reduces transaction overhead and enhances spectrum utilization rates.

Dynamic spectrum trading between VONs in EONs can benefit from blockchain. Ding et al. [108] introduce a spectrum trading scheme that leverages blockchain to match timely fluctuations in capacity, ensuring dynamic and efficient spectrum trading.

Combining blockchain and NS takes the form of a hierarchical framework for blockchain-empowered spectrum trading in RANs. Boateng et al. [127] present this framework, enabling secure decentralized spectrum trading, autonomous RAN slicing, and adjustments in spectrum slices based on traffic demand fluctuations.

Ensuring fairness in spectrum trading is pivotal, and blockchain technologies play a crucial role. Li et al. [135] introduce a consortium blockchain-based DSS framework that adapts MNOs to become either spectrum providers or requesters based on demand. The framework employs a Multi-leader Multi-follower Stackelberg game to ensure fairness, and SCs record spectrum allocations. A new blockchain-based framework for spectrum trading [136], divided into three layers: access, distribution, and core. Each layer focuses on specific functions, simplifying the complex blockchain spectrum-sharing process and maximizing user benefits in spectrum trading matching schemes.

Reputation mechanisms and blockchain empower Decision Support Systems for optimal spectrum trading decisions. Yang et al. [147] propose a novel reputation

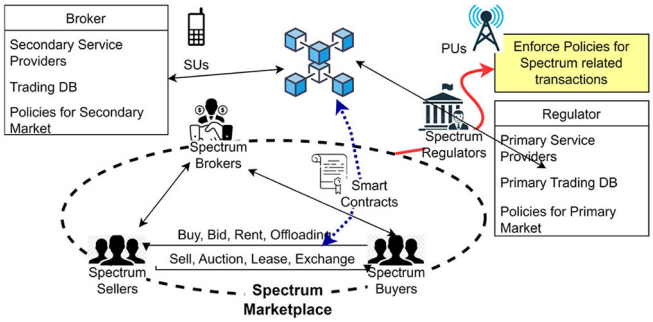

FIGURE 18. BC-based Services for Spectrum Marketplace.

mechanism-based blockchain-empowered DSS system. This system considers historical transaction success rates and communication throughput to enable optimal spectrum trading decisions, fostering a Stackelberg game for incentive maximization.

Blockchain-enabled spectrum trading methods tackle the challenge of secure information sharing among different parties. Lin et al. [115] propose a spectrum-sharing method based on blockchain and intelligent contracts, enhancing data-sharing effectiveness, security, and automation.

Despite the advantages, blockchain-based spectrum trading methods face inherent limitations. Xue et al. [92] present the Spectrum Trading Blockchain (STBC), a decentralized distributed spectrum trading protocol. STBC addresses issues like low spectrum utilization rates, high transaction delays, and energy waste through a novel consensus mechanism, ensuring efficiency and security.

In summary, blockchain technologies bring transformative benefits to the spectrum marketplace by enhancing security, transparency, and automation in trading, auctioning, and related activities (see figure 18. These advancements address challenges in satellite spectrum management, bidder privacy, scarcity of spectrum resources, fairness in trading, and information sharing among different parties. Despite inherent limitations, innovative solutions like STBC and improved consensus mechanisms continue to push the boundaries, making blockchain a pivotal force in reshaping the current spectrum marketplace.

G. NO DIRECT MECHANISM TO VERIFY THE SPECTRUM OWNERSHIP

1) INTRODUCTION TO ISSUE

The verification of spectrum ownership holds paramount importance due to the limited nature of the spectrum, often considered the exclusive property of the government within a country. Ownership of specific spectrum bands is typically regulated by a regulatory body and passed on to exclusive users through a competitive bidding process or a physical event. While exclusive spectrum users/PUs may opt to share the spectrum with SUs, this introduces several security challenges. A key issue arises as SUs lack a clear method for distinguishing between the spectrum bands allocated to exclusive users and potentially malicious users. This lack of differentiation leads to conflicts among all parties involved in the spectrum-sharing process, as highlighted in [21]. The consequence is interference and degradation of QoS within the exclusive spectrum users' allocated bands, emphasizing the critical need for robust mechanisms to verify and authenticate spectrum ownership in DSA scenarios.

2) POSSIBLE BC BASED SOLUTION

The utilization of NFTs, a blockchain-based technology, offers a promising solution for authenticating ownership of spectrum bands. NFTs, as highlighted in [148], are on-chain credentials that generate unique, indivisible, and non-interchangeable representations of assets. Integrating NFTs with SCs facilitates the straightforward verification of the existence and attributes of digital assets. In the context of DSA, spectrum can be transformed into a digital asset and corresponding NFTs can be minted, providing a secure and verifiable method for authenticating ownership of spectrum bands. The inherent transferability of NFTs, supported by transparent records of ownership stored in the blockchain, streamlines spectrum-related asset transactions, offering a robust mechanism for verifying and managing ownership in dynamic spectrum scenarios.

VI. BLOCKCHAIN PLATFORMS

A. ETHEREUM

1) INTRODUCTION TO THE PLATFORM

Ethereum, a second-generation blockchain technology, extends the capabilities of traditional blockchain by embracing a broader range of applications. Proposed by Vitalik Buterin, co-founder of Bitcoin Magazine, Ethereum emerged in 2014 with the vision of creating a fully functional open platform for decentralized applications (DApps) [149]. Serving as a decentralized computing platform, Ethereum introduces its cryptocurrency, Ether (ETH). This platform facilitates the launch of applications, databases, and services through SCs, referred to as DApps in the Ethereum context. In an Ethereum network, nodes or computers play dual roles: recording transactions and creating SCs. Notably, Ethereum employs a PoS consensus mechanism, which is more secure, energy-efficient, and scalable compared to the previous Proof of Work (PoW) architecture. The versatility of Ethereum extends to various use cases, including Ethereum coins, Initial Coin Offerings (ICOs), DApps like Uniswap (a Decentralized Automated Exchange protocol), decentralized identities (DIDs), and even real estate transactions where Ethereum facilitates communication between buyers and sellers within a distributed operating system.

2) EXAMPLE SCENARIOS FOR DSM

Ethereum, as a second-generation blockchain, transcends the limitations of first-generation blockchains like Bitcoin by offering a more versatile and programmable platform. Unlike Bitcoin, Ethereum allows users to go beyond digital currency and develop their own programs through SCs. These SCs,

also known as "autonomous agents" when user-programmed, and "multi-signature" accounts when managing participation and providing utility to other SCs, unlock a plethora of use cases.

In the context of DSM, Ethereum-based SCs have been instrumental in the development of spectrum auctioning and trading platforms. These platforms, leveraging the autonomy and security features of SCs, facilitate trading in CBRS band [112]. Additionally, for Heterogeneous Spacecraft Networks, Ethereum-based SCs power spectrum auctioning systems [79], while a consortium model based on Ethereum SCs and DSS is implemented in Hyperledger Fabric for multi-operator scenarios [135].

Ethereum SCs extend their utility to spectrum violation detection through systems like SenseChain [129], which employs a Reputation System for Distributed Spectrum Enforcement. By utilizing Ethereum SCs, violations in the CR environment can be identified, ensuring adherence to specified conditions. Moreover, for spectrum management in SDN architecture, Ethereum Virtual Machines (VMs) are employed to monitor transactions among multiple users, detect frequency access violations, and ensure SLA compliance [122].

In the pursuit of scalability and secure DSA, a Blockchain-based Scalable model has been developed using Ethereum and multiple sidechains connected to the mainchain via bridges [125]. This model harnesses the inherent capabilities of Ethereum blockchains to ensure seamless interoperability and efficient spectrum management.

3) PROS AND CONS

Ethereum brings forth several advantages that distinguish it in the blockchain space. One notable benefit is its support for rapid development, particularly facilitated by platforms like Hyperledger Besu, enabling the swift deployment of private blockchain networks. Ethereum's flexibility extends to accommodating both private and public blockchains, ensuring compliance with regulatory and security standards. It stands out in supporting a massive number of nodes, a crucial factor for spectrum sensing, with its mainnet capable of handling millions of nodes. The introduction of consensus mechanisms like Proof of Authority (PoA), bespoke block times, and gas limits contributes to higher transaction rates, further enhanced by solutions like Danksharding for increased scalability.

Ethereum offers privacy granularity through private transaction layers, encrypting information and restricting access to permissioned parties. Customizable consensus mechanisms, such as RAFT and IBFT, ensure immediate transaction finality based on application requirements. The use of tokens on the Ethereum platform, differentiating it from Hyperledger, enables novel incentive mechanisms like crowd-sourcing data management.

However, Ethereum is not without challenges. Its ecosystem, while diverse, is not confined to a single IT environment, potentially making the codebase more complex. The native language, Solidity, though similar to C++, Python, or Java, may be considered intricate. The broad range of use cases exposes Ethereum to errors, malfunctions, and security threats, posing scalability challenges. Additionally, as Ethereum supports cryptocurrencies, inherent risks associated with digital currency investments are present.

B. HYPERLEDGER

1) INTRODUCTION TO THE PLATFORM

Hyperledger, initiated by the Linux Foundation in 2015, stands as a collaborative effort to develop a robust and high-performance blockchain framework. Unlike Bitcoin or Ethereum, Hyperledger does not function as a cryptocurrency or an independent organization; rather, it serves as a foundational infrastructure for constructing blockchain-based systems and applications. This collaborative venture spans various sectors, including finance, manufacturing, and IoT technology.

Within the Hyperledger umbrella, several projects contribute to its comprehensive ecosystem:

- Hyperledger Fabric: This project offers blockchain-based solutions tailored for business use cases [150]. The defunct Hyperledger Composer, previously a separate layer, has been seamlessly integrated into Fabric.
- Hyperledger Cello: Operating as an on-demand service deployment model, Cello enhances the flexibility and efficiency of blockchain implementations.
- Hyperledger Explorer: Designed to monitor and maintain blockchain development data, Explorer provides transparency and insights into the blockchain network.
- Hyperledger Burrow: Serving as a permissioned Ethereum Smart Contract platform, Burrow runs on the Ethereum Virtual Machine, providing compatibility with Ethereum-based applications.
- Hyperledger Sawtooth: This enterprise-level, modular blockchain platform operates with a permissioned network and incorporates a Proof of Elapsed Time consensus algorithm, ensuring secure and scalable transactions.
- Hyperledger Caliper: As a benchmark tool, Caliper is instrumental in evaluating the performance and efficiency of Hyperledger blockchain implementations.

Hyperledger adopts a layered architecture comprising multiple layers: the consensus layer, responsible for creating agreements and authentication; the SC layer, managing transaction processing and authorization; the communication layer facilitating interaction between nodes; identity management services ensuring secure user access; and an API layer providing a structured interface for seamless integration and development. This layered approach enhances the modularity, security, and functionality of Hyperledger, making it a versatile and reliable blockchain framework.

2) EXAMPLE SCENARIOS FOR DSM

Hyperledger Fabric emerges as a versatile blockchain framework with applications spanning modular architectures,

resource trading, spectrum management, and network slicing. In the context of spectrum sensing in CR networks, Hyperledger Fabric, coupled with HAWK, forms a permissioned blockchain platform, leveraging SCs to define features and roles effectively [98]. Similarly, spectrum trading platforms find a robust foundation in Hyperledger Fabric. For instance, a Hyperledger Fabric-based permissioned blockchain (HFST) powers a spectrum trading platform for resource allocation in optical network virtualization [146]. The platform employs SCs to facilitate trading and is implemented using a consortium network.

Hyperledger Fabric extends its utility to address spectrum-level violations. In scenarios where SLA representation and violation detection are paramount, Hyperledger proves instrumental [151]. Multi-Operator Dynamic Spectrum Sharing utilizes a Hyperledger Fabric consortium network to identify and rectify violations within a multi-operator environment [135]. The platform ensures efficient spectrum sharing while maintaining security through the permissioned nature of the blockchain.

In the realm of network slicing for B5G, the BC-Enabled Network Slicing platform, known as BENS - B5G, harnesses Hyperledger Fabric SCs for consent management and information storage on the blockchain, optimizing the overall slicing process [152]. Privacy-centric applications also benefit from Hyperledger. A Blockchain-enabled Tripartite Anonymous Identification Trusted Service Provisioning for industrial IoT leverages Hyperledger Fabric for secure, efficient, and anonymous access to trusted services [147]. The use of the Raft-based consensus algorithm further enhances efficiency and security.

In the context of 5G RAN, a consortium BC platform for spectrum trading has been developed, utilizing Hyperledger Iroha-based SCs to facilitate secure spectrum trading among multiple providers and requesters [127]. Hyperledger's permissioned architecture and consensus mechanisms ensure the integrity and security of spectrum trading platforms across various applications, making it a reliable choice for blockchain-based solutions.

3) PROS AND CONS

Hyperledger presents a modular architecture with plug-in capabilities, offering developers the advantage of reduced burden and the ability to reuse existing systems in new architectures. Its distinctive feature lies in the development of permissioned blockchains, a contrast to Bitcoin and Ethereum, reducing security risks by limiting access to known, validated entities. Membership service providers further enhance validation in permissioned blockchains. Hyperledger's scalability is notable, achieving faster transaction rates without relying on resource-intensive PoW or crypto mining, meeting the demand for high-performance blockchain solutions.

The security aspect is fortified through the encapsulation of sensitive data, known as channels, providing an additional layer of protection by physically separating critical information. The integration of Hardware Security Models (HSM) ensures the safeguarding of digital keys, enhancing overall security measures. The presence of a vibrant community, comprising experts in blockchain technology, contributes to ongoing development and support for Hyperledger platforms.

However, Hyperledger faces challenges in terms of proven use cases, with its applications yet to be extensively demonstrated and adopted across various industries. Additionally, the scarcity of skilled Hyperledger programmers poses a limitation in unleashing the full potential of this blockchain framework.

C. IOTA

Established in 2015, IOTA stands out as a distributed ledger platform and cryptocurrency distinguished by its unconventional lack of a traditional blockchain. With a total of 2.8 Peta IOTA coins already in existence, the platform eliminates the need for mining. Gaining recognition among the top ten cryptocurrencies, IOTA focuses on facilitating transactions specifically tailored for the Internet of Things (IoT) devices, utilizing a Hash Directed Acyclic Graph (DAG) known as Tangle. Unlike conventional blockchains, IOTA's Tangle relies on participants to engage in the proof-of-work (PoW) consensus process, circumventing the limitations associated with traditional blockchains. Tangle's DAG structure comprises interconnected transactions, validated by solving cryptographic puzzles. Each new transaction involves the validation of two previous transactions, ensuring robust security and preventing spam. To enhance efficiency, IOTA employs advanced tip selection methods like Random Un-Weighted Walk Monte Carlo and Weighted Random Walk. Notable features of IOTA encompass distributed data transactions, real-time micro-transactions with zero fees, a scalable ledger, Masked Authentication Messaging (MAM), and quantum computing protection. MAM facilitates secure communication through encrypted messages and supports remote control commands. IOTA's quantum resistance is achieved via the Winternitz One-Time Signature Scheme. Collectively, these features position IOTA as a versatile and innovative solution for executing secure and scalable transactions within the IoT ecosystem.

Unlike traditional blockchains, IOTA allows for simultaneous transactions through the Tangle network. As a non-blockchain structure, IOTA's cryptocurrency operates independently, and users can choose a wallet that suits their specific needs. IOTA systems are known for their cost-effectiveness, efficiency, and lower power demands, offering instantaneous validation of transactions. A notable application is seen in a novel Electromagnetic Spectrum market implemented using IOTA, as presented in [156]. This market facilitates the trading of both unlicensed and licensed spectrum assets, compensating PUs for leasing their spectrum rights to SUs. IoT devices equipped with spectrum sensing capabilities scan and transmit

TABLE 7. Blockchain-based platform comparison.

Platform	Strengths	Weaknesses	Use Cases
Ethereum [153]	Rapid Deployment Permissioned and permissionless networks Network size - support millions of nodes Private transaction (private transaction layer) Tokenization (fungible and NFT) Interoperability and open source standards (fungible and NFT)	High network and gas fees Difficulty for new users Slow transaction time/scalability issues	Easily deployable SCs and builtin trading platforms facilitating Spectrum trading and auctioning [113], [80] Consortium Blockchains for applications with higher security and privacy [136] Ethereum Virtual Machines (VMs)for monitoring transactions among multiple users [123] Ethereum and multiple sidechains connected to the mainchain via bridges for interoperability [126] Various standards for token development for resource sharing
Hyperledger [154]	Modular architecture - easier plugin and development Permissioned network - support the stringent requirement of private business Performance and scalability - PoW or any other consensus mechanism Channels for data partitioning - enable physical separation of sensitive data Community support - a broad range of membership organizations HSM (Hardware Security Model) - hardware-based digital key protection	Lack of proven use scenarios Tokenization inability	Hyperledger with modular architecture for resource trading, spectrum management, and network slicing [99], [148] Hyperledger customization allows the complex SLA development through SCs [153], [136] Efficient processing due to plugging consensus capabilities [149]
IOTA [155]	higher scalability No transaction fees and micro-transaction capability scalability lightweight Quantum resistance	Lack of research Lack of SCs	Cost-effectiveness, efficiency, and lower power demands, offering instantaneous validation of transactions [158]
Holochain [157]	Highly scalable Low energy	lack of proper research lack of trustworthiness	No works related to DSM has been explored

spectrum opportunities, earning compensation in the form of IOTA crypto assets. Zhang et al. (2021) introduce a DAG blockchain-enhanced user-autonomy spectrum-sharing model to address the challenges of increasing IoT devices in future wireless communication networks, especially in sixth-generation (6G) networks. The model encourages swarm intelligence among users, leading to convergence in the blockchain consensus process. The study explores the impact of the DAG blockchain's tip selection method on spectrum allocation utility, introducing a dynamic tip selection method to enhance global utility. The greedy algorithm is recommended for users with limited computing power to optimize spectrum allocation in dynamic and challenging network conditions [104], [158].

D. HOLOCHAIN

Holochain emerges as an innovative peer-to-peer (P2P) post-blockchain ledger system and decentralized application development framework, offering a compelling alternative to traditional blockchain platforms like Ethereum. Tackling scalability and energy consumption concerns, Holochain introduces a unique toolkit called hApps, distinct from

DApps and free from reliance on blockchain technology. In the Holochain network, individual nodes autonomously secure their data through hashed structures with digital signatures, leveraging Distributed Hash Technology (DHT) for decentralized validation based on predefined rules. Holochain's groundbreaking use of hash chains, ensuring data immutability similar to blockchains, is achieved through iterative hash functions applied to datasets. Notably, Holochain's scalability is enhanced by forgoing resource-intensive mining operations in favor of DHT, resulting in a more sustainable and scalable solution for decentralized applications. The comprehensive architecture empowers participants with individual ledgers, emphasizing a user-centric design philosophy. Users exercise control over their identity, manage data, and seamlessly execute personalized back-end code through the Holochain runtime. Key components include Source Chain, DHT for data redundancy, DNA for functionality, Zomes for core logic, Clients for UI, and Conductors for runtime management. Holochain's departure from the uniform system state model in traditional blockchains reduces replication and consensus costs, showcasing an agent-centric methodology that enhances user control, security, and overall efficiency in decentralized application development [159].

Furthermore, Holochain offers a flexible platform for developing and deploying decentralized applications (dApps) that seamlessly interact with Internet of Things (IoT) devices. The integration of smart IoT applications with Holochain involves various approaches, such as integration through Oracles, enabling dApps to interact with IoT devices and exchange data securely. Holochain facilitates secure and peer-to-peer data exchange between IoT devices and dApps, supporting real-time communication. The agent-driven approach of Holochain allows for decentralized and distributed management of IoT devices, enabling each device to function as an autonomous agent within the network. This approach also emphasizes data ownership and protection, aligning with IoT application principles, giving users complete control over their data, and ensuring privacy and consent. In summary, Holochain provides a robust platform for constructing decentralized applications that seamlessly integrate with and leverage the capabilities of smart IoT applications, enabling developers to create innovative solutions that empower users and facilitate secure, scalable, and autonomous interactions between IoT devices and dApps [160]. Regardless of these features of Holochains, the application of the technology in the DSM setting has not been explored yet.

VII. BLOCKCHAIN DEPLOYMENT CHALLENGES FOR DSM

This section discusses five aspects that could challenge blockchain-based DSM deployments. Although these challenges are common for any blockchain-based deployment, the extent to which each aspect impacts the DSM context differs and can be seen in Fig. 19.

A. FEASIBILITY DUE TO LACK OF STANDARDS

1) INTRODUCTION TO ISSUE

The DSS is standardized by the 3GPP in their releases 15 and 16 while extending to NR in release 17 [161]. This standardization covers the channel access scheme and the migration of the DSS function from LTE to NR. Spectrum violations, however, is not been one of the main focuses of the 3GPP until now. Currently, there is a formidable amount of research conducted on DSA violations, studying on nature of possible violations (i.e., misuse of transmission power, carrier frequency manipulation, or excessive spectrum usage duration) and introducing schemes to evaluate the reputation of the spectrum users based on the violation nature [162]. As stated in Section II-F, blockchain is a prominent solution for detecting spectrum violations and even managing the DSM function within a trusted framework. Standardization for blockchain technology is a complicated matter. The aspects of interoperability among various DLT protocols and frameworks, governance on best practices of decentralized platforms, making a compliant identity framework across different platforms, overall operational security across extended networks, and best practices for safe and secure SCs utilization are the main directives to be considered for achieving a successful standardization. Blockchain technology, specifically its DLT-based deployments, are subjected to standards and regulations by various standardization bodies such as ISO, ITU-T, IEEE-SA, StandICT, ETSI, CEN, CENELEC, and INATBA [163], [164]. However, 3GPP being the prime standardization body for the DSS, hasn't covered the blockchain technology in their releases. That is understandable considering the 3GPP, or other telecommunication or networking standardization bodies, rarely come across blockchain in their scope. DSM-based blockchain deployments in the future will face a standardization dilemma due to this imperceptive progress on regulations.

2) POSSIBLE DIRECTIONS TO MITIGATE

The ETSI, ITU-T, IEEE, and 3GPP are closely working together to standardize the concept related to 5G and its driving technologies, aiding in optimizing the holistic network infrastructure [165]. Such a collaboration is essential for the establishment of standards and regulations for this blockchain-enabled DSS solutions. In fact, blockchain technology provides the perfect framework to guarantee and mediate the regulations to be defined. Since comprehensive studies are already conducted on all viable spectrum-sharing violations [162], they are providing the intrinsic framework to launch the regulations and policies for spectrum violations. Once such policies are defined, and the factors such as allowable transmission and receiving power levels, carrier frequency tolerance, spectrum usage timing, and minimal spectrum access demand are established, a blockchain-based method can be introduced to detect the violations conveniently.

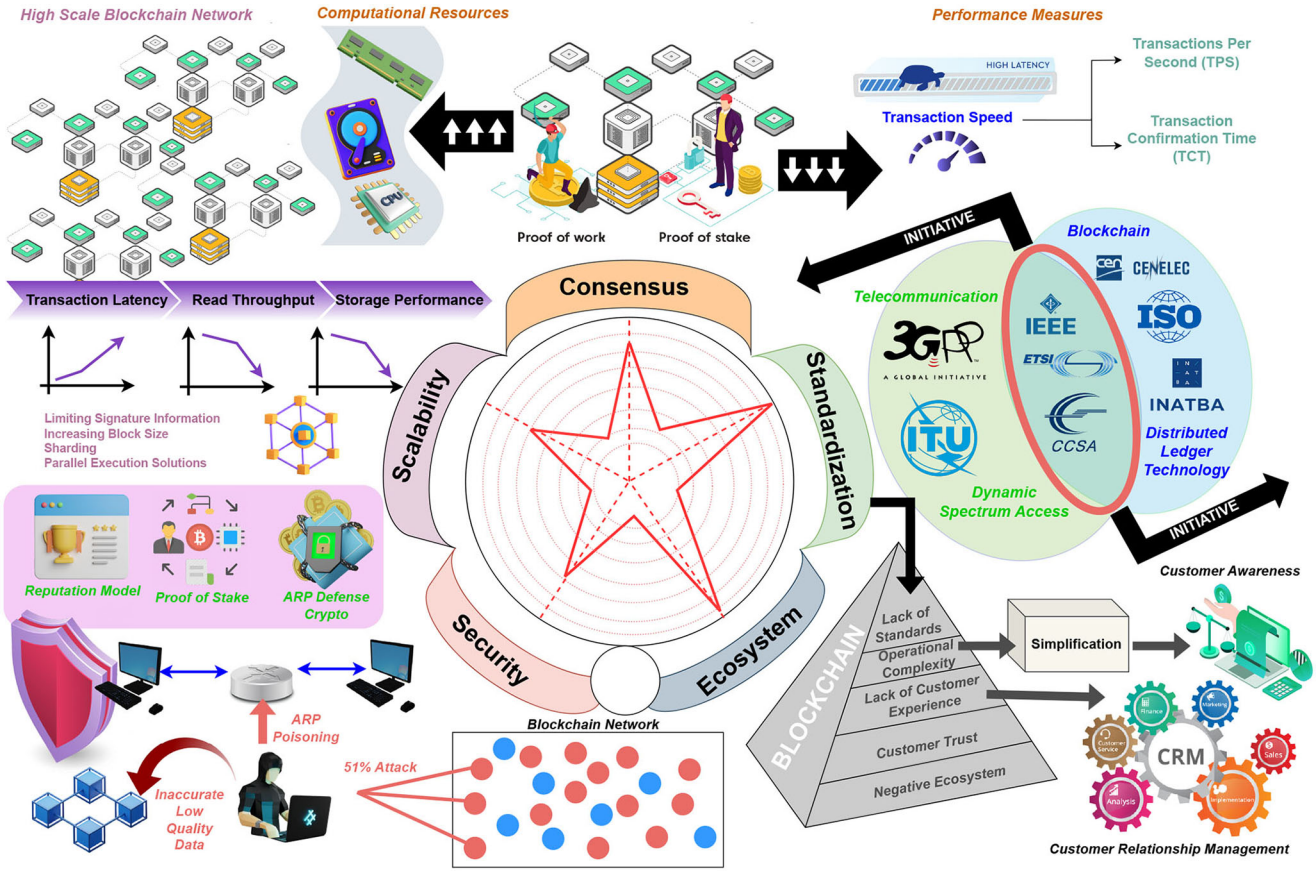

FIGURE 19. Deployment Challenges for Blockchain-Enabled DSM Services.

B. POSITIVE ECOSYSTEM (HOW TO MOTIVATE THE USERS TO PARTICIPATE)

1) INTRODUCTION TO ISSUE

Similar to other economic frameworks, the usability of Blockchain-based technologies is highly reliant on user trust and experience that reflects blockchain's reputation as a viable replacement for current financial platforms. The complexity of its operation is a downside to its reputation. As most consumers tend to rely on simplistic technologies, they understand when selecting their products and services, even in the digital domain, the functional methodology of blockchain presents a massive drawback for its marketing context. Further, for a consumer to switch from an existing functional economic trading platform to a newer platform with higher complexity (i.e., blockchain), the inertia presents a marketing dilemma for blockchain to thrive in the digital economy. Trust is an essential aspect of any consumer trade or business that incorporates various products and services as their merchandise. Formulating trust in the marketing context is divided into calculative approaches based on transaction cost economics and relational approaches based on social psychology and sociology [166]. The trust and trustworthiness of blockchain technology depend on its expertise, reliability, and intent. Available expert knowledge and personnel on the blockchain are quite satisfactory in this era. In addition, the reliability of this technology is well-proven for less scalable and decentralized applications, and the statistics are easily accessible to a regular consumer [167], [168]. Though Blockchain is an institutional technology that offers a new model of economic coordination and governance with the integration of logical, mathematical, and cryptographic means, the intent of its perceived actions is highly reliant on the institutional goals of the governing authority [169]. The recent cryptocurrency marketing manipulations of Pumping & Dumping (P&D) occurrences are not aiding the blockchain technology on its consumer trust front [170], [171]. Despite blockchain being utilized in many fields besides the financial sector, its reputation heavily depends on its financial applications. In the context of blockchain-enabled DSS applications, the stakes are higher for a mobile network operator or a service provider when purchasing a spectrum slot. The above-mentioned aspects weigh in when deciding whether to engage in a blockchain-enabled or traditional DSA scheme presented by the radio spectrum regulatory body. The lack of customer experience studies or models for DSA is another downfall in creating a perfect ecosystem for blockchain-based DSS schemes.

2) POSSIBLE DIRECTIONS TO MITIGATE

Consumer experience is critical for creating a positive ecosystem based on reinforcement provisioned through a proper feedback system for any digital system. In fact,

Customer Relationship Management (CRM) is essential to improve trust in blockchain technology. To this end, Ghazaleh and Zabadi [172] is proposing an Analytical Hierarchical Process (AHP) that weighs in the blockchain investments in the current CRM industry. The dimensions of enhanced security, maintenance of transparency, data challenges, and smart loyalty programs were considered level 2 objectives: that extend to 19 level 3 factors that form the CRM-blockchain model. Such a blockchain-enabled CRM scheme is essential for DSM-based deployments to improve the required trust and accountability of consumer interactions.

C. NEW SECURITY AND PRIVACY ISSUES RELATED TO BLOCKCHAIN

1) INTRODUCTION TO ISSUE

The 51% attack is a well-known blockchain-based security attack that can be perpetrated by a collective of adversaries that control at least 51% of the hashing power in the blockchain network [173]. In this threat, the blockchain can be forked to conduct various altercations to the conducted transactions, as in spending double or triple the amount of its original value. In the context of DSM, this is a highly plausible threat, considering the processing capability available with wealthy mobile network operators. Address Resolution Protocol (ARP) attacks, though they are quite conventional, can pose a threat to novel blockchain applications [174]. ARP threats divert the traffic destined for one or more hosts on a local blockchain network and can expose access to the network. ARP poisoning attacks can be conducted in Man-in-the-Middle (MitM), DoS, or session hijacking manners. The Balance attack is possible against the PoW mechanisms in blockchains [175]. Since the envisaged DSS schemes are to be implemented in the lower layers of the TCP/IP protocol stack, ARP-based threats are a feasible threat that can compromise the entire blockchain-based system. Despite that blockchain can assure the originality of the data, the accuracy of the data instilled into the blockchain cannot be guaranteed [176], [177]. This is creating a poisonous attack that resembles the effect of the blockchain service. In the context of DSM, the accuracy of the entered data is ever so vital.

2) POSSIBLE DIRECTIONS TO MITIGATE

An obvious way to prevent the 51% attack is to change the consensus mechanism from PoW to any other method. Enrolling Proof of Stake (PoS) into the operation would expose the user stake in the system, and can provide the required accountability for the threat. Further, increasing the hashing rate, enforcing centralized consensus, and regular audits mitigate the attack. For preventing ARP-based poisoning threats on the blockchain, statically mapping ARP tables, Dynamic ARP Inspection (DAI), ensuring physical access security, network isolation, and encryption can be presented as solutions. Further, reputation-based systems can be utilized to validate the blockchains' data quality.

D. CONSENSUS (ENERGY AND PROCESSING)

1) INTRODUCTION TO ISSUE

The consensus mechanism is a prime concern of blockchain deployments, specifically due to the higher processing times and energy consumed by the respective processes. Around 30 consensus algorithms are being used currently [174]. The existing blockchain mining strategies are designed as Search-Based Software Engineering (SBSE) problems, where the time complexity $O(2^n)$ is an NP-hard problem. The increment of the complexity of this strategy results in exponential growth in the possible search space of the SBSE problem [178]. The PoW mechanisms in blockchain are used for establishing trust among peers. Such PoW mechanisms employ different cryptographic puzzles (i.e., typically hash algorithms, e.g., SHA256 in Bitcoin) to determine the SBSE outcome. Since studying the frequency of the observable solutions of the SBSE process leads to estimated minimum hashes required to solve the puzzle, a minimum estimate of the energy consumption can be computed for various PoW mechanisms. Assuming that the revenue resulting from mining is higher than the associated cost of the process, an upper bound to the energy consumption can be estimated associating total mining revenue, mining cost, unit energy consumption, minimum reward, and transaction fees [179]. Though, these computations are only covering the energy consumption of the triumphant miner, not the entire energy wasted by other miners. In fact, the Bitcoin network consumes 137.2 TWh of electricity per year according to the Cambridge Bitcoin Electricity Consumption Index [180]. It is evident that the current Proof-of-Work (PoW) mechanisms that crypto-currencies engage in are disproportionate to the respective currency's actual utility [179]. This fact creates a legitimacy concern from the crypto-currency point of view since a standardized currency should feature a constant cost per creation.

2) POSSIBLE DIRECTIONS TO MITIGATE

It is evident that novel consensus algorithms or methods are required to solve this issue on the blockchain. The evolutionary algorithm is an approach followed by [178] for optimizing the energy consumption of blockchain networks. This research has formulated the energy minimization problem as a Search-Based Software Engineering Problem with the objectives of energy consumption, carbon emission, decentralization, and trust. Such a solution is adaptable for DSM-based schemes where the consensus can be attained in an optimized manner to minimize the energy consumption of the miners.

E. SCALABILITY

1) INTRODUCTION TO ISSUE

In spite of its advancements and guarantees offered in the areas of privacy, autonomy, security, transparency, immutability, and efficiency, scalability is a major concern of Blockchain [181]. This constricts blockchain technology

from progressing to its highest potential due to the bottlenecks created through its operational flow (i.e., consensus workflow) in highly scaled applications. The scalability concerns in blockchain technology can be categorized into transaction latency (i.e., writing performance based on block size and block arrival time), read throughput or latency (i.e., the response from blockchain nodes upon a data request), and storage performance. The fact that blockchain-based solutions such as Bitcoin and Ethereum are comfortably overtaken by their counterparts of Visa and PayPal (i.e., 4 and 15 against 1667 and 193 transactions per second) raises the same issue on scalability for Blockchain applications that aim to deploy on a larger scale. As pointed out, in addition to transactions, blockchain generates a higher cost of storage, which would eventually deplete the resources of a capacity-heavy information system over time due to its digital dependency. There is no finite limit to how much data can be appended to a blockchain. Thus, the issues with storage scalability are adverse to transaction scalability as they threaten the sustainability of any blockchain-enabled information system. In fact, storage scalability issues impact the read performance of the blockchain servers by accumulating the load on read access. Mitigation and management of this scalability issue of blockchain are possible by exploiting the trade-off between trust, decentralization, security, and privacy aspects. For instance, a highly-scaled blockchain network might utilize a less complicated consensus for better efficiency.

2) POSSIBLE DIRECTIONS TO MITIGATE

We can follow the same categorization that formulated the scalability issues in revealing the mitigation options for the problem. In managing the write performance load, using segregated witnesses in limiting the signature information [182], and adapting Merkelized Abstract Syntax Tree (MAST) [183] as block size reducing ploys. Further, directly increasing block size, sharding, DAG based solutions, and parallel execution solutions are some of the write performance managing methods. There are various off-chain, cross-chain, and consensus layer solutions that are capable of managing the scalability up to an admissible level. Though these solutions are targeting mainly financial applications, DSM applications can adopt the same principles to mitigate their scalability issues.

Table 8 presents several state-of-the-art solutions available for addressing the issues and their correspondence to the stated challenges.

VIII. LESSONS LEARNED AND FUTURE RESEARCH DIRECTIONS

This section discusses the insights gained during this survey and extends the discussion by pointing out the research gaps in those corresponding areas through research questions, while preliminary solutions that can overcome the stated issues/aspects are listed. Further, the possible future directions are mentioned to provide an understanding of the advancement in each aspect.

A. DSA

1) LESSONS LEARNED

As existing spectrum may be unused or underutilized, DSA can greatly increase spectrum efficiency. Moreover, it can also enable new services, lower the cost of operation for secondary users, and create a potential revenue stream for licensed users. DSA can be divided into different categories. Based on the architecture, we can have centralized and distributed networks. Based on spectrum sensing behavior, we can have non-cooperative and cooperative networks. Finally, based on the spectrum access method, we will have to interweave, overlay, and underlay networks. A device engaging in DSA must fulfill several functionalities. These include spectrum sensing, spectrum management and decision, spectrum sharing, and spectrum mobility. One of the key features of DSA is spectrum identification. Methods for spectrum identification include geolocation databases, energy detection, cyclostationary feature detection, eigenvalue detection, matched filter-based detection, beacon detection, and interference temperature-based detection.

2) REMAINING RESEARCH QUESTIONS

- How to manage interference within a DSA environment:Lack of coordination, bad data in spectrum sensing, inefficient spectrum allocation schemes for dynamic setting, inadequate power control mechanisms
- How to best design the control channel between different entities: Unreliable spectrum sensing methods for the common control channel, interferences
- How to ensure fairness to different users: Spectrum fragmentation on-demand, heterogeneous users, spectrum externalities, challenges due to information asymmetry, regulatory compliances
- How to design more efficient spectrum sensing schemes: Lack of powerful spectrum sensing mechanisms to address noisy and dynamic environments, complexities of existing spectrum sensing schemes
- How to improve security in a DSA environment: Lack of spectrum ownership authentication mechanisms, inability to differentiate spectrum sensing data, lack of spectrum hijacking identification schemes

3) PRELIMINARY SOLUTION

To alleviate interference issues to primary users, current research works have suggested guard regions or exclusion regions around PUs where no secondary transmissions take place [49]. In addition, other research works have suggested a capped transmission power for all secondary user transmissions. Spectrum identification methods have been suggested for both centralized and distributed networks. These include relatively simple schemes prone to error such as energy detection [55], schemes applicable to centralized networks such as geolocation databases [43], [57], schemes

TABLE 8. Blockchain-based solutions for addressing the DSM challenges.

Solution	Ref.	Description	Addressable Challenges				
			Standardization	Ecosystem	Consensus	Security	Scalability
Optimizing Energy Consumption	[178]	Evolutionary algorithms for energy minimization			✓		✓
Reducing the block size	[182]	Using segregated witnesses for limiting the signature size					✓
	[183]	Adapting Merkelized Abstract Syntax Tree					✓
Blockchain Consumer Experience Improvement	[172]	Analytical hierarchical process based customer relationship management model for blockchain	✓	✓			
Reputation system	[184]	Reputation system for mitigating low-quality data inputting to the blockchain	✓	✓		✓	
Novel consensus	[185]	Two tired conses mechanism that combines proof of work and proof of stake			✓	✓	
	[186]	proof-of-hardware-stake (PohS) consensus mechanism and a regulatory mechanism based on a consortium blockchain that scales the consensus through sharding			✓	✓	
	[187]	Hybrid consensus algorithm with PoS and PoW approaches			✓	✓	
	[188]	quantum blockchain designed with randomness, irreversibility, and quantum zero-knowledge proof			✓	✓	
	[189]	Introduces a novel consensus protocol called Delegated Proof of Accessibility (DPoAC) based on secret sharing, PoS random selections, and an interplanetary file system			✓		
	[190]	Quantum computing based consensus			✓		

involving additional spectrum resources such as beacon detection [64], or schemes that have a high level of complexity such as cyclostationary feature detection and eigenvalue detection [15], [62]. In-band and out-of-band control channels have been suggested for the common control channel [37], [191], [192], while methods such as CSMA, CDMA, TDMA, DOSS, SRAC. OS MAC, C MAC, and COMNET have been suggested for spectrum sharing between different SUs[37], [60], [192], [193].

4) POSSIBLE FUTURE DIRECTIONS

Future research needs to address several critical challenges in distributed architectures for spectrum identification. Current methods are limited by their reliance on prior knowledge, resource intensiveness, additional spectrum requirements, lack of resilience, or centralized architectures. Moreover, interference mitigation methods between SUs and primary networks, as well as among SUs themselves, require further investigation. In spectrum sensing, existing approaches for identifying bad data often overlook colluding attacks, emphasizing the need for enhanced mechanisms to detect and filter out such data from decision-making processes. Additionally, there is a pressing need to design scalable and resilient common control channels for distributed systems to ensure efficient communication and coordination among network nodes. Ensuring fairness in spectrum allocation while adhering to regulatory compliance can be achieved through advanced analysis of individual spectrum fragments against global counterparts, all while safeguarding user privacy. Furthermore, addressing security concerns in DSA requires innovative solutions to enable SUs to verify the authenticity of spectrum bands. Utilizing Blockchain-based tokens like NFTs could offer a promising approach to mitigate security risks and enhance trust in spectrum allocation processes. By focusing research efforts on these

areas, we can advance the capabilities of DSA systems, improve spectrum utilization efficiency, and ensure equitable access to spectrum resources while maintaining regulatory compliance and security.

B. TECHNICAL ASPECTS

1) LESSONS LEARNED

The technical facets integral to Blockchain for DSM encompass scalability, security, privacy, and optimization. DSM necessitates a meticulous optimization of all its components to preclude spectrum and resource underutilization. Achieving spectrum-related optimization involves addressing design specifications such as optimal power usage, speed, reduction of idle spectrum holes, identification of innovative methods for balancing spectrum sensing and mining, enhancing efficiency, and minimizing conflicts in spectrum access.

Security threats to DSM span sensing and mining, DSA-related issues, attacks on DSS, spectrum trading-related concerns, as well as assaults on search engines and mobility. Attacks can manifest as disruptions to spectrum sensing, DSA, DSS, spectrum trading, and mobility. In the DSM ecosystem, nodes contributing to the system, including PUs, SUs, or other regulatory entities, harbor distinct goals, rendering the environment vulnerable to various attacks. These DoS attacks, system penetrations, repudiation, spoofing, authorization violations, malware infections, data modifications, on-off attacks, and free-riding attacks.

Mitigating the impact of malicious nodes has been achieved through the integration of Blockchain alongside data analysis techniques, encompassing primitive spread spectrum methods or incorporating ML techniques to monitor and identify transactions within the blockchain network.

Preserving the privacy of nodes contributing to spectrum management emerges as a pivotal requirement within DSM. The necessity to share sensitive information, such as real-time locations, identities, spectrum usage metadata, and transmission parameters, during spectrum access and sharing exposes vulnerabilities that could be exploited by malicious entities for personal gain. With the escalating number of IoT devices and spectrum users, effectively supporting diverse use cases becomes challenging with limited spectrum resources. While Blockchain integration somewhat mitigates scalability issues in DSM, the operational costs associated with it introduce delays, impacting the overall scalability of the system.

2) REMAINING RESEARCH QUESTIONS

- How to jointly optimize other aspects of DSM robustly, and remove the effects of interferences: Inefficient spectrum sensing, resource allocation leads to poor spectrum allocation and interference management, which affects other aspects of DSM. Realizing optimized DSM requires efficient mechanisms designed for the dynamic nature of the system as a whole
- How to address the heterogeneity of applications and their effect on DSM: Diverse requirements and use cases which require fine-grained resource allocation mechanism, capability to identify conflicting requirements, and dynamic workloads
- How to address multi-currency exchange issues while preserving the privacy of DSM: Handling diverse spectrum resources and application requirements among blockchain frameworks
- How to improve scalability under mobile scenarios while reducing spectrum delays under a generalized approach: Existing methods such as off-chain spectrum processing lack security privacy and security, quality of predictive spectrum management methods depends on quality of data (bad data problem in blockchain
- How to detect security and privacy threats in a distributed environment promptly: The transactions recorded in blockchains could be tracked and analyzed, adhering to regulatory compliances, eclipse attacks, Sybil attacks

3) PRELIMINARY SOLUTION

The preliminary solutions of blockchain-based technical aspects aimed at DSM encompass diverse strategies informed by recent research. Wu et al. propose enhanced spectrum game models that foster cooperation and consider the spectrum occupancy of all stakeholders [80]. Choi et al. advocate for reducing spectrum under-utilization through clustering based on specific features [82], while Fan et al. explore blockchain-based methods for achieving the same [81]. Energy consumption of sensing nodes is addressed by Rani et al. through an improvement strategy [83], and Jiang et al. present a decentralized approach for the same purpose [14].

Efficiency gains in DSM processes are pursued by Guo et al. through adaptive optimization among several factors and offloading processing [85]. Additionally, optimizing among spectrum sensing and mining times is proposed by Hu et al. [72], while Chen et al. focus on reducing data redundancies, either through data separation or further analysis to determine patterns [6], [84].

The security of DSM undergoes a transformative shift from centralized to decentralized models, eliminating single-point failures [71], [89]. For secure spectrum allocation under auctioning, Zhu et al. emphasize cautious handling [91], and Boateng et al. suggest leveraging network slicing and virtual networks for securing spectrum trading [127]. The impact of malicious nodes is addressed through identification and isolation, monitored via transaction history [92], [99], [100], or by dissuading their activities [5], [76]. Jain et al. propose utilizing SCs (SC) for private transactions [98].

Preserving privacy in DSM involves a multi-faceted approach. Vuppula et al. suggest a blockchain-based CRN to protect the geographical location of nodes [73], while Liu et al. and Yu et al. recommend using

SC and cryptographic techniques to safeguard privacy during spectrum trading and auctions against collusion attacks [74], [79], [102]. Differential privacy schemes, in conjunction with SCs, are explored by Tu et al. [78], and Zhu et al. propose ring signatures[104] and restrictions on access related to privacy [103].

Addressing scalability challenges, Guler et al. and Ding et al. suggest strategies like reducing the sharing of QoS-based information to pathlets [86], [108]. Improving capacity using SDN and VON is explored by Ye et al. [105], and Zhang et al. propose enhancing transaction rates through application-specific consensus mechanisms, Blockchain-based DAG techniques [109], [194]. Architectural changes involving hierarchy and clustering nodes using ML techniques are suggested by Hu et al. [110], while Ling et al. recommend multi-sided platforms [111]. Combining these architectural changes with improved processing speeds using queuing mechanisms is explored by Cheng et al. [112].

4) POSSIBLE FUTURE DIRECTIONS

Rather than adopting a narrow focus on specific aspects of DSM and tailoring solutions accordingly, a holistic approach to simultaneously optimize various facets of DSM can be cultivated by infusing intelligence into the underlying architecture through AI. While SCs are currently utilized for managing collaboration among multiple operators, enhancing their adaptability by dynamically determining transaction rules based on prevailing conditions within the spectrum environment can significantly elevate their efficacy and responsiveness.

The pivotal strategy to preempt security and privacy concerns in DSM revolves around the proactive detection of malicious nodes. Employing ML techniques such as SVM and K-Means clustering for identifying and isolating these nodes is a foundational step. However, transitioning towards unsupervised ML approaches can enhance autonomy, making the system more adept at identifying malicious nodes independently.

Additionally, the integration of FL into models can fortify security measures by detecting malicious nodes, imposing penalties, and calculating reputations that serve as a deterrent against engaging in malicious activities. Addressing privacy concerns related to multi-currency transactions can be achieved through the implementation of mixcoin, a promising solution that has demonstrated efficacy in enhancing privacy during transactions. This comprehensive and intelligent integration of AI and ML methodologies not only boosts the overall throughput of DSM but also fortifies its security, privacy, and adaptability to evolving spectrum conditions.

C. BLOCKCHAIN BASED SERVICES

1) LESSONS LEARNED

Blockchain plays a central role in various services within DSM, spanning Automation via SCs, Reputation Management, SLA Management, and Tokenization. Automation through SCs streamlines DSM processes, with SCs often coupled with ML techniques for effective detection of spectrum-related violations. Reputation-related services serve as robust tools for executing tasks such as DSA and dissuading malicious users, enhancing security and credibility. SLA Management in the evolving mobile network landscape is bolstered by BC, incorporating virtualization and network slicing for diverse use cases. Tokenization digitizes spectrum-related assets, using tokens as rewards for transactions and incentivizing activities in DSM. Lastly, ML and AI approaches analyze data stored in the BC network, discerning patterns to enhance understanding of DSM dynamics and contribute to informed decision-making. Together, these BC-based services collectively fortify the efficiency, security, and credibility of DSM operations.

2) REMAINING RESEARCH QUESTIONS

- How to address the heterogeneous nature of edge resources: Ensuring interoperability among heterogeneous edge devices with resource diversity for seamless spectrum management, coordinating spectrum sensing among heterogeneous edge devices
- How to incorporate the nature of transactions related to DSM: Coordinating among diverse participants, complex and multifaceted transactions
- How to handle user mobility in a spectrum trading environment: Identification real-time spectrum availability with location and time, pricing of spectrum bands, dynamic network slices to support mobile users with varying QoS demands
- How to implement a spectrum management-auction-transaction system: Managing spectrum licenses after the auction, (leasing, trading, and renewal processes), preventing hoarding or underutilization of spectrum assets, and resolving disputes among license holders
- How to incorporate SLA into SDN such that it facilitates seamless operation: Real-time SLA Monitoring, orchestrating spectrum resources and network services to meet SLA requirements while optimizing spectrum utilization into SDN architecture
- How to detect and prevent spectrum violations promptly: Lack of efficient spectrum violation methods, lack of real-time spectrum usage monitoring methods
- How to address additional cost introduced by SCs towards the scalability of the network: Computational overheads, storage requirements, resource competition that limits scalability of the blockchain-based DSM systems
- How to incorporate DAG-based consensus algorithms to address the scalability and fairness in DSS: Even though DAG-based consensus promises high throughput and low latency, incorporating DAG methods in dynamic environments would come with higher latency
- How to maximize energy efficiency and improve the resilience of incorporating blockchain into DSM: Even though incorporating blockchain into DSM comes with

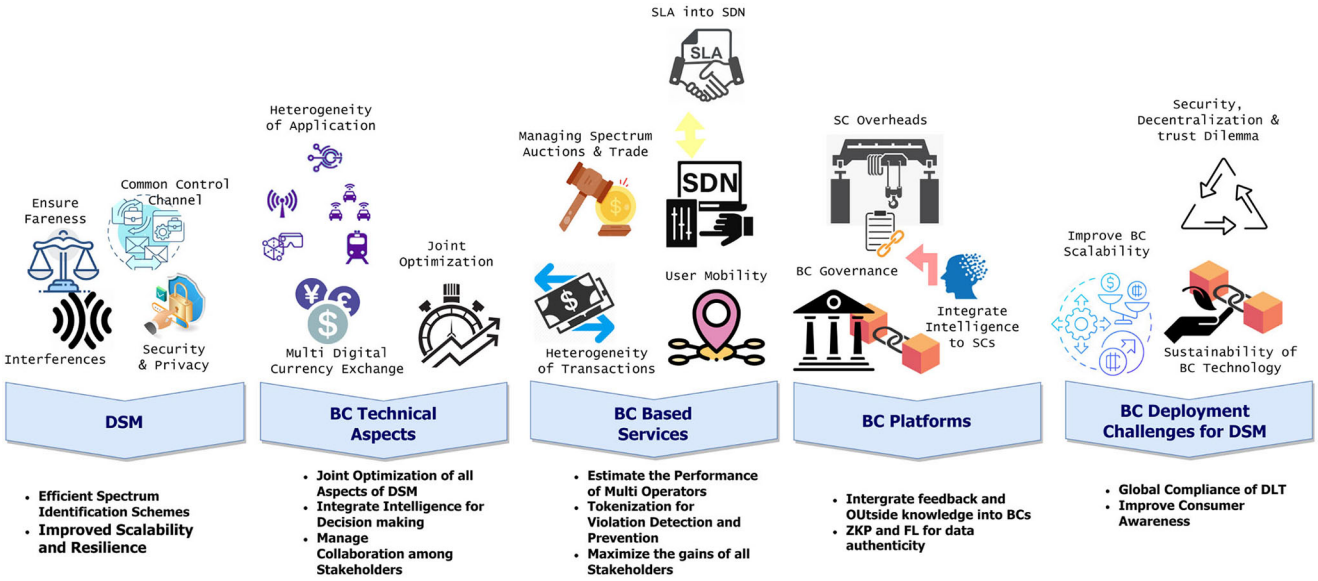

FIGURE 20. Challenges and Future Directions for BC based DSM.

all the advantages the operational overheads and scalability issues require further exploration

3) PRELIMINARY SOLUTION

The decentralized nature of blockchain and SCs play a pivotal role in automating DSA processes, ranging from spectrum sensing to trading, aiming to maximize profits for each party while mitigating interference and avoiding suboptimal decisions [14], [89], [102], [106], [114], [115], [117].

To address scalability issues and reduce SC-related costs, detecting malicious nodes through transaction history analysis stored in BCs is employed [135]. SCs are utilized to automate DSA and prevent conflicts [143], and they regulate spectrum, aiding in the detection of violations [122], [129]. Tokenization emerges as a powerful incentive mechanism for encouraging node participation in spectrum sensing and mining, promoting adherence to rules and standards [71], [105], [114]. Tokens are also leveraged for spectrum trading [117], [120], [121], and they find application in digitizing spectrum trading-related infrastructure and supporting spectrum-sharing SLAs [80], [109], [119]. SLAs are further incorporated into SCs to ensure seamless interoperability among multiple MNOs [119], and SCs facilitate the entry of MNOs into SLAs[122], [123].

Reputation-based services are integral to various DSM aspects, from spectrum sensing and relay node selection to decision-making and policy enforcement. Reputation-based approaches, such as those in spectrum sensing [98], [124], [125], DSA relay node selection [126], DSS addressing malicious nodes [82], and spectrum trading/resource allocation [97], [127], [128], ensure a secure and credible environment. Integrating AI into DSM involves the analysis of data patterns stored in BCs through ML algorithms for early detection of malicious users and optimized spectrum access, enabling intelligent decision-making [110], [130], [132]. RL and DRL approaches like Q-learning gain prominence due to their unsupervised nature [127], [133], while supervised schemes are phased out. The synergistic integration of BC and AI technologies marks a transformative leap in enhancing the efficiency, security, and adaptability of DSM systems.

4) POSSIBLE FUTURE DIRECTIONS

In future research directions, integrating AI and ML techniques holds promise for estimating the performance of multi-operator spectrum marketplaces and identifying potential violations. Expanding on this, ML and tokenization methods can enhance the detection of violations within the spectrum infrastructure market. These detection techniques can be used alongside NFTs and tokens to digitize all resources within networks, making it easier to identify ownership and misuse of spectrum bands, and isolate perpetrators. Similarly, AI and ML techniques can analyze heterogeneous spectrum data collected from edge devices. Novel schemes can facilitate equitable exchanges of spectrum and related resources. DAG-based consensus algorithms could be explored in specific use cases not bound by delay but requiring scalability. Exploring optimization strategies offers an opportunity to jointly optimize spectrum auctioning methods and apply Stackelberg games for spectrum trading, aiming to maximize gains for all stakeholders. Additionally, ML techniques can recognize and categorize various transaction types, grouping them based on spectrum transactions and channel parameters. These categorized transactions, combined with differential transnational recordings, offer a comprehensive approach to understanding and managing different aspects of spectrum transactions. Dynamic SLA Negotiation could be implemented for dynamic negotiation

and renegotiation of SLAs based on changing network conditions and user demands. SDN controllers can dynamically adjust SLA parameters such as bandwidth allocation, latency requirements, and priority levels to optimize spectrum utilization and meet user expectations

D. BC PLATFORMS

1) LESSONS LEARNED

In contrast to the first generation of blockchain networks, the emergence of second-generation blockchain networks such as Ethereum and Hyperledger has introduced SCs. This innovation has empowered developers to launch their cryptocurrency projects and applications, and the utility of SCs has been explored within the domain of DSM platforms. Ethereum and Hyperledger stand out as the most commonly utilized platforms for implementing blockchain in DSM systems. However, beyond blockchain technologies, other DLTs like IoTA and Holochain have also found applications in DSM implementations. Notably, these alternative DLT technologies offer advantages in terms of scalability compared to traditional blockchain platforms.

2) REMAINING RESEARCH QUESTIONS

- How to address overheads introduced by SCs towards scalability: Implementing complex smart contracts for DSM, requires selection/design of energy efficient consensus mechanisms
- How to incorporate AI algorithms as a part of SCs if the AI algorithm does not result in deterministic outcomes: Issues of trust and predictability, change in the behavior of SCs leading towards undesirable outcomes
- How to address BCs scalability issue without compromising Security and decentralization aspects: Balancing security and scalability while exploring alternative consensus mechanisms
- How to develop sound governance models for BC platforms: Designing governance frameworks that are flexible, transparent, and inclusive in a fair manner without hindering participation

3) PRELIMINARY SOLUTION

In addressing preliminary solutions, the Ethereum platform has been instrumental in developing SCs-based spectrum trading platforms [112], [146], as well as DSS platforms capable of detecting violations [112]. Additionally, Ethereum's sidechain feature has been explored for DSA. In contrast, Hyperledger, designed as a collaborative blockchain development platform without its digital currency, has found applications in developing modular architectures [147], SC-based spectrum trading [108], [127], and detecting spectrum violations [135], [143] for DSS. Notably, Ethereum's inclusion of Ether, its digital currency, has led to applications with Tokenization in the context of DSM. Despite Ethereum's initial scalability challenges, Ethereum 2.0's shift from PoW to PoS, coupled with innovations like Danksharding and channels, has significantly improved scalability and security.

4) POSSIBLE FUTURE DIRECTIONS

Future research should focus on enhancing the scalability of blockchain networks while preserving decentralization and security. Additionally, exploring the integration of AI and ML techniques within blockchain networks is crucial. Innovative approaches, such as incorporating oracles into SCs with embedded ML algorithms, can be explored. Oracles, serving as nodes, enable the extraction of external data for triggering events based on both sets of data. While this introduces new possibilities, the complexities and security concerns associated with Oracle nodes warrant further investigation. Moreover, the integration of AI can lead to the development of AI-specific consensus protocols tailored to specific applications. Introducing fog nodes into the network can act as localized cloud platforms, reducing costs and addressing latency issues. XAI technologies could be used to improve trust and fairness in incorporating nondeterministic ML methods-based SCs.

E. BC DEPLOYMENT CHALLENGES

1) LESSONS LEARNED

For any technology to thrive in the current market, proper standardization is an imperative requirement. The absence of standardization would lead to creating doubt in the consumer's mind regarding various aspects such as effectiveness, return on investment, energy consumption, cost efficiency, security, privacy, and ethical conduct. With the approaches that utilize blockchain for DSM however, global compliance is a clear conundrum, since there isn't any common standardization body actively working on the combined subject area of DSM and blockchain. With the hesitancy and confusion created by the lack of standards of the perceived blockchain DSM services, consumer trust is hard to come by. Thus, it is difficult to motivate mobile network operators to use blockchain DSM services. Though accountability and privacy are unique features provisioned by blockchain beyond other digital marketing platforms, it is operational complexity and recent occurrences of pumping and dumping market manipulations could increase the hesitancy from the subscriber front, and alleviates the distrust in the overall service. In addition, security threats that are unique to blockchain-based deployments, such as 51% attacks, ARP-based threats, and data quality concerns can compromise a blockchain service. The mere existence of such threats increases the distrust of blockchain DSM consumers.

It is obvious that consensus mechanisms play a vital role in realizing a feasible blockchain deployment. In fact, the consensus is directly impacting the scalability of the blockchain services. In the context of DSM, with the involved spectrum sensing nodes, novel consensus mechanisms are required that are more efficient than the typical PoW methods. Scalability plays a critical role in Blockchain technology's success in multi-disciplinary industries. It is established that the lack of standards for blockchain in the telecommunication

standardization bodies is restricting the progression of blockchain-enabled DSM-based deployments. Further, to manage the scalability and ensure the sustainability of the blockchain technology as a whole, enforcing the restriction on the limits on a blockchain (e.g., in terms of maximum transactions or storage possible for a blockchain) utilization is quite imperative. For DSM, since the number of mobile network operators or PUs is not highly scalable, scalability is impacting on a moderate scale.

2) REMAINING RESEARCH QUESTIONS

- How to ensure the sustainability of blockchain technology: The key behind sustaining BC-based solutions, in the long run, lies in its scalable and convenient deployment, diverse cost factors, and effectiveness measured in terms of customer feedback for their convenience. Thus, guidelines and requirements/specifications should be formulated to ensure that these metrics are achieved at a satisfactory level.
- How to standardize the blockchain-enabled DSM technologies: Standardization of the BC-enabled technologies in the DSM context amalgamating the expertise of various standardization bodies is a prime requirement to succeed in this directive. Establishing compliance among these bodies on objectives driven by various stakeholders is going to be a challenge that should be studied in depth.
- How to exploit the trade-off between trust, decentralization, security, and privacy of blockchain: The decentralized deployments expected with BC-enabled DSM applications will be considering the additional costs (timing and processing) enforced by the embedded security/privacy/trust ensuring measures of BC. Optimizing this trade-off will enable the long-term sustainability of these deployments.
- What are the most efficient defense mechanisms to be adopted with the blockchain deployments without compromising their performance: Securing BC-based deployments against novel threats that target weaknesses of such systems is a prime requirement. The extent to which these defenses would impact the performance of the BC should be studied circumspectly.
- Which transactional specifications, approaches, or methods are optimal for highly scaled blockchain networks: Scalability should be a prime goal of blockchain development in their design stages. Scalability specifications should be defined based on the application and the nature of the deployment.

3) PRELIMINARY SOLUTION

Despite the lack of initiative among blockchain and DSM standardization bodies, discussions have favored the blockchain-based spectrum-sharing approaches in China Communications Standards Association (CCSA) work groups at their technical report level [195]. Regulations and standardization specifications outlined by such mandates can improve consumer trust and mitigate market violations. Customer relationship management systems are key to understanding the doubts and hesitancies drawn around blockchain-based deployments. The presented solution in [172] can eventually lay the path for improving the customer experience on blockchain DSM services. The security defenses of employing Proof-of-Stake for 51% attack mitigation [173], typical ARP defense mechanisms, and utilizing reputation systems for mitigating the low-quality data inputting [184] can be employed for defending against blockchain-specific threats. There are various novel consensus mechanisms proposed specific and most suited to different applications [196], [197], [198]. These mechanisms are comfortably outperforming the typical PoW consensus mechanisms. In addition to the scalability solutions proposed in Section VII-E.2, application-specific scalability solutions on smart homes [199], and supply chain management [200] state that the scalability aspect can be managed depending on the deployment context and its circumstances.

4) POSSIBLE FUTURE DIRECTIONS

Since ETSI, ITU-T, and IEEE are working together on 5G-related and blockchain technologies, it is imperative to form a workgroup aligning with the respective Industry Specification Group to initialize the standardization process. The already available standardization layouts on DSA and DLT technologies will provide the intrinsic foundation to launch blockchain-enabled DSM services. Since ETSI, IEEE, and CCSA share a common directive on future technologies and are coinciding with telecommunication and DLT-related regulatory domains, they should take the initiative to form these alliances that can achieve global compliance in this subject area. In order to improve consumer trust in the blockchain DSM technologies, the blockchain technology should be explicated in a simplified manner to raise consumer awareness. Further, customer experience on blockchain-related services is vital for the progression of this ideology, specifically for the DSM context. The consensus issues are partly impacting the scalability. Thus, employing lightweight but complex computational methods for consensus, as in quantum computing approaches [190] opens up future research possibilities into new avenues.

IX. CONCLUSION

In this paper, we provide a comprehensive survey on the blockchain-related aspects of DSM. DSM has been shown as the best solution to address the most critical and timely issue of spectrum under-utilization. To get an overview, we provided a state-of-the-art DSM and related taxonomy. Furthermore, several issues with existing DSM approaches have been highlighted taking blockchain as the optimal solution with its added features of SCs, ability to integrate AI, and tokenization all of which provide excellent means of automating the DSM system with added intelligence for decision making and fair and optimal utilization of spectrum

as a resource. The existing unstructured approaches for DSM suffer from a lack of real-time spectrum violation and misuse detection methods, real-time spectrum usage information collection methods, and violation detection methods. This survey identifies the possible research gaps that need to be addressed, depending on the various requirements for DSM under B5G networks.

REFERENCES

[1] C. De Alwis et al., "Survey on 6G frontiers: Trends, applications, requirements, technologies and future research," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 836–886, 2021.

[2] J. M. Peha, "Approaches to spectrum sharing," *IEEE Commun. Mag.*, vol. 43, no. 2, pp. 10–12, Feb. 2005.

[3] T. S. Rappaport et al., "Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond," *IEEE Access*, vol. 7, pp. 78729–78757, 2019.

[4] N. C. Luong, P. Wang, D. Niyato, Y.-C. Liang, Z. Han, and F. Hou, "Applications of economic and pricing models for resource management in 5G wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3298–3339, 4th Quart., 2018.

[5] M. S. Miah, M. S. Hossain, and A. G. Armada, "Machine learning-based malicious users detection in blockchain-enabled CR-IoT network for secured spectrum access," in *Proc. IEEE Int. Symp. Broadband Multimedia Syst. Broadcast. (BMSB)*, 2022, pp. 1–6.

[6] Z. Chen, L. Wang, and Y. Zhang, "Blockchain structure electromagnetic spectrum database in distributed cognitive radio monitoring system," *IEEE Trans. Cogn. Commun. Netw.*, vol. 8, no. 4, pp. 1647–1664, Dec. 2022.

[7] S. Bhattarai, J.-M. J. Park, B. Gao, K. Bian, and W. Lehr, "An overview of dynamic spectrum sharing: Ongoing initiatives, challenges, and a roadmap for future research," *IEEE Trans. Cogn. Commun. Netw.*, vol. 2, no. 2, pp. 110–128, Jun. 2016.

[8] 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.

[9] J. Mitola, "Cognitive radio for flexible mobile multimedia communications," in *Proc. IEEE Int. Workshop Mobile Multimedia Commun.*, 1999, pp. 3–10.

[10] M. M. Sohul, M. Yao, T. Yang, and J. H. Reed, "Spectrum access system for the citizen broadband radio service," *IEEE Commun. Mag.*, vol. 53, no. 7, pp. 18–25, Jul. 2015.

[11] S. Bayhan, A. Zubow, and A. Wolisz, "Spass: Spectrum sensing as a service via smart contracts," in *Proc. IEEE Int. Symp. Dyn. Spectr. Access Netw. (DySPAN)*, 2018, pp. 1–10.

[12] Y. Xu, Y. Xu, and A. Anpalagan, "Database-assisted spectrum access in dynamic networks: A distributed learning solution," *IEEE Access*, vol. 3, pp. 1071–1078, 2015.

[13] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access," *IEEE Veh. Technol. Mag.*, vol. 13, no. 1, pp. 32–39, Mar. 2018.

[14] M. Jiang, Y. Li, Q. Zhang, G. Zhang, and J. Qin, "Decentralized blockchain-based dynamic spectrum acquisition for wireless downlink communications," *IEEE Trans. Signal Process.*, vol. 69, pp. 986–997, Jan. 2021, doi: 10.1109/TSP.2021.3052830.

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

[16] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 428–445, 1st Quart., 2013.

[17] S. Kusaladharma and C. Tellambura, *An Overview of Cognitive Radio Networks*. Hoboken, NJ, USA: Wiley, 2017, pp. 1–17. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/047134608X.W8355

[18] A. Nasser, H. Al Haj Hassan, J. A. Chaaya, A. Mansour, and K.-C. Yao, "Spectrum sensing for cognitive radio: Recent advances and future challenge," *Sensors*, vol. 21, no. 7, p. 2408, 2021.

[19] M. A. Jasim, H. Shakhatreh, N. Siasi, A. H. Sawalmeh, A. Aldalbahi, and A. Al-Fuqaha, "A survey on spectrum management for unmanned aerial vehicles (UAVs)," *IEEE Access*, vol. 10, pp. 11443–11499, 2021.

[20] M. Li, P. Li, L. Guo, and X. Huang, "PPER: Privacy-preserving economic-robust spectrum auction in wireless networks," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2015, pp. 909–917.

[21] H. Xu, Z. Li, Z. Li, X. Zhang, Y. Sun, and L. Zhang, "Metaverse native communication: A blockchain and spectrum prospective," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, 2022, pp. 7–12.

[22] S. Nakamoto. "Bitcoin: A peer-to-peer electronic cash system: Cryptography mailing list." Mar. 2009. [Online]. Available: https://metzdowd.com

[23] W. S. H. M. W. Ahmad et al., "5G technology: Towards dynamic spectrum sharing using cognitive radio networks," *IEEE Access*, vol. 8, pp. 14460–14488, 2020.

[24] Q. Zhao and B. M. Sadler, "A survey of dynamic spectrum access," *IEEE Signal Process. Mag.*, vol. 24, no. 3, pp. 79–89, May 2007.

[25] N. C. Luong et al., "Applications of deep reinforcement learning in communications and networking: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3133–3174, 4th Quart., 2019.

[26] M. B. 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.

[27] 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*.

[28] K. Yue et al., "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.

[29] S. T. Muntaha, P. I. Lazaridis, M. Hafeez, Q. Z. Ahmed, F. A. Khan, and Z. D. Zaharis, "Blockchain for dynamic spectrum access and network slicing: A review," *IEEE Access*, vol. 11, pp. 17922–17944, 2023.

[30] S. Shi et al., "Challenges and new directions in securing spectrum access systems," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6498–6518, Apr. 2021.

[31] Y. Zuo, J. Guo, N. Gao, Y. Zhu, S. Jin, and X. Li, "A survey of blockchain and artificial intelligence for 6G wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 4, pp. 2494–2528, 4th Quart., 2023.

[32] S. Wang and C. Sun, "Blockchain empowered dynamic spectrum sharing: Standards, state of research and road ahead," *IEEE Commun. Stand. Mag.*, vol. 7, no. 3, pp. 72–80, Sep. 2023.

[33] K. Zaheer, M. H. Rehmani, and M. Othman, *Network Coding-Based Broadcasting Schemes for Cognitive Radio Networks*. Cham, Switzerland: Springer, 2019, pp. 65–114. [Online]. Available: https://doi.org/10.1007/978-3-319-91002-4_4

[34] M. Sherman, A. Mody, R. Martinez, C. Rodriguez, and R. Reddy, "IEEE standards supporting cognitive radio and networks, dynamic spectrum access, and coexistence," *IEEE Commun. Mag.*, vol. 46, no. 7, pp. 72–79, Jul. 2008.

[35] S. Filin, H. Harada, H. Murakami, and K. Ishizu, "International standardization of cognitive radio systems," *IEEE Commun. Mag.*, vol. 49, no. 3, pp. 82–89, Mar. 2011.

[36] H. Sawada et al., "Path loss and throughput estimation models for an IEEE 802.11af prototype," in *Proc. IEEE Veh. Technol. Conf.*, 2015, pp. 1–5.

[37] L. Gavrilovska, D. Denkovski, V. Rakovic, and M. Angjelichinoski, "Medium access control protocols in cognitive radio networks: Overview and general classification," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 2092–2124, 4th Quart., 2014.

[38] A. Ivanov, K. Tonchev, V. Poulkov, and A. Manolova, "Probabilistic spectrum sensing based on feature detection for 6G cognitive radio: A survey," *IEEE Access*, vol. 9, pp. 116994–117026, 2021.

[39] C. S. Sum, L. Lu, M. T. Zhou, F. Kojima, and H. Harada, "Design considerations of IEEE 802.15.4m low-rate WPAN in TV white space," *IEEE Commun. Mag.*, vol. 51, no. 4, pp. 74–82, Apr. 2013.

[40] H. Kour, R. K. Jha, and S. Jain, "A comprehensive survey on spectrum sharing: Architecture, energy efficiency and security issues," *J. Netw. Comput. Appl.*, vol. 103, pp. 29–57, Feb. 2018.

[41] C. Jiang, B. Wang, Y. Han, Z.-H. Wu, and K. R. Liu, "Exploring spatial focusing effect for spectrum sharing and network association," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4216–4231, Jul. 2017.

[42] N. Zhang, S. Zhang, J. Zheng, X. Fang, J. W. Mark, and X. Shen, "QoE driven decentralized spectrum sharing in 5G networks: Potential game approach," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 7797–7808, Sep. 2017.

[43] F. Paisana, N. Marchetti, and L. DaSilva, "Radar, TV and cellular bands: Which spectrum access techniques for which bands?" *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1193–1220, 3rd Quart., 2014.

[44] H. Venkataraman and G. Muntean, *Cognitive Radio and its Application for Next Generation Cellular and Wireless Networks*. Dordrecht, The Netherlands: Springer, 2012.

[45] S. Atapattu, C. Tellambura, and H. Jiang, "Energy detection based cooperative spectrum sensing in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1232–1241, Apr. 2011.

[46] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Comput. Netw.*, vol. 50, no. 13, pp. 2127–2159, 2006. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128606001009

[47] S. Srinivasa and S. Jafar, "Cognitive radios for dynamic spectrum access—The throughput potential of cognitive radio: A theoretical perspective," *IEEE Commun. Mag.*, vol. 45, no. 5, pp. 73–79, May 2007.

[48] B. Wang and P. Mu, "Dirty-paper coding based secure transmission for multiuser downlink in cellular communication systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 99, pp. 5947–5960, Jul. 2017.

[49] L. Vijayandran, P. Dharmawansa, T. Ekman, and C. Tellambura, "Analysis of aggregate interference and primary system performance in finite area cognitive radio networks," *IEEE Trans. Commun.*, vol. 60, no. 7, pp. 1811–1822, Jul. 2012.

[50] M. Grissa, B. Hamdaoui, and A. A. Yavuz, "Unleashing the power of multi-server PIR for enabling private access to spectrum databases," *IEEE Commun. Mag.*, vol. 56, no. 12, pp. 171–177, Dec. 2018.

[51] R. Kalidoss, M. Saravanan, and K. Manikannan, "Analytic hierarchy processes for spectrum sharing in 5G new radio standard," *Wireless Pers. Commun.*, vol. 103, pp. 639–655, Feb. 2018.

[52] H. Jiang, T. Wang, and S. Wang, "Multi-scale hierarchical resource management for wireless network virtualization," *IEEE Trans. Cogn. Commun. Netw.*, vol. 4, no. 4, pp. 919–928, Dec. 2018.

[53] S. Lin et al., "Advanced dynamic channel access strategy in spectrum sharing 5G systems," *IEEE Wireless Commun.*, vol. 24, no. 5, pp. 74–80, Oct. 2017.

[54] M. Rebato, F. Boccardi, M. Mezzavilla, S. Rangan, and M. Zorzi, "Hybrid spectrum sharing in mmWave cellular networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 3, no. 2, pp. 155–168, Jun. 2017.

[55] S. Atapattu, C. Tellambura, H. Jiang, and N. Rajatheva, "Unified analysis of low-SNR energy detection and threshold selection," *IEEE Trans. Veh. Technol.*, vol. 64, no. 11, pp. 5006–5019, Nov. 2015.

[56] M. T. Masonta, M. Mzyece, and N. Ntlatlapa, "Spectrum decision in cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1088–1107, 3rd Quart., 2013.

[57] S. K. Sharma, T. E. Bogale, S. Chatzinotas, B. Ottersten, L. B. Le, and X. Wang, "Cognitive radio techniques under practical imperfections: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 1858–1884, 4th Quart., 2015.

[58] G. Wang, Q. Liu, R. He, F. Gao, and C. Tellambura, "Acquisition of channel state information in heterogeneous cloud radio access networks: Challenges and research directions," *IEEE Wireless Commun.*, vol. 22, no. 3, pp. 100–107, Jun. 2015.

[59] S. Atapattu, C. Tellambura, and H. Jiang, *Energy Detection for Spectrum Sensing in Cognitive Radio*. New York, NY, USA: Springer, 2014.

[60] Y. C. Liang, K. C. Chen, G. Y. Li, and P. Mahonen, "Cognitive radio networking and communications: An overview," *IEEE Trans. Veh. Tech.*, vol. 60, no. 7, pp. 3386–3407, Sep. 2011.

[61] R. Tandra and A. Sahai, "SNR walls for signal detection," *IEEE J. Select. Topics Signal Process.*, vol. 2, no. 1, pp. 4–17, Feb. 2008.

[62] Y. Zeng and Y. C. Liang, "Eigenvalue-based spectrum sensing algorithms for cognitive radio," *IEEE Trans. Commun.*, vol. 57, no. 6, pp. 1784–1793, Jun. 2009.

[63] J. Ma, G. Y. Li, and B. H. Juang, "Signal processing in cognitive radio," *Proc. IEEE*, vol. 97, no. 5, pp. 805–823, May 2009.

[64] L. Barlemann and S. Mangold, *Cognitive Radio and Dynamic Spectrum Access*. Hoboken, NJ, USA: Wiley, 2009.

[65] M. Derakhshani and T. Le-Ngoc, "Aggregate interference and capacity-outage analysis in a cognitive radio network," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 196–207, Jan. 2012.

[66] K. Bian, J.-M. Park, L. Chen, and X. Li, "Addressing the hidden terminal problem for heterogeneous coexistence between TDM and CSMA networks in white space," *IEEE Trans. Veh. Technol.*, vol. 63, no. 9, pp. 4450–4463, Nov. 2014.

[67] A. Ghasemi and E. Sousa, "Interference aggregation in spectrum-sensing cognitive wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 2, no. 1, pp. 41–56, Feb. 2008.

[68] A. M. Wyglinski, M. Nekovee, and T. Hou, *Cognitive Radio Communications and Networks: Principles and Practice*. Amsterdam, The Netherlands: Elsevier, 2010.

[69] B. Jalaeian, R. Zhu, H. Samani, and M. Motani, "An optimal cross-layer framework for cognitive radio network under interference temperature model," *IEEE Syst. J.*, vol. 10, no. 1, pp. 293–301, Mar. 2016.

[70] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5G beyond," *IEEE Netw.*, vol. 33, no. 3, pp. 10–17, May/Jun. 2019.

[71] Y. Pei, S. Hu, F. Zhong, D. Niyato, and Y.-C. Liang, "Blockchain-enabled dynamic spectrum access: Cooperative spectrum sensing, access and mining," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2019, pp. 1–6.

[72] S. Hu, Y. Pei, and Y.-C. Liang, "Sensing-mining-access tradeoff in blockchain-enabled dynamic spectrum access," *IEEE Wireless Commun. Lett.*, vol. 10, no. 4, pp. 820–824, Apr. 2021.

[73] R. Vuppula and H. S. Pradhan, "Blockchain-oriented location privacy preserving for cooperative spectrum sensing in 6G wireless networks," *IET Blockchain*, vol. 3, no. 3, pp. 74–97, 2023.

[74] M. Liu, Q. Wu, Y. Hei, D. Li, and J. Hu, "Fair and smart spectrum allocation scheme for IIoT based on blockchain," *Ad Hoc Netw.*, vol. 123, Dec. 2021, Art. no. 102686.

[75] L. Liu, M. Shafiq, V. R. Sonawane, M. Y. B. Murthy, P. C. S. Reddy, and K. C. K. Reddy, "Spectrum trading and sharing in unmanned aerial vehicles based on distributed blockchain consortium system," *Comput. Electr. Eng.*, vol. 103, Oct. 2022, Art. no. 108255.

[76] M. Patnaik, G. Prabhu, C. Rebeiro, V. Matyas, and K. Veezhinathan, "ProBLeSS: A proactive blockchain based spectrum sharing protocol against SSDF attacks in cognitive radio IoBT networks," *IEEE Netw.ing Lett.*, vol. 2, no. 2, pp. 67–70, Jun. 2020.

[77] 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.

[78] Z. Tu, K. Zhu, C. Yi, and R. Wang, "Blockchain-based privacy-preserving dynamic spectrum sharing," in *Proc. Int. Conf. Wireless Algorithms, Syst., Appl.*, 2020, pp. 444–456.

[79] L. Yu, J. Ji, Y. Guo, Q. Wang, T. Ji, and P. Li, "Smart communications in heterogeneous spacecraft networks: A blockchain based secure auction approach," in *Proc. IEEE Cogn. Commun. Aerosp. Appl. Workshop (CCAAW)*, 2019, pp. 1–4.

[80] P. Wu, W. Chen, H. Wu, K. Qi, and M. Liu, "Enhanced game theoretical spectrum sharing method based on blockchain consensus," in *Proc. IEEE 94th Veh. Technol. Conf.*, 2021, pp. 1–7.

[81] 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.

[82] Y. Choi and I.-G. Lee, "Game theoretical approach of blockchain-based spectrum sharing for 5G-enabled IoTs in dense networks," in *Proc. IEEE 90th Veh. Technol. Conf.*, 2019, pp. 1–6.

[83] S. Rani, H. Babbar, S. H. A. Shah, and A. Singh, "Improvement of energy conservation using blockchain-enabled cognitive wireless networks for smart cities," *Sci. Rep.*, vol. 12, no. 1, 2022, Art. no. 13013.

[84] 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./Apr. 2020.

[85] F. Guo, F. R. Yu, H. Zhang, H. Ji, M. Liu, and V. C. Leung, "Adaptive resource allocation in future wireless networks with blockchain and mobile edge computing," *IEEE Trans. Wireless Commun.*, vol. 19, no. 3, pp. 1689–1703, Mar. 2020.

[86] E. Guler, M. Karakus, and S. Uludag, "Blockchain-enhanced cross-ISP spectrum assignment framework in SDONs: SpectrumChain," *Comput. Netw.*, vol. 223, Mar. 2023, Art. no. 109579.

[87] H. Zhang, S. Leng, Y. Wei, and J. He, "A blockchain enhanced coexistence of heterogeneous networks on unlicensed spectrum," *IEEE Trans. Veh. Technol.*, vol. 71, no. 7, pp. 7613–7624, Jul. 2022.

[88] S. Ma, X.-Y. Liu, L. Fu, X. Tian, X. Gan, and X. Wang, "On the greedy resource occupancy threat in dynamic spectrum access," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 11233–11248, Dec. 2017.

[89] P. Lv, H. Zhao, and J. Zhang, "Blockchain based spectrum sensing: A game-driven behavior strategy," in *Proc. IEEE 9th Joint Int. Inf. Technol. Artif. Intell. Conf. (ITAIC)*, vol. 9, 2020, pp. 899–904.

[90] N. Dewangan, A. Kumar, and R. Patel, "A framework for secure cooperative spectrum sensing based with blockchain and deep learning model in cognitive radio," in *Proc. Int. Conf. Artif. Intell. Knowl. Discov. Concurr. Eng. (ICECONF)*, 2023, pp. 1–6.

[91] R. Zhu, H. Liu, L. Liu, X. Liu, W. Hu, and B. Yuan, "A blockchain-based two-stage secure spectrum intelligent sensing and sharing auction mechanism," *IEEE Trans. Ind. Informat.*, vol. 18, no. 4, pp. 2773–2783, Apr. 2022.

[92] L. Xue, W. Yang, W. Chen, and L. Huang, "STBC: A novel blockchain-based spectrum trading solution," *IEEE Trans. Cogn. Commun. Netw.*, vol. 8, no. 1, pp. 13–30, Mar. 2022.

[93] Z. Pourgharehkhan, A. Taherpour, T. Khattab, and R. Hamila, "Efficient collaborative spectrum sensing under the smart primary user emulation attacker network," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2015, pp. 1–7.

[94] Y. Zhang and Z. Fang, "Dynamic double threshold spectrum sensing algorithm based on block chain," in *Proc. 3rd Int. Conf. Electron. Inf. Technol. Comput. Eng. (EITCE)*, 2019, pp. 1090–1095.

[95] M. Yan, L. Du, L. Huang, L. Xiao, and J. Tang, "Game-theoretic approach against selfish attacks in cognitive radio networks," in *Proc. 10th IEEE/ACIS Int. Conf. Comput. Inf. Sci.*, 2011, pp. 58–61.

[96] M. Patnaik, V. Kamakoti, V. Matyáš, and V. Řchák, "PROLEMus: A proactive learning-based MAC protocol against PUEA and SSDF attacks in energy constrained cognitive radio networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 5, no. 2, pp. 400–412, Jun. 2019.

[97] J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator's perspective," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 451–466, Jan. 2020.

[98] A. Jain, N. Gupta, and M. Sreenu, "Blockchain based smart contract for cooperative spectrum sensing in cognitive radio networks for sustainable beyond 5G wireless communication," *Green Technol. Sustain.*, vol. 1, no. 2, 2023, Art. no. 100019.

[99] G. Rathee, F. Ahmad, F. Kurugollu, M. A. Azad, R. Iqbal, and M. Imran, "CRT-BIoV: A cognitive radio technique for blockchain-enabled Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4005–4015, Jul. 2021.

[100] G. Zhang, "Research on cognitive radio spectrum sensing security mechanism based on blockchain," *J. Phys., Conf. Series*, vol. 1578, no. 1, 2020, Art. no. 012045.

[101] M. Grissa, A. A. Yavuz, and B. Hamdaoui, "When the hammer meets the nail: Multi-server pir for database-driven CRN with location privacy assurance," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, 2017, pp. 1–9.

[102] K. Zhu et al., "Privacy-aware double auction with time-dependent valuation for blockchain-based dynamic spectrum sharing in IoT systems," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6756–6768, Apr. 2023.

[103] Y. Xiao et al., "Decentralized spectrum access system: Vision, challenges, and a blockchain solution," *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 220–228, Feb. 2022.

[104] H. Zhang, S. Leng, F. Wu, and H. Chai, "A DAG blockchain-enhanced user-autonomy spectrum sharing framework for 6G-enabled IoT," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8012–8023, Jun. 2022.

[105] 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.

[106] M. Grissa, A. A. Yavuz, and B. Hamdaoui, "TrustSAS: A trustworthy spectrum access system for the 3.5 GHz CBRS band," in *Proc. INFOCOM IEEE Conf. Comput. Commun.*, 2019, pp. 1495–1503.

[107] Z. Li, W. Wang, J. Guo, Y. Zhu, L. Han, and Q. Wu, "Blockchain-assisted dynamic spectrum sharing in the CBRS band," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, 2021, pp. 864–869.

[108] S. Ding, G. Shen, K. X. Pan, S. K. Bose, Q. Zhang, and B. Mukherjee, "Blockchain-assisted spectrum trading between elastic virtual optical networks," *IEEE Netw.*, vol. 34, no. 6, pp. 205–211, Dec. 2020.

[109] Z. Zhang, M. Zhang, Y. Li, B. Fan, and L. Jiang, "Directed acyclic graph blockchain for secure spectrum sharing and energy trading in power IoT," *China Commun.*, vol. 20, no. 5, pp. 182–197, May 2023.

[110] 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.

[111] X. Ling, J. Wang, Y. Le, Z. Ding, and X. Gao, "Blockchain radio access network beyond 5G," *IEEE Wireless Commun.*, vol. 27, no. 6, pp. 160–168, Dec. 2020.

[112] Z. Cheng, Y. Liang, Y. Zhao, S. Wang, and C. Sun, "A multi-blockchain scheme for distributed spectrum sharing in CBRS system," *IEEE Trans. Cogn. Commun. Netw.*, vol. 9, no. 2, pp. 266–280, Apr. 2023.

[113] V. Y. Kemmoe, W. Stone, J. Kim, D. Kim, and J. Son, "Recent advances in smart contracts: A technical overview and state of the art," *IEEE Access*, vol. 8, pp. 117782–117801, 2020.

[114] T. Ariyarathna, P. Harankahadeniya, S. Isthikar, N. Pathirana, H. D. Bandara, and A. Madanayake, "Dynamic spectrum access via smart contracts on blockchain," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2019, pp. 1–6.

[115] J. Lin, B. Tian, J. Wu, and J. He, "Spectrum resource trading and radio management data sharing based on blockchain," in *Proc. IEEE 3rd Int. Conf. Inf. Syst. Comput. Aided Educ. (ICISCAE)*, 2020, pp. 83–87.

[116] C. Sengul, "Distributed ledgers for spectrum authorization," *IEEE Internet Comput.*, vol. 24, no. 3, pp. 7–18, Jun. 2020.

[117] S. Zheng, T. Han, Y. Jiang, and X. Ge, "Smart contract-based spectrum sharing transactions for multi-operators wireless communication networks," *IEEE Access*, vol. 8, pp. 88547–88557, 2020.

[118] 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)*, 2020, pp. 1–6.

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

[120] L. Wang, Y. Zheng, Y. Zhang, and F. Li, "Secure spectrum sharing for satellite Internet-of-Things based on blockchain," *Wireless Pers. Commun.*, vol. 131, pp. 357–369, Apr. 2023.

[121] M. A. Khan, M. M. Jamali, T. Maksymyuk, and J. Gazda, "A blockchain token-based trading model for secondary spectrum markets in future generation mobile networks," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–12, Aug. 2020.

[122] A. A. Okon, I. Elgendi, O. S. Sholiyi, J. M. Elmirghani, A. Jamalipour, and K. Munasinghe, "Blockchain and SDN architecture for spectrum management in cellular networks," *IEEE Access*, vol. 8, pp. 94415–94428, 2020.

[123] D. B. Rawat and A. Alshaikhi, "Leveraging distributed blockchain-based scheme for wireless network virtualization with security and QoS constraints," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, 2018, pp. 332–336.

[124] X. Zhang and Y. Zhao, "Smart contract-based distributed spectrum sensing for blockchain-enabled spectrum sharing," in *Proc. IEEE 96th Veh. Technol. Conf. (VTC)*, 2022, pp. 1–5.

[125] A. A. Makhdomi and G. R. Begh, "Blockchain based scalable model for secure dynamic spectrum access," *Phys. Commun.*, vol. 55, Dec. 2022, Art. no. 101874.

[126] E. M. Ghourab, L. Bariah, S. Muhaidat, P. C. Sofotasios, M. Al-Qutayri, and E. Damiani, "Reputation-aware relay selection with opportunistic spectrum access: A blockchain approach," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 389–403, 2023.

[127] 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.*, vol. 22, no. 10, pp. 5801–5815, Oct. 2023.

[128] F. Li, K.-Y. Lam, M. Jia, J. Zhao, X. Li, and L. Wang, "Blockchain-based approach for securing spectrum trading in multibeam satellite systems," 2020, *arXiv:2012.10681*.

[129] M. A. A. Careem and A. Dutta, "Sensechain: Blockchain based reputation system for distributed spectrum enforcement," in *Proc. IEEE Int. Symp. Dyn. Spectr. Access Netw. (DySPAN)*, 2019, pp. 1–10.

[130] C. Rajesh Babu and B. Amutha, "Blockchain and extreme learning machine based spectrum management in cognitive radio networks," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 10, 2022, Art. no. e4174.

[131] M. Kalra, A. Vohra, and N. Marriwala, "Hybrid blockchain-based spectrum sharing algorithm for dynamic channel selection in cognitive radio," *Meas., Sensors*, vol. 25, Feb. 2023, Art. no. 100648.

[132] T. Maksymyuk et al., "AI-enabled blockchain framework for dynamic spectrum management in multi-operator 6G networks," in *Future Intent Based Networking: On the QoS Robust and Energy Efficient Heterogeneous Software Defined Networks*. Cham, Switzerland: Springer, 2021, pp. 322–338.

[133] P. Bhattacharya et al., "A deep-Q learning scheme for secure spectrum allocation and resource management in 6G environment," *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 4989–5005, Dec. 2022.

[134] A. Khanna, P. Rani, T. H. Sheikh, D. Gupta, V. Kansal, and J. J. Rodrigues, "Blockchain-based security enhancement and spectrum sensing in cognitive radio network," *Wireless Pers. Commun.*, vol. 127, pp. 1899–1921, Dec. 2022.

[135] Z. Li, W. Wang, Q. Wu, and X. Wang, "Multi-operator dynamic spectrum sharing for wireless communications: A consortium blockchain enabled framework," *IEEE Trans. Cogn. Commun. Netw.*, vol. 9, no. 1, pp. 3–15, Feb. 2023.

[136] Y. Zhou, L. Yu, Z. Jiang, Z. Zhi, J. Kang, and Z. Han, "An improved spectrum trading design based on dynamic credit aggregate-signature blockchain," *IEEE Wireless Commun. Lett.*, vol. 12, no. 4, pp. 625–629, Apr. 2023.

[137] 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.

[138] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 1023–1043, 2nd Quart., 2015.

[139] A. K. BR and C. Reshma, "Blockchain based spectrum mapping and access to secondary users for enhanced channel security efficiency in CRN," in *Proc. Int. Conf. Invent. Comput. Technol. (ICICT)*, 2023, pp. 1781–1786.

[140] A. Mustafa, M. N. U. Islam, and S. Ahmed, "Dynamic spectrum sensing under crash and Byzantine failure environments for distributed convergence in cognitive radio networks," *IEEE Access*, vol. 9, pp. 23153–23167, 2021.

[141] O. H. Toma, M. Lopez-Benitez, D. K. Patel, and K. Umebayashi, "Estimation of primary channel activity statistics in cognitive radio based on imperfect spectrum sensing," *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2016–2031, Apr. 2020.

[142] X. Luo, "Secure cooperative spectrum sensing strategy based on reputation mechanism for cognitive wireless sensor networks," *IEEE Access*, vol. 8, pp. 131361–131369, 2020.

[143] P. C. Pappa, A. Sarbhai, A. Baset, S. Kasera, and M. Buddhikot, "Spectrum sharing in CBRS using blockchain," in *Proc. IEEE 17th Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, 2020, pp. 631–639.

[144] Z. Sun, F. Qi, L. Liu, Y. Xing, and W. Xie, "Energy-efficient spectrum sharing for 6G ubiquitous IoT networks through blockchain," *IEEE Internet Things J.*, vol. 10, no. 11, pp. 9342–9352, Jun. 2023.

[145] P. Fernando, K. Dadallage, T. Gamage, C. Seneviratne, A. Madanayake, and M. Liyanage, "Proof of sense: A novel consensus mechanism for spectrum misuse detection," *IEEE Trans. Ind. Informat.*, vol. 18, no. 12, pp. 9206–9216, Dec. 2022.

[146] J. Zhao et al., "Spectrum trading based on blockchain for resource allocation of optical network virtualization," in *Proc. Opto Electron. Commun. Conf. (OECC)*, 2021, pp. 1–3.

[147] Y. Yang, X. Xu, S. Han, B. Wang, and G. Wang, "Reputation mechanism designed for blockchain empowered dynamic spectrum sharing system," in *Proc. IEEE 33rd Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, 2022, pp. 1191–1196.

[148] Q. Wang, R. Li, Q. Wang, and S. Chen, "Non-fungible token (NFT): Overview, evaluation, opportunities and challenges," 2021, *arXiv:2105.07447*.

[149] V. Buterin et al., "A next-generation smart contract and decentralized application platform," *White Paper*, vol. 3, no. 37, pp. 2–1, 2014.

[150] E. Androulaki et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys. Conf.*, 2018, pp. 1–15.

[151] V. Theodorou et al., "Blockchain-based zero touch service assurance in cross-domain network slicing," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, 2021, pp. 395–400.

[152] S. Singh, C. R. Babu, K. Ramana, I.-H. Ra, and B. Yoon, "BENS-B5G: Blockchain-enabled network slicing in 5G and beyond-5G (B5G) networks," *Sensors*, vol. 22, no. 16, p. 6068, 2022.

[153] (Ethereum, Silicon Valley, CA, USA). *What Is the Difference Between Ethereum and Bitcoin?*. Accessed: Dec. 20, 2023. [Online]. Available: https://ethereum.org/en/what-is-ethereum/

[154] (Hyperledger, San Francisco, CA, USA). *Understanding Use Cases and Applications of Blockchain Technology*. Accessed: Dec. 20, 2023. [Online]. Available: https://www.hyperledger.org/use.

[155] "IOTA." Accessed: Dec. 20, 2023. [Online]. Available: https://wiki.iota.org/learn/about-iota/an-introduction-to-iota/

[156] J. V. Moreira and A. M. Alberti, "Mercado de Espectro com IOTA," in *Proc. Anais do V Workshop em Blockchain, Teoria, Tecnologias e Aplicações*, 2022, pp. 15–25.

[157] "What is Holochain?" Accessed: Dec. 20, 2023. [Online]. Available: https://www.holochain.org/what-holochain/

[158] W. F. Silvano and R. Marcelino, "Iota tangle: A cryptocurrency to communicate Internet-of-Things data," *Future Gener. Comput. Syst.*, vol. 112, pp. 307–319, Nov. 2020.

[159] P. Fernando, A. Braeken, and M. Liyanage, "Breaking chains, empowering IoT: A comparative study of holochain and blockchain," in *Proc. IEEE Latin Am. Conf. Commun. (LATINCOM)*, 2023, pp. 1–6.

[160] S. Gaba et al., "Holochain: An agent-centric distributed hash table security in smart IoT applications," *IEEE Access*, vol. 11, pp. 81205–81223, 2023.

[161] "NR dynamic spectrum sharing (DSS); (Release 17)," 3GPP, Sophia Antipolis, France, Rep. 860043, 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/WorkItem/WorkItemDetails.aspx?workitemId=860043

[162] M. M. Butt, I. Macaluso, C. Galiotto, and N. Marchetti, "Fair dynamic spectrum management in licensed shared access systems," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2363–2374, Sep. 2019.

[163] X. Tang, "Towards an aligned blockchain standard system: Challenges and trends," in *Proc. 3rd Int. Conf. Blockchain Trustworthy Syst.*, Guangzhou, China, 2021, pp. 574–584.

[164] "Blockchain standards." EUC. Jun. 2022. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/blockchain-standards

[165] S. K. Sharma, T. E. Bogale, L. B. Le, S. Chatzinotas, X. Wang, and B. Ottersten, "Dynamic spectrum sharing in 5G wireless networks with full-duplex technology: Recent advances and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 674–707, 1st Quart., 2017.

[166] T. M. Tan and S. Saraniemi, "Trust in blockchain-enabled exchanges: Future directions in blockchain marketing," *J. Acad. Market. Sci.*, vol. 51, pp. 914–939, Jul. 2023.

[167] S. K. Lo, X. Xu, M. Staples, and L. Yao, "Reliability analysis for blockchain oracles," *Comput. Elect. Eng.*, vol. 83, May 2020, Art. no. 106582.

[168] Y. Liu, K. Zheng, P. Craig, Y. Li, Y. Luo, and X. Huang, "Evaluating the reliability of blockchain based Internet of Things applications," in *Proc. 1st IEEE Int. Conf. Hot Inf. Centric Netw. (HotICN)*, 2018, pp. 230–231.

[169] T. M. Tan and J. Salo, "Ethical marketing in the blockchain-based sharing economy: Theoretical integration and guiding insights," *J. Bus. Ethics*, vol. 183, no. 4, pp. 1113–1140, 2023.

[170] F. Eigelshoven, A. Ullrich, and D. A. Parry, "Cryptocurrency market manipulation: A systematic literature review," in *Proc. Int. Conf. Inf. Syst.*, 2021, pp. 1–17.

[171] M. La Morgia, A. Mei, F. Sassi, and J. Stefa, "Pump and dumps in the Bitcoin era: Real time detection of cryptocurrency market manipulations," in *Proc. 29th Int. Conf. Comput. Commun. Netw. (ICCCN)*, 2020, pp. 1–9.

[172] M. A. Ghazaleh and A. M. Zabadi, "BlockChain (BC) upending customer experience: Promoting a new customer relationship management (CRM)," *J. Mgmt. Sustain.*, vol. 11, no. 1, p. 203, 2021.

[173] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Appl. Sci.*, vol. 9, no. 9, p. 1788, 2019.

[174] A. Guru, B. K. Mohanta, H. Mohapatra, F. Al-Turjman, C. Altrjman, and A. Yadav, "A survey on consensus protocols and attacks on blockchain technology," *Appl. Sci.*, vol. 13, no. 4, p. 2604, 2023.

[175] P. Ekparinya, V. Gramoli, and G. Jourjon, "Impact of man-in-the-middle attacks on Ethereum," in *Proc. IEEE 37th Symp. Reliable Distrib. Syst. (SRDS)*, 2018, pp. 11–20.

[176] A. AbuHalimeh and O. Ali, "Comprehensive review for healthcare data quality challenges in blockchain technology," *Front. Big Data*, vol. 6, May 2023, Art. no. 1173620.

[177] C. Cappiello, M. Comuzzi, F. Daniel, and G. Meroni, "Data quality control in blockchain applications," in *Proc. Int. Conf. Bus. Process Manag.*, 2019, pp. 166–181.

[178] A. Alofi, M. A. Bokhari, R. Bahsoon, and R. Hendley, "Optimizing the energy consumption of blockchain-based systems using evolutionary algorithms: A new problem formulation," *IEEE Trans. Sustain. Comput.*, vol. 7, no. 4, pp. 910–922, Dec. 2022.

[179] 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, 2020.

[180] C. B. E. C. Index, *Comparison, Cambridge Center Alternative Finance*, Univ. Cambridge, Cambridge, U.K., 2020. [Online] Available: https://cbeci.org/comparisons

[181] A. I. Sanka and R. C. Cheung, "A systematic review of blockchain scalability: Issues, solutions, analysis and future research," *J. Netw. Comput. Appl.*, vol. 195, 2021, Art. no. 103232.

[182] E. Lombrozo, J. Lau, and P. Wuille, "BIP141: Segregated witness (consensus layer)," *link. Acessado em*, vol. 21, Dec. 2015. [Online]. Available: https://scholar.google.com/scholar?cluster=5913767807377273508&hl=en&oi=scholarr

[183] J. Rubin, M. Naik, and N. Subramanian, "Merkelized abstract syntax trees," *XP055624837*, vol. 16, no. 3, pp. 1–3, 2014.

[184] J. Adler, R. Berryhill, A. Veneris, Z. Poulos, N. Veira, and A. Kastania, "Astraea: A decentralized blockchain oracle," in *Proc. IEEE Int. Conf. Internet Things (IThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Physical Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, 2018, pp. 1145–1152.

[185] A. Endurthi and A. Khare, "Two-tiered consensus mechanism based on proof of work and proof of stake," in *Proc. 9th Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, 2022, pp. 349–353.

[186] X. Feng, J. Ma, Y. Miao, X. Liu, and K.-K. R. Choo, "Regulatable and hardware-based proof of stake to approach nothing at stake and long range attacks," *IEEE Trans. Services Comput.*, vol. 16, no. 3, pp. 2114–2125, Jun. 2023.

[187] N. A. Akbar, A. Muneer, N. ElHakim, and S. M. Fati, "Distributed hybrid double-spending attack prevention mechanism for proof-of-work and proof-of-stake blockchain consensuses," *Future Internet*, vol. 13, no. 11, p. 285, 2021.

[188] X.-J. Wen, Y.-Z. Chen, X.-C. Fan, W. Zhang, Z.-Z. Yi, and J.-B. Fang, "Blockchain consensus mechanism based on quantum zero-knowledge proof," *Opt. Laser Technol.*, vol. 147, Mar. 2022, Art. no. 107693.

[189] M. Kaur, S. Gupta, D. Kumar, C. Verma, B.-C. Neagu, and M. S. Raboaca, "Delegated proof of accessibility (DPoAC): A novel consensus protocol for blockchain systems," *Mathematics*, vol. 10, no. 13, p. 2336, 2022.

[190] Q. Li, J. Wu, J. Quan, J. Shi, and S. Zhang, "Efficient quantum blockchain with a consensus mechanism QDPoS," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 3264–3276, 2022.

[191] Q. Chen, W.-C. Wong, M. Motani, and Y.-C. Liang, "MAC protocol design and performance analysis for random access cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 11, pp. 2289–2300, Nov. 2013.

[192] X. Y. Wang, A. Wong, and P. H. Ho, "Stochastic medium access for cognitive radio ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 770–783, Apr. 2011.

[193] A. D. Domenico, E. C. Strinati, and M. G. D. Benedetto, "A survey on MAC strategies for cognitive radio networks," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 1, pp. 21–44, 1st Quart., 2012.

[194] J. Xie, K. Zhang, Y. Lu, and Y. Zhang, "Resource-efficient DAG blockchain with sharding for 6G networks," *IEEE Netw.*, vol. 36, no. 1, pp. 189–196, Feb. 2022.

[195] C. Sun and S. Wang, "Blockchain based spectrum sharing," 2023, *arXiv:2303.07550*.

[196] T. Do, T. Nguyen, and H. Pham, "Delegated proof of reputation: A novel blockchain consensus," in *Proc. 1st Int. Electron. Commun. Conf.*, 2019, pp. 90–98.

[197] K. Saadat, N. Wang, and R. Tafazolli, "AI-enabled blockchain consensus node selection in cluster-based vehicular networks," *IEEE Netw. Lett.*, vol. 5, no. 2, pp. 115–119, Jun. 2023.

[198] R. Song, Y. Song, Z. Liu, M. Tang, and K. Zhou, "GaiaWorld: A novel blockchain system based on competitive PoS consensus mechanism," *Comput., Mater. Continua*, vol. 60, no. 3, 2019.

[199] G. Liu, Z. Wu, Y. Zhou, Y. Liu, and H. Kang, "Communitychain: Towards a scalable blockchain in smart home," *IEEE Trans. Netw. Service Manag.*, vol. 20, no. 3, pp. 2898–2911, Sep. 2023.

[200] J. H. Khor, M. Sidorov, and S. A. B. Zulqarnain, "Scalable lightweight protocol for interoperable public blockchain-based supply chain ownership management," *Sensors*, vol. 23, no. 7, p. 3433, 2023.

LAVAN PERERA (Student Member, IEEE) received the B.Sc. degree (First-Class Hons.) in electrical and electronic engineering from the University of Sri Jayewardenepura, Sri Lanka, in 2021. He is currently pursuing the Ph.D. degree with the School of Computer Science, University College Dublin, Ireland, and a Doctoral Student/Research Engineer of the EU CONFIDENTIAL 6G Project. He is currently working in the field of Blockchain-based aspects of DSM. Before his Ph.D. studies, he served as a Lecturer with the Department of Electrical and Electronic Engineering, Faculty of Engineering, University of Sri Jayewardenepura, Sri Lanka, from 2022 to 2023.

PASIKA RANAWEERA (Member, IEEE) received the bachelor's degree (with Hons.) in electrical and information engineering from the Faculty of Engineering, University of Ruhuna, Sri Lanka, in 2010, the master's degree in information and communication technology from the University of Agder, Norway, in 2013, and the Ph.D. degree from University College Dublin (UCD), Ireland, on improving the security of service migrations of MEC in 2023, where he is a Lecturer/Assitant Professor with the School of Electrical and Electronic Engineering. He has been a Postdoctoral Researcher with the School of Computer Science, UCD from February 2023 to August 2023. He is the Project Manager of the CONFIDENTIAL-6G Project, funded by the EU H2022-SNS Grant ID: 101096435. Prior to his Ph.D. degree, he served as a Lecturer with the Department of Electrical and Information Engineering, Faculty of Engineering, University of Ruhuna, Sri Lanka, from 2014 to 2018. He is experienced in conducting teaching/ instructing/ demonstration work at international universities (UCD-Ireland, BDIC-China). He is a member of the NetsLab, PEL, and CONNECT research groups/centers based at UCD. He is focused on enhancing the security measures in 5G and beyond 5G mobile networks, while his main research focus is directed at Federated Learning-based security issues and how to overcome them utilizing Blockchain. His additional research directives extend to lightweight security protocols, formal verification, security, service quality optimization, 5G and MEC integration technologies (SDN, NFV, Blockchain), privacy preservation techniques, and IoT security. He received the Lanekassen Scholarship for pursuing the master's degree from the University of Agder. More information can be found at https://people.ucd.ie/pasika.ranaweera.

SACHITHA KUSALADHARMA (Member, IEEE) received the B.Sc. degree (First-Class Hons.) in electrical and telecommunication engineering from the University of Moratuwa, Sri Lanka, in 2010, and the M.Sc. and Ph.D. degrees in electrical and computer engineering from the University of Alberta, Edmonton, AB, Canada, in 2013 and 2017, respectively. Since 2017, he was a Postdoctoral Fellow with Concordia University, Canada, and since 2020, he has been a Postdoctoral Fellow with the University of Toronto, Canada. Since 2022, he has been working with the University College Dublin. He received the Alberta Innovates Technology Futures Graduate Student Scholarship in 2013, the Horizon Postdoctoral Fellowship in 2017, and the NSERC Postdoctoral Fellowship in 2020. His research interests include CR networks, communication theory, multiple-input–multiple-output systems, and wireless sensor networks.

SHEN WANG (Senior Member, IEEE) received the M.Eng. degree from Wuhan University, China, and the Ph.D. degree from Dublin City University, Ireland. He is currently an Assistant Professor with the School of Computer Science, University College Dublin, Ireland. He has been involved with several EU projects as a co-PI, WP, and Task leader in big trajectory data streaming for air traffic control and trustworthy AI for intelligent cybersecurity systems. Some key industry partners of his applied research are IBM Research Brazil, Boeing Research and Technology Europe, and Huawei Ireland Research Centre. His research interests include connected autonomous vehicles, explainable AI, and security and privacy for mobile networks. He is the recipient of the IEEE Intelligent Transportation Systems Society Young Professionals Travelling Fellowship 2022.

MADHUSANKA LIYANAGE (Senior Member, IEEE) received the Doctor of Technology degree in communication engineering from the University of Oulu, Oulu, Finland, in 2016. He is an Assistant Professor/Ad Astra Fellow and the Director of the Graduate Research, School of Computer Science, University College Dublin, Ireland. He is leading the Network Softwarization and Security Labs, UCD School of Computer Science which mainly focuses on the security and privacy of future mobile networks, including 5G and 6G. He is also acting as a Docent/Adjunct Professor with the Center for Wireless Communications, University of Oulu and a Honorary Adjunct Professor with the University of Ruhuna, Sri Lanka, and the University of Sri Jayawardhanepura, Sri Lanka. His research interests are 5G/6G, blockchain, network security, AI, explainable AI, federated learning, network slicing, Internet of Things, and multiaccess edge computing. He was also a recipient of the prestigious Marie Skłodowska-Curie Actions Individual Fellowship and the Government of Ireland Postdoctoral Fellowship from 2018 to 2020. In 2020, he received the "2020 IEEE ComSoc Outstanding Young Researcher" Award from IEEE ComSoc EMEA. In 2021 and 2022, he was ranked among the World's Top 2% Scientists (2020 and 2021) in the List prepared by Elsevier BV, Stanford University, USA. He was also awarded an Irish Research Council Research Ally Prize as part of the IRC Researcher of the Year 2021 awards for the positive impact he has made as a supervisor. In 2022, he received "2022 The Tom Brazil Excellence in Research Award" from SFI CONNECT Center. He has secured over 5 Million Euro research funding via various research projects. He is currently a PI for two large EU H2020/Horizon Europe projects. Two research projects (MEVICO and SIGMONA projects) received the CELTIC Excellence and CELTIC Innovation Awards in 2013, 2017, and 2018. He is also an Expert Consultant with European Union Agency for Cybersecurity. Moreover, he is an expert reviewer at different funding agencies in France, Qatar, UAE, Sri Lanka, and Kazakhstan. More information can be found at www.madhusanka.com.