Distributed Ledger Technologies for Cellular Networks and Beyond 5G: a survey

Meroua Moussaoui[1,2] Nischal Aryal[1,2] Emmanuel Bertin[1,2] Noel Crespi[1]

[1] Orange Innovation, 14000 Caen, France

[2] IMT, Telecom SudParis, Institut Polytechnique de Paris, 91764 Palaiseau, France

Emails : {meroua.moussaoui, nischal.aryal, emmanuel.bertin}@orange.com and noel.crespi@it-sudparis.eu

Abstract— **Cellular networks have played a critical role in building today's Internet. However, they are facing more and more challenges such as softwarization and programmability, decentralization, as well as opening to new business models, while keeping a very high level of trust and reliability. DLT (Distributed Ledger Technology) is a promising field to address these challenges in an innovative way. In this paper, we present a comprehensive analysis of DLT applications for cellular networks, covering the Radio Access Network (RAN), Core Network (CN), Applications & services, as well as Inter-actor communication & cooperation.**

Keywords—Distributed Ledger Technologies, blockchain, cellular networks, 5G.

I. Introduction

Voice-over-IP, teleconferencing, data transfer via text messaging, audio and video streaming, as well as other internet applications are growing more popular, putting more pressure on cellular networks. Supporting a large number of subscribers with varying QoS requirements, frequent mobility between multiple administrative domains, fine-grained evaluation and control, centralized network management, real-time adaptation, user privacy, information security, and other numerous challenges that today's networks face provide a fertile field for DLT to demonstrate all of its claimed benefits of revolutionizing the digital era, thanks to its decentralization and capacity to provide privacy and data integrity in even the most untrustworthy contexts.

In order to overcome the aforementioned challenges, industry and academia are working feverishly to incorporate DLT into cellular networks. We provide in this paper a survey of recent research on the use of DLT in favor of cellular networks, which divides our work into four parts, each of which addressing a layer of the cellular network architecture: the Radio Access Network (RAN), the Core Network (CN), the Applications & services, and finally, the Inter-actor communication & cooperation. Figure 1 details the taxonomy of our paper.

The rest of this paper is structured as follows: Section II will examine and compare related works to ours and will highlight our contributions. Section III will list the various solutions proposed for integrating DLT in the different layers of the cellular networks. Section IV will present a detailed discussion of the discovered results and the current challenges. Section V will wrap up this paper with some future research directions and a conclusion to hover over what we've covered.

II. Related works & paper contribution

Owing to the increased interest in blockchain (BC) and cryptocurrencies, the networking academics and industrial groups have begun to explore DLT's potential beyond its financial and economic scope by leveraging its decentralization, reliability, immutability, and traceability advantages. We could identify several surveys that address the usage of DLT in cellular networks, however, the most of them, in some form, are focused on one single topic or enabling technology, such as: Cloud computing [1]–[3], Fog/Edge computing [4]–[6], Software Defined Networking (SDN) [7], [8], Network Slicing (NS) [9], Network security [10], [11], Service Level Agreement (SLA) management [12], [13], and Machine Learning-empowered networks [14].

Only a few literature reviews have looked at the usage of DLT in networking from a global perspective, considering all of its components and technologies. Table 1 shows the main contributions of these works and compares them to this present paper. Our paper provides a literature review on up-to-date applications of DLT in cellular networks. In summary the main contributions of this survey are:

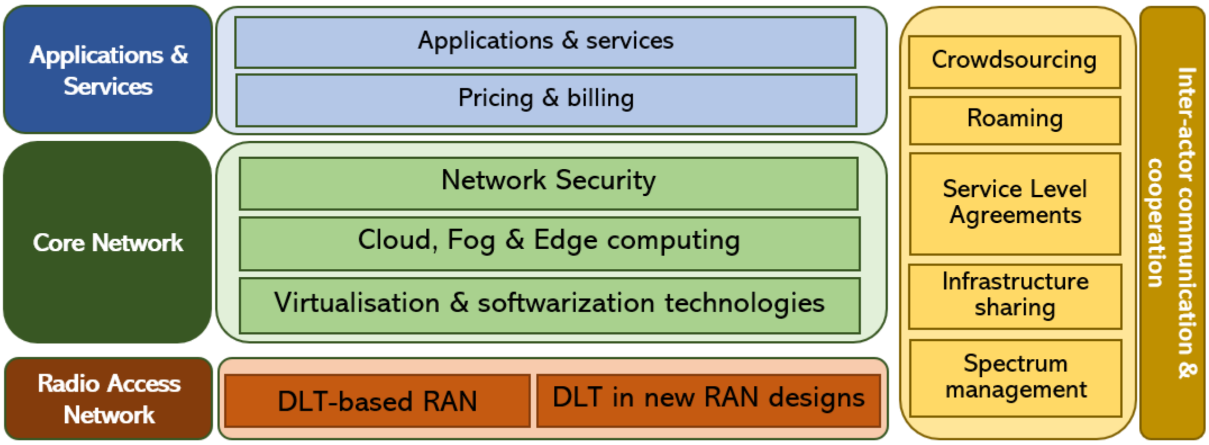

Fig. 1. Paper's taxonomy.

- To discuss and put together the main works on the integration of DLT in different layers of cellular networks, while providing an overview on the main DLTs used in these networks.
- To discuss whether the use of DLT is really needed in cellular networks.
- To highlight the remaining challenges and the future research directions.

TABLE 1 RELATED WORKS

Ref.	Main contribution	Limitations & comparison with our contribution
[15]	A survey on DLT integration with 5G and beyond networks, including cellular networks.	Out of date, and many more studies on the usage of CLT in cellular networks have been published in the recent three years.
[16]	A survey on the most commun DLT applications for smartphones and the recent industry and research advances in DLT-based applications.	Papers about other types of networks, were also mentioned. Also, our study focuses on cellular networks as a whole rather than only smart-phone end-devices.
[17]	An examination of the use of DLT in wireless networks from several perspectives: resource sharing, trusted data interaction, secure access control, privacy protection, traceability, certification, and supervision.	This paper's taxonomy is focused on topics of application of DLT in wireless networks. Many other topics were not covered such as network outsourcing and roaming. Our study focuses only on cellular networks, and our taxonomy is unique in that it examines each tier of the network separately for a more thorough analysis.

III. WORKS ON THE USE OF DLT IN CELLULAR NETWORKS

A. Radio Access Network (RAN)

1) DLT-based RAN

The BC Radio Access Network (B-RAN) is a DLT-based RAN that aims to promote trust, transparency, decentralization, and data traceability. Many articles have addressed this emerging concept, suggesting original designs and architectures to realize it. For 6G networks, [18] proposes a dual-hop B-RAN (DH-BRAN) architecture, which comprises of a two-level network, each with its own BC, allowing intermediary nodes to become wireless access providers, whether owned by individuals or service providers (SPs), and smart contracts (SCs) are used to create SLAs between the participating nodes. This solution delivers great security and privacy at the expanse of latency. B-RAN is viewed as an enabling technology for reliable and effective 6G networks in [17]. The paper proposes an eight-layer B-RAN system with six fundamental capabilities: user application, resource/asset trade, BC consensus, network, secure connection, and physical storage and data. The tests were carried out on a Proof-of-Work (PoW)-based B-RAN prototype, and the findings reveal that it provides much reduced service latency than traditional PoW-based BCs (like Bitcoin and Ethereum).

A common challenge for cellular networks is to provide ubiquitous and seamless cross-domain connectivity. Using Hyperledger Fabric (HLF) BC to provide seamless handover, [19] builds a three-layer cross domain RAN data-sharing architecture, made up of: a privacy-preserving layer, a user access layer, and a platform layer. The shared RAN data are the foreign cells' configuration parameters and are exchanged via SCs between Mobile Network operators (MNOs) from various countries.

2) DLT in new RAN paradigms

Many RAN design paradigms have lately surfaced, including C-RAN, O-RAN, and FRAN. Cloud RAN (C-RAN) is a software-enabled RAN paradigm for 5G broadband access, but its centralized structure creates a serious trust issue amongst the many operators. To address this, [20] proposes a BC-enabled 5G C-RAN (BC-RAN) with a Trust-based PBFT (Practical Byzantine Fault Tolerance) consensus algorithm to prevent insider threats and secure data exchange and asset transaction. It also provides a tri-chain structure to make transaction storage and traceability more convenient.

O-RAN is an emerging design that connects interoperable virtualized and softwarized RAN components via open standard interfaces. The solution proposed in [21] expands the traditional O-RAN architecture with a private BC by adding a distributed RAN sharing broker enabled by SCs to manage and deliver virtualized RAN resources following two mechanisms : auctioning and open marketplaces. In [22], BE-RAN, a BC-enabled O-RAN, is described and it consists of a unique privacy-preserving framework with zero-trust identity management and mutual authentication.

Fog RAN (F-RAN) is another breakthrough RAN concept that uses Fog computing to relieve the traffic burden from the cloud to the network edge. However, it is vulnerable to a variety of security threats. [23] proposes a BC-based F-RAN (BF-RAN) architecture, which consists of a three-chain architecture with cross-chain interaction that enables for transparent, secure, and traceable service provision, as well as distributed data storage, administration, and sharing. This method is anticipated to be capable of meeting the demanding needs of future 6G networks. Also, [24] presents a BC-based architecture for granting responsibilities and permissions to F-RAN services and nodes. SCs are used for providing verifiable automation of physical activities between the nodes.

B. Core network (CN)

1) Virtualisation & softwarization technologies

Because the Northbound interface serves as a link between the applications and the SDN controller resources, its security is critical for the entire network. For this purpose, [25] proposes a BCNBI, a BC-based security framework for Northbound Interface in SDN, with the goal of providing tamper-proof data storage, a lightweight decentralized SDN design based on customized private BC and a trust evaluation monitoring system. Also, [26] describes BlockAS, a BC-based Authentication, Authorization, and Accounting System allowing applications to access SDN controller resources. The Crash Fault-Tolerant (CFT) consensus mechanism was used to implement the prototype on HLF. DoS/DDoS attacks are a significant threat to SDN networks, and numerous researchers have addressed this issue by developing BC-enabled systems for detecting and mitigating them, such as: [27], [28]. For multiple-controller SDN, [29] proposes BlockREV, a secure multi-controller rule enforcement verification method inspired by the bitcoin system, to enable cross-domain forwarding. Meanwhile, [30] leverages the benefits of Ethereum SCs to create BCC, a multi-controller SDN coordinator based on PBFT consensus.

The authors of [31] propose an innovative platform based on PBFT consensus-BC to secure service function chaining, configuration, and migration of Virtual Network Functions (VNFs). This solution is later improved in [32] as a BC-enabled secure Network Function Virtualization (NFV) orchestrator, called BSec-NFVO, that provides agility and traceability to multi-tenant and multi-domain NFV orchestration.

For network slicing (NS), the authors of [33] propose DBNS, a Distributed BC-enabled NS framework, which employs a BC-based bidding mechanism for dynamic resource leasing and service provisioning. In [33], HLF is used to provide an end-to-end BC-enabled slicing solution for mobile 5G networks, while Ethereum SCs are used in [34] to automatically manage and negotiate trust relations between actors for slice deployment. Many additional studies leverage the benefits of BC and SCs to create NS brokering solutions, such as NSBchain [35], a PBFT-based HLF framework that enables automated and secure network resource allocation between brokers and tenants. Furthermore, [36] presents a secure resource trading and autonomous 5G RAN slicing platform based on a consortium network and a PBFT-based HLF BC.

CoNTe, is a novel permissionless blockchain protocol based on federated byzantine agreement that allows lifecycle control and network function compatibility [37]. It may be used as stand-alone temporal storage or packed with current 5G core VNFs to create a BC-enabled 5G core network.

2) Cloud, Fog, & Edge computing

For cloud storage, [38] provides an Ethereum-based cloud data management (CBDM) architecture for cloud storage that is privacy-preserving, open, transparent, and controlled. With the purpose of improving cloud data security, [39] presents a secure public auditing schema to address a variety of cloud data storage challenges, including the 51 percent attack (where more than 51% of hostile nodes seize control of the network), and significant computing and communication overhead. It also protects data integrity and keeps track of dishonest behavior, by logging abnormalities into dedicated files. In addition, [40] has proposed a multi-tenant BC-based data integrity protection system that takes advantage of the features of SCs and distributed mobile agent technology to provide cooperative trust assurance by detecting data tempering actions based on changes in the hash of the stored files. Moreover, [41] proposes BlockCloud, a data provenance verification platform for federated cloud storage, powered by PoW-based permissioned BC, in order to address the security vulnerabilities posed by the cloud's multi-tenancy and perceived dynamicity at the data exchange level.

Fog computing extends Cloud computing by offloading data, storage, and computing resources to a fog layer between the cloud and the network's edge. It has a lot of advantages in terms of network bandwidth use and latency, however, it comes with a slew of security concerns. In some applications, and for a better performance, mobile edge devices can offload their tasks to fog servers, which can in some cases be compromised or include some privacy breaches. As a solution to this problem, BMO, a BC-based Mobility aware Offloading, was proposed in [42] to manage geo-localized fog server security, improve offloading efficiency by leveraging mobility-aware offloading techniques, and provide a decentralized charging schema for Fog computing. Individual mobility and offloading prediction, concurrency, the lack of a single point of failure, and BC-enabled security and accounting are all advantages of this design. The system was implemented with Ethereum and SCs. In order to motivate nodes to engage in fog resource contribution, [43] introduces a BC-based model that employs a punishment/ reward mechanism to assess the satisfaction level of the delivered fog services by the providers. The BC in question employs an enhanced Delegated Proof-of-Stake (DPoS) consensus that has been tailored to the proposed architecture.

Edge computing goes beyond Fog computing in that it extends Cloud computing all the way down to data generating sources, with all computing and processing taking place on or closer to end-devices for low-latency services. This has the drawback of being resource constrained, which can be overcome by all edge nodes cooperating in a decentralized network based on computation offloading between the various edge servers. However, such environments necessitate trust and incentivization, which can be achieved by leveraging the benefits of DLT. To this purpose, [44] presents CoopEdge, a BC-enabled system for cooperative Edge computing that encourages peers to participate in the network by incentivizing task offloading and rapid task completion. It also assures trust with a reputation system based on peer performance history. This platform is built on an HLF Sawtooth BC and employs a unique novel consensus called Proof-of-Edge-Reputation (PoER). A BC-based adaptive resource allocation and computing offloading paradigm for Mobile Edge Computing (MEC) is also proposed in [45]. It uses a modified consensus based on PBFT and DPoS, with SCs managing the computation task execution. Furthermore, the authors of [46] establish an Edge computing-oriented security consensus model (ECBCM) that uses the DPoS consensus to provide BC-enabled Edge computing networks with more efficiency and flexibility.

3) Network Security

For an efficient and secure identity management in cognitive cellular networks, [47] harnesses the benefits of BC and SCs to provide a privacy-enhancing end-to-end user identity management system, from user assertion to user billing. It enables network access through the use of pseudonymous identities and includes the necessary mechanisms for establishing access contracts and charging users. The tests were carried out on a private Ethereum BC, and the results show that the proposed solution speeds up access provisioning and payment settlement while reducing network signaling traffic. In addition, [48] offers a self-sovereign identity management and authentication strategy for mobile networks, based on a redactable BC (a BC that allows editing and rewriting the content of the ledger's blocks), in which users have ownership over their own identifying data, so even if the user changes operators, this approach allows them to retain their identification and personal identifying information. This system is supplemented by a lightweight BC-based authentication protocol that is used between users and their network operators and SPs, with no requirement for consumers to store their keys. Another advantage is that this technique eliminates the requirement for a revocation list, which reduces authentication latency and storage expense. In order to prevent Rogue Cellsite, man-in-the-middle, or Stingray attacks in handover procedures, [49] suggests the usage of BC for identity management of the next generation NodeB (gNB) for user equipment (UE). This will provide handover security while also prohibiting the UE from connecting to an untrusted gNB and exchanging confidential information with it.

Another key aspect of cellular network security is access control. The authors of [50] propose an access control framework that is independent of AKA-based access methods and addresses the security threats that arise from the centralization of users' authentication and access management by using BC and SCs without introducing any computation or maintenance costs. Scalability, decentralization, and resistance to DoS attacks are the advantages that this solution presents. The same authors use BC and SCs in [51] to provide a novel attribute-based access control technique for Internet-based service provisioning. It enables network providers and SPs to share resources by decentralizing the access system, which improves security and lowers maintenance costs. This solution enables access control outsourcing without the requirement for a trusted third party and increases the system's flexibility and automation through the use of SCs.

C. Applications & services

1) Pricing & billing

Cellular networks can take use of DLT's financial aspects by leveraging its decentralization, incentivization, and lack of dependency on third parties to develop a billing and charging mechanism for the participating nodes, resulting in a more trustworthy and secure system. For example, [52] makes use of SCs and Ethereum BC to create agreements for charging users in roaming scenarios, where users' roaming records are shared across the network between the different operators

2) Applications & services

Several applications and services operate over cellular networks, each with its own set of QoS needs and performance requirements. Social media has captivated a broad audience in the recent decade, emphasizing the necessity to protect users' privacy and security. [53] presents a social media content notarization system based on BC that assures that content recorded in the BC hasn't been forged before its insertion, in order to curb the "falsifying data attack", which entails introducing corrupted data into the BC in order to fool the participants. Using a public key infrastructure (PKI) protocol, the solution allows the social media service provider to check content authenticity.

Application marketplaces are the initial point of contact for users who want to download an application, that’s why B2MDF, a BC-based Malware Detection Framework for identifying malicious mobile applications in mobile application marketplaces, was described in [54]. The system employs a dual-private BC system for feature extraction and storage in order to identify malware.

D. Inter-actor communication & cooperation

1) Spectrum management

With spectrum being the most precious and necessary component for all cellular networks' services and revenue generation, spectrum management is a significant arena in which DLT advantages may be used to improve spectrum usage among the expanding number of stakeholders and players. Many papers have addressed the application of BC and SCs in spectrum management services such as spectrum sharing (SSh), spectrum access (SA), spectrum sensing (SS), and spectrum trading (ST). Following the intended application, many consensus algorithms have been utilized, including PBFT [55], [56], Interference-based consensus [57], Proof-of-Authority (PoA) [58], Proof-of-Strategy [59], and PoW [60]. Incentivization is an important feature to boost users efficient participation in the network, several works have leveraged existing cryptocurrencies or have created their own digital assets, such as spectrum coin [60] and auction coin [56]. The goal of these works is mainly to address the four key difficulties of spectrum management: privacy, trust, incentivization, and decentralization. Table 2 summarizes the most important papers that tackled the different spectrum management aspects (SSh, SA, SS, and ST) as well as the type of BC they use, the platform used if mentioned, and whether they use SCs or not.

TABLE 2 THE MAIN PAPERS ON SPECTRUM MANAGEMENT SERVICES.

Ref	BC	Platform	SC	SSh	SA	SS	ST
[55]	Private	Ethereum	Yes	✓			
[61]	Private	HLF	No		✓		
[62]	Private	Sidechain	Yes	✓	✓	✓	
[57]	/	/	Yes	✓			✓
[63]	Public	Ethereum	Yes				
[64]	Public	/	Yes	✓		✓	
[56]	Private	Ethereum	No			✓	
[65]	Private	Own BC	No	✓			
[66]	Public	Ethereum	Yes	✓			
[58]	Private	/	Yes	✓			
[60]	Private	Own BC	No	✓			
[59]	Private	Own BC	Yes		✓		
[67]	Private	Ethereum	Yes	✓			✓

2) Infrastructure sharing

One of the most promising strategies for lowering network installation and maintenance costs is infrastructure sharing across various operators. It does, however, necessitate strict isolation and effective resource management among the many participants. In [68], the authors make use of BC to provide a distributed Home Subscriber Server (HSS) that can be used securely by the main networks of several operators. In addition, SCs are used to create a distributed Self-Organizing Network (SON) to conduct self-transactions amongst MNOs in exchange for sharing small cell infrastructure. Also, [69] presents a BC-based SDN strategy for controlling radio spectrum access between MNOs in small cell networks, and it employs SCs to validate transactions between MNOs. Simulation results show that, in contrast to a break in connectivity in the absence of an agreement, this system ensures seamless handoff and high availability between multiple operators. The authors of [70] propose BRAIN, a BC-based reverse auction method for providing a safe VNFs marketplace and a transparent competition amongst Infrastructure providers (InPs) to offer the VNF hosting infrastructure.

3) Service-Level Agreement (SLA)

The majority of the studies on the use of BC and SCs for SLA management [71]–[74] focus on Cloud computing and are all Ethereum-based, thanks to Ethereum's capacity to do complex calculations and Turing-completeness feature that enables SCs. In the meanwhile, the works in [75], [76] employ the HLF platform. All of these efforts, focus mainly on guaranteeing transparency and trustworthiness between cloud providers and consumers, SLA monitoring and violation detection, as well as compensation.

In [77], the authors suggest an automatic SLA monitoring system for cloud providers and consumers to ensure transparency and trustworthiness. They use the Multichain permissioned blockchain and implement a round robin consensus mechanism. As for SLA compliance and trust establishment in edge-based NFV, a private Ethereum BC-powered infrastructure is proposed in [78].

4) Roaming

Roaming allows mobile users to maintain service continuity across national and international borders. The growing mobility and density of cellular network users necessitates improved roaming solutions to meet the severe criteria of uninterrupted connectivity and resource availability. Many frameworks for DLT integration in roaming were proposed. The solution introduced in [79], employs a HLF-based roaming architecture that enables non-trusting mobile carriers to conduct peer-to-peer self-transactions using SC agreements to simplify charging and billing settlements. Moreover, [80] presents a new Ethereum-based Decentralized Application (DApp)-based architecture for Local 5G Operators to enable offload and roaming services, as well as other services such as automatic selection of the best-rated network for a subscriber and automatic execution of load balancing techniques. Authors of [81] offer a BC approach based on Tendermint (a consensus mechanism that does not require mining) to address two of the major issues with international roaming: intermediaries and high costs. It eliminates the requirement for roaming agreements to be changed on a regular basis and reduces processing time.

Roaming fraud is a major issue that occurs when a user uses the visited network after the session has ended, and the home network MNO is unable to charge the user owing to synchronization delays yet is forced to pay the visited network MNO for the given service. To address this problem, the authors of [82] develop a novel PoS-based BC framework for mobile roaming service management. It adopts the Ouroboros consensus mechanism which has significant low delay advantages over existing PoW consensus algorithms. They improve this work in [83] by creating their own PoS consensus mechanism to reduce transaction confirmation time, called “BlockRoam’s consensus mechanism”.

Roaming also places strict security constraints on the management and trust of users and operators. [84] offers a secure and efficient user subscription data access control scheme based on Ethereum SCs, as well as a flexible user authentication scheme based on derivable tokens, and a data encryption and storage scheme that is further optimized by virtualizing threshold secret sharing. Also, [85] creates AUGChain, a new authentication system that runs on HLF. It is immune to a wide range of security threats and optimizes computation and battery utilization.

5) Crowdsourcing

Crowdsourcing is an emerging approach that allows participants to exchange data, making it ideal for latency-sensitive services. In cellular networks, one type of crowdsourcing is "crowd spectrum sensing," which is an efficient and cost-effective framework for realizing large-scale and broadband spectrum sensing. However, the centralized architecture on which it relies poses significant technical issues and security vulnerabilities. To address these issues, [86] proposes a BC-based Crowd Spectrum Sensing (BCSS) system for low-cost spectrum sensing. Another issue with crowdsourced networks is the equitable distribution of consumer funds to infrastructure providers, who want to be compensated for their investments while users want better coverage and stability. That’s why [87] developed a new transparent, automated, decentralized, and secure economic model called Fair, which uses MeshDApp (a value transfer platform for mesh networks that uses a local Ethereum PoA BC) to create a win-win situation for all parties involved. Finally, the limited battery life of mobile terminals is an obstacle for extended-time services. To solve this, BPCM was suggested in [88], a BC-powered crowdsourcing solution for reducing service time in crowdsourced mobile contexts, based on improved dynamic programming (IDP), clustering technics, and multiple decision-making criteria.

IV. Discussions & challenges

Cellular networks have come a long way, leapfrogging into what we now assume to be the Beyond-5G era, although many aspects of such networks still face challenges. The good news is that most of these challenges correlate with the numerous benefits that DLTs provide. The decentralized secure access and incentivization properties of DLTs can be used to enhance handover and cross-domain/cross-border connectivity continuity. The decentralized, distributed trustless BC functionality may be used to solve trust concerns that arise from the centralization of SDN and cloud-based systems. By integrating transparency and safe payment, DLT is a potential candidate in scenarios that need brokering, such as NS and VNF marketplaces. As infrastructure installation fees increase with the increasing needs for the higher capacity and storage that 5G services introduce, infrastructure sharing and outsourcing paradigms appear to be a promising solution, especially when combined with DLT, which offers a secure environment and, more importantly, monetizes the exchanged resources to boost parties’ participation in the network. Spectrum management is another hot topic in cellular networks, especially with the emergence of new entities such as micro-operators and the migration of many operators to unlicensed bands. Here, DLTs can have a big impact by providing a way to incentivize spectrum and thus allow a fair usage among the different entities, as well as securing its management and preventing scenarios of fraudulent spectrum usage. SLA and roaming management are two more interesting sectors where several studies have demonstrated the impact that DLTs may have, particularly in terms of increasing openness and transparency in the collaboration between different operators. Switching to the use of digital assets for billing in exchange for networking services is a concept that had been the topic of more than one paper as cryptocurrencies enter their golden age. Furthermore, the adoption of DLTs helps alleviate a variety of security and privacy issues.

Public or permission-less BCs are accessible to anybody, making them ideal for low to zero-trust situations in which users do not have to trust each other but rather the BC they are joining, as in connectivity crowdsourced networks, and services that target a large public of customers, such as roaming and billing, as well as decentralized autonomous virtual resource management and SONs. Due to the vast dispersion of transaction validation and the distributed record keeping mechanism, the network gets more secure as more individuals join it. Also, each participant holds the ledger locally, which promotes the openness and transparency of the network. However, it lowers transaction rates, increases energy usage and storage resources, which make it non suitable for services that require low delays, and applications that should be executed on end-devices or resource-restricted fog/edge servers, which can also cause synchronization overhead. On the other hand, private or permissioned BCs have the benefit of faster consensus and consequently higher transaction rates due to their restrictive and highly constrained character, which make them suitable candidates for latency-sensitive services such as remote driving, as well as confined networks that require high privacy and secrecy such as private 5G networks. However, because of the secret nature of the transactions' information, trust must be developed in such networks, necessitating the creation of a centralized entity or consortium of entities to allow participant entrance.

The advent of the SC concept was a watershed moment in the development of DLTs, enhancing even more the benefits of these technologies in terms of security, accuracy, speed, efficiency, transparency, and trust. However, because they lack a subjective aspect that allows for variable outputs, they limit the network's flexibility and versatility. As a result, the outcome in SCs is always logically predictable and cannot be modified depending on the context. It also might potentially cause network congestion and delay transactions. On the flip side, many articles have shown that SCs are an appropriate solution for many cellular network difficulties, particularly in circumstances where significant automation of repeated activities is required, such as frequent handover, and spectrum sensing due to their self-executing and self-verification nature. Because of their self-enforceability and lack of dependency on intermediaries, they also make defining business logics and privacy policies easier, as well as helping to establish collaboration and secure links between diverse entities.

Consensus algorithms are also an important component in DLT. The most common consensus algorithms in literature are PoW, PoS, DPoS, and PBFT. They differ in terms of consensus speed, reward distribution, energy and computing resource consumption, as well as their vulnerability to the 51% attack. Many research publications contribute to the body of knowledge by developing their own consensus algorithms and digital assets that meet the needs of their applications, with different requirements in different environments.

The question remains whether DLT is truly needed in cellular networks, or if it is simply a "hop on the trend" due to all the hype surrounding it, especially since most of the buzz features of DLT were established earlier by other distributed databases that have now existed for decades, such as immutability, log-centricity, and only-appendability, in databases like immudb, CouchDB, Google File System (GFS) and its clone Hadoop Distributed File System (HDFS), as well as their capability of multi-level encryption: cell/ column level, page level, and backup level. However, the unique features of DLT, like its distributed structure, transaction validation based on specialized consensus algorithms, and incentivization of network involvement through digital assets set it apart from other distributed storage solutions.

Because all the aforementioned DLT benefits come at the expense of a massive amount of storage space, as well as high energy consumption and communication delays, deciding whether to use DLT in cellular networks, particularly in latency-sensitive use-cases, highly private applications, and end-device embedded applications, requires more reflection on whether the leveraged benefits in terms of automation, costs, and settlement and maintenance expenses can only be obtained via this technology, or any other distributed database can achieve them, without sacrificing privacy, latency, or computing and storage resources. To sum up, DLT offers value in situations requiring digital data assets, automated trust, autonomy, and data traceability. Distributed databases, on the other hand, are more beneficial in cases where data must be stored and accessed with an emphasis on facilitating analysis and retrieval as well as operational support.

The integration of BC and SCs into cellular networks will face a number of challenges, including the use of cryptocurrencies for user incentivization, which raises other issues such as digital asset interoperability between platforms and the possibility of cellular network cryptocurrencies being uniformed. Another stumbling block is the legal environment, since rules and policies are still not up-to-date with the technological advancements that cellular networks are seeing today, and aspects of the legislations are still ambiguous, particularly when it comes to cryptocurrencies. Standardization groups should consider opening their systems to DLT integration policies and extensions as well, which may need a full reshaping of the existing standards. The introduction of DLT into cellular networks will have a significant impact on the ecosystem dynamics by introducing new roles such as BC providers and BC-as-a-Service providers, as well as eliminating other roles, namely the trusted third parties in value exchange, that may migrate, in their turns, to other forms of participation in the value-creation. As a result, DLT is expected to be a disruptive step in the evolution of cellular networks, requiring a complete rethinking of the underpinning foundations.

V. Conclusion & Future Research Directions

Starting with the RAN layer, the CN layer, the applications & services layer, and ending with the inter-actor communication & cooperation transversal layer, we reviewed the most prominent and current publications in literature that tackled the use of DLT in cellular networks.

Many technological advancements can be made by leveraging the benefits of DLT in cellular networks, but many areas still require more research, such as the introduction of user incentivization platforms for network services and the possibility of using digital assets, as well as the integration of DLT into RAN technologies and the B-RAN paradigm. More research is needed to improve consensus algorithms, especially with the advent of DLT in Fog/Edge computing, which has limited processing and storage resources. BC and SCs appear to be strong candidates for crowdsourcing connection and roaming, and a real implementation would be an intriguing study topic. Finally, beyond identity management, authentication, and access control, DLT may be used in network security to provide solutions for data provenance and better user and data privacy.

References

[1] K. Gai, J. Guo, L. Zhu, and S. Yu, “Blockchain meets cloud computing: A survey,” *IEEE Commun. Surv. Tutor.*, vol. 22, no. 3, pp. 2009–2030, 2020.

[2] P. Sharma, R. Jindal, and M. D. Borah, “Blockchain technology for cloud storage: A systematic literature review,” *ACM Comput. Surv. CSUR*, vol. 53, no. 4, pp. 1–32, 2020.

[3] M. R. Dorsala, V. N. Sastry, and S. Chapram, “Blockchain-based solutions for cloud computing: A survey,” *J. Netw. Comput. Appl.*, vol. 196, p. 103246, 2021.

[4] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, “Integrated blockchain and edge computing systems: A survey, some research issues and challenges,” *IEEE Commun. Surv. Tutor.*, vol. 21, no. 2, pp. 1508–1532, 2019.

[5] H. Baniata and A. Kertesz, “A survey on blockchain-fog integration approaches,” *IEEE Access*, vol. 8, pp. 102657–102668, 2020.

[6] Y. I. Alzoubi, A. Al-Ahmad, and H. Kahtan, “Blockchain technology as a Fog computing security and privacy solution: An overview,” *Comput. Commun.*, vol. 182, pp. 129–152, 2022.

[7] T. Alharbi, “Deployment of blockchain technology in software defined networks: A survey,” *IEEE Access*, vol. 8, pp. 9146–9156, 2020.

[8] H. N. Nguyen, H. A. Tran, S. Fowler, and S. Souihi, “A survey of Blockchain technologies applied to software-defined networking: Research challenges and solutions,” *IET Wirel. Sens. Syst.*, 2021.

[9] F. Javed, K. Antevski, J. Mangues-Bafalluy, L. Giupponi, and C. J. Bernardos, “Distributed Ledger Technologies for Network Slicing: A Survey,” *IEEE Access*, vol. 10, pp. 19412–19442, 2022.

[10] S. Manimurgan, T. Anitha, G. Divya, G. C. P. Latha, and S. Mathupriya, “A Survey on Blockchain Technology for Network Security Applications,” in *2022 2nd International Conference on Computing and Information Technology (ICCIT)*, 2022, pp. 440–445.

[11] Y. Ma, Y. Sun, Y. Lei, N. Qin, and J. Lu, “A survey of blockchain technology on security, privacy, and trust in crowdsourcing services,” *World Wide Web*, vol. 23, no. 1, pp. 393–419, 2020.

[12] N. Hamdi, C. El Hog, R. Ben Djemaa, and L. Sliman, “A Survey on SLA Management Using Blockchain Based Smart Contracts,” in *International Conference on Intelligent Systems Design and Applications*, 2022, pp. 1425–1433.

[13] W. Li, J. Wu, J. Cao, N. Chen, Q. Zhang, and R. Buyya, “Blockchain-based trust management in cloud computing systems: A taxonomy, review and future directions,” *J. Cloud Comput.*, vol. 10, no. 1, pp. 1–34, 2021.

[14] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. Leung, “Blockchain and machine learning for communications and networking systems,” *IEEE Commun. Surv. Tutor.*, vol. 22, no. 2, pp. 1392–1431, 2020.

[15] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Blockchain for 5G and beyond networks: A state of the art survey,” *J. Netw. Comput. Appl.*, vol. 166, p. 102693, 2020.

[16] A. Ometov *et al.*, “An overview on blockchain for smartphones: State-of-the-art, consensus, implementation, challenges and future trends,” *IEEE Access*, vol. 8, pp. 103994–104015, 2020.

[17] J. Wang, X. Ling, Y. Le, Y. Huang, and X. You, “Blockchain-enabled wireless communications: a new paradigm towards 6G,” *Natl. Sci. Rev.*, vol. 8, no. 9, p. nwab069, 2021.

[18] T. Sachinidis, A.-A. A. Boulogeorgos, and P. Sarigiannidis, “Dual-hop Blockchain Radio Access Networks for Advanced Coverage Expansion,” in *2021 10th International Conference on Modern Circuits and Systems Technologies (MOCAST)*, 2021, pp. 1–5.

[19] A. Heider-Aviet *et al.*, “Blockchain Based RAN Data Sharing,” in *2021 IEEE International Conference on Smart Data Services (SMDS)*, 2021, pp. 152–161.

[20] W. Tong, X. Dong, Y. Shen, and J. Zheng, “Bc-ran: Cloud radio access network enabled by blockchain for 5g,” *Comput. Commun.*, vol. 162, pp. 179–186, 2020.

[21] L. Giupponi and F. Wilhelmi, “Blockchain-enabled Network Sharing for O-RAN,” *ArXiv Prepr. ArXiv210702005*, 2021.

[22] H. Xu, L. Zhang, and Y. Sun, “BE-RAN: Blockchain-enabled Open RAN with Decentralized Identity Management and Privacy-Preserving Communication,” *ArXiv Prepr. ArXiv210110856*, 2021.

[23] Z. Wang, B. Cao, C. Liu, C. Xu, and L. Zhang, “Blockchain-based fog radio access networks: Architecture, key technologies, and challenges,” *Digit. Commun. Netw.*, 2021.

[24] J. Jijin, B.-C. Seet, and P. H. J. Chong, “Blockchain enabled opportunistic fog-based radio access network: A position paper,” in *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)*, 2019, pp. 1–3.

[25] S. Algarni, F. Eassa, K. Almarhabi, A. Algarni, and A. Albeshri, “BCNBI: A Blockchain-Based Security Framework for Northbound Interface in Software-Defined Networking,” *Electronics*, vol. 11, no. 7, p. 996, 2022.

[26] H. D. Hoang, P. T. Duy, and V.-H. Pham, “A security-enhanced monitoring system for northbound interface in SDN using blockchain,” in *Proceedings of the Tenth International Symposium on Information and Communication Technology*, 2019, pp. 197–204.

[27] S. Jiang *et al.*, “BSD-Guard: A Collaborative Blockchain-Based Approach for Detection and Mitigation of SDN-Targeted DDoS Attacks,” *Secur. Commun. Netw.*, vol. 2022, 2022.

[28] Z. Abou El Houda, A. S. Hafid, and L. Khoukhi, “Cochain-SC: An intra-and inter-domain DDoS mitigation scheme based on blockchain using SDN and smart contract,” *IEEE Access*, vol. 7, pp. 98893–98907, 2019.

[29] P. Li, S. Guo, J. Wu, and Q. Zhao, “BlockREV: Blockchain-Enabled Multi-Controller Rule Enforcement Verification in SDN,” *Secur. Commun. Netw.*, vol. 2022, 2022.

[30] W. Fan, S.-Y. Chang, S. Kumar, X. Zhou, and Y. Park, “Blockchain-based Secure Coordination for Distributed SDN Control Plane,” in *2021 IEEE 7th International Conference on Network Softwarization (NetSoft)*, 2021, pp. 253–257.

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

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

[33] M. A. Togou *et al.*, “DBNS: A distributed blockchain-enabled network slicing framework for 5G networks,” *IEEE Commun. Mag.*, vol. 58, no. 11, pp. 90–96, 2020.

[34] S. B. Saad, A. Ksentini, and B. Brik, “An end-to-end trusted architecture for network slicing in 5G and beyond networks,” *Secur Priv.*, vol. 5, no. 1, 2022.

[35] L. Zanzi, A. Albanese, V. Sciancalepore, and X. Costa-Pérez, “Nsbchain: a secure blockchain framework for network slicing brokerage,” in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–7.

[36] G. O. Boateng, D. Ayepah-Mensah, D. M. Doe, A. Mohammed, G. Sun, and G. Liu, “Blockchain-Enabled Resource Trading and Deep Reinforcement Learning Based Autonomous RAN Slicing in 5G,” *IEEE Trans. Netw. Serv. Manag.*, 2021.

[37] S. Platt, L. Sanabria-Russo, and M. Oliver, “CoNTe: A Core Network Temporal Blockchain for 5G,” *Sensors*, vol. 20, no. 18, p. 5281, 2020.

[38] L. Zhu, Y. Wu, K. Gai, and K.-K. R. Choo, “Controllable and trustworthy blockchain-based cloud data management,” *Future Gener. Comput. Syst.*, vol. 91, pp. 527–535, 2019.

[39] J. Li, J. Wu, G. Jiang, and T. Srikanthan, “Blockchain-based public auditing for big data in cloud storage,” *Inf. Process. Manag.*, vol. 57, no. 6, p. 102382, 2020.

[40] P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, “Blockchain data-based cloud data integrity protection mechanism,” *Future Gener. Comput. Syst.*, vol. 102, pp. 902–911, 2020.

[41] D. Tosh, S. Shetty, X. Liang, C. Kamhoua, and L. L. Njilla, “Data provenance in the cloud: A blockchain-based approach,” *IEEE Consum. Electron. Mag.*, vol. 8, no. 4, pp. 38–44, 2019.

[42] W. Dou, W. Tang, B. Liu, X. Xu, and Q. Ni, “Blockchain-based mobility-aware offloading mechanism for fog computing services,” *Comput. Commun.*, vol. 164, pp. 261–273, 2020.

[43] H. Wang, L. Wang, Z. Zhou, X. Tao, G. Pau, and F. Arena, “Blockchain-based resource allocation model in fog computing,” *Appl. Sci.*, vol. 9, no. 24, p. 5538, 2019.

[44] L. Yuan *et al.*, “Coopedge: A decentralized blockchain-based platform for cooperative edge computing,” in *Proceedings of the Web Conference 2021*, 2021, pp. 2245–2257.

[45] 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. Wirel. Commun.*, vol. 19, no. 3, pp. 1689–1703, 2019.

[46] S. Xuan *et al.*, “ECBCM: a prestige-based edge computing blockchain security consensus model,” *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 6, p. e4015, 2021.

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

[48] J. Xu, K. Xue, H. Tian, J. Hong, D. S. Wei, and P. Hong, "An identity management and authentication scheme based on redactable blockchain for mobile networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6688–6698, 2020.

[49] W. Crowe and T. T. Oh, "Distributed Unit Security for 5G Base-Stations using Blockchain," in *2020 International Conference on Software Security and Assurance (ICSSA)*, 2020, pp. 10–14.

[50] F. Ghaffari, E. Bertin, and N. Crespi, "A novel approach for network resource sharing via blockchain," in *Proceedings of the SIGCOMM'21 Poster and Demo Sessions*, 2021, pp. 50–52.

[51] F. Ghaffari, E. Bertin, N. Crespi, S. Behrad, and J. Hatin, "A novel access control method via smart contracts for internet-based service provisioning," *IEEE Access*, vol. 9, pp. 81253–81273, 2021.

[52] A. Refaey, K. Hammad, S. Magierowski, and E. Hossain, "A blockchain policy and charging control framework for roaming in cellular networks," *IEEE Netw.*, vol. 34, no. 3, pp. 170–177, 2019.

[53] G. Song, S. Kim, H. Hwang, and K. Lee, "Blockchain-based notarization for social media," in *2019 IEEE international conference on consumer electronics (icce)*, 2019, pp. 1–2.

[54] S. Homayoun, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "A blockchain-based framework for detecting malicious mobile applications in app stores," in *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*, 2019, pp. 1–4.

[55] N. Suzuki, T. Yoshioka, A. Hasegawa, H. Yokoyama, and T. Maeyama, "Implementation and evaluation of spectrum sharing technology using smart contracts," in *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, 2022, pp. 0922–0928.

[56] 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," *Wirel. Pers. Commun.*, pp. 1–23, 2021.

[57] 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.

[58] 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, 2020.

[59] H. Zhang, S. Leng, and H. Chai, "A blockchain enhanced dynamic spectrum sharing model based on proof-of-strategy," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[60] 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, 2020.

[61] Y. Xiao *et al.*, "Decentralized Spectrum Access System: Vision, Challenges, and a Blockchain Solution," *IEEE Wirel. Commun.*, 2022.

[62] A. Ashraf and G. Begh, "Blockchain Based Scalable Model for Secure Dynamic Spectrum Access," *Blockchain Based Scalable Model Secure Dyn. Spectr. Access*.

[63] F. Patel, P. Bhattacharya, S. Tanwar, R. Gupta, N. Kumar, and M. Guizani, "Block6Tel: Blockchain-based spectrum allocation scheme in 6G-envisioned communications," in *2021 International Wireless Communications and Mobile Computing (IWCMC)*, 2021, pp. 1823–1828.

[64] 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. Inform.*, vol. 18, no. 4, pp. 2773–2783, 2021.

[65] S. Balamurugan, "SECURE AND SPECTRUM EFFICIENT FRAMEWORK USING BLOCKCHAIN FOR 5G HETEROGENEOUS SYSTEMS".

[66] H. Alhosani, M. H. ur Rehman, K. Salah, C. Lima, and D. Svetinovic, "Blockchain-based solution for multiple operator spectrum sharing (MOSS) in 5G networks," in *2020 IEEE Globecom Workshops (GC Wkshps*, 2020, pp. 1–6.

[67] 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.

[68] B. Mafakheri, T. Subramanya, L. Goratti, and R. Riggio, "Blockchain-based infrastructure sharing in 5G small cell networks," in *2018 14th International Conference on Network and Service Management (CNSM)*, 2018, pp. 313–317.

[69] A. Okon, N. Jagannath, I. Elgendi, J. M. Elmirghani, A. Jamalipour, and K. Munasinghe, "Blockchain-enabled multi-operator small cell network for beyond 5G systems," *IEEE Netw.*, vol. 34, no. 5, pp. 171–177, 2020.

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

[71] R. B. Uriarte, H. Zhou, K. Kritikos, Z. Shi, Z. Zhao, and R. De Nicola, "Distributed service-level agreement management with smart contracts and blockchain," *Concurr. Comput. Pract. Exp.*, vol. 33, no. 14, p. e5800, 2021.

[72] H. Zhou, X. Ouyang, J. Su, C. de Laat, and Z. Zhao, "Enforcing trustworthy cloud sla with witnesses: A game theory–based model using smart contracts," *Concurr. Comput. Pract. Exp.*, vol. 33, no. 14, p. e5511, 2021.

[73] Z. Shi, S. Farshidi, H. Zhou, and Z. Zhao, "An Auction and Witness Enhanced Trustworthy SLA Model for Decentralized Cloud Marketplaces," in *Proceedings of the Conference on Information Technology for Social Good*, 2021, pp. 109–114.

[74] N. Kapsoulis, A. Psychas, A. Litke, and T. Varvarigou, "Reinforcing SLA Consensus on Blockchain," *Computers*, vol. 10, no. 12, p. 159, 2021.

[75] A. K. Pandey, D. G. Narayan, and K. Shivaraj, "SLA Violation Detection and Compensation in Cloud Environment using Blockchain," in *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2021, pp. 1–6.

[76] R. Ranchal and O. Choudhury, "SLAM: A Framework for SLA Management in Multicloud ecosystem using Blockchain," in *2020 IEEE Cloud Summit*, 2020, pp. 33–38.

[77] K. M. Khan, J. Arshad, W. Iqbal, S. Abdullah, and H. Zaib, "Blockchain-enabled real-time SLA monitoring for cloud-hosted services," *Clust. Comput.*, vol. 25, no. 1, pp. 537–559, 2022.

[78] M. S. Rahman, I. Khalil, and M. Atiquzzaman, "Blockchain-Enabled SLA Compliance for Crowdsourced Edge-Based Network Function Virtualization," *IEEE Netw.*, vol. 35, no. 5, pp. 58–65, 2021.

[79] B. Mafakheri, A. Heider-Aviet, R. Riggio, and L. Goratti, "Smart contracts in the 5G roaming architecture: the fusion of blockchain with 5G networks," *IEEE Commun. Mag.*, vol. 59, no. 3, pp. 77–83, 2021.

[80] N. Weerasinghe, T. Hewa, M. Dissanayake, M. Ylianttila, and M. Liyanage, "Blockchain-based roaming and offload service platform for local 5G operators," in *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, 2021, pp. 1–6.

[81] M. R. M. Bailon and L. Materum, "International roaming services optimization using private blockchain and smart contracts," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 3, p. 544, 2019.

[82] C. T. Nguyen, D. N. Nguyen, D. T. Hoang, H.-A. Pham, N. H. Tuong, and E. Dutkiewicz, "Blockchain and stackelberg game model for roaming fraud prevention and profit maximization," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, 2020, pp. 1–6.

[83] C. Nguyen *et al.*, "Blockroam: Blockchain-based roaming management system for future mobile networks," *IEEE Trans. Mob. Comput.*, 2021.

[84] K. Xue, X. Luo, H. Tian, J. Hong, D. S. Wei, and J. Li, "A Blockchain Based User Subscription Data Management and Access Control Scheme in Mobile Communication Networks," *IEEE Trans. Veh. Technol.*, 2021.

[85] S. K. Palit, M. Chakraborty, and S. Chakraborty, "AUGChain: blockchain-based mobile user authentication scheme in global mobility network," *J. Supercomput.*, vol. 78, no. 5, pp. 6788–6816, 2022.

[86] W. Chen, W. Wang, Z. Li, Q. Ye, and Q. Wu, "Joint pricing and task allocation for blockchain empowered crowd spectrum sensing," *Peer--Peer Netw. Appl.*, pp. 1–10, 2022.

[87] E. San Miguel, R. Timmerman, S. Mosquera, E. Dimogerontakis, F. Freitag, and L. Navarro, "Blockchain-enabled participatory incentives for crowdsourced mesh networks," in *International Conference on the Economics of Grids, Clouds, Systems, and Services*, 2019, pp. 178–187.

[88] X. Xu, Q. Liu, X. Zhang, J. Zhang, L. Qi, and W. Dou, "A blockchain-powered crowdsourcing method with privacy preservation in mobile environment," *IEEE Trans. Comput. Soc. Syst.*, vol. 6, no. 6, pp. 1407–1419, 2019.