IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 27, 2020, accepted June 6, 2020, date of publication June 17, 2020, date of current version July 2, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3003020

A Review on Application of Blockchain in 5G and Beyond Networks: Taxonomy, Field-Trials, Challenges and Opportunities

MOHAMMAD TAHIR[1], (Member, IEEE), MOHAMED HADI HABAEBI[2], (Senior Member, IEEE), MOHAMMAD DABBAGH[1], (Member, IEEE), AMNA MUGHEES[1], ABDUL AHAD[1], AND KAZI ISTIAQUE AHMED[1]

[1]Department of Computing and Information Systems, School of Science and Technology, Sunway University, Subang Jaya 47500, Malaysia
[2]Department of Electrical and Computer Engineering, International Islamic University Malaysia, Kuala Lumpur 53100, Malaysia

Corresponding author: Mohammad Tahir (tahir@sunway.edu.my)

This work was supported by Sunway University Internal Grant Scheme under Grant GRTIN-RSF-SST-DCIS-04-2020.

ABSTRACT Until now, every evolution of communication standard was driven by the need for providing high-speed connectivity to the end-user. However, 5G marks a radical shift from this focus as 5G and beyond networks are being designed to be future-proof by catering to diverse requirements of several use cases. These requirements include Ultra-Reliable Low Latency Communications, Massive Machine-Type Communications and Enhanced Mobile Broadband. To realize such features in 5G and beyond, there is a need to rethink how current cellular networks are deployed because designing new radio access technologies and utilizing the new spectrum are not enough. Several technologies, such as software-defined networking, network function virtualization, machine learning and cloud computing, are being integrated into the 5G networks to fulfil the need for diverse requirements. These technologies, however, give rise to several challenges associated with decentralization, transparency, interoperability, privacy and security. To address these issues, Blockchain has emerged as a potential solution due to its capabilities such as transparency, data encryption, auditability, immutability and distributed architecture. In this paper, we review the state-of-art application of Blockchain in 5G network and explore how it can facilitate enabling technologies of 5G and beyond to enable various services at the front-haul, edge and the core. Based on the review, we present a taxonomy of Blockchain application in 5G networks and discuss several issues that can be solved using Blockchain integration. We then present various field-trials and Proof of concept that are using Blockchain to address the challenges faced in the current 5G deployment. Finally, we discuss various challenges that need to be addressed to realize the full potential of Blockchain in beyond 5G networks. The survey presents a broad range of ideas related to Blockchain integration in 5G and beyond networks that address issues such as interoperability, security, mobility, resource allocation, resource sharing and management, energy efficiency and other desirable features.

INDEX TERMS Blockchain, 5G, network slicing, C-RAN, D2D, SDN, NFV, smart contracts, reinforcement learning, network security, network management, spectrum management, resource allocation, V2V, cloud computing, MEC.

I. INTRODUCTION

The cellular standards have evolved continuously where each generation offered new services and features based on market needs. The primary focus of this evolution was mostly based on increasing throughput, coverage and capacity. With several advances in other technological domains, the demand has extended beyond the need for higher throughput to support massive machine to machine (M2M) type communication and applications that require high reliability and low latency communication. All these factors will result in an exponential increase in the traffic volume as it is expected that the demand

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

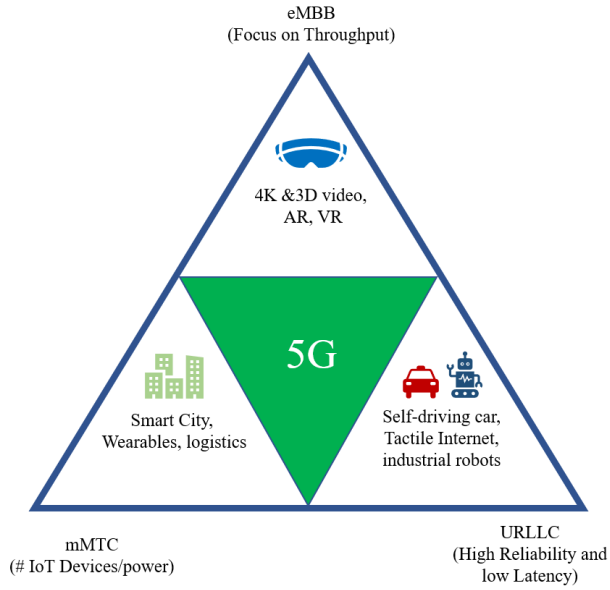

FIGURE 1. 5G use case.

for data traffic will increase 1000 folds by 2020 [1]. Also, the number of connected devices is increasing exponentially and it is expected that there will be approximately 50 billion devices by 2021 [2]. The wide ranges of use cases that 5G aims to address, as shown in Figure 1, are broadly classified under the following categories:

- Enhanced Mobile Broadband (eMBB): This use case is in line with the previous generation use cases where the aim is to provide a higher data rate. 5G aims to provide 10 to 100× improvement over 4G and 4.5 networks which is equivalent to 10Gbps.
- Ultra-Reliable Low-Latency Communication (URRLC): This use is geared to those mission-critical services that require extremely low error rate (high reliability) and low latency. These applications usually do not require a high data rate.
- Massive Machine Type Communications (mMTC): With the rise of the Internet of Things (IoT) the ubiquity of devices has necessitated the development of connectivity standards that can support high device density with low power consumption. Usually, IoT devices operate on battery and are expected to last several years (≈10 years). The previous generations did not consider such scenarios.

It should be noted that the use cases mentioned are typical use cases of 5G. There might be some applications that may need a combination of such typical use cases.i.e. high data rate and low latency. The 5G road map comprises a broad vision and aims to realize 10–100× peak-rate data rate, 1000× network capacity, 10× energy efficiency and 10–30× lower latency compared to current 4G standards to pave the way towards Gigabit wireless. Realizing and fulfilling such a diverse set of requirements needs a radical shift in the way networks are designed. This is particularly important because point-to-point link throughput is very close to the theoretical limits.

To address the issues of past generations and meet the diverse requirements, several technological breakthroughs are being integrated into wireless communication networks. These technologies applied at different levels in the network include Software-Defined Network (SDN), Network Function Virtualization (NFV), multi-access edge computing and cloud computing. Besides the new technologies, several new radio access techniques such as millimetre wave (mmWave), massive MIMO, ultra-densification and device-to-device connectivity will also assist in meeting the key 5G specifications. These technologies, as shown in Table 1, are the cornerstone for building a flexible and scalable network. It is necessary to use such a wide range of technologies because the 5G networks need to be flexible and able to evolve in future. There have been several successful deployments of the 5G networks across almost all the continents to test the capabilities of the 5G network [3]. Most of the promises that 5G networks are expected to deliver (e.g. 8K video streams, fully connected cars) will be demonstrated at commercial scale during summer Olympics and Paralympic Games in Tokyo (postponed to 2021) [4].

However, integration of so many technologies to deliver various services creates several challenges for security, network resiliency, privacy, robustness and data integrity. At present most networks rely on centralized architecture which will not work well with a rapid rise of devices and data. The centralized architecture also creates a security issue for the 5G ecosystem. All devices are identified, authenticated and connected by the corresponding authentication centre. The communication between devices has to go through the network even when they are in the vicinity. Such a model is prone to bottlenecks, downtime and coordinated attacks that might affect the operation of the entire network. To overcome this issue, one solution is to make use of decentralized and distributed architecture. Unlike traditional networks, future networks are expected to be distributed and decentralized in nature. A distributed design of 5G network can yield massive performance gains from the physical layer all the way up to the application layer. Also, the 5G networks will operate in a dynamic and complex environment where the nodes will interact and cooperate to improve their performance.

Despite several technological advances, the 5G networks are still a long way from being autonomous, self-managed, cooperative and decentralized. Distributed and decentralized networks are crucial to the success of various IoT use cases, Vehicle to Vehicle (V2V), Device to Device (D2D), computing and storage. In general, any use case that needs collaboration and cooperation can benefit immensely from the decentralized design of the network. Blockchain, in particular, offers huge potential to address several challenges across the entire ecosystem and deal with the continuous growth of wireless devices, data traffic and services. Blockchain is a distributed ledger that is immutable, transparent and

TABLE 1. Enabling technologies for 5G.

Tier	Technology	Role in 5G	Features offered
Core	SDN	Separate control and data plane that allows for flexible and programmable 5G infrastructure with fine-grained control over applications and services.This separation results in a swift response to changing market and user needs.	Network Slicing, Flexible deployment of network functions, enhanced QoE, easier maintenance and provisioning.
	NFV	Virtualizes network functions (.e.g.firewall, VPN) so that they can deploy on-demand anywhere in the network without relying on specialized hardware. This helps in enabling 5G network slicing that allows running multiple networks on top of a single physical infrastructure.	
	Cloud Infrastructure	Use a well-established cloud computing paradigm to make the cellular network more agile, flexible, and scalable. This allows the network operator to deliver innovative and customized services/applications to end-user.	Analytics, hosting Data center
Edge	Cloud RAN	Provide a flexible and scalable RANs to resolve capacity and coverage issues efficiently using cloud computing	Reduced capex/opex, reduced delay, energy saving improved management.
	Multi-access Edge	Enables the data to be processed closer to the user enabling the network to deliver ultra-low latency required by mission-critical applications.	Storage, Computing, Analytics
Radio access network	Massive MIMO	Using antenna array with over 100 elements to provide spatial multiplexing and diversity gain.	Beamforming, spatial multiplexing
	mmWave	Use of high frequency band (30 GHz) to provide increased bandwidth for high data rate.	ultra high bandwidth and throughput
	Full-Duplex	Increase system capacity by simultaneous transmission and reception over the same frequency band.	Spectrum efficiency, reduced latency, energy efficiency
	Device to Device	Allow the device to communicate directly to allow low latency, high data rate and coverage. The control plane can be managed by the Base station.	Reduced latency, improved capacity, connectivity and throughput.
	Ultra-densification	The goal of using small cells is to increase the number of cells per square kilometre. This increases capacity and frequency reuse.	Increased throughput, improved coverage

decentralized in design which works on the peer-to-peer (P2P) network architecture. The potential of Blockchain has resulted in gaining considerable attention in the telecom industry [5], [6]. Besides, Blockchain has been studied for its potential to be applied on other domains, such as IoT [7], V2V [8], [9], edge computing [10], cloud/fog computing [11] and radio access networks (RANs) [12].

A. MOTIVATION

As highlighted in the previous section, the 5G networks need to handle a massive amount of data generated by IoT devices and provide connectivity to billions of devices with varying degree of Quality of service (QoS). Additionally, delivering the services via a combination of several technologies needs intricate coordination and collaboration that requires an open, transparent, and secure system across the entire 5G ecosystem. For example, the ultra-dense small cell networks in 5G infrastructure used to provide data rates and low latencies introduce security and reliability concerns in the network. The security issues may arise due to installation of evil-twin whereas the reliability issues may result due to frequent handover because of cell size. Therefore, providing a reliable and secure connection is important but at the same time challenging for 5G networks.

Blockchain is one of the most promising technology that has the potential to revolutionize the way services are offered across various industries, with 5G being no exception. It provides a distributed, immutable, single source of truth that everyone agrees upon without relying on a middleman. Blockchain has the potential to be integrated with the 5G network to enable end-to-end services delivery across the entire 5G ecosystem. Furthermore, Blockchain has been identified as one of the key enablers for 6G networks at the Mobile World Congress (MWC).[1] Therefore, Blockchain will play a significant role in realizing the full potential of the 5G and beyond networks that include autonomic resource management, security and fraud prevention, ubiquitous computing, reliable content distribution and data management. Blockchain with its inherent properties will enable data transactions in a P2P manner with high security and trustworthiness to enable a variety of services in the 5G networks. At present, the biggest challenge for current 5G platforms is the need to guarantee an open, transparent, and fair system within the extraordinary number of resources and several malicious users [17]. Blockchain with its unique features of decentralization, high level of data privacy, security, transparency and immutability become an obvious choice. Therefore, there is a need to integrate Blockchain into 5G architecture. This architecture will result in a self-maintaining, self-servicing, and self-managing network that can carry out transactions, handle automatic and secure update without the need of a central broker. A Blockchain framework will assist a new generation of distributed wireless networks by allowing seamless provisioning between heterogeneous access nodes and devices. With Blockchain, provisions and agreements between access nodes, networks, and subscribers are negotiated on-the-fly as digital smart contracts. Blockchain will allow devices on the network to negotiate the best service with the network operator which will be then executed using the smart contract. This model will allow for customized service delivery to individual nodes on the network resulting in new charging and business models in the 5G network [5]. Also, the integration of various technologies has led to a new core architecture which will phase out the current Evolved Packet Core (EPC).

[1] https://www.mwcbarcelona.com/, accessed December 2019.

TABLE 2. Existing surveys on 5G and Blockchain.

Reference	Scope	Focus	Limitations
[13]	opportunities and use cases	high-level technical details including system designs and architectures	Lacks depth and coverage of application with respect to 5G ecosystem
[14]	Holistic review of Blockchain application in 5G network	Detailed discussion on Blockchain adoption for 5G enabling technologies, services and use cases in IoT.	Lacks Layered wise systematic analysis and taxonomy of Blockchain application in 5G application.
[15]	Review of Blockchain application in 5G Enabled IoT network	Detailed discussion on Blockchain adoption for IoT networks.	lacks emphasis in context to application in 5G network.
[16]	Blockchain for 5G based Industrial Automation	comprehensive review on Blockchain-based 5G-enabled IoT and discussed its potential industrial applications.	Lack emphasis and detailed discussion in context to 5G network.

Since the 5G architecture is still in the roll-out phase it is important to integrate the Blockchain to realize the full potential of 5G networks.

Besides the benefit of Blockchain in the 5G network, 5G will enable widespread use of Blockchain-based solutions as well. For example, 5G will accelerate the adoption of IoT by providing ubiquitous connectivity at low energy and low cost. In order to secure and enable micro-transaction between billions of IoT devices Blockchain solutions such as IoTA [18] may be used. Furthermore, Blockchain and 5G along with Artificial Intelligence (AI) will combine to form a new stack of technologies that will accelerate the adoption of Fourth Industrial Revolution (IR 4.0) adoption.

B. COMPARISON WITH EXISTING LITERATURE

Surveys have been conducted in relation to application of Blockchain in several areas such as IoT [19], industry [20], smart city [21], Unmanned Aerial Vehicles (UAVs) [22], edge computing [23] and artificial intelligence [24]. There are limited surveys [13], [14] on the application of Blockchain in 5G networks with varying degree of scope. In [13], various opportunities and challenges concerning the application of Blockchain in 5G are presented. However, the discussion is limited to application to a few areas and does not discuss the Blockchain application from an architecture point of view. The survey presented in [14], provides a comprehensive coverage addressing various aspects of 5G application to Blockchain but excludes taxonomy and layered wise approach for Blockchain integration. Based on the evaluation of existing work, our survey is significantly different as we provide a holistic coverage on the application of Blockchain from a layered perspective which has not been covered so far in such a comprehensive manner. Table 2 provides a summary of the existing literature in a comparative manner, which also supports our claim of lack of comprehensive survey as presented in this paper.

C. NOVELTY AND CONTRIBUTION

In this paper, we present a detailed survey on the application Blockchain in the 5G network which forms the foundation of future networks such as beyond 5G and 6G. This survey aims to address a range of issues faced by various 5G enabling technologies such as Multi-access Edge Computing (MEC), SDN, NFV, cloud computing, network slicing, and D2D communication. In particular, the main contributions of this paper are summarized as follows:

1) A detailed discussion on the benefits of applying Blockchain into the 5G ecosystem.
2) Taxonomy of application of Blockchain in 5G networks found in the literature.
3) End to End categorization of Blockchain applications in the 5G ecosystem using a layered approach.
4) Summary of recent field trials and Proof of Concept (PoC) using Blockchain in 5G network.
5) Research challenges, open issues and research directions for the application of Blockchain in the 5G ecosystem.

To the best of our knowledge, this survey is unique since it captures the application of Blockchain from a different perspective that allows researchers to understand how the Blockchain can be applied to 5G networks using the end-to-end approach. Our work specifically focuses on the opportunities and challenges which come with the application of Blockchain in a distributed 5G deployment for enabling new service delivery models across the entire 5G ecosystem.

D. ARTICLE ORGANISATION

Section II presents a brief overview of Blockchain, 5G and the key driving factor for Blockchain integration in 5G. Section III presents the proposed taxonomy of Blockchain application in 5G based on the work found in the literature. Section IV summarizes the key field trials and PoCs underlining the importance of Blockchain integration in 5G. Section V discusses various challenges and possible research directions for the readers interested in pursuing research in the area. Finally, the conclusion is drawn in Section VI.

II. BRIEF OVERVIEW OF BLOCKCHAIN AND 5G

At first, the need for Blockchain in 5G may not seem to be a necessity. But when we look at the benefits of Blockchain it warrants its applicability in 5G as it addresses several key challenges faced in terms of decentralization and network management. In this section, we give a brief overview of Blockchain and 5G and draw a parallel between the features of Blockchain and its applicability in the 5G networks.

A. BLOCKCHAIN OVERVIEW

Blockchain has been revolutionizing various industries since its inception as an underlying technology behind Bitcoin. Blockchain facilitates a decentralized, reliable, secure, and immutable ledger which permits transactions to be performed between two nodes without the need to be processed by a

central entity. Since Blockchains are decentralized there is no single point of failure or attack. All data recorded on Blockchain is visible to all participating nodes and can be verified by all involved nodes. All transactions in the Blockchain network are recorded in the Blocks which is then verified by the participating nodes in a given timespan using a consensus algorithm. The Blockchain is built by linking such verified Blocks using a linked list, or chain of blocks. The prominent privileges of Blockchain have directed governments and business leaders towards transforming their business processes using this emerging technology in recent years. Some of the well-known Blockchain platforms, other than Bitcoin, are Ethereum [25] and Hyperledger Fabric [26].

1) TYPES OF BLOCKCHAIN

There are three types of Blockchain referred to as public, private and consortium. In a public Blockchain, like Bitcoin, any node can join the Blockchain network and can participate in Blockchain operations. A private Blockchain is a restricted Blockchain that operates in a closed network within an organization where only selected members are participants of a Blockchain network. Private Blockchains are used when scalability and compliance with data privacy rules and other regulatory issues are required. Consortium Blockchain is managed by more than one organization. Consortium Blockchains are typically used by bank and network operators. The key component and characteristics of Blockchain are:

- Shared database or ledger – It is an append-only ledger that records all transactions and is shared with all involved participants.
- Smart contract – A piece of executable computer code that is stored on Blockchain and is executed once certain conditions are met.
- Consensus- Consensus refers to an agreement among the participating nodes in a P2P network for approving the transaction.
- Trustless – No reliance on the third-party for ensuring authenticity and protection of the information. The P2P network of nodes protects the network and builds trust using a consensus algorithm.
- Transparency – All nodes in the network are aware of all transactions and can independently verify each transaction.
- Provenance- All the transactions in the network can be tracked and verify how the ownership of data has changed over time.
- Immutability- All recorded data recorded on Blockchain is tamper-resistant. Changing the data stored on Blockchain requires control of the majority of the nodes (51% attack) in the Blockchain network.

2) CONSENSUS PROTOCOL

Consensus protocol acts as an integral component of any Blockchain platform. Before adding any new block to the chain of existing blocks, an agreement must be reached among all participating nodes distributed in the P2P network. This approval procedure is performed through a mechanism referred to as the consensus protocol. Consensus protocols play a crucial role in adopting a Blockchain platform into an enterprise since they directly affect the characteristics and functionalities of a given Blockchain platform. Some of the popular consensus protocols include Proof of Work (PoW), Proof of Stake (PoS), Proof of Activity (PoA), Practical Byzantine Fault Tolerance (PBFT), LibraBFT, etc. Some of the objectives considered while designing the consensus protocols are:

- Agreement: Reach an agreement on the transactions among the majority of the nodes in the network.
- Collaboration: Each node works toward a common goal for the interest of the network.
- Rights: The contribution of each node is counted and taken for approving the transaction.
- Participation: Every node in the network needs to contribute toward an agreement.
- Activity: Every node in the network is equally active and has the same responsibility.

3) SMART CONTRACT

A smart contract is a piece of executable computer code (functions and data) written using a specific programming language. Smart contracts are stored on top of a Blockchain network and will be executed once certain conditions are met. They facilitate decentralized automation by allowing all participating nodes in a Blockchain to perform transactions without the need of a third-party entity. The most well-known Blockchain platform that supports the creation of a smart contract is Ethereum. It deploys a scripting language called Solidity to implement smart contracts. Hyperledger Fabric Blockchain platform uses another term, called chaincode instead of a smart contract. Chaincode can be implemented using Go or Java programming language. The smart contract can run concurrently in the network or maybe deployed dynamically.

B. 5G OVERVIEW

5G is the next generation of cellular networks developed in response to meet the growing demand for a variety of new services such as autonomous vehicles and massive IoT. The 5G study was initiated by 3GPP in Rel-14 to study the feasibility of 5G. At the moment, in Rel 16 the specification of 5G is expected to be finalized by 2020. In this section, we provide a brief overview of 5G design requirements, architecture and enabling technologies.

1) 5G DESIGN REQUIREMENTS

5G aims to provide high data rates, coverage, connectivity and bandwidth, with a massive reduction in latency and energy consumption. A summary of certain requirements that 5G needs to support is provided in Table 3. The requirements

TABLE 3. 5G requirement (based on IMT-2020).

Metric	Minimum Requirement	Use case	Enabling Technology
Peak Data rate	Downlink peak data rate - 20Gbps Uplink peak data rate - 10Gbps	eMBB	Millimeter wave communications; Massive MIMO; Ultra-densification Beamforming
Peak Data rate (dense deployment)	Downlink : 100Mbps Uplink : 50Mbps	eMBB	
Peak Spectral Efficiency	Downlink : 30 bit/s/Hz Uplink :15 bit/s/Hz	eMBB	
Latency (User Plane)	4 ms	eMBB	D2D communications; Big data; MEC, SDN, NFV
	1 ms	URLLC	
Density	connection density is 1,000,000 devices per km^2	mMTC	Ultra-densification; D2D communications; Software-defined networking

are quite strict and improve significantly on the specifications that were set for 4G. The data rate requirement is 10 times more than traditional LTE network theoretical peak data rate of 1 Gbps and the latency reduction is by the same factor of 10.

2) 5G ARCHITECTURE

To achieve the requirements listed in Table 3 and overcome the limitation of traditional wireless network design, the cellular networks of future are going to be multi-tier heterogeneous network consisting of macrocells, microcells, picocells, femtocells. In addition to the cell-based design, the network will be supplemented by a large number of low power nodes such as small cells, relays, remote radio heads (RRHs) along with the provisioning for D2D and M2M communication. This deployment will result in a very dense network that provides flexible coverage area and improves spectral efficiency. To cope up with the dense deployment and reduce the CAPEX and OPEX concept of Cloud RAN (C-RAN) is adopted in 5G. Along with C-RAN, network virtualization and softwarization will enable to deliver various services on-demand [27]. Network virtualization allows the same physical resources to be shared with a variety of services by slicing the physical infrastructure logically. Whereas, softwarization will allow the network to be programmable, flexible, and adaptable by using software programming to design, implement, deploy, manage and maintain network equipment/components/service. Both virtualization and softwarization of the network are important for meeting 5G network requirements as well as to provide E2E service management and improve the end-users QoE [28]. The E2E service platform unification will be realized by network softwarization, and virtualization using SDN, NFV and cloud computing technologies. Using the softwarization and virtualization technologies will enable the operators to quickly build application-aware networks and network-aware applications to deliver customized services and business models. In this following subsections, we briefly discuss various enabling technologies and how they will shape 5G.

3) 5G ENABLING TECHNOLOGIES

Here, we will briefly discuss various enabling technologies that are going to be an integral part of 5G networks.

1) **Cloud Computing**: Cloud computing enables resources sharing by virtualizing physical infrastructure that can be provisioned dynamically to accommodate requests for applications, platforms, and heterogeneous computing infrastructures. The physical resources that can be shared include servers, networks, storage, service and applications. The cloud computing environment consists of Infrastructure Providers (InPs) and Service Providers (SPs). The InPs operates and manages the physical infrastructure whereas the SPs lease the resource to provide services to the end-user. The same concept can be extended to 5G networks to create virtualized wireless networks where the network operator may lease the resource from InPs. As an example, the InPs may own the physical cellular infrastructure and radio resources. The Mobile Virtual Network Operator (MVNO) leases the resources from InP, creates and operates virtual resources, and assigns to the subscribers to provide various services. This creates exciting opportunities for innovation, rapid development and delivery of services that were not possible before. Furthermore, the application of cloud computing to RAN architecture results in improved flexibility, scalability and resource utilization. A Cloud-RAN or Centralized-RAN (C-RAN) are being designed to leverage cloud computing to provide flexible and scalable RANs to resolve capacity and coverage issues efficiently. In C-RAN, the Baseband processing unit of the base station is separated from the analog unit (RRHs) and moved to the cloud (referred to as the BBU pool). A BBU pool serves a group of RRH of a particular area. The transmission and reception of the signal are carried out by RRH which involves digital processing, digital to analog conversion, analog to digital conversion, power amplification and filtering. On the other hand, the processing of the signals such as coding, modulation, Fast Fourier Transform (FFT) is done at the BBU pool in the cloud. The use of densely deployed RRHs and C-RAN enhances the scalability, improves network capacity, and extends the coverage of future 5G systems.
2) **Software-defined networking (SDN)**: SDN [29] is an approach that allows the users to manage the network

equipment using the software that can run on commodity hardware rather than directly on switches or routers. In the case of 5G network, SDN is capable of orchestrating and controlling applications/services in fine-grained and network-wide manner [30]. This is done by separating the network control from the data plane where the centralized control plane manages several devices. The separation provides flexibility and centralized control with global visibility of the entire network allowing it to respond rapidly to changing network conditions and end-user needs.

3) **Network Function Virtualization (NFV)**: NFV enables the virtualization of entire network functions (firewall, VPN, router, switches) that were implemented in specialized hardware to run on cloud infrastructure. Specialized hardware, which is usually very expensive, has interoperability issues and is barely programmable. These constraints result in low agility, leading to longer product cycles for the network operator. NFV decouples physical hardware from the associated network functions and allows it to run on generic cloud servers, thus providing advantages in scalability and flexibility. The SDN and NFV are complementary to each other and are an essential part of the 5G network. The similarity between SDN and NFV is that both use network abstraction and depend heavily on virtualization. SDN separates network control functions from network forwarding functions, whereas NFV separates network functions from the hardware on which it runs.
   SDN and NFV differ in how they separate functions and abstract resources. SDN abstracts physical networking resources such as switches, routers and moves decision making to a virtual network control plane. The virtual control plane decides where to send traffic, while the hardware continues to handle the traffic. NFV aims to virtualize all physical network resources beneath a hypervisor, which allows the network to grow by spinning virtual machines without adding devices in the network. While, both SDN and NFV provide flexibility and make the network more dynamic, they perform different roles in defining those architectures and the infrastructure they support.
4) **Multi-Access Edge Computing (MEC)**: The idea was proposed by ETSI to make use of distributed computing close to UEs to reduce the network congestion and therefore achieve a faster response. In 5G networks, MEC enables the delivery of cloud computing capabilities at the edge of the network [31]. MEC enables the data to be processed closer to the user enabling the network to deliver ultra-low latency required by mission-critical applications. Also, by processing data locally, MEC can significantly reduce data transfer costs. Other benefits include enhanced QoS/QoE to end-users, optimization of mobile resources by bringing computationally intensive applications at the network edge and transforming radio access nodes into intelligent service hubs where context-aware services can be provided.
5) **Device to device (D2D)**: In existing cellular networks, all the communication happens between base stations and devices. Even when the two devices are in the vicinity, the communication has to go through the base station. This way of communication is inefficient for real-time services requiring high data rates and low latency. Therefore, to improve spectral efficiency, the concept of D2D communication was proposed in [32] to create multi-hop relays among devices. In 5G networks, the D2D link will be facilitated with the help of the base stations to enable applications such as file sharing, gaming, and social networking. D2D communications will help to improve QoS of the cellular network, increase the data rates of the users at the cell edge and offload the BS capacity by reducing unwanted traffic. From the application point of view, D2D communications facilitate the development of several innovative applications and services. For example, in the case of natural disasters, cellular networks may not be available, in such scenarios D2D communications can be used for rescue and relief operations. D2D communications will assist in machine-type communications requiring low-latency especially vehicle-to-vehicle communications where it can be used to get information on accidents, alerts about routes and other relevant information.
6) **Network Slicing**: Applications like video streaming, remote surgery and smart metering vary vastly in terms of their requirement of QoS and QoE. Therefore, the network needs to cater to such diverse QoS needs. Until now, the focus of the cellular network was on delivering high-speed connectivity making the network seemingly rigid that only caters for specific use cases. But with technologies like SDN and NFV, it is now possible to slice the physical network infrastructure into multiple virtual networks which are referred to as network slices. Network slicing enables logical networks that are customized to meet the QoS required by each application. This creation of a logical network creates opportunities for new products and services that can be brought to market quickly and can be adapted to the changing demands. Network slices can be set up based on various service characteristics such as data rate, bandwidth and latency demand. For example, a network slice can be created for Augmented Reality (AR) that requires high throughput and low latency, another slice for Massive IoT that provides connectivity for smart electricity meters and a slice for applications that require high-reliability and security levels.

C. DRIVERS FOR BLOCKCHAIN INTEGRATION

5G networks are expected to deliver a wide range of services across several vertical sectors. This will require a rapid

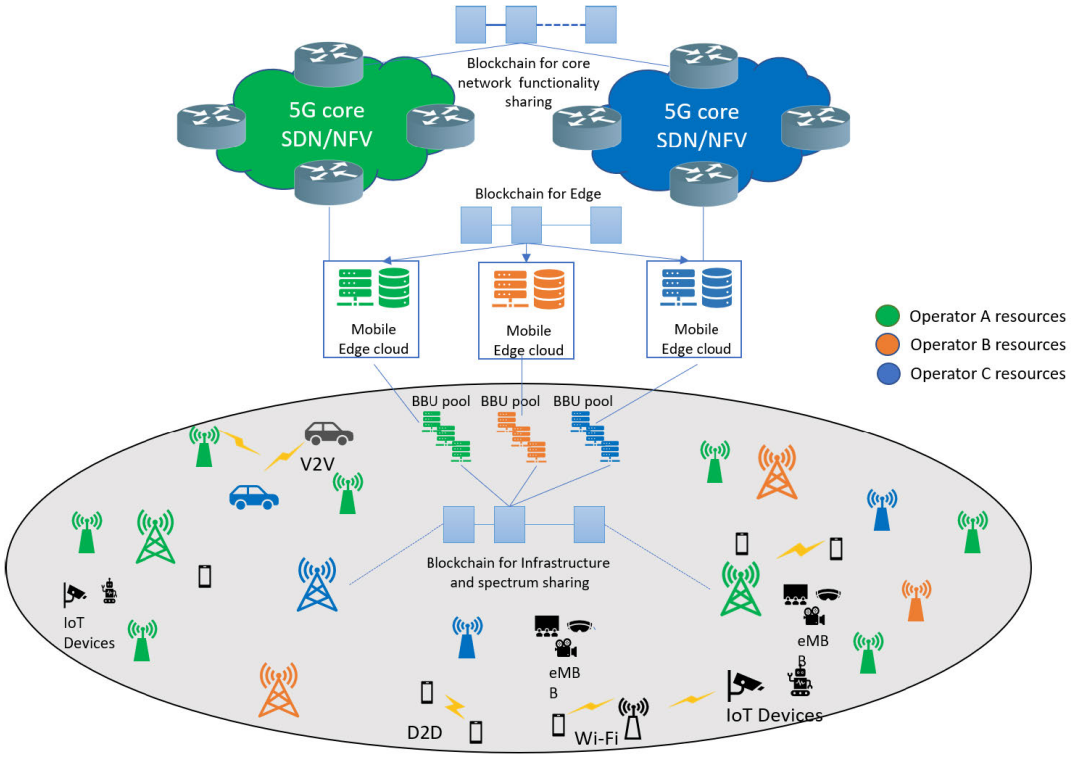

FIGURE 2. 5G architecture with Blockchain integration.

allocation of resource and network orchestration. Some of the verticals that are expected to be enabled by 5G are:

- IoT for several application like smart city, transportation, smart grid, critical infrastructure monitoring and smart-health
- Vehicle to Vehicle communication
- Collaborative gaming, AR, VR and UHD video streaming.

These verticals are quite diverse in their requirements in terms of speed, latency and capacity as presented in Table 3. To meet such diverse requirements on the fly, a high degree of coordination and configurability in the network is required that can be done automatically in a secure and reliable manner. Furthermore, 5G networks are going to be highly distributed and require the addition of several new technologies such as edge computing, small-cells, SDN, NFV, cloud and D2D. It is possible that the complexity of 5G and beyond 5G network will surpass the capability of a single operator to manage the network from end to end. It will not be a viable option to deploy such a large amount of network elements from both cost and manageability point of view. Therefore, the resources need to be shared between several stakeholders to provide services across the regions to the end-users. For example, radio infrastructure can be shared among operators, the spectrum can be leased, storage and computation can be shared. Therefore, in the future 5G network, a high degree of coordination will be required across several stakeholders. All these requirements present several challenges such as security & privacy, manageability, service level agreements (SLAs) and interoperability.

Blockchain, specifically the consortium Blockchain, is perfectly poised to solve these challenges in 5G networks. Blockchain is a decentralized network itself that can fit perfectly in a distributed network like 5G. Since multiple stakeholders are involved it is difficult to build trust and at the same time guarantee security, privacy and hassle-free settlement of dues. With Blockchain, no single stakeholder will be in control and all the data will be available to everyone. To share or lease resources, the stakeholder needs to enter into an agreement using a smart contract to ensure agreed SLA implementation. The smart contract based on the agreed SLA will automate the process of resource allocation and network orchestration involving several stakeholders across the entire 5G network to deliver seamless service to end-users. The entire process will be transparent to all stakeholders providing a secure, reliable and auditable trail of transactions on the Blockchain. A conceptual diagram showing the integration of Blockchain in a 5G network consisting of several operators is presented in Figure 2. In the following section, we present the Taxonomy of Blockchain application in 5G and discuss various examples where the application of Blockchain can improve the performance by addressing various key issues.

III. TAXONOMY OF BLOCKCHAIN APPLICATION IN 5G

The Blockchain, when integrated into the 5G network, will offer many benefits at various levels in the entire

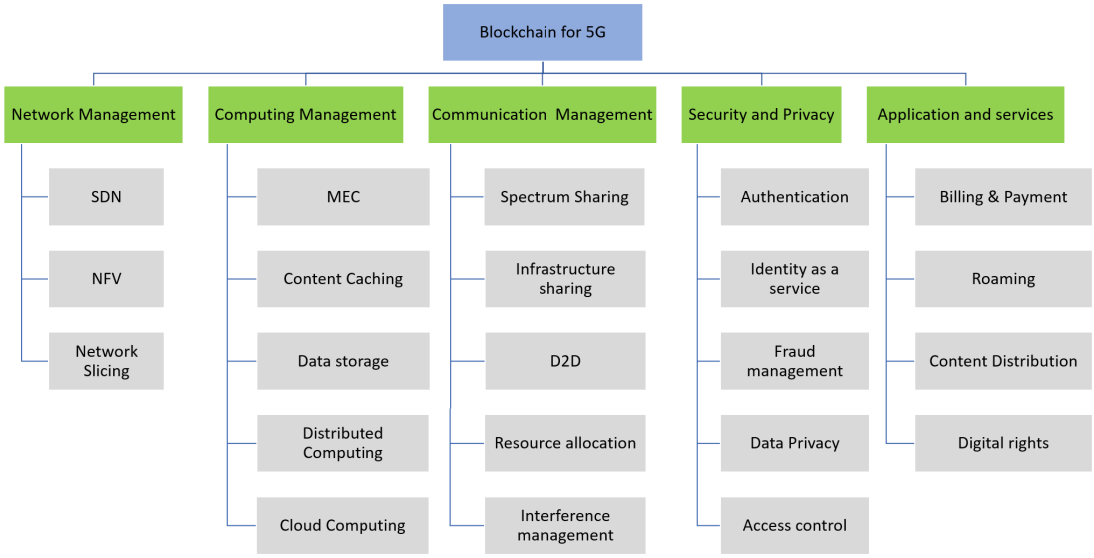

FIGURE 3. Taxonomy of Blockchain application in 5G.

5G ecosystem. Networks integrated with Blockchain can be customized based on location and subscriber needs and adjusted dynamically to meet the supply and demand. Blockchain can help improve the internal operation in the core network such as Operational Support Systems (OSS) and Business Support Systems (BSS) to reduce costs and increase flexibility. Several functions from OSS and BSS can be delegated to the edge using P2P negotiation aided by Blockchain transactions that will help in reducing latency. In this section, we provide a taxonomy of Blockchain applications in 5G networks. The proposed taxonomy presented in Figure 3 is based on the relative application of Blockchain in the 5G ecosystem and existing work found in the literature. The following subsection presents a detailed overview of various classification and its implications.

A. NETWORK MANAGEMENT

As discussed earlier, network virtualization and softwarization will be a common practice to meet the constantly changing demands of the end-users and businesses. SDN, NFV and network slicing will be a crucial part of this softwarization effort to build application-aware networks and network-aware applications. Such dynamic network orchestration and management presents a challenge in terms of running the network efficiently, optimally, and securely. To streamline the process and overcome the challenges several researchers are investigating the application of Blockchain in network management.

1) SDN

SDN allows the network to be more flexible in deployment and results in shorter provisioning time for new IP based services by exploiting network resources more efficiently. However, there are several challenges for the application SDN in 5G network in terms of scalability, performance, reliability, interoperability that can be addressed by Blockchain.

- **Decentralization**: In a traditional network, in case of network device failure the data is routed through alternative routes to keep the flow of data. However, centralization of the control plane in SDN can result in a single point of failure [33] when under attack or compromised. Therefore, there is a need for developing a distributed SDN architecture with provisions for an alternate controller that can handle traffic flow to ensure network reliability. Research work [34], [35] have emphasized on the need for distributed control planes in a software-defined wide area network (SD-WAN) architecture where multiple controllers on real WAN topologies can benefit both control plane latency and fault-tolerance. However, the best and most optimal approach to decentralizing the control plane in order to harness the full potential of SDN is still a research challenge. Furthermore, scalability, reliability, consistency, and interoperability are also major concerns in the case of distributed SDN architectures as they are highly impacted by the structure of the distributed control plane [36].
- **Scalability**: SDN architecture contains centralized or partially distributed controllers that interface with the data planes on multiple network devices. The controller can become the performance bottleneck as the network grows. In particular, a network with large networking requests, such as a 5G network, can overwhelm the controllers. The scalability issue can be addressed by a decentralized control architecture that contains split or distribute the control planes. Decentralization of the control plane has its challenges such as convergence and numerous control instances to configure and manage.
- **Performance** - The separate control and data plane architecture can introduce latency into SDN. In large

networks, this can result in an unacceptable level of delay and degrade network performance. Controller response time and throughput can contribute to poor performance resulting in scalability issues. The solution for several performance issues in large and growing networks is to push more intelligence to the data plane or move to a distributed control plane architecture of some type. While this can improve SDN performance, it tends to replicate traditional networks built on fully distributed intelligent devices. A balance has to be sought where virtualization is maintained without degrading network performance or introducing potential single points of failure.

- **Security** - Control plane plays a central role in an SDN architecture, therefore security strategies must focus on protecting the controller. In particular, it is important to authenticate access to the control plane. Also, the decentralization of the SDN control minimizes the risk due to a single point of failure and attacks (e.g., DDoS attack). However, the integrity of the flow of information between the SDN controllers and switches is vulnerable. An attacker can compromise the network by masquerading as an SDN controller. Also, the lack of standards and guidelines for software development can lead to security vulnerabilities. For example, third-party providers can access the network and modify control rules without the consent of SDN controllers, leading to serious data leakage risks. Another aspect related is the isolation (in the case of multi-tenancy) of flows and network related to network virtualization. SDN will be secure if they are deployed using equipment from a single provider and no communication beyond the defined trust boundary [37]. Such deployment would limit several benefits offered by SDN as it would only implement only a subset of various SDN features.
- **Network monitoring**: Collecting relevant information without affecting network performance is a challenging task. The continuous monitoring of network data may result in large overheads that may affect network performance. While the lack of monitoring may cause unexpected behaviour of management applications. Furthermore, ensuring transparency of mapping information is another challenge in monitoring the networks [38].

It can be seen, several issues need to be addressed for SDN to be fully utilized in the 5G and beyond networks. In the past few years, researchers have tried to integrate Blockchain in SDN architecture to address the above-mentioned issues. In [39], DistBlockNet is proposed for a distributed secure IoT network that uses SDN and Blockchain to provide adaptability, reliability, scalability and security. It makes use of Blockchain to update a flow rule table by securely verifying the version of the flow rule table, validating flow rule table and downloading the latest flow rules table for the IoT forwarding devices. Since IoT will be a key part of 5G the same proposed architecture is very well applicable for the 5G ecosystem or any distributed network in general. In [40] a Blockchain-based framework for IoT networks in SDN-enabled 5G-VANET is presented to enhance the security and efficiency of the vehicular system. The Blockchain protocol runs on every active unit (on-board units, Roadside units and gNodebs) in the vehicular network forming an overlay network. The Blockchain is used to record all the messages from the vehicles to make sure the information has not tampered and easily verifiable. Also, at the same time used as trust management to identify malicious nodes. The system was shown to be capable of deployment in large-scale deployment. While the system addresses the issue of security, it lacks a discussion on the applicability of decentralized SDN control plane which may act as a single point of failure. Similarly, in [41] a Blockchain-SDN-enabled architecture for the Internet of Vehicles (IoV) is presented to enhance the efficiency of management in SDN and enhance trust among the vehicle. The management responsibilities are shared between the Blockchain and the SDN, to reduce the burden at the controller.

An improved authentication approach is proposed using Blockchain and SDN to minimize performance degradation due to frequent handover among dense heterogeneous 5G cells [42]. The proposed authentication mechanism minimizes the need for re-authentication during handover resulting in lower delay and service disruption. To achieve this a distributed SDN controller architecture is proposed which is controlled by the Blockchain. The Blockchain stores the users public and private keys which are used for authentication during the initial attach process. Once the authentication is done the Blockchain distributes the information to adjacent cells. Also, the Blockchain authenticates every node in the network (SDN controller, Base stations). This sharing of information in a secure way reduces the handover time as the need for authentication is minimised.

2) NFV

Virtual network functions (VNFs) are the implementation of a network function in software that is decoupled from the underlying hardware. VNFs are deployed on top of NFV infrastructure, that may span multiple physical locations, dynamically. This results in agile networks, with significant OPEX and CAPEX savings. Along with the benefits, there are several challenges for the network operators that need to be addressed before deploying the VNFs at a large scale. The challenges that can be addressed with the help of Blockchain are as follows:

- **Orchestration and Management** - The network operators should be able to deploy VNFs at the right location and at the right time, dynamically scale the resources and connect them for service chaining [43]. This level of flexibility presents new challenges in managing both virtual and legacy appliances for service provisioning. Also, the network carrier usually over-provision the services to ensure service availability resulting in inefficient utilization of resources. Blockchain can play a

significant role by allowing the automatic provisioning of services as and when required by storing the VNFs configuration on the Blockchain and executing based on the smart contract.

- **Reliability and scalability** - For the flexibility in service provisioning, aggregation and migration of VNFs based on traffic, load and user demand is required. Such operations create new points of failure that should be handled automatically. Requirements for the configuration of NFV systems such as traceability and high availability can be ensured by Blockchain.
- **Security** - During the deployment, it is possible that the VNFs may run on devices not owned by network operators directly. This may result in security vulnerabilities. Therefore, it is important to ensure the correctness of VNF chains to execute in trustless environment [44]. Even in the case of centralized operation under a single network operator the underlying networking and storage can also introduce new security threats. For example, a software router in a Virtual Machine (VM) that shares the physical resources with another network function may affect each other. Moreover, the VNFs may be offered by different vendors, potentially creating security holes due to integration complexity [43].
- **Monitoring & Auditing** - To identify a faulty or compromised VNF configuration it is important to have immutable and auditable records of previous configuration history. Blockchain-based configuration repository can be used to address the auditability requirement. The use of Blockchain provides immutability and traceability of the configuration update history registered in the form of transactions.

In [45], a Blockchain-based NFV MANO solution is proposed for data centres that host multiple network services from different clients. The proposed Blockchain-based NFV architecture addresses requirements such as confidentiality, traceability, anonymity and authentication. The prototype implementation shows that the proposed architecture ensures high availability and eliminates single-point-of-failure. However, in the design, the Blockchain node placements and incentives for peers in maintaining Blockchain are not discussed.

Authors in [46] proposed a Blockchain-based system, referred to as BSec-NFVO, for securely orchestrating VNFs in a multi-tenant and multi-domain environment that provides auditability, non-repudiation and integrity. In the architecture, the Blockchain validates all the transactions before they are executed by the orchestration module. The proposed system was implemented on Open Platform for Network Function Virtualization (OPNFV) with a simplified Byzantine fault-tolerant consensus protocol (not handling exceptions nor leader election) to provide low-latency consensus. In [47] Blockchain-based system is used as a provenance management system for the applications running in a virtual machine hosted on the cloud to establish trust and accountability. However, the proposed system only protects the logs of application state changes.

A Virtual Machine Orchestration Authentication (VMOA) framework [48] is proposed for authentication to establish a trustful VM execution environment. In the proposed system, Blockchain is used for authentication instead of using an internal or external trusted authenticator. Each orchestration request for VNFs is first authenticated by Blockchain and then sent to the virtualization server. Each request is stored in the Blockchain in the form of a transaction to provide auditability.

VNFs are typically shared and deployed in the form of packages which can be used on virtualization infrastructure. These packages can be purchased from the marketplace for quick and easy deployment. A common challenge of such marketplace-based and traditional NFV solutions is establishing a trusted computing environment. The work in [49] extends the Blockchain-based NFV management and orchestration to create a trusted repository for VNF packages to verify the package integrity without relying on a third-party for remote attestation. This is an important requirement according to ETSI Trust and Security Guidance specification for a safe NFV environment [50].

In [51], [52] business and management related aspects concerning NFV are addressed using Blockchain. Work presented in [51] focuses on promoting competition among infrastructure providers hosting VNFs to reduce the cost while at the same time improving VNFs performance. The proposed work based on Blockchain provides an auditable solution to promote trust and transparency. The Blockchain-based solution referred to as BRAIN, works on a reverse auction mechanism where Infrastructure providers compete to host the VNFs. Reverse auction helps to solve the discovery and selection of infrastructures allowing for efficient hosting of VNF based on user-specific demands. Whereas [52] discusses the use of DApps (decentralized applications) built on Blockchain to enable multi-domain service orchestration. The future deployment of 5G will involve multi-domain administration to provide various 5G services (IoT, AR and VR). Such deployment needs to be distributed and automated (management/orchestration) to meet specified SLAs. Therefore, solutions based on Blockchain are highly desirable to solve challenges involved with non-trusting administrative domains such as complex inter-domain transactions, billing and SLAs.

3) NETWORK SLICING

As mentioned earlier, the 5G network caters to a wide range of services with a diverse set of performance requirements. To support such performance, network slicing is a viable and promising solution. A network slice is an end-to-end logically isolated network that includes 5G devices in addition to access, transport, and core network functions. Creation of network slice may present challenges in certain cases where it needs to be created dynamically (on-demand) without any prior knowledge on the service requirements.

The most challenging part of network slicing is dealing with scenarios where different slices should provide services with significantly varying requirements concerning functionality, latency, reliability, security, latency, and capacity. There are several fundamental questions on how to obtain efficient resource utilization, guaranteed QoS, charging policies, security and proper isolation between slices.

- **Performance** - When dedicated resources are allocated to the network slices the required performance levels will be met, however, this leads to inefficient resource utilization. This is undesirable as the tenant is allocated a finite set of resources. One way to resolve this issue is to allow resource sharing. Resource sharing requires adequate resource management mechanisms that enable resource sharing among slices when necessary without violating required performance levels. To accomplish the sharing issue, Blockchain can assist in resource provisioning and automation with the help of a smart contract executed on the Blockchain network.
- **Management and orchestration** - The flexibility and scalability offered by the network slicing, results in management and orchestration challenges in a multi-tenant environment. To flexibly assign resources on-demand to the slices, the optimization policy that governs the orchestration policy can be executed in a distributed manner with the help of smart contracts where resource demands vary considerably in relatively short duration. Also, the highly customized configuration of resources, management models, system parameters for various use cases can be efficiently handled using Blockchain.
- **Security and privacy** - The creation and management of any slice need to be authenticated, approved and logged for security and auditing purposes. All virtual functions that make up a network slice instance (end-to-end) need to be authenticated and their integrity should be verified to make sure the network manager is not impersonator (or trying to exploit resources) and correct VNF is deployed [53].

In [54] a network slice broker (NSB) based on Blockchain is proposed. The role of NSB is to handle the slice requests from various industry verticals and pass it to the mobile infrastructure resource orchestrator. The proposed solution enables the InPs to allocate network resources to the broker based on the agreed smart contracts. The broker, in turn, allocates and re-distribute their resources among tenants in a secure, cost-efficient, automated and scalable manner. The Blockchain in the proposed architecture is responsible for enforcing policy, billing and resource management. Since the transaction is recorded and executed on the Blockchain it enables a much faster process for the resource allocation transactions.

The work in [55] leverages distributed Blockchain to create a virtual wireless network (similar to network slice) on the fly by leasing the resources from the primary owner. The resources that are leased can be either RF spectrum or infrastructure based on the service level agreements stored in the smart contract. The proposed resource sharing scheme provides security to both the owner and the leaser. Also, the scheme prevents the primary owner from over-committing (to prevent double-spending) and helps the virtual wireless network to meet the QoS requirements of the end-users. The proposed scheme securely creates a virtual wireless network without sharing private information and enhances overall network capacity and coverage. However, the focus was on the resource sharing in the fronthaul of the network with no consideration on the backhaul.

In the context of the vehicular network, Blockchain-based network slicing to dynamically control the reliability of the source and integrity of the message is presented in [56]. The usage of Blockchain allows building trust in a trustless environment. Each node in the vehicular network can verify the data transmitted by other nodes and inform the network about its reliability. This is crucial in a vehicular network because any faulty or compromised node could destabilize the network and cause life-threatening situations. The work presents a detailed discussion on security with little information on consensus protocols to achieve the complete solution.

Lastly, in [46] extension to NFV-MANO architecture is presented that uses dedicated APIs for configuring and orchestrating the network slice. The work highlights the need for consensus algorithms to efficiently manage a large number of interactions in a highly heterogeneous network for securely creating an end to end slice.

B. COMPUTING MANAGEMENT

Computing management refers to the placement of data processing and storage resources to achieve the desired level of performance in 5G verticals. Dynamic allocation and placement of resources securely are challenging in a highly heterogeneous and dynamic network like 5G.

1) CLOUD COMPUTING

The role of cloud computing has been well studied in 5G for resource optimization, processing, data storage and transmission management. Cloud computing considerably improves the development, delivery and management process. However, there are several issues in current cloud computing techniques from a security and management point of view that still needs considerable attention for the research community.

- **Management** - The 5G core network will be deployed in cloud centres in the form of software packages. The orchestrator needs to trigger automated service deployment on request and dynamically manage the life-cycle of RAN functions. Also, the 5G network will make use of a combination of third-party clouds and operators making it difficult to manage across several stakeholders.
- **Resource allocation** - C-RAN involves us several resources across multiple dimensions such as radio resources, computation resources, storage resources.

Resource allocation at large scale across these resources is challenging due to its inherent complexity, protocol barrier and stringent delay constraints. Also, C-RAN and RRHs need to be allocated resource optimally, considering the number of active BBUs in the BBU pool and network load (traffic demand from UE/RRHs) [57]. To reduce the complexity, the existing resource sharing algorithms need to be enhanced considering RRHs and BBUs in the cloud.

- **security** - Security is the biggest challenge in going cloud-native for 5G networks. The core network will be deployed at various local and national data centres to manage calls in a hierarchical model. This results in data being collected, stored and shared between dynamic cloud networks. This presents serious challenges from data privacy, integrity and ownership. Authentication of across multiple domains, stakeholders and devices (virtual or real) becomes challenging in a trustless environment. Furthermore, it is important to make sure the data is immune to modification not only from the attacker but also from unintentional activity. A generic C-RAN would struggle in guaranteeing the service security and device credibility.

To overcome the problem associated with centralized access authentication of each terminal in the 5G network, a Blockchain-based trusted authentication (BTA) architecture is presented in [58] by using Blockchain-based anonymous access scheme. The proposed BTA makes use of tripartite agreement between device manufacturer, end-user and the network operator to enable trusted access resulting in privacy protection and improved network credibility. Also, it enhances trust between the network; multiple resources are integrated by the cooperation of Blockchain and SDN control plane resulting in global optimization of radio and processing resources. All-access identification is stored on Blockchain and protected from tampering in a distributed system.

The solution to guarantee data integrity due to the dynamic nature of IoT data in the cloud currently relies on third-party audit (TPAs) which are usually unsatisfactory. To deal with this issue a Blockchain-based data Integrity framework is proposed in [59]. The data owner generates and uploads the data, where multiple data owners and data consumers are responsible for data integrity verification on Blockchain. The data owner writes the data to the Blockchain with the help of a smart contract and becomes available to other users after consensus. The Blockchain contains the hash of the generated data whereas the actual data is stored in the cloud. Relevant protocols are defined for any consumer wishing to verify the integrity by querying the hash stored on the Blockchain and the hash of the data on the cloud. In [60], Blockchain-based data provenance in the cloud is proposed to enhance the privacy and availability of the provenance data. Blockchain collects and verifies cloud data provenance, by embedding the provenance data into Blockchain transactions with an unalterable timestamp and generating Blockchain receipt for each of the data records. Similar work for data provenance in the context of cloud-centric IoT in the heterogeneous multi-layered system was proposed in [61] utilizing Blockchain smart contracts. The cryptographic hash of data generated by the device is stored in the Blockchain whereas actual data is in the cloud.

In IoT, the key distribution from centralized cloud centres requires trust in the third-party which is not attractive for many users in privacy-oriented scenarios. Therefore, to overcome this challenge, a Blockchain-based distributed key management architecture is proposed in [62] that is deployed at fog nodes to reduce latency. Also, it uses another Blockchain running in the cloud for interconnection and traceability among Blockchains running on the fog nodes to enable cross-domain interaction. The proposed scheme presents several authorization assignment modes and group access patterns to provide extensibility and hierarchical access control in IoT.

To address the issue with the centralized scheduler for resource allocation, an intelligent energy-aware resource management scheme for data centres based on Blockchain is proposed in [63]. The use of Blockchain eliminates the need for a scheduler resulting in reduced energy cost and increased robustness in the cloud data centre. The energy cost is reduced by handling a series of requests that are added to the Blockchain as a transaction and verified by consensus by participating data centres. This Blockchain allows the request for resource allocation to be scheduled by the data centre themselves without depending on the centralized scheduler. A smart contract gets executed every time a transaction is received and migrates the request and VMs. The data centre that has the lowest load receives requests and VMs. To minimize the breach detection gap (BDG) Blockchain-enabled federated cloud framework is presented in [64]. The Blockchain is used to share information between the participants in a secure, reliable and restricted manner that is continuously monitored and analyzed using a specialized tool.

2) MEC

Bringing the cloud capabilities to the edge brings reduced end-to-end latency and reduces network congestion. This helps in achieving the low-latency requirement set by 5G. However, there several challenges associated with MEC which are as follows:

- **Identity management and Authentication** - With several devices connecting to MEC, the need for identity management and authentication is important in a secure and scalable manner. Also, the data needs to be stored and protected against unwanted modification especially in case of IoT where a large amount of data will be collected at the edge.
- **Privacy and provenance** - Earlier the operators usually owned the infrastructure and the access was limited to trusted parties. But 5G with MEC, the distributed deployment in both public and private cloud leads to several concerns over data privacy. Also, verifying the

data provenance such as where it originated from and identifying the ownership is challenging.

- **Trust Management** - In MEC, multiple decentralized participants need to cooperate to manage edge resources. Therefore, a multi-party Authentication, Authorization, Accounting (AAA) platform and trust anchors that can scale while reducing management complexity are needed.

To solve the trust issue in heterogeneous MEC, a distributed Blockchain-based trusted MEC collaboration architecture is presented in [65]. The proposed architecture enables cross-domain collaboration among MEC servers by providing trusted routing solutions and privacy protection. To protect the privacy of the network, a virtual topology is used to represent the actual topology without revealing the actual physical identity of the components. The virtual topology is exchanged between collaborating domains. The virtual topology is used to initialize the Blockchain and updated through consensus among participating domains. The data stored in the Blockchain is then used to achieve a multi-domain collaborative routing consensus. Any changes to the routing are verified and updated based on the consensus and can adapt to the dynamic changes of network topology.

In a 5G network, resource sharing will be common among service providers to maximize the utilization of limited resources at the network edge and achieve the required SLAs. In [66], to address the issue of a fair resource sharing among multiple service providers, a Blockchain-based architecture establishing trust is presented. The optimal application deployment at the edge is modelled using stochastic programming and implemented using the heuristic algorithm. The smart contract takes in the logic of the algorithm and available edge resources into account to determine the optimal placement. All transactions are transparent and traceable among all participating entities. To allocate the network resource in MEC based on the user priorities for healthcare application is presented in [67]. The network resources are allocated based on the authenticity of priority level using Blockchain consensus so that the communication and computation resources can be allocated optimally to minimize the end-to-end delay.

The mining process is computationally intensive and it cannot be implemented in the device with limited storage and battery. To address this issue, MEC has been used to enable mobile Blockchain in [68], [69]. The work in, [68] presents reinforcement learning-based algorithms that enable the mobile nodes to determine optimal offloading decisions while preserving user privacy. Whereas [69] uses a pricing-based approach to support mobile Blockchain applications to encourage task offloading to MEC servers. To obtain optimal output, a two-phase Stackelberg game is adopted to maximize the benefit for both MEC servers and the users. In the context of 5G IoT, [70] proposed a smart Blockchain-based platform to solve the network congestion resulting due to transfer of raw data between a publisher and workers in Industrial IoT (IIoT) involving many MEC servers.

3) CONTENT CACHING, DATA STORAGE AND COMPUTING

Caching the content in a distributed fashion in the network with the help of MEC improves the throughput and minimizes latency. Usually, in a centralised managed system global information about content demand is easily available, however, it is rare in a decentralised system. Hence, there is a need for a dynamic content caching approach in a distributed system. Furthermore, the special characteristics of MEC networks such as limited coverage, storage and computing power presents several challenges for content caching and storage [71]. In terms of security, due to distributed and pervasive deployment, confidentiality and authentication become a key concern. Instead of using the core network, the MEC has to authenticate each user before serving the content. From the user perspective, their content history has to be protected. While at the same time, the historical information is important for recommendation and proactive caching.

In the case of computational task offloading, especially for smart/autonomous vehicles several problems arise due to the distributed and dynamic nature of the network. The end node may not have enough computational power and may have to offload certain computational activities to the nearby nodes. The computational task will involve data with varying degree of criticality and QoS requirement. Therefore, it is important to have proper authentication and privacy protection so that it is easy to recognize a legitimate user from a malicious user. Moreover, user information should be protected to prevent data breaching.

All these issues are optimization problems that need to take into account the resources at MEC, end-users behaviour and the network operator to find the optimal balance that maximizes the utility for every entity in the network. However, for the security and automated management of resources, Blockchain is the best match in such heterogeneous, dynamic and distributed 5G networks. Furthermore, it keeps track of all the transactions that allows the prices to be calculated in real-time benefiting both end-users and network operators.

In [72], content caching framework for vehicular edge network based on deep reinforcement learning and permissioned Blockchain is presented to overcome the trust issue for caching the user content in untrusted caching providers. The Blockchain is maintained on the base stations whereas the content caching is done on the vehicles securely and reliably. To achieve consensus between base stations for adding new blocks, proof-of-utility (PoU) based consensus is proposed. The PoU consensus takes factors in the computing, processing abilities of edge nodes and the latency requirements of vehicles. The base stations also facilitate the matching process between cache requester and provider, where the cache providers are incentivized. The work in [73] proposed a decentralized framework based on Blockchain for autonomous and proactive caching in hierarchical wireless networks containing untrusted nodes. The Blockchain helps

the cache providers to adapt their strategy based on the market dynamics and enforces the truthfulness among untrusted nodes through financially enforced contracts.

In the context of distributed computing, [74] presented a Blockchain-based computation offloading method to minimize the loss of data integrity. The tasks that require real-time operations are processed at the edge node, whereas, the rest is processed at the core network. The Blockchain keeps a record of offloading transactions information between users and edge nodes. The edge nodes maintain the Blockchain and act as miners recording each offloading transaction as an immutable block providing verifiability and traceability. Similar work was presented in [75] with a focus on energy-efficient offloading. The energy efficiency is achieved by determining the shortest path to the edge node for offloading of computation tasks. In [76], an access control scheme based on Blockchain is proposed to protect the edge node against malicious nodes in 5G IoT. The goal is to detect the malicious nodes and prevent them from exploiting computing resources with the help of a smart contract. Smart contract performs user authentication, offloading verification and manages offloaded mobile data to ensure security and privacy.

Several other research has been performed in addressing the issue of data offloading [77]–[80] and content caching [81]–[83] using Blockchain.

C. COMMUNICATION MANAGEMENT

Communication management in the proposed taxonomy refers to managing the RAN resources (mostly fronthaul) ranging from managing infrastructure to spectrum management. In this subsection, we present how Blockchain is going to help in communication management.

1) INFRASTRUCTURE MANAGEMENT

There is no doubt that the number of base station deployment for 5G is going to overtake the 4G deployment due to small-cell architecture. According to [84], the 5G deployment will overtake 4G by 2024. The installation of a large number of the base stations will lead to high CAPEX and OPEX expenditure of the Network operators. In this scenario, the best way to move forward is to share the infrastructure between the network operators instead of deploying all from end to end. In this way, based on the requirement, multiple network operators can share the resources of the same 5G base station. This enables flexible and on-demand allocation of network infrastructure that reduces the cost for the network operators. The infrastructure may belong to any player in the market that may want to lease out the infrastructure. Therefore, the network operator may have lease resources from the various players in the market such as base station provider and spectrum provider. This presents various challenges as well as opportunities for realizing new business models creating value across the whole ecosystem. Besides infrastructure sharing, crowdsourcing can also be used where smaller infrastructure providers can install base stations that will be part of the operator infrastructure. These smaller infrastructure providers need to be registered, managed, and also automatically paid upon the use of their towers [13].

Because multiple parties involved in the entire chain, establishing trust, authentication, identity management and confidentiality are the biggest challenges. To address this issue Blockchain is the best solution as it is designed to operate in a trustless environment. Also, at the same time guaranteeing all the desirable features such as confidentiality, immutability, auditability and transparency. The network operators can quickly find suitable resources (infrastructure, spectrum) with minimum cost to meet the end-user demands with transparency and traceability throughout the lifecycle. The smart contract can be used to handle the automated billing across various players and ensure SLA via secure and auditable transactions.

In [85], infrastructure sharing solution is proposed where the user information is stored on Blockchain acting as a distributed Home Subscriber Server. A consortium of the network operators in the Blockchain has access to the user details such as IMSI, subscription information and security procedures by communicating with the Blockchain. This allows the user to switch the network easily and served by a group network operator when not in the coverage area of the parent network operator. The charging information, on any particular network, is based on the connection duration and resource utilized, is stored on Blockchain. Once the information is stored on Blockchain, the smart contract checks whether it was served by the parent network operator or the visiting network operator. The smart contract uses the information to charge the user based on the smart contract agreement between user and network operator. In [86], Blockchain-based infrastructure sharing termed as ''Small-Cell-as-a-Service'' is proposed. Any individual or business can be a service provider for the network operator, where the network has no base station or want to reduce the cost of deployment and management. The Blockchain is used to implement SLA in the smart contract between the network operator and small cell provider that includes various factors such as QoS class identifier (QCI), packet loss rate and packet delay.

2) SPECTRUM MANAGEMENT

Spectrum is becoming crowded and at the same time, the cost to acquire the exclusive right for spectrum usage is becoming higher. The operators can either use the spectrum for their use or lease out to interested parties. However, the actual licensed spectrum is largely under-utilized in vast temporal and geographic dimensions. A remedy to solve the issue of spectrum scarcity and under-utilization is to allow dynamic spectrum utilization to licensed and unlicensed users. The spectrum can be allowed to be used dynamically either by spectrum auction or spectrum sharing. The dynamic access of spectrum requires a seamless transaction and fulfil SLA to avoid any services disruption. Earlier approaches of a centralized database for spectrum sharing are not flexible, scalable and

are vulnerable to a single point of failure. Furthermore, there is a lack of proper incentive mechanism for primary users and secondary users, authentication mechanism to minimize the misuse and transparently ensure fair competition/pricing. Again, the Blockchain with smart contracts can be used to efficiently and securely share and auction spectrum in an automated, transparent, and trusted manner without intermediaries. Besides, Blockchain is recommended for spectrum management for beyond 5G networks [87].

There have been several works that proposed the use of Blockchain for spectrum management in the literature. Recently, a Blockchain-enabled spectrum sharing in 5G heterogeneous network was proposed in [88]. The proposed framework allows for maximizing the spectrum usage by sharing the spectrum between the M2M (referred to as SU) devices and the conventional users (referred to as PU). The base station encourages the PU to share the underutilized spectrum in return for incentives. The base station prepares the contract that contains all relevant information such as the amount of spectrum required and the incentives. Once the contract from multiple PU is in place, the matching theory is utilized to match the PU spectrum with the SU. Both SU and PU prepare a preference list and are matched using the Gale-Shapley algorithm. Once the PU fulfils the contract the payment to PU is released and Block is created which is verified and added to the Blockchain. The use of Blockchain provides privacy, guarantees the incentives for spectrum sharing to the PUs and provides efficient low complexity decentralized spectrum sharing scheme. However, the work does not consider the case of multiple Base stations where the PUs may have multiple contracts. Therefore, a cooperative framework needs to be considered in such cases.

In [89], multi-operator spectrum sharing is proposed to improve spectrum utilization using a consortium Blockchain. The consortium Blockchain allows for spectrum trading between network operators using the smart contract. The use of Blockchain in the case of multi-operator eliminates the need for centralized spectrum brokers and enforces the policies of reward and punishment based on the smart contract. The smart contract is designed based on double auction and free trading market principle to match the spectrum seller to the buyer. This smart contract allows sharing spectrum autonomously addressing the reliability, spectrum efficiency and security issues related to the interaction between trustless entities.

Initially, the use of Blockchain for spectrum sharing was popularized in cognitive radio networks [90], [91]. In [90], a secure distributed medium access protocol is proposed for cognitive radios (CRs) to lease and access the spectrum securely and dynamically. The availability of the spectrum is sent out on the control channel, thus eliminating the need for spectrum sensing. The transmission on control triggers the auction and the successful bidder is allowed to use the spectrum based on the agreed conditions. Each spectrum leasing transaction is verified by Blockchain and added after consensus from the mining nodes. Whereas in [91], instead of using a centralized fusion centre to process and store the result of a Blockchain-based spectrum access framework is proposed to avoid a single point of failure. The proposed scheme treats SU as both miner and spectrum sensor. The SUs decides between sensing and mining operations and is rewarded with tokens. The token is used by the SUs to bid for the spectrum and access it. Once the bidding is over the bidding information is sent to all nodes and the SUs acting as the miner will update the information about the available and occupied spectrum via Proof of sensing consensus mechanism. With the optimal sensing and mining policies, the system maximizes the energy and spectrum efficiency while providing the desired security features with the help of Blockchain.

3) D2D

D2D is useful in several aspects for the 5G networks. First, it can be used to provide extended coverage to the users at the cell edge by relaying the signal from the base station. Second, D2D can allow direct communication between two devices, hence reducing network overloading and congestion. Third, it can enable distributed computing and content caching for cases such as IoT. Lastly, it can result in improved spectrum utilization, reduced interference management, enhanced throughput and network performance. All these benefits are very difficult to achieve from centralized control in a highly heterogeneous network with varying QoS requirements. Also, establishing trust in a network where nodes join and leave the network frequently, authenticating new nodes, providing data integrity and confidentiality is very challenging. Furthermore, varying user preference on the available resource, developing suitable incentives mechanisms and designing dynamic agreement further complicates the things.

To address the issue of content caching in the D2D network, a Blockchain-enabled content sharing strategy is proposed in [92]. The selfish nature and varied content preference of users are considered in developing an incentive mechanism. The reward is offered by the base station by reserving computational resources for mining bitcoin for the device that successfully shares the content. To maximize the profit, an optimal content placement strategy is proposed based on the allocated computational power and shared data size. However, there is no discussion on the security aspect of content and user authentication.

A Blockchain-based access control framework is presented in [93] for D2D networks to verify the authenticity of reported channel state information (CSI). The CSI is an important factor in assigning the resource to improve the QoS of the user as well as improving the network performance. The malicious node may report a higher CSI to get more network resources thereby affecting the QoS of legitimate users. The framework makes use of consensus mechanism and stores the output on two Blockchain that maintain the verified CSI and fraudulent CSI. If the consensus cannot be reached in the network, the framework makes use of a deep learning

algorithm to identify fraudulent CSI by comparing with the predicted CSI using convolution neural network to reach an agreement. The use of Blockchain to verify CSI authenticity results in improved spectral efficiency.

In [94], Blockchain-based MEC assisted by D2D is presented for resource pooling to offload tasks during peak hours to reduce the burden at the edge. The device requiring computing resources broadcasts the request to the network containing relevant details on specifications such as completion time, required computing power and memory. After the request is received, the Blockchain will check whether the request can be served based on the available resources. Once the available resources are identified, a selection contract is generated and the payment contract delivers the reward after the request is served. Each transaction of a resource request and resource allocation is recorded on Blockchain providing a verifiable trail and secure transaction.

Recently, a Blockchain-enabled transcoding system was proposed to provide decentralized trusted collaborative transcoding services via D2D network. The Blockchain-based transcoding can provide more efficient transcoding services by splitting large video files and assigning it to a group of transcoders, without any intermediaries. This allows creating a direct transaction between the content creators and transcoders through D2D networks that can relieve the backhaul links. Whereas the smart contract can ensure security, transparency and payments of the transcoding tasks in an automated manner. In the proposed system the content creator submits a transcoding job, which is verified and added to the Blockchain. Once the job is added deep reinforcement learning is used to optimally select nodes that will perform transcoding. After the transcoding node selection, the content is sent to the node which then performs transcoding and receives the reward. Each step is recorded in the Blockchain and any node in the network can become a Blockchain node. The proposed model maximizes the revenue while satisfying the QoS requirement in a dynamic environment in a secure, trusted and reliable manner.

4) NETWORK ACCESS MANAGEMENT

Today the cellular networks operate in a centralized client-server based model where the rules stored at the server are pushed to the devices. This causes delays and does not allow seamless provisioning between access networks for the device. Blockchains can aid in 5G wireless access technology deployments and selection by providing seamless access across a diverse number of networks to the user equipment (UE) and IoT endpoints. A UE upon entering the coverage area may have several options to connect to the network through various access technologies such as Wi-Fi, LTE and 5G. Providing network access through various technologies, a core feature of 5G technology, can be realized only when network operators can manage diverse access nodes and mechanisms [95]. The main challenge is to quickly select the access node for every user in the network. Integrating Blockchain as a part of the radio access network in such a scenario can help the devices to establish a connection to various networks quickly. Also, it can help in forming a cooperative network of different access technologies/operators to provide quality service with improved resource utilization while protecting the interests of all participants.

5G RAN must have high flexibility to allow operators managing a heterogeneous set of access technologies and to optimize the access according to the required service capabilities. In [96], some of the challenges associated with network selection are highlighted. Access Network Discovery and Selection Function (ANDSF) in EPC assists the device to connect to non-3GPP access networks such as Wi-Fi. A centralized server stores the rules that are sent to the UE. This results in several issues such as delays due to centralization of ANDSF server, continuous provisioning among the access network and no provision for real-time operations with dynamic change of rules. To overcome these challenges a distributed Blockchain network is proposed that can be used to connect 3GPP networks such as 5G with non-3GPP networks such as Wi-Fi. Every access point (Wi-Fi, eNodeB) will monitor the UE and will help in deciding which access nodes will be provisioned for a given UE. If there is more than one access point in the vicinity of the UE, the device will select the best based on the service agreement in the smart contract. The smart contract will evaluate various parameters set by the CSP and allocate the best access point. The smart contract will contain the rules and agreements between the various network carriers and users. This smart contract also allows the dynamic change of policy, whenever a new set of rules are required, they can be deployed to the Blockchain.

To improve network density and reduce the cost of deployment for the network operators, a Blockchain-based access network is proposed for improving the connectivity for the end user [97]. It involves the use of local actors (someone willing to deploy access nodes) that are rewarded by the network operators. The network operators are the trusted entities that offer the connectivity platform and link while the local actor is the intermediary entities which deploy access nodes/antennas and are rewarded based on the amount of traffic carried. To allow access control and transactions, a distributed bandwidth and identity ledger are proposed which is a consortium between network operators and contains the information of each participating node. This approach results in densified deployment and improved coverage for the end-users with secure access to the operator network. The Proof-of-Bandwidth consensus is used to measure the traffic for charging the end-user and reward the local actor.

To manage network access and authentication in a trustless network, a Blockchain radio access network (B-RAN) architecture is presented in [12] to build decentralized, secure and efficient mechanisms. The user and access point agree on contract terms that include the payment conditions and resource allocation. This contract is recorded on the Blockchain and authorized by the user. The smart contract is verified to ensure that both parties have enough resources (credit balance for the user and network resource for an access

point) before executing the contract. Once the conditions in the smart contract are met, the Block is added to the existing Blockchain. The architecture results in secure access and protects both user and access point via smart contracts. The proposed architecture can be used for developing a large self-organizing RAN by combining multiple entities without relying on a centralized controller, hence avoiding a single point of failure.

5) INTERFERENCE MANAGEMENT AND RESOURCE ALLOCATION

Interference is a known factor that affects wireless network performance. Due to dense deployment in 5G networks, the management of interference will be even more challenging than the current wireless network due to intra-cell, inter-cell and inter-user interference. Also, the cooperative and collaborative communication is going to be an integral part of the 5G network, managing heterogeneous networks and devices for resource allocation to meet the varying level of QoS from a centralized base station is quite challenging. There have been several techniques such as Inter-cell Interference Coordination (ICIC), Coordinated Multipoint (CoMP) and coordinated scheduling (CS) that are proposed to manage the interference. These techniques, however, require coordination and cooperation between the participating entities such as base station and end nodes to allocate resources optimally to meet the QoS requirement. The cooperation may be achieved easily among the homogeneous network belonging to the same operator. But in a diverse network such as 5G, where the network operators have to coordinate among various network elements belonging to other operators is challenging. Furthermore, developing cooperation strategy that rewards and punishes in a dynamic environment securely and transparently is highly challenging. The Blockchain may provide a solution to some of these problems by distributed interference management.

In this regard, the authors in [98] proposed cooperative interference management using Blockchain-enabled distributed coordination protocol. The scheme comprises a monetary mechanism to establish mutual trust and coordination protocol for cooperative zero-forcing and interference avoidance. The monetary mechanism allows the user to offer channel usage in return for credit which can be used in future to access the channel. Any node that wishes to transmit has to pay from the earned credit. The distributed scheme based on Blockchain was shown to achieve the same level of performance as the centralized scenario.

In [99] a joint transaction transmission and channel selection scheme for Blockchain-based cognitive radio network is proposed. The secondary users use the idle channel of primary users to transmit the sensing decision which is stored in Blockchain. This sensing data can be used by the secondary users to access the network without causing the interference. However, due to unpredictable primary user activity and uncertainty in the Blockchain system the cognitive radios may not be able to make the optimal decision for channel selection and transmission. To overcome this limitation, a Deep Q-Learning is presented which maximizes the number of successful transaction transmissions while minimizing the channel cost and transaction fee. The system was proposed to support IoT devices acting as secondary users that access the idle spectrum of the primary users thus improving the IoT performance. While at the same time enhancing Primary user spectrum utilization.

Placement of IoT nodes that enables Blockchain-based IoT is presented in [100]. The work considers two types of IoT nodes which are referred to as Transaction nodes (typical IoT node) and Full nodes (powerful IoT node). The role of a full node is to mine and verify the block whereas the transaction node broadcasts the transaction to full nodes. Due to transaction broadcast by the transaction nodes interference is generated. An expression for SINR, transaction data packet (TDP) and the communication throughput is derived by considering the Blockchain characteristics, such as transaction packet length, low Transaction node active rate and limited transaction throughput. Based on the derived expression, optimal deployment of the full node is proposed to achieve maximum Block transaction and communication throughput with the minimum full node density.

To meet the QoS requirement, a resource allocation scheme for Blockchain-based femtocell is presented in [101] to build a decentralized network with low power consumption. The work considers a two-tier network of macrocell and femtocell to design a joint power allocation and pricing strategy to meet the QoS requirement for both macro and femto users. Since the femtocell uses the spectrum of macro-cell there are chances of co-channel interference. A Stackelberg game in which macrocell acts as the leader sets the interference price (the penalty for causing interference) on femtocell users to maximize its transmission rate. Whereas, the femtocell uses the interference price to optimize its power allocation and payments with the constraint of a time delay for completing the transaction in time to meet the QoS of the mobile user.

D. SECURITY AND PRIVACY

Privacy and security are the biggest challenges in a distributed and heterogeneous network comprising billions of devices. Currently, all the privacy and security related matters are handled by a centralized authority or trusted third-party. This exposes the system to a single point of failure. The decentralized, transparent and trustless nature of Blockchain can help address security and privacy issues in 5G networks.

1) DATA PRIVACY

Data privacy is the main security requirement in any network to prevent the information from being accessed by an unauthorized entity. In a distributed and decentralized network, providing not only data confidentiality but data provenance is also equally important to prevent misuse. The data confidentiality needs to be considered for data sharing, data flows between various network elements, centralized data and involvement of any third-party. The data flow and

storage in such a complex network needs to be managed efficiently since it is shared not only by multiple end-users but also by multiple operators. In this regard, Blockchain offers several benefits in monitoring user data when sharing on the network, unlike traditional approaches where users are unable to track their data. Also, to provide data privacy one of the ways is to hide the user identity known as data anonymization using techniques like K-anonymity and L-diversity. Most Blockchain implementations provide pseudo-anonymous user privacy.

To solve the problem of privacy issues in the content-centric mobile network a Blockchain-based scheme that establishes mutual trust between user and content provider is presented in [102]. The Blockchain is used to provide access control and privacy to the content provider. The Blockchain stores the pointer to actual data storage locations in the cloud. When a user wants to access the content, it is checked with Blockchain if the user is allowed to access the requested information. Once the user is authenticated the requested content is checked among the miner if the content is not available among the miner the pointer to the cloud storage of content is shared. Every transaction of request and content adding is stored in the Block and added to the Blockchain after consensus. The proposed scheme secures efficiently and provides data confidentiality to preserve privacy.

Similar work in the context of IoT is presented in [103], Blockchain-based secure store with access control is proposed to solve the ownership and privacy issue. Each transaction in Blockchain contains the data owner information with an identifier. If the data owner needs to share the data, another transaction is added to the Block. The data from every user is chunked and encrypted, integrity protected, and authenticated. Each request to the access data is queried against the Blockchain to check for the access rights to the information. Data, in both the storage nodes (either centralized or P2P) and the Blockchain, is encrypted due to which the information stored is protected. This mitigates the threat of malicious storage nodes granting access to data without proper access rights.

Data sharing is very important to optimize the network performance especially in the case of heterogeneous 5G networks where multiple network operators might be sharing the same infrastructure. At present, each mobile network operator utilizes its own network data from the infrastructures to optimize the network operations without data sharing due to data privacy concerns. This limits the performance of the 5G network. In [104], to solve the issue for data sharing between mobile network operators Blockchain-based scheme for AI-powered network operations is presented. The proposed scheme utilizes fine-grained access control based on the smart contract executed on the Blockchain. It makes use of two Blockchain referred to as DataChain and BehaviorChain. DataChain is used for data access control, and BehaviorChain is used as a data access record, to provide auditability. These two Blockchains provide authority control and supervision simultaneously.

In [105], privacy-preserving and secure decentralized learning framework utilizing Blockchain is proposed to protect the data privacy issue. To provide privacy, a differential privacy mechanism is used in the local gradient computing process. The Blockchain enables the computation in a decentralized manner among the nodes that want to build a global prediction model. The nodes, however, have limited data and hence need to share the information to build the desired model. Computation parameters and information are kept in the block without revealing the owner's data.

2) AUTHENTICATION AND ACCESS CONTROL

Every participant in the network needs to be authenticated to ensure that only known and trusted devices can access the network. Whereas the access control determines the privileges of the authenticated user to identify what services the user can use. There have been several techniques proposed to improve the state of authentication and access control in 5G network [106]. However, with the growing number of the device, especially due to the rise of IoT devices, the authentication from the centralized core may result in a bottleneck and increased latency. To overcome this limitation, the authentication and access control related task may be delegated (or leased) to third-party, just as in the case of leasing the infrastructure from third-party. Also, dynamic allocation of resources in a 5G network to enable various services requires synergy between several intermediaries, that provides various resources (infrastructure, computing, storage etc.), and need to be addressed in a decentralized manner. The Blockchain can help to implement simplified authentication in any part of the 5G mobile network.

In [107], an authentication scheme based on Blockchain is proposed to overcome the issue of authentication due to frequent handover in an ultra-dense network. Instead of authenticating on each handover, the concept of trusted APs group (APG) built using Blockchain is presented. The APG chain is created using the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism. After the APG chain creation, APG and user equipment mutually authenticate each other. The result of authentication is shared with APG with the help of Blockchain, hence eliminating the need for frequent authentication. Similarly, a fast authentication scheme during handover is proposed in [108] by using tamper-resistance property Blockchain to provide several desirable features such as mutual authentication, key agreement, anonymity, traceability etc.

For authentication of new users in the MEC [109], the keys generated during the authentication with the previous MEC group stored on the Blockchain are used. This enables local authentication without the need for authentication from the cloud, hence improving the latency at the same time providing traceability. Similar works can be found for cloud computing [58], NFV [110] and SDN [111] in the literature that makes use of Blockchain-enabled authentication to overcome several challenges.

Blockchain has also been studied for authentication and access control in IoT. In [112], instead of using centralized authentication, the user wishing to access the IoT resource authenticates itself to Blockchain via smart contract. Once the smart contract verifies the user, an access token is issued to the user that contains the services that a user can request from the IoT device. Instead of IoT device authentication, the access token is used. Therefore, this reduces the computational requirement for IoT users while implementing a decentralized authentication scheme that is secure. Similarly, in [113] an attribute-based access control scheme which is stored on a distributed Blockchain ledger is presented. The proposed scheme provides efficient access control that requires a lightweight calculation at IoT devices.

3) INTEGRITY PROTECTION

The Data integrity mechanism is required to make sure that the information is not tampered by any unauthorized party. The integrity of data exchanged between billions of devices on the 5G network is required to make sure that the data is not changed maliciously or unintentionally. In a complex network such 5G, providing end-to-end integrity, reliability, accuracy, consistency and trustworthiness of the information over its entire lifecycle is challenging. At present, data validation is done via encryption techniques or by a trusted party, which add to the security risk of trust and a single point of failure. Due to the tamper-proof nature of Blockchain, transparency and immutability, the data integrity in the wireless networks can be ensured.

To provide data integrity, Keyless signature infrastructure (KSI) using Blockchain technology have become popular [114]. Blockchain-based KSI provides data integrity and security by hashing all data requests and storing it in time-stamped Merkel Tree. A Merkle tree is a binary hash tree used for searching and storing data elements. Using the timestamps, the Merkle tree is arranged in chronological order to protect data from alteration. In [115], a Blockchain-based KSI is proposed to overcome the data integrity and data control loss for IoT.

A Blockchain-based scheme for data integrity using a smart contract is presented in [59] for producer-consumer architecture. The proposed framework performs integrity checks for both data owners and data users. The data is usually stored in cloud services, while the location to the data stored in the cloud is saved on Blockchain as an encrypted hash. The owner of data generates the hash and sends it to the Blockchain as a smart contract or a transaction. Any party that requests the data calculates the hash of retrieved data and compares with the hash stored on Blockchain to check for any tampering.

In [111], issues related to Blockchain due to large computational and communication overhead is addressed by Bilinear mapping-based Data Integrity Scheme (BB-DIS) for large-scale IoT data. The data integrity is achieved with the help of bi-linear mapping in the form of Blockchain transactions executed via smart contracts. The proposed BB-DIS slices the data into equal-length data shards and homomorphic verifiable tags are generated that contain authentication metadata. The authentication metadata is stored via the Blockchain transaction. This follows with the series of challenges and responses to ensure the data integrity involving multiple smart contracts before data gets stored on the cloud server. To detect the fake contents, Ethereum based smart contract is used for tracking and tracking the provenance and history of video content to its original source is presented in [116]. The content can be tracked even if copied multiple times.

E. APPLICATION AND SERVICES

Blockchain is expected to enable several services and applications for network operators that will result in a new business model driving business growth and innovations across the entire ecosystem. Blockchain can build trust and carry out a transaction in a distributed manner allowing multiple parties in the mobile communication industry to work together without friction. Integration of Blockchain will result in cost reductions, better services and build distributed systems that are autonomous and flexible.

1) CONTENT DISTRIBUTION

Ever-growing demands for the data and streaming services such as YouTube and Netflix results in increased bandwidth requirements and congestion of networks that strains the networking infrastructure. Therefore, there is a need for an efficient Content Delivery Network (CDN) that will help in reducing such bottlenecks and meet QoS/QoE of end-users. At present, CDN uses geographically distributed servers for caching the content to meet the demands. In the CDN architecture, content placement and polices are key points to deliver the contents to the end-users with minimum latency. The content provider and network operators need to work closely to efficiently optimize the content delivery because both are affected due to poor delivery of content [117]. By creating a collaborative model, the resource and cache management can be done more effectively. More importantly, offering the services of distributing digital content through the 5G network will generate revenues and provide increased value to customers.

While the content creators and network operators tend to collaborate, the collaboration between content creators is restricted and limited due to the lack of a secure and efficient platform. To solve this issue, a Blockchain-based management platform for content providers and users is presented in [118]. The Blockchain is used to manage the user subscription to various content providers. Use of Blockchain minimizes the cost for content providers as they do not have to authenticate and manage the subscription. The Blockchain guarantees user anonymity and privacy while letting the content providers access a shared database to optimize the delivery of content. The content providers can use a feature-based edge caching algorithm to improve the cache hit ratio and

reduce the delivery time by utilizing the data stored in the Blockchain.

In some cases, the selection of content cache might not be optimal because uneven peaks on the request distribution result from high bandwidth requests. Traditionally, the nearest content caching node is selected to serve the user that may not have the content or might be overloaded. To solve this issue, Blockchain aided orchestration and routing framework is presented in [119] to avoid increased load scenarios. All the content caching nodes are part of Blockchain that allows real-time data sharing and routing of the content to the right caching node in case of overloading. Also, the content to be cached can be determined, due to data sharing, using Blockchain resulting in reduced latency and increased content hit rate.

2) ROAMING, BILLING AND FRAUD MANAGEMENT

The current methods used by operators to authenticate the roaming users are not going to be effective in the 5G network due to several reasons that include authentication delays, cost and security concerns. The SS7 signalling used for authentication in roaming cases is not considered secure anymore [120]. Therefore, a new secure way of authenticating the users is needed that is reliable, robust and most importantly cost-effective. Besides, it is important to keep track of the roaming for billing purposes as well to avoid any charging issues and frauds. The current inter-operator policies along with transaction and billing overhead are complex and expensive.

The 5G network operators need to track the device to charge the device accordingly. The device may move around and attach to several networks during roaming. This presents a major challenge of the network operators in a highly heterogeneous and densely packed network. Since it is nearly impossible for the network operators to install the base station in all locations, the network operators may agree on roaming contracts with various other network operators. The network operator and mobile device may also agree upon a contract which charges automatically. In such situations, to protect all parties, there is a need for smart contracts to enable Blockchain-based solutions to prevent frauds. Since the smart contracts will be executed automatically when certain agreed-upon conditions are met and results are stored on the Blockchain after a consensus is reached, the chances of Fraud are reduced due to transparency and immutability of Blockchain. Blockchain can help devices to be tracked and charged based on their connections to hotspots and Wi-Fi, duration etc. Also, Blockchain-based roaming solution provides homogeneous schema and standardized transaction processing with the help of smart contracts providing better security and reduced delay compared to the existing solution.

For billing, invoicing, and other transactions Blockchain creates a fully recorded transaction audit trail enabling network operators to efficiently manage contracts and financial reconciliations. The Blockchain can allow the user to track the billing in real-time instead of a monthly basis. The smart contacts can be used to offer a highly customized plan that will cater to individual user requirements rather than having a few selected options. Furthermore, mobile money and micro-payments can be made much easier with Blockchain as an alternative to established intermediaries for monetary transactions that will be supported by network operators.

To solve the roaming issue a smart contract-based policy and charging control framework implemented in the core mobile network is presented in [121]. It makes use of several Ethereum smart contracts between home network, visited network and the roaming user to implement the roaming procedure. The roaming agreement between network operators is stored on Blockchain using smart contracts and defines various policies and information that can be accessed. A temporary contract is then created when the user is on roaming that allows the visited network to make changes to the users charging records. All the transactions are agreed upon by consensus mechanism and added to the Blockchain thereby reducing the risk of fraud, over-charging and privacy issues.

To allow free-roaming in a cross-domain, authentication scheme for Wi-Fi access is presented in [122]. Both the user and Authentication server (AS) act as a node on the Blockchain network and are authenticated by a group of trusted AS. For the node to be authenticated on different Wi-Fi network, the user sends its digital signature to AS. The AS acting as miner node will broadcast the request to all peer nodes and follow a consensus mechanism to authenticate the users to the network. Similarly, an untrusted AS is also authenticated by the set of trusted AS. A similar work to authenticate roaming user in multiple areas was proposed in the context of Vehicle-to-Grid networks (V2G) of smart grid [123]. The proposed method used Blockchain as a database to store user credentials which are referred for authentication.

A summary of this section is presented in Figure 4 which highlights the key role of Blockchain in the 5G ecosystem using a layered approach. The key takeaway is that the Blockchain will reduce the complexity associated with collaboration and network management involving multiple heterogeneous entities. Furthermore, it will be crucial for delivering services in a secure, reliable and automated manner.

IV. CURRENT TRIALS AND DEPLOYMENT

Because of the huge potential and benefits of using Blockchain in 5G networks, network operators around the world have started integrating the Blockchain technologies in their network. According to Ovum's ICT Enterprise Insight survey [124], 55% of telecoms industry are planning to deploy a Blockchain-based solution in their operation as a trial or Proof of concept. Majority of these telecom operators are tier-1 operators. In this section, we discuss some of the significant implementations of Blockchain in the telecom sector and their use case.

IBM and Telefonica [125] partnered to use Blockchain technology to streamline core business processes in the

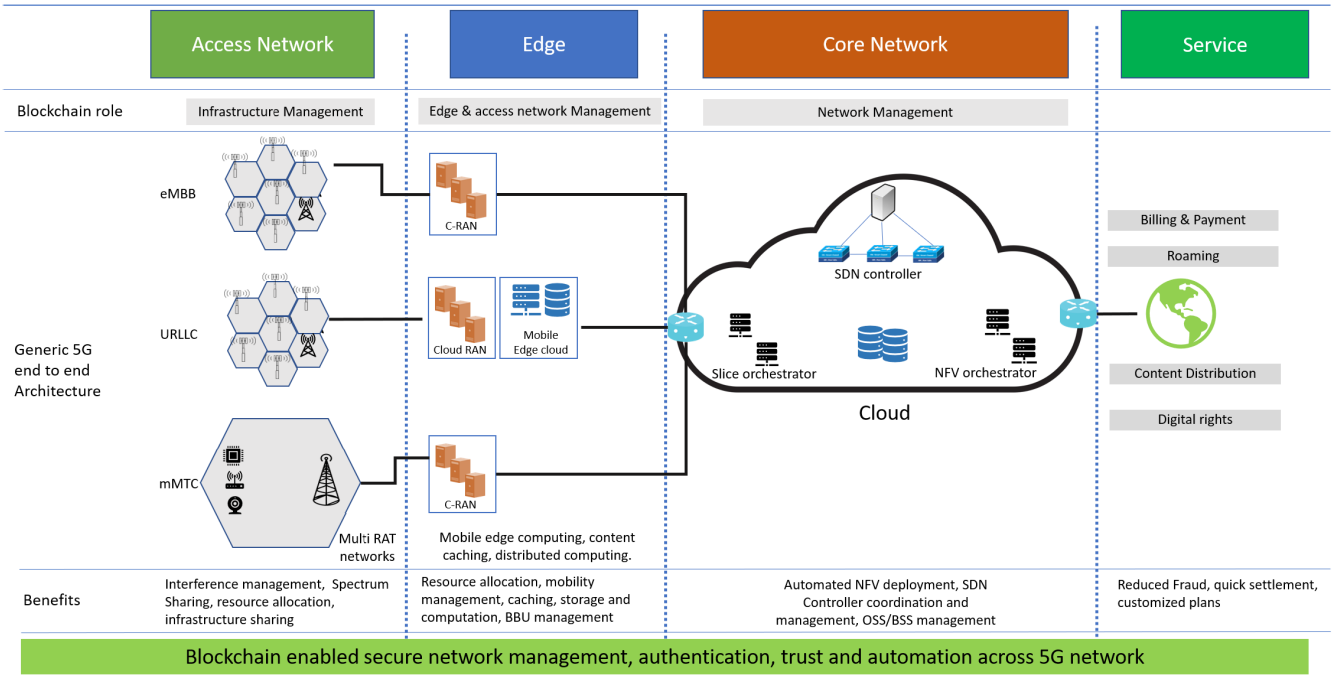

FIGURE 4. **Blockchain role in 5G.**

operator's network. The main issue the trial was meant to address was registering and managing data from different business and network processes. The project aims to improve the transparency and reliability of the data collected by the various networks during routing of international calls. The permissioned Blockchain platform allows tracking the international calls in real-time and its attributes (such as origin country, destination and duration) between the participating operators.

In another project, IBM completed a Blockchain trial run with Telecom regulatory of India (TRAI) to address the issue of unsolicited commercial communication (UCC). In UCC, the user opts not to receive the communication that is made through telecommunications service. The Blockchain, in this case, was used to coordinate among multiple operators concerning Do Not Call (DNC) entries and mobile number portability. This will protect the mobile subscriber from unwanted calls and messages allowing full control over the messages or calls the user wants to receive. All major telecom operators are now working towards implementing the Blockchain solution across the multi-cloud environment to roll out across the entire country [126].

South Korea's largest telecommunication provider has launched a Blockchain-powered 5G network GiGA chain that aims to secure IoT devices [127]. The GiGA chain protects the IoT devices from attackers by hiding the IP address. Beyond security, GiGA chain has allowed the network provider to evolve its business model by offering Blockchain as a service, allowing companies to perform the transaction using a smart contract without using a middleman. Also, the same platform has been used for payment and digital vouchers by the government.

China's major telecom operators China Mobile, China Unicom and China Telecom used the Blockchain platform pilot project to share information on Know Your Customer (KYC) procedures for quick customer identification [128]. This allows the customer of all the participating operators to port their data between seamlessly and securely, thereby preventing and detecting fraud in the early stages. This pilot is part of a larger project that allows the use of Blockchain SIM instead of a physical SIM that will allow the customers to manage and share accounts over various devices. This Blockchain SIM will be used to generate the private key and digital signature allowing for a new digital economy where users can not only manage personal data but can perform other transactions as well.

In 2018, China Mobile, NTT DoCoMo (Japan) and KT mobile (Korea) formed a Blockchain pilot project for the identification of customers in roaming to handle roaming [129]. The smart contract on the Blockchain allowed for real-time calculation and automated payments for international data roaming operations.

Under TM Forum Catalyst project, several Blockchain-based projects are being explored for their potential application in 5G [130]. A Blockchain-based data sharing platform was showcased for data management to monetize the massive data assets. Based on Blockchain technology, a generalized mechanism of data sharing, trust chain between consumer and data asset management was developed. The obvious advantage was in terms of privacy, traceability,

anonymous data exchange and auditability. Another project called ''Blockchain-based Telecom Infrastructure Marketplace'' is looking into the possibility allowing various network operators to procure infrastructure and assets on demand seamlessly and reliably to enable new business models and at the same deliver high-quality service to the end-user. The assets (both physical and virtual) can be traded in a marketplace and charged using Blockchain to setup desired functionality. Infrastructure and resource sharing are important to reduce CAPEX and OPEX. Blockchain is key to enable shared economy and service delivery.

Besides the PoC and trails, there have been some startups that are offering Blockchain-based solutions for network operators. Using Blockchain, Bubbletone platform allows mobile telephone users, network operators and service providers to interact directly [131]. Any network operator can become a member of the Blockchain network and provide its services to roaming customers from different countries. To achieve this, the network operators need to publish the plans in the form of smart contracts. Users can choose preferred tariff or service abroad without the need for a new SIM card, thereby reducing operating costs and time.

Xeniro [132] offers Blockchain for network operators to monetize their edge infrastructure to handle and monetize IoT transactions from billions of devices. The Platform provides enables on high-frequency nano-transactions between IoT devices. Also, it enables the network operators to rent RAN to an authorized third party via Blockchain, hence creating a new business model and value chain.

Irbis network created by SC telecom creates a decentralized network using Blockchain [133]. It brings together network operators, IoT devices, messengers and 5G technologies using Blockchain that creates secure routing and a trusted environment. It is designed to eliminate the vulnerabilities present in the SS7/GSM protocol. In the Ibris decentralized network, nodes that provide communication services can be either from network operation or can be registered on the network and maintained by the community member. The Blockchain stores the actual rate for communication provided by various operators, register the nodes, billing and execute smart contracts.

As it can be seen there have several deployments and PoC due to the benefits Blockchain offers in terms of security, sharing and automation. Several leading network operators are now looking into exploiting the benefits based on the early trials. Besides, several industry-related consortia are now focusing on bringing Blockchain to telecoms. For example, Hyperledger [26] an open-sourced Blockchain project contains leading network operators such as Deutsche Telekom and Swisscom. The Carrier Blockchain Study Group (CBSG) [134], consists of network operators from across the globe exploring the potential to build a next-generation, cross-carrier Blockchain network for various use cases. The current use cases that are deployed, though promising, are still very limited. Based on the amount of research work that has been done, the full potential of Blockchain is yet to be realized.

V. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

The Blockchain has the potential to solve the various problems associated with 5G ranging from security, automation, resource management in a distributed and decentralized manner. However, several issues need to be investigated before the Blockchain can be integrated into the 5G network to enhance network operation and security. In this section, we highlight some of the open issues and challenges associated with it.

1) **Scalability and Performance** - The rate at which transactions are approved in a Blockchain is measured in transactions per second (TPS), and the low transaction speed of Blockchain is a major concern for several industries adopting the solution especially 5G. Most of the existing Blockchain solutions suffer from poor transaction rate and are not suitable for 5G networks. The throughput of the Blockchain is determined primarily by two factors. First, the consensus algorithms that determine how to reach an agreement to add the block. Second, the way Blockchain is designed i.e. private, public or consortium. A private or consortium Blockchain, which is most likely the case for 5G, is expected to achieve a higher transaction rate due to a controlled environment and limited participants involved in approving the transaction compared to public Blockchain. For the consensus algorithms, there are several solutions but most of them are designed to achieve a transaction rate comparable to VISA which processes 2000 TPS [135]. High TPS is important in 5G to meet low latency commitment of 5G and Beyond-5G networks that requires coordination between several entities,e.g. setting up network slices. There have been studies that have achieved transaction rates up to 300,000 TPS compared to 4.6 TPS for Bitcoin [136]. These high TPS are theoretical and achieved in a controlled environment. Further studies are required on how such consensus algorithms can scale and be used in a dynamic and heterogeneous network that involves a large volume of transactions from a variety of devices at various levels in the 5G network.
2) **Security** - Even though Blockchain is widely accepted as a solution to solve various security issues in the 5G network and IoT, there are several security issues related to Blockchain itself. For example, consensus protocols that are the fundamental component of Blockchain technologies, are more often a target of attackers. Furthermore, if the attacker can control more than 50% of the nodes in the Blockchain network, also known as 51% attack, then the blocks can be manipulated. The security of consensus algorithms needs to be extensively tested before being deployed at a massive scale. Also, the smart contract that is critical to the success of Blockchain may be insecure due to poorly written code. Although there have been studies

on mitigating individual attacks on Blockchain using various solutions [137], the main research challenge is to combine these solutions to provide resiliency against combined attacks on Blockchain networks deployed for 5G. The permissioned Blockchain has its own set of issues in terms of authentication and control over data. For example, who has the authority to grant permission to a node for joining the network and how will the system ensure the authenticity of permission granter. Besides, permissioned Blockchain gives the permission granter more control (to make changes) over the data.

3) **Network deployment and Interoperability** - Although as discussed in Section IV, there have been few trials and PoC at a limited scale by various network operators. It is still not clear how the Blockchain will be deployed in the 5G or beyond 5G network that involves various technologies such as MEC, SDN and NFV. Several questions need to be investigated to implement Blockchain efficiently in the network. Some of the questions that are worth investigating are (i) Will Blockchain be an overlay network? (ii) Will there be multiple Blockchain deployed in the network for managing operations? (iii) If multiple Blockchains are deployed how will be the interoperability issue addressed?
4) **Resource Constraints and Allocation** - Blockchain requires computation on the transaction before it is accepted or rejected. The consensus algorithms required for this purpose can be computationally intensive. Therefore, it is not feasible for all the nodes in the network to participate in the transaction validation process. For example, an MEC (or C-RAN) node may be already operating at full capacity providing services to the users and might not be able to perform the required computation for block validation in time hence resulting in delay. Such a situation may lead to bottleneck and network performance degradation as the required resource might not be provisioned in time. Due to resource constraint, an optimization framework that dynamically selects the mining node in a permissioned network is required for the 5G network. Therefore, resource provisioning for computing to support a Blockchain in a 5G network needs to be investigated. Besides, not all nodes are capable of running Blockchain, especially IoT devices. To overcome this challenge optimal placement of dedicated validating nodes may be needed in the network that needs to be investigated. Furthermore, the Blockchain requires broadcast of the transaction to be approved that may result in significant overhead adding to network traffic. Thus, reducing the overhead to minimize the storage and the processing burden brings additional challenges in adopting Blockchain in 5G network.
5) **Energy Efficiency** - 5G network is going to significantly increase energy consumption due to network design and increased network equipment. With ongoing efforts to emphasize green communication, Blockchain will be a big hurdle due to the computationally intensive mining process. Most of the power in the Blockchain network is consumed due to the consensus algorithm. There have been efforts to develop energy-efficient consensus algorithms such as Proof-of-Space [138] and mini-Blockchain [139]. However, these works still need to be tested on a large scale and there is a lot of space for further improvement. Therefore, designing an energy-efficient consensus algorithm is a significant research challenge for Blockchain adoption in the 5G network.
6) **Incentive Mechanism** : The 5G network is going to be a highly diverse and heterogeneous environment where several resources need to be shared between network operators and authorized third party. The operator may have to lease computing resources from other users in the network. This presents a unique business model, revenue opportunity and optimal utilization of resources in the network. Therefore, it is important to design a suitable incentive mechanism to encourage participation in such resource sharing scenarios.
7) **Standardization Requirement** - Even though Blockchain has been around for quite some time it has recently started gaining traction of network operators. Therefore, to get a wide acceptance the network operators need to come together and work toward standardization of Blockchain integration in 5G network and beyond. To address this, several consortia have been formed to address the issue of interconnectivity and interoperability. For example, Carrier Blockchain Study Group (CBSG) consortia consisting of leading network operators is working toward building a next-generation and cross-carrier Blockchain network. Similarly, Hyperledger [26] which is an open-source initiative across various industries consisting of leading network operators. Despite the efforts, there is a long way to go to agree upon protocols, coding languages and format for the smart contract, consensus mechanisms and privacy measures. This process will require multiple phases of implementation and requires collaboration across industry and researchers.
8) **Data Management**- In Blockchain the same data may be shared by several participating nodes. In the case of 5G networks, the data may be exchanged between edge, core and mobile users over Blockchain. Therefore, there is a need for a standardized method for ingesting, aligning and enriching the data from different sources using different data formats into a common data model with well-understood semantics. This is important to derive actionable insights and decisions. Besides, it is important to determine what kind of data will be stored on the Blockchain and what will be stored off-chain in the cloud. Since Blockchain is suitable for

storing a small amount of reference data. Addressing this issue will be crucial to ensure interoperability and adoption across the ecosystem.

9) **Networking and Storage**: Blockchain requires significant computational power and overhead to reach consensus. This overhead can consume significant bandwidth in the network. In certain scenarios, the resources may be limited hence limiting the ability to reach consensus in a timely manner resulting in high latency. Furthermore, the transaction keeps on adding on to the Blockchain which results in increased storage consumption. Certain Blockchain solutions require the node to possess the entire copy of Blockchain transaction data which is not feasible in devices with constrained resources. There have been some efforts in this direction, for example, IoTA [18] shows promises that can address the issues related to limited resources. However, further research and validation are needed to be used in 5G and beyond networks.
10) **Selection of suitable Blockchain platform**: There have been several Blockchain platforms in the marketplace since the inception of Bitcoin. However, there are not sufficient experimental studies to report the suitability of one platform over the other one. This creates a challenge for adopting a suitable Blockchain platform on 5G networks which would be able to accommodate diverse requirements, such as performance, infrastructure cost, and data privacy, etc. This challenge cannot be tackled unless further experimental evidence could be provided. Hence, the Blockchain research community needs to conduct more pilot research projects to explore and report the suitability of different Blockchain platforms for integration with 5G networks and beyond.
11) **Integration with machine learning**: Data is important for training a machine learning model effectively. Recently, machine learning algorithms are being investigated for improving various network operations. However, training machine learning models is challenging due to the lack of data from across the network elements. There is an opportunity to build better machine learning models by using Blockchain. As Blockchain allows for data sharing in a safe and secure manner it will result in convergence of data from silos across several stakeholders. This will result in valuable data-driven insights, decision support, prediction and optimization. There have been some efforts in this direction that investigates the potential of such integration of machine learning and Blockchain. For example, deep reinforcement learning with Blockchain is proposed for orchestration and resource management securely in [15]. More such works using various machine learning models are needed to explore this area further that make use of Blockchain.

VI. CONCLUSION

Blockchain has moved beyond the realm of cryptocurrency and is now revolutionizing several industries. The interest is gone beyond the hype as several industries have started adopting the Blockchain-based solution to improve business processes. In the same way, 5G network and beyond 5G network are no exception as several studies have been conducted to bring the benefits of Blockchain to 5G network. As future 5G networks are expected to be highly distributed and decentralized in nature, the network management and security issues become more prevalent and challenging compared to the previous generations which are highly centralized. Blockchain, due to its secure design concepts, addresses core security issues such as integrity, authentication, trust and availability in a distributed fashion. Also, the smart contracts can enable end-to-end resource allocation/sharing, network management and orchestration delivering desired services envisioned by 5G. Furthermore, Blockchain will enable several new business models, reduce the hassle associated with cooperation among network operators and seamlessly handle several processes.

In this paper, we reviewed the state-of-the-art literature that uses Blockchain to address several key issues faced in the 5G network. Based on the review we provided the taxonomy of Blockchain application in 5G network under network management, computing management, communication management and services. Furthermore, we summarized various field-trials and PoC that uses Blockchain for various operations in the current mobile network. We believe Blockchain holds immense potential for 5G and future networks. If implemented properly it has the potential to roll out 5G connectivity around the world in a secure, cost-effective and efficient manner. Beside several advantages, various challenges need to be addressed. For this, we highlighted some of the key challenges that need to be thoroughly investigated and provided future research direction.

REFERENCES

[1] J. Rodriguez, *Fundamentals of 5G Mobile Networks*. Hoboken, NJ, USA: Wiley, 2015.
[2] *Internet of Things—Number of Connected Devices Worldwide 2015-2025*. Accessed: Apr. 1, 2020. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide
[3] *Ookla 5G Map*. Accessed: Apr. 25, 2020. [Online]. Available: https://www.speedtest.net/ookla-5g-map
[4] *Intel 5G Technology at the 2020 Tokyo Olympics to Play a Transformative Role From Sports to Transportation*. Accessed: Apr. 25, 2020. [Online]. Available: https://newsroom.intel.com/editorials/intel-5g-technology-olympic-games-tokyo-2020-play-role-transforming-everything-sports-transportation/#gs.4yd84p
[5] *Blockchains in Mobile Networks*. Accessed: Mar. 20, 2020. [Online]. Available: https://e.huawei.com/us/publications/global/ict_insights/201703141505/core-competency/201703150928
[6] *Blockchain Telco*. Accessed: Mar. 20, 2020. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/za/Documents/technology-media-telecommunications/za_TMT_Blockchain_TelCo.pdf
[7] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for Internet of Things," *Comput. Commun.*, vol. 136, pp. 10–29, Feb. 2019.
[8] X. Zhang and X. Chen, "Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 58241–58254, 2019.

[9] T. Jiang, H. Fang, and H. Wang, "Blockchain-based Internet of Vehicles: Distributed network architecture and performance analysis," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4640–4649, Jun. 2019.

[10] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 33–39, Aug. 2018.

[11] Z. Xiong, S. Feng, W. Wang, D. Niyato, P. Wang, and Z. Han, "Cloud/fog computing resource management and pricing for blockchain networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4585–4600, Jun. 2019.

[12] X. Ling, J. Wang, T. Bouchoucha, B. C. Levy, and Z. Ding, "Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm," *IEEE Access*, vol. 7, pp. 9714–9723, 2019.

[13] A. Chaer, K. Salah, C. Lima, P. P. Ray, and T. Sheltami, "Blockchain for 5G: Opportunities and challenges," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2019, pp. 1–6.

[14] D. C Nguyen, P. N Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and beyond networks: A state of the art survey," 2019, *arXiv:1912.05062*. [Online]. Available: http://arxiv.org/abs/1912.05062

[15] 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 2019.

[16] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges," *Mech. Syst. Signal Process.*, vol. 135, Jan. 2020, Art. no. 106382.

[17] M. A. R. Chaudhry and Z. A. Soptimizer, "Blockchain: A key enabler for 5G," *IEEE Standards Univ.*, vol. 10, no. 1, 2019. [Online]. Available: https://www.standardsuniversity.org/e-magazine/may-2019-volume-9-issue-1-blockchain-standards/blockchain-a-key-enabler-for-5g/

[18] R. Alexander, *Iota-Introduction to the Tangle Technology: Everything You Need to Know About the Revolutionary Blockchain Alternative*. Independently Published, 2018.

[19] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2019.

[20] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE Access*, vol. 7, pp. 36500–36515, 2019.

[21] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2794–2830, 3rd Quart., 2019.

[22] P. Mehta, R. Gupta, and S. Tanwar, "Blockchain envisioned UAV networks: Challenges, solutions, and comparisons," *Comput. Commun.*, vol. 151, pp. 518–538, Feb. 2020.

[23] 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. Surveys Tuts.*, vol. 21, no. 2, pp. 1508–1532, 2nd Quart., 2019.

[24] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019.

[25] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, Apr. 2014.

[26] T. Blummer, M. Sean, and C. Cachin, "An introduction to hyperledger," Hyperledger Under Linux Found., White Paper, 2018. [Online]. Available: https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf

[27] M. Condoluci and T. Mahmoodi, "Softwarization and virtualization in 5G mobile networks: Benefits, trends and challenges," *Comput. Netw.*, vol. 146, pp. 65–84, Dec. 2018.

[28] A. A. Barakabitze, N. Barman, A. Ahmad, S. Zadtootaghaj, L. Sun, M. G. Martini, and L. Atzori, "QoE management of multimedia streaming services in future networks: A tutorial and survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 526–565, 1st Quart., 2020.

[29] I. F. Akyildiz, A. Lee, P. Wang, M. Luo, and W. Chou, "A roadmap for traffic engineering in SDN-OpenFlow networks," *Comput. Netw.*, vol. 71, pp. 1–30, Oct. 2014.

[30] D. Kreutz, F. M. V. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proc. IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2015.

[31] G. A. Carella, M. Pauls, T. Magedanz, M. Cilloni, P. Bellavista, and L. Foschini, "Prototyping nfv-based multi-access edge computing in 5G ready networks with open baton," in *Proc. IEEE Conf. Netw. Softwarization (NetSoft)*, Jul. 2017, pp. 1–4.

[32] Y.-D. Lin and Y.-C. Hsu, "Multihop cellular: A new architecture for wireless communications," in *Proc. IEEE Conf. Comput. Commun., 19th Annu. Joint Conf. IEEE Comput. Commun. Societies (INFOCOM)*, vol. 3, Mar. 2000, pp. 1273–1282.

[33] K. Kalkan and S. Zeadally, "Securing Internet of Things with software defined networking," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 186–192, Sep. 2018.

[34] M. T. I. ul Huque, W. Si, G. Jourjon, and V. Gramoli, "Large-scale dynamic controller placement," *IEEE Trans. Netw. Service Manage.*, vol. 14, no. 1, pp. 63–76, Mar. 2017.

[35] B. Heller, R. Sherwood, and N. McKeown, "The controller placement problem," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 42, no. 4, pp. 473–478, Sep. 2012.

[36] F. Bannour, S. Souihi, and A. Mellouk, "Distributed SDN control: Survey, taxonomy, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 333–354, 1st Quart., 2018.

[37] S. Scott-Hayward, S. Natarajan, and S. Sezer, "A survey of security in software defined networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 623–654, Fir. 2016.

[38] P.-W. Tsai, C.-W. Tsai, C.-W. Hsu, and C.-S. Yang, "Network monitoring in software-defined networking: A review," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3958–3969, Dec. 2018.

[39] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, 2017.

[40] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs," *IEEE Access*, vol. 7, pp. 56656–56666, 2019.

[41] J. Gao, K. O.-B. Obour Agyekum, E. B. Sifah, K. N. Acheampong, Q. Xia, X. Du, M. Guizani, and H. Xia, "A blockchain-SDN-enabled Internet of Vehicles environment for fog computing and 5G networks," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4278–4291, May 2020.

[42] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.-K.-R. Choo, "Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks," *IEEE Trans. Netw. Sci. Eng.*, early access, Aug. 28, 2020, doi: 10.1109/TNSE.2019.2937481.

[43] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network function virtualization: Challenges and opportunities for innovations," *IEEE Commun. Mag.*, vol. 53, no. 2, pp. 90–97, Feb. 2015.

[44] S. Lal, T. Taleb, and A. Dutta, "NFV: Security threats and best practices," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 211–217, Aug. 2017.

[45] I. D. Alvarenga, G. A. F. Rebello, and O. C. M. B. Duarte, "Securing configuration management and migration of virtual network functions using blockchain," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS)*, Apr. 2018, pp. 1–9.

[46] G. A. F. Rebello, I. D. Alvarenga, I. J. Sanz, and O. C. M. B. Duarte, "BSec-NFVO: A blockchain-based security for network function virtualization orchestration," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.

[47] S. Zawoad and R. Hasan, "SECAP: Towards securing application provenance in the cloud," in *Proc. IEEE 9th Int. Conf. Cloud Comput. (CLOUD)*, Jun. 2016, pp. 900–903.

[48] N. Bozic, G. Pujolle, and S. Secci, "Securing virtual machine orchestration with blockchains," in *Proc. 1st Cyber Secur. Netw. Conf. (CSNet)*, Oct. 2017, pp. 1–8.

[49] M. Keller, "Design and implementation of a blockchain-based trusted VNF package repository," Ph.D. dissertation, Dept. Inform., Univ. Zürich, Zürich, Switzerland, 2019.

[50] M. Bursell, A. Dutta, H. Lu, M. Odini, K. Roemer, K. Sood, M. Wong, and P. Wörndle, "Network functions virtualisation (NFV), NFVv security, security and trust guidance, v. 1.1. 1," Eur. Telecommun. Standards Inst., Sophia Antipolis, France, Tech. Rep. gs nfv-sec 003, 2014.

[51] 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 *Proc. IFIP Netw. Conf. (IFIP Netw.)*, May 2019, pp. 1–9.

[52] R. V. Rosa and C. E. Rothenberg, "Blockchain-based decentralized applications for multiple administrative domain networking," *IEEE Commun. Standards Mag.*, vol. 2, no. 3, pp. 29–37, Sep. 2018.
[53] N. Alliance, "5G security recommendations Package# 2: Network Slicing," NGMN, Frankfurt, Germany, Tech. Rep., Apr. 2016, pp. 1–12. [Online]. Available: https://www.ngmn.org/publications/5g-security-recommendations-package-2-network-slicing.html
[54] L. Zanzi, A. Albanese, V. Sciancalepore, and X. Costa-Perez, "NSBchain: A secure blockchain framework for network slicing brokerage," 2020, *arXiv:2003.07748*. [Online]. Available: http://arxiv.org/abs/2003.07748
[55] 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)*, Mar. 2018, pp. 332–336.
[56] V. Ortega, F. Bouchmal, and J. F. Monserrat, "Trusted 5G vehicular networks: Blockchains and content-centric networking," *IEEE Veh. Technol. Mag.*, vol. 13, no. 2, pp. 121–127, Jun. 2018.
[57] E. Hossain and M. Hasan, "5G cellular: Key enabling technologies and research challenges," *IEEE Instrum. Meas. Mag.*, vol. 18, no. 3, pp. 11–21, Jun. 2015.
[58] H. Yang, H. Zheng, J. Zhang, Y. Wu, Y. Lee, and Y. Ji, "Blockchain-based trusted authentication in cloud radio over fiber network for 5G," in *Proc. 16th Int. Conf. Opt. Commun. Netw. (ICOCN)*, Aug. 2017, pp. 1–3.
[59] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Jun. 2017, pp. 468–475.
[60] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput. (CCGRID)*, May 2017, pp. 468–477.
[61] S. Ali, G. Wang, M. Z. A. Bhuiyan, and H. Jiang, "Secure data provenance in cloud-centric Internet of Things via blockchain smart contracts," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Oct. 2018, pp. 991–998.
[62] M. Ma, G. Shi, and F. Li, "Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario," *IEEE Access*, vol. 7, pp. 34045–34059, 2019.
[63] C. Xu, K. Wang, and M. Guo, "Intelligent resource management in blockchain-based cloud datacenters," *IEEE Cloud Comput.*, vol. 4, no. 6, pp. 50–59, Nov. 2017.
[64] O. O. Malomo, D. B. Rawat, and M. Garuba, "Next-generation cybersecurity through a blockchain-enabled federated cloud framework," *J. Supercomput.*, vol. 74, no. 10, pp. 5099–5126, Oct. 2018.
[65] H. Yang, Y. Liang, J. Yuan, Q. Yao, A. Yu, and J. Zhang, "Distributed blockchain-based trusted multi-domain collaboration for mobile edge computing in 5G and beyond," *IEEE Trans. Ind. Informat.*, early access, Jan. 7, 2020, doi: 10.1109/TII.2020.2964563.
[66] H. Zhu, C. Huang, and J. Zhou, "EdgeChain: Blockchain-based multi-vendor mobile edge application placement," in *Proc. 4th IEEE Conf. Netw. Softwarization Workshops (NetSoft)*, Jun. 2018, pp. 222–226.
[67] D. Lin, S. Hu, Y. Gao, and Y. Tang, "Optimizing MEC networks for healthcare applications in 5G communications with the authenticity of Users' priorities," *IEEE Access*, vol. 7, pp. 88592–88600, 2019.
[68] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Privacy-preserved task offloading in mobile blockchain with deep reinforcement learning," 2019, *arXiv:1908.07467*. [Online]. Available: http://arxiv.org/abs/1908.07467
[69] Z. Xiong, S. Feng, D. Niyato, P. Wang, and Z. Han, "Optimal pricing-based edge computing resource management in mobile blockchain," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.
[70] J. Xu, S. Wang, B. K. Bhargava, and F. Yang, "A blockchain-enabled trustless crowd-intelligence ecosystem on mobile edge computing," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3538–3547, Jun. 2019.
[71] D. T. Hoang, D. Niyato, D. N. Nguyen, E. Dutkiewicz, P. Wang, and Z. Han, "A dynamic edge caching framework for mobile 5G networks," *IEEE Wireless Commun.*, vol. 25, no. 5, pp. 95–103, Oct. 2018.
[72] Y. Dai, D. Xu, K. Zhang, S. Maharjan, and Y. Zhang, "Deep reinforcement learning and permissioned blockchain for content caching in vehicular edge computing and networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4312–4324, Apr. 2020.
[73] W. Wang, D. Niyato, P. Wang, and A. Leshem, "Decentralized caching for content delivery based on blockchain: A game theoretic perspective," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.
[74] X. Xu, Y. Chen, X. Zhang, Q. Liu, X. Liu, and L. Qi, "A blockchain-based computation offloading method for edge computing in 5G networks," *Softw., Pract. Exper.*, Sep. 2019, doi: 10.1002/spe.2749.
[75] X. Xu, Y. Li, T. Huang, Y. Xue, K. Peng, L. Qi, and W. Dou, "An energy-aware computation offloading method for smart edge computing in wireless metropolitan area networks," *J. Netw. Comput. Appl.*, vol. 133, pp. 75–85, May 2019.
[76] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Secure computation offloading in blockchain based IoT networks with deep reinforcement learning," 2019, *arXiv:1908.07466*. [Online]. Available: http://arxiv.org/abs/1908.07466
[77] W. Chen, Z. Zhang, Z. Hong, C. Chen, J. Wu, S. Maharjan, Z. Zheng, and Y. Zhang, "Cooperative and distributed computation offloading for blockchain-empowered industrial Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8433–8446, Oct. 2019.
[78] X. Qiu, L. Liu, W. Chen, Z. Hong, and Z. Zheng, "Online deep reinforcement learning for computation offloading in blockchain-empowered mobile edge computing," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 8050–8062, Aug. 2019.
[79] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, "Computation offloading and content caching in wireless blockchain networks with mobile edge computing," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11008–11021, Nov. 2018.
[80] S. Seng, X. Li, C. Luo, H. Ji, and H. Zhang, "A D2D-assisted MEC computation offloading in the blockchain-based framework for UDNs," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.
[81] V. Sharma, I. You, D. N. K. Jayakody, D. G. Reina, and K.-K.-R. Choo, "Neural-Blockchain-Based ultrareliable caching for edge-enabled UAV networks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 10, pp. 5723–5736, Oct. 2019.
[82] S. Mori, "Secure caching scheme by using blockchain for information-centric network-based wireless sensor networks," *J. Signal Process.*, vol. 22, no. 3, pp. 97–108, 2018.
[83] Q. Xu, Z. Su, and Q. Yang, "Blockchain-based trustworthy edge caching scheme for mobile cyber-physical system," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 1098–1110, Feb. 2020.
[84] J. Borland, P. Dawkins, D. Johnson, and R. Williams, "Small cells market status report," Small Cell Forum, Brighton, U.K., Tech. Rep. 050.10.03, 2018.
[85] B. Mafakheri, T. Subramanya, L. Goratti, and R. Riggio, "Blockchain-based infrastructure sharing in 5G small cell networks," in *Proc. 14th Int. Conf. Netw. Service Manage. (CNSM)*, 2018, pp. 313–317.
[86] E. Di Pascale, J. McMenamy, I. Macaluso, and L. Doyle, "Smart contract SLAs for dense Small-Cell-as-a-Service," 2017, *arXiv:1703.04502*. [Online]. Available: http://arxiv.org/abs/1703.04502
[87] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, "6G wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 28–41, Sep. 2019.
[88] 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. 2020.
[89] S. Zheng, T. Han, Y. Jiang, and X. Ge, "Smart contract-based secure spectrum sharing in multi-operators wireless communication networks," 2020, *arXiv:2002.00771*. [Online]. Available: http://arxiv.org/abs/2002.00771
[90] 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.
[91] 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)*, Dec. 2019, pp. 1–6.
[92] H. Cui, Z. Chen, N. Liu, and B. Xia, "Blockchain-driven contents sharing strategy for wireless cache-enabled D2D networks," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2019, pp. 1–5.

[93] D. Lin and Y. Tang, "Blockchain consensus based user access strategies in D2D networks for data-intensive applications," *IEEE Access*, vol. 6, pp. 72683–72690, 2018.

[94] A. Zhou, Q. Sun, and J. Li, "BCEdge: Blockchain-based resource management in D2D-assisted mobile edge computing," *Softw., Pract. Exper.*, Oct. 2019, doi: 10.1002/spe.2758.

[95] H. Klessig, D. Öhmann, A. I. Reppas, H. Hatzikirou, M. Abedi, M. Simsek, and G. P. Fettweis, "From immune cells to self-organizing ultra-dense small cell networks," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 4, pp. 800–811, Apr. 2016.

[96] G. Praveen, V. Chamola, V. Hassija, and N. Kumar, "Blockchain for 5g: A prelude to future telecommunication," *IEEE Netw.*, early access, Apr. 30, 2020, doi: 10.1109/MNET.001.2000005.

[97] V. Messie, G. Fromentoux, X. Marjou, and N. L. Omnes, "BALAdIN for blockchain-based 5G networks," in *Proc. 22nd Conf. Innov. Clouds, Internet Netw. Workshops (ICIN)*, Feb. 2019, pp. 201–205.

[98] A. El Gamal and H. El Gamal, "A single coin monetary mechanism for distributed cooperative interference management," *IEEE Wireless Commun. Lett.*, vol. 8, no. 3, pp. 757–760, Jun. 2019.

[99] N. C. Luong, T. T. Anh, H. T. Thanh Binh, D. Niyato, D. I. Kim, and Y.-C. Liang, "Joint transaction transmission and channel selection in cognitive radio based blockchain networks: A deep reinforcement learning approach," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2019, pp. 8409–8413.

[100] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, and M. A. Imran, "Blockchain-enabled wireless Internet of Things: Performance analysis and optimal communication node deployment," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5791–5802, Jun. 2019.

[101] Z. Liu, L. Gao, Y. Liu, X. Guan, K. Ma, and Y. Wang, "Efficient QoS support for robust resource allocation in blockchain-based femtocell networks," *IEEE Trans. Ind. Informat.*, early access, Sep. 3, 2019, doi: 10.1109/TII.2019.2939146.

[102] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," *IET Commun.*, vol. 12, no. 5, pp. 527–532, Mar. 2018.

[103] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of IoT data," in *Proc. Cloud Comput. Secur. Workshop (CCSW)*, 2017, pp. 45–50.

[104] G. Zhang, T. Li, Y. Li, P. Hui, and D. Jin, "Blockchain-based data sharing system for AI-powered network operations," *J. Commun. Inf. Netw.*, vol. 3, no. 3, pp. 1–8, Sep. 2018.

[105] X. Chen, J. Ji, C. Luo, W. Liao, and P. Li, "When machine learning meets blockchain: A decentralized, privacy-preserving and secure design," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2018, pp. 1178–1187.

[106] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196–248, 1st Quart., 2020.

[107] Z. Chen, S. Chen, H. Xu, and B. Hu, "A security authentication scheme of 5G ultra-dense network based on block chain," *IEEE Access*, vol. 6, pp. 55372–55379, 2018.

[108] Y. Zhang, R. Deng, E. Bertino, and D. Zheng, "Robust and universal seamless handover authentication in 5G HetNets," *IEEE Trans. Dependable Secure Comput.*, early access, Jul. 9, 2019, doi: 10.1109/TDSC.2019.2927664.

[109] S. Zhang and J.-H. Lee, "A group signature and authentication scheme for blockchain-based mobile-edge computing," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4557–4565, May 2020.

[110] E. J. Scheid, M. Keller, M. F. Franco, and B. Stiller, "BUNKER: A blockchain-based trUsted VNF pacKagE repository," in *Proc. Int. Conf. Econ. Grids, Clouds, Syst., Services*. Cham, Switzerland: Springer, 2019, pp. 188–196.

[111] H. Wang and J. Zhang, "Blockchain based data integrity verification for large-scale IoT data," *IEEE Access*, vol. 7, pp. 164996–165006, 2019.

[112] A. Z. Ourad, B. Belgacem, and K. Salah, "Using blockchain for IOT access control and authentication management," in *Proc. Int. Conf. Internet Things*. Cham, Switzerland: Springer, 2018, pp. 150–164.

[113] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019.

[114] A. Buldas, A. Kroonmaa, and R. Laanoja, "Keyless signatures' infrastructure: How to build global distributed hash-trees," in *Proc. Nordic Conf. Secure IT Syst.* Berlin, Germany: Springer, 2013, pp. 313–320.

[115] H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu, and J. Xing, "Hyperconnected network: A decentralized trusted computing and networking paradigm," *IEEE Netw.*, vol. 32, no. 1, pp. 112–117, Jan. 2018.

[116] H. R. Hasan and K. Salah, "Combating deepfake videos using blockchain and smart contracts," *IEEE Access*, vol. 7, pp. 41596–41606, 2019.

[117] E. Bastug, M. Bennis, and M. Debbah, "Living on the edge: The role of proactive caching in 5G wireless networks," *IEEE Commun. Mag.*, vol. 52, no. 8, pp. 82–89, Aug. 2014.

[118] T. X. Vu, S. Chatzinotas, and B. Ottersten, "Blockchain-based content delivery networks: Content transparency meets user privacy," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–6.

[119] E. Ak and B. Canberk, "BCDN: A proof of concept model for blockchain-aided CDN orchestration and routing," *Comput. Netw.*, vol. 161, pp. 162–171, Oct. 2019.

[120] *SS7 Vulnerabilities and Attack Exposure Report*, Positive Technol., London, U.K., 2000.

[121] 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, May 2020.

[122] C. Li, Q. Wu, H. Li, and J. Liu, "Trustroam: A novel blockchain-based cross-domain authentication scheme for Wi-Fi access," in *Proc. Int. Conf. Wireless Algorithms, Syst., Appl.* Cham, Switzerland: Springer, 2019, pp. 149–161.

[123] D. Liu, D. Li, X. Liu, L. Ma, H. Yu, and H. Zhang, "Research on a cross-domain authentication scheme based on consortium blockchain in V2G networks of smart grid," in *Proc. 2nd IEEE Conf. Energy Internet Energy Syst. Integr. (EI)*, Oct. 2018, pp. 1–5.

[124] *Blockchain in Telecoms*. Accessed: Apr. 10, 2020. [Online]. Available: https://www.omdia.com/resources/product-content/blockchain-in-telecoms-spt001-000029

[125] *Telefónica and IBM Collaborate to Apply Blockchain to Streamline Telco Processes*. Accessed: Apr. 11, 2020. [Online]. Available: https://www.telefonica.com/en/web/press-office/-/telefonica-and-ibm-collaborate-to-apply-blockchain-to-streamline-telco-processes

[126] *Vodafone Idea, Jio, Airtel & BSNL Executing World's Largest Blockchain Use Case to Curb Pesky Calls, SMS*. Accessed: Apr. 11, 2020. [Online]. Available: https://telecom.economictimes.indiatimes.com/news/how-vodafone-idea-jio-airtel-bsnl-executing-worlds-largest-blockchain-use-case-to-curb-pesky-calls-sms/69506143

[127] *South Korea's Telecom Giant kT Launches DLT-Powered 5G Brand to Prevent Hacks*. Accessed: Apr. 11, 2020. [Online]. Available: https://cointelegraph.com/news/south-koreas-telecom-giant-kt-launches-dlt-powered-5g-brand-to-prevent-hacks

[128] *China Telecom Introduces Its Blockchain SIM Card Project*. Accessed: Apr. 11, 2020. [Online]. Available: https://forkast.news/watch-china-telecom-introduces-its-blockchain-sim-card-project/

[129] *Chinese Telecoms Are Racing to Add Blockchain to Mobile Services*. Accessed: Apr. 11, 2020. [Online]. Available: https://forkast.news/china-blockchain-report-telecom-mobile//

[130] *Blockchain-Based Telecom Infrastructure Marketplace Enables 'Pop-Up' Networks and on-the-Fly Business Models*. Accessed: Apr. 11, 2020. [Online]. Available: https://inform.tmforum.org/catalyst/2019/05/blockchain-infrastructure-marketplace-enables-pop-networks-fly-business-models/?_ga=2.245488324.1793324658.1586548075-1688432296.1585584770/

[131] *Bubbletone*. Accessed: Apr. 11, 2020. [Online]. Available: https://blockchaintele.com/

[132] *Xeniro*. Accessed: Apr. 10, 2020. [Online]. Available: https://xeniro.io/

[133] *Irbis*. Accessed: Apr. 10, 2020. [Online]. Available: https://safecalls.io/ieo/

[134] *CBSG Consortium is Reshaping Mobile Payments With Cross-Carrier Blockchain Platform*. Accessed: Apr. 27, 2020. [Online]. Available: https://www.telecomtv.com/content/blockchain/cbsg-consortium-is-reshaping-mobile-payments-with-cross-carrier-blockchain-platform-36346/

[135] *No, Visa Doesn't Handle 24,000 TPS and Neither Does Your Pet Blockchain*. Accessed: Apr. 27, 2020. [Online]. Available: https://news.bitcoin.com/no-visa-doesnt-handle-24000-tps-and-neither-does-your-pet-blockchain/

[136] *Five Best Blockchains With High Transaction Speeds in 2019*. Accessed: Apr. 27, 2020. [Online]. Available: https://www.blockchain-council.org/blockchain/five-best-blockchains-with-high-transaction-speeds-in-2019/
[137] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.
[138] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of space," in *Proc. Annu. Cryptol. Conf.* Berlin, Germany: Springer, 2015, pp. 585–605.
[139] J. D. Bruce, "The mini-blockchain scheme," White Paper, 2014.

MOHAMMAD TAHIR (Member, IEEE) received the M.Sc. and Ph.D. degrees in electrical and computer engineering from the Department of Electrical and Computer Engineering, International Islamic University Malaysia, in 2011 and 2016, respectively. Prior to joining academics, he has worked with the Research and Development Division of industry for seven years on several projects related to the Internet of Things and cognitive radio. His research interests include 5G, the Internet of Things, game theory for wireless networks, wireless security, blockchain, and autonomic computing.

MOHAMED HADI HABAEBI (Senior Member, IEEE) received the degree from the Civil Aviation and Meteorology High Institute, Libya, in 1991, the M.Sc. degree in electrical engineering from Universiti Teknologi Malaysia, in 1994, and the Ph.D. degree in computer and communication system engineering from University Putra Malaysia, in 2001. He is currently an full-time Professor and the Post Graduate Academic Advisor with the Department of Electrical and Computer Engineering, International Islamic University Malaysia, where he heads the research works on the Internet of Things. He has supervised many Ph.D. and M.Sc. students, published more 120 articles and papers, and sits on the Editorial Boards of many international journals. He is actively publishing in M2M communication protocols, wireless sensor and actuator networks, cognitive radio, small antenna systems and radio propagation, and wireless communications and network performance evaluation. He is an Active Member of the IEEE and an Active Reviewer of many international journals.

MOHAMMAD DABBAGH (Member, IEEE) received the Ph.D. degree in computer science, specialization in software engineering, from the University of Malaya (UM), Malaysia, in 2015. He is currently a Senior Lecturer and the Programme Leader of the Department of Computing and Information Systems, Sunway University, Malaysia. Prior to joining Sunway University, he has acquired enormous working experiences as a Lecturer and a Researcher in the computer science discipline. He has published several research papers in prestigious international journals and conference proceedings. His research interests include blockchain, requirements engineering, empirical software engineering, big data analytics, and the Internet of Things. He has been recognized as a Certified Professional in Requirements Engineering (CPRE) by the International Requirements Engineering Board (IREB). He is also a member of the IEEE Computer Society and Malaysian Software Testing Board.

AMNA MUGHEES received the M.S. degree from the Department of Electrical and Computer Engineering, Comsats University Pakistan, in 2014. She is currently pursuing the Ph.D. degree with the Department of Computing and Information Systems, Sunway University, Malaysia. Her research interests include 5G, wireless networks, handover, the Internet of Things, and artificial intelligence.

ABDUL AHAD received the M.Sc. degree in computer science from Swat University, Pakistan, in 2014, and the M.S. degree in computer science from Virtual University, Pakistan, in 2017. He is currently pursuing the Ph.D. degree in computer science with Sunway University, Malaysia. His research interests include 5G, the Internet of Things, wireless networks, wireless body area networks (WBANs), and artificial intelligence.

KAZI ISTIAQUE AHMED received the Bachelor of Science Engineering degree in computer science and engineering from the Bangladesh University of Business and Technology, Bangladesh, in 2012, and the master's degree in electrical and computer engineering from the Kulliyyah of Engineering, International Islamic University Malaysia, Malaysia, in 2018. He is currently pursuing the Doctor of Philosophy degree in computing with the Department of Computing and Information Systems, School of Science and Technology, Sunway University, Malaysia. He has worked for the industries for more than four years in the field of database administration. He is also the Oracle 10g Certified Professional. His research interests include the IoT, the IoT security, digital image and video processing, biomedical image processing, network security, information theory and coding, and pattern recognition.