IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 31, 2022, accepted February 7, 2022, date of publication February 11, 2022, date of current version February 23, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3151150

Distributed Ledger Technologies for Network Slicing: A Survey

FARHANA JAVED[1], KIRIL ANTEVSKI[2], JOSEP MANGUES-BAFALLUY[1], LORENZA GIUPPONI[1], AND CARLOS J. BERNARDOS[2]
[1]Centre Tecnològic de Telecomunicacions de Catalunya (CTTC/CERCA), Castelldefels, 08860 Barcelona, Spain
[2]Telematic Engineering Department, Universidad Carlos III de Madrid (UC3M), 28911 Getafe, Spain

Corresponding author: Farhana Javed (farhana.javed@cttc.es)

This work was supported in part by the Spanish Formación Personal Investigador (FPI) under Grant PRE2018-086061, in part by the TRUE5G under Grant PID2019-108713RB-C52/AEI/10.13039/501100011033, and in part by the European Union (EU) H2020 The 5G Infrastructure Public Private Partnership (5GPPP) 5Growth Project 856709.

ABSTRACT Network slicing is one of the fundamental tenets of Fifth Generation (5G)/Sixth Generation (6G) networks. Deploying slices requires end-to-end (E2E) control of services and the underlying resources in a network substrate featuring an increasing number of stakeholders. Beyond the technical difficulties this entails, there is a long list of administrative negotiations among parties that do not necessarily trust each other, which often requires costly manual processes, including the legal construction of neutral entities. In this context, Blockchain comes to the rescue by bringing its decentralized yet immutable and auditable lemdger, which has a high potential in the telco arena. In this sense, it may help to automate some of the above costly processes. There have been some proposals in this direction that are applied to various problems among different stakeholders. This paper aims at structuring this field of knowledge by, first, providing introductions to network slicing and blockchain technologies. Then, state-of-the-art is presented through a global architecture that aggregates the various proposals into a coherent whole while showing the motivation behind applying Blockchain and smart contracts to network slicing. And finally, some limitations of current work, future challenges and research directions are also presented.

INDEX TERMS Distributed ledger technologies, blockchain, network slicing, beyond 5G, 6G, smart contracts.

I. INTRODUCTION

Fifth Generation (5G) is currently being rolled out globally. As it continues to take shape, network slicing has become one of the fundamental technologies to enable a wide range of use cases of 5G. The introduction of network slicing in networks has motivated their transformation based on software solutions, such as software-defined networking (SDN) and network function virtualization (NFV) [1]. In particular, network slicing helps achieve flexibility and modularity to create multiple virtual networks, each specified for a use-case, on top of a shared network to support various applications belonging to diverse verticals. An inherent characteristic to network slices is their End-to-End (E2E) nature, including both the E2E services and the E2E resources associated with this service. In a general case, this will involve multiple parties, each providing a chunk of the E2E service/resources.

The possibility of creating on-demand and cost-efficient E2E network slices and dedicating them to the various services is an essential feature of 5G networks. E2E network slicing aims for facilitating a service delivery from the service providers to the consumers prolonging various administrative domains, i.e., a slice that combines resources belonging to distinct infrastructure providers. Also, it combines various network layers and heterogeneous technologies, including Radio Access Networks (RAN), core network, transport network and cloud [2].

In particular, each network slice instance is established E2E and may include distinct sub-networks of different administrative domains. Likewise, it may be logically or physically isolated from another network slice instance [2], [3]. One of the primary objectives of 5G was to enable an E2E ecosystem to provide a consistent experience. The E2E network slicing aims for enhanced Quality of Service (QoS) for consumers and cost-effective solutions for network operators supporting the transformation that the 5G

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

network brings, along with many advancements that are yet to come in future networks [4].

This is a fundamental characteristic that makes Blockchain appear on scene in this context, as further developed next.

Vertical industries span many different domains with highly diverse requirements. They include autonomous driving and vehicle-to-everything (V2X) applications [5], Industry 4.0 [6], online health monitoring, remote diagnosis, remote robotic surgery and drug delivery [7], 4K and 8K content over the virtualized content delivery network (vCDN) [8], smart cities [9], mobile Augmented Reality (AR)/ Virtual Reality (VR) applications [10], and many more. However, vertical industries are rather broad, and the service characteristics of the corresponding vertical segment determines their requirements. The above approach is often referred to as ''network as a service'' [11] (or network slice as a service for our purposes) and it is seen as the tool for implementing dedicated and customized virtual E2E networks, enabling vertical industries to deploy their services efficiently.

In a separate thread, some work appeared in [12] and [13] that advocate for Distributed Ledger Technologies (DLT) or Blockchain as a solution for the existing challenges to meet the complex requirements of network slicing for vertical applications. In this sense, DLT may become the basis of a decentralized and transparent platform for multi-party negotiation between stakeholders of the next generation network ecosystem. Also, DLT may provide a solution to ensure the main security principles, including confidentiality, authentication, authorization, availability, and integrity. Moreover, DLT-based new business models for network slicing services can improve profit for providers and better experience and cost-effective solutions for the consumers.

Blockchain is fundamentally an immutable, transparent and decentralized ledger. The concept relies on the architecture of Peer-to-Peer (P2P) networks [14] that efficiently manages all network members and does not need to be controlled by any single centralized authority for transaction information. In particular, Blockchain has many favourable traits, namely decentralization, immutability, transparency and sustainable storage of databases. Due to these properties, Blockchain has the potential to be integrated with network slicing. It is predicted that Blockchain will be a crucial technology for novel applications from resource sharing, ubiquitous computing, and reliable content-based storage [15].

This is even more important in a next generation network context, where the number of stakeholders involved to offer an E2E network slice is expected to grow. It includes Virtual Network Function (VNF) providers, multiple administrative domains under the control of different operators and resource providers as they do not have essential trust established. This lack of trust has traditionally been solved through offline processes for contract negotiations or even through the creation of neutral, yet centralized, trusted entities. However, Blockchain may bring the advertisement of services and automation of administrative negotiations in the form of an open marketplace. It offers the technical substrate to automate all the varied administrative interactions among such diverse stakeholders in a decentralized way and through records that are immutable and auditable. If we add to this the capability of dynamically monitoring such administrative processes through smart contracts, it is expected that all this potential is somehow realized in the short-term. In this sense, it may eventually become a fundamental piece of the telco ecosystem.

Currently, applications of Blockchain are under study, together with its possible integration with Artificial Intelligence (AI) [16], [17], Edge Computing [18], [19], Machine Learning [20], 5G [21], Internet of Things (IoTs) [22], and smart cities [23].

Research works on the application of Blockchain as a DLT to Beyond 5G (B5G) or Sixth-Generation (6G) networks are also available [24]–[26].

The preexisting surveys explored various aspects of Blockchain with 5G. Some of these are discussed as follows: In [25] authors discuss the Blockchain for 5G and beyond networks where they aim to provide a study on the integration of Blockchain and 5G technologies for delivering services. The authors discuss opportunities that Blockchain brings to 5G services. Similarly, the authors in [27] take a look at decentralizing applications with Blockchain and examine the state-of-art 5G and beyond DApps. This study also looks at other aspects, such as security, privacy and tokenization. Also, the study presented in [28] gives an overview of the integration of Blockchain with 5G-enabled IoT focused on industrial automation. The authors discuss various applications for integrating Blockchain with 5G-enabled IoT. This study also illustrates open issues and challenges for Blockchain and industrial automation integration. Finally, the authors in [29] present a review on the application of Blockchain in 5G and beyond networks. This paper discusses the benefits of applying Blockchain into the 5G ecosystem using the E2E approach to enable service delivery models.

The discussion above demonstrates that the recent research has provided a perspective on integrating Blockchain with 5G and beyond networks. However, the existing literature has limitations. Although they present the review on Blockchain for 5G and beyond 5G networks, the in-depth and thorough discussion on network slicing is missing from the literature. In addition, the focus of these current surveys lacks an extensive discussion on the motivation, state-of-the-art and frameworks of Blockchain-based network slicing in the existing literature. Furthermore, network slicing focused future research directions are not discussed in-depth in the current literature. Therefore, based on the observation, we can conclude that this article can fill the gap and provide a review on DLT and Blockchain for network slicing dedicating on current efforts, limitations and future research direction which can add value in the academia. Also, we believe that this article can be an excellent opportunity to further increase reader's knowledge and take a closer look at the integration

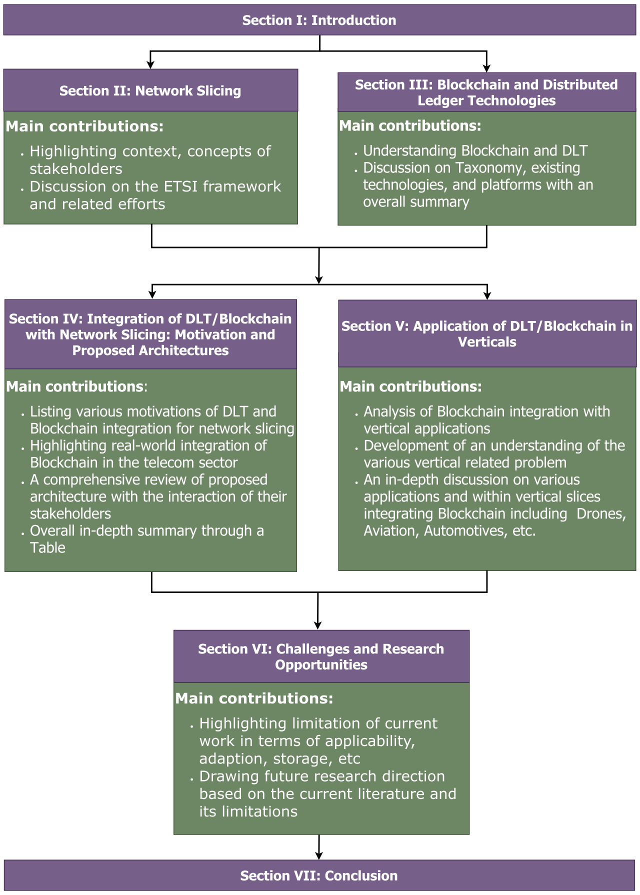
Section I: Introduction
Section II: Network Slicing
Main contributions:
. Highlighting context, concepts of stakeholders
. Discussion on the ETSI framework and related efforts
Section III: Blockchain and Distributed Ledger Technologies
Main contributions:
. Understanding Blockchain and DLT
. Discussion on Taxonomy, existing technologies, and platforms with an overall summary
Section IV: Integration of DLT/Blockchain with Network Slicing: Motivation and Proposed Architectures
Main contributions:
. Listing various motivations of DLT and Blockchain integration for network slicing
. Highlighting real-world integration of Blockchain in the telecom sector
. A comprehensive review of proposed architecture with the interaction of their stakeholders
. Overall in-depth summary through a Table
Section V: Application of DLT/Blockchain in Verticals
Main contributions:
. Analysis of Blockchain integration with vertical applications
. Development of an understanding of the various vertical related problem
. An in-depth discussion on various applications and within vertical slices integrating Blockchain including Drones, Aviation, Automotives, etc.
Section VI: Challenges and Research Opportunities
Main contributions:
. Highlighting limitation of current work in terms of applicability, adaption, storage, etc
. Drawing future research direction based on the current literature and its limitations
Section VII: Conclusion

FIGURE 1. The structure of this review.

of DLT with network slicing by reviewing current efforts, limitations, and further research directions.

Motivated by the limitations discussed above, the aim of this paper is to narrow down the discussion to the area of network slicing and to present a review of the integration of Blockchain as a DLT technology with it.

In summary, the main contributions of this review article follow:

- To provide an overview of network slicing, concepts and current challenges;
- To overview enabling technologies of DLT (i.e. smart contracts, platforms and its consensus algorithm) and their characteristics;
- To discuss and structure the state-of-art on the integration of DLT with network slicing;
- To provide an in-depth discussion on application of DLT to verticals served by network slicing;
- To highlight the remaining challenges and future directions.

The structure of this review is shown in Fig 1, which also highlights the major contribution of this work. This paper is organized as follow: Section II presents an overview of network slicing. We discuss the basic terminologies, key enabling technologies, principles and global efforts towards its realization, hence providing an overview of the network slicing basics. In Section III, we present a detailed overview of Blockchain as a DLT technology, its basic concepts, how it works, consensus algorithms and the key features such as smart contracts enabled on different platforms. In Section IV we illustrate and analyze the the meaningful works we found in the literature, their aim and functionalities as they integrate DLT features in their network slicing frameworks. The application of DLT for various important verticals industries is presented in Section V. Finally, we summarize the limitations, challenges and future directions in Section VI. Moreover, the list of acronyms used in this review are presented in Table 1.

II. NETWORK SLICING

This section gives a brief overview of the main concepts underlying network slicing as well as those characteristics that make Blockchain fit in this context.

A. CONCEPT

There are various organizations working on (hence defining and refining) the term network slice (e.g., Next Generation Mobile Networks (NGMN), Third-Generation Partnership Project (3GPP), Internet Engineering Task Force (IETF)). In brief, it could be defined as follows [30]: "A network slice is a complete logical network with specific services offered to customers over a shared compute, storage and network infrastructure, e.g. a network operator can build a network slice including an Access Network (AN) and a Core Network (CN) to enable communication services."

There are two implicit characteristics in this definition that are fundamental in network slicing that should be made explicit:

- *End-to-End*: Network slices offer E2E performance guarantees, which implies that if the provider to which the network slice is requested does not have full control of the whole E2E slice and associated resources, it has to reach agreements with other providers and then stitch all the segments into a single E2E network slice. Therefore, there must be mechanisms in place to settle these agreements at the technical and at the administrative levels. While focusing on the 5G networks architectures, an E2E network slice is considered a composition of virtual functions. These virtual functions comprise the access and core networks, which enable mobile connectivity, with added virtual applications instantiated at the cloud domains or edge, while interconnection is provided at the transport level.
- *Network slice resources*: The network slice is a complete (logical) network consisting of underlying resources over which the slice is deployed. Therefore, any slicing framework must embed schemes to isolate them from those of other slices. As mentioned above, managing the virtualized networking elements related to access, core and transport domains must be driven and complemented by the orchestration of the virtual application functions. Also, QoS requirements, security,

TABLE 1. Abbreviations.

Acronym	Terms
3G	Third Generation
3GPP	Third-Generation Partnership Project
4G	Fourth Generation
5G	Fifth Generation
6G	Sixth Generation
5GT	5G Transformers
5Gr-RL	5Growth Resource Layer
5Gr-SO	5Growth Service Orchestrator
5Gr-VS	5Growth Vertical Slicer
AD	Administrative Domain
API	Application Programming Interface
AI	Artificial Intelligence
AR	Augmented Reality
B5G	Beyond 5G
B2B	Business-to-Business
B2C	Business-to-Customer
B2B2C	Business-to-Business-to-Customer
BFT	Byzantine Fault Tolerance
CA	Certificate Authority
CCN	Content-Centric Networking
DAPPs	Distributed Applications
DLT	Distributed Ledger Technology
E2E	End-to-End
eMBB	Enhanced Mobile Broadband
ETH	Ether
ETSI	European Telecommunications Standards Institute
EVM	Ethereum Virtual Machine
IaaS	Infrastructure-as-a-Service
Industry 4.0	The Fourth Industrial Revolution
InP	Infrastructure Provider
IoTs	Internet of Things
ISG	Industry Specification Group
MANO	Management and Orchestration
ML	Machine Learning
mMTC	Massive Machine Type Communication
MNO	Mobile Network Operator
MNVO	Mobile Network Virtual Operators
MTP	Mobile Transport Platform
NG-SON	Next Generation Self-Organizing Networks
NGMN	Next Generation Mobile Networks
NFV	Network Function Virtualization
NFs	Network Functions
NaaS	Network-as-a-Service
NFVIaaS	NFV Infrastructure as a Service.
NFVI	NFV Infrastructure
NFVO	NFV Orchestrator
OS	Operating System
P2P	Peer-to-Peer
PBFT	Practical Byzantine Fault Tolerance
PoS	Proof-of-Stake
PoW	Proof-of-Word
QoS	Quality of Service
RAN	Radio Access Network
RPCs	Remote Procedure Calls
SLAs	Service Level Agreements
SO	Service Orchestrator
SDN	Software-Defined Networking
UAVs	Unmanned Aerial Vehicles
URLLC	Ultra-Reliable Low-Latency Communications
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
V2X	Vehicle to Everything
VMs	Virtual Machines
VNF	Virtual Network Function
VNFaaS	Virtual Network Function as-a-Service
VNFM	Virtualized Network Function Manager
vCDN	Virtualized Content Delivery Network
VIM	Virtualized Infrastructure Manager
VR	Virtual Reality
WAN	Wide Area Network

dynamicity, resource consumption and isolation should be considered.

Other related characteristics to the above ones that are associated with network slicing are [1], [2]:

- *E2E programmability*: Softwarization brings programmability, which simplifies the management of services and networks, as well as their integration and operational challenges - especially for supporting communication services. Furthermore, it permits third parties to have control over the allocated slice resources, via open Application Programming Interfaces (APIs) that present network capabilities facilitating on-demand service-oriented customization [3].
- *E2E automated network operation:* It is a need to enable an on-demand and dynamic configuration of network slices (e.g., creation, removal and deployment) without the need for fixed contractual agreements and manual intervention to handle Service Level Agreements (SLAs) [2].
- *Resource isolation*: It is crucial for network slicing that it assures performance guarantees even when other slices compete from the resources of the same shared network [31].
- *Resource slice customization*: Resources must be adapted to the needs of a variety of services with diverse requirements [32].
- *Network resources elasticity*: Resources consumed by a slice must dynamically adapt to varying network conditions and service needs. For instance, slice elasticity can be offered by scaling up/down/in/out the allocated resources, or by relocating VNFs, or by adjusting the applied policy and re-programming the functionality of specific data and control plane elements [33]. Therefore, flexibility ensures that the requested SLA.

B. CONTEXT

It has been widely discussed that 5G will support a variety of services from a plethora of vertical industries over the same shared infrastructure. At a more technical level, this will translate into the deployment of three types of logical networks (or slices) to serve their needs, namely massive Machine Type Communications (mMTC), enhanced Mobile Broadband (eMBB), and Ultra Reliable Low Latency Communications (URLLC). According to [34] in a 5G network, the network operators have several motivations to introduce E2E network slicing. These motivations include customized network services to satisfy each consumer's SLA, flexibility, and cost-efficiency. And this same trend is only expected to increase in 6G networks.

These services are supported with the help of "network slicing" and the capabilities offered by the underlying shared infrastructure. For instance, network slicing can be an answer for telecom operator's on how to construct and manage a targeted network that can meet the emerging necessities of a wide range of enterprises [35]. Moreover, for vertical industries, network slicing is a powerful enabler for telecom operators to expand their service offerings towards industry consumers, produce new services, and enhance network value. To achieve a sliced network, it is remodeled into a set of logical networks on top of a shared infrastructure. Moreover, each logical network is designed to serve a defined business purpose and comprises all the necessary network resources, configured, and combined E2E [2].

In this section, we will discuss the basic concepts including architecture, NFV, orchestration and management in network slicing, and future trends and present limitations. But before that, let us set the context by introducing the stakeholders involved in network slice deployment.

C. STAKEHOLDERS

In addition to the diversity of technologies and use cases to be served on top of a shared infrastructure, 5G and B5G networks are also complex because of the variety of stakeholders. In fact, softwarization and programmability bring open architectures with clearly defined interfaces. In turn, open interfaces define the borders among potentially different stakeholders, hence defining new business relationships.

The 3GPP defined some of the business roles required when dealing with network slices [36], including communication service customer, communications service provider, network operator, network equipment vendor (incl. virtual network function provider), virtualization infrastructure service provider, network function virtualization infrastructure supplier, data center service provider, and hardware provider. These basic roles have been further elaborated and an operational architecture has been designed, implemented, deployed, and evaluated in the project 5G-Transformer [30], [37]) and its follow-up 5Growth [38]. The various service offerings by each stakeholder have been defined as well.

At a high level, and according to the NGMN description of the slicing concept [39], the stakeholders were distributed in three layers. First, the service instance layer consumes the services offered by the underlying providers, which exposes a vertical-oriented API so that the customer can focus on its business logic and request the required services by using parameters understandable by the vertical. Second, the network slice instance layer is in charge of providing the requested E2E services to the vertical. This entails the translation from vertical-oriented service descriptions to network slices, which are eventually instantiated in the network in the form of NFV network services. Finally, at the resource layer, we find all those providers whose service offerings are related with resource provisioning in its various flavors (e.g., cloud computing, edge computing, transport, resource aggregators).

Though the ecosystem is continuously evolving, in general, it has been the norm that the various roles inside each of the layers have been played by the same organization, hence not introducing administrative boundaries between the entities playing each of the roles. It is also common that the network slice instance layer and the resource layers are under the same administrative domain.

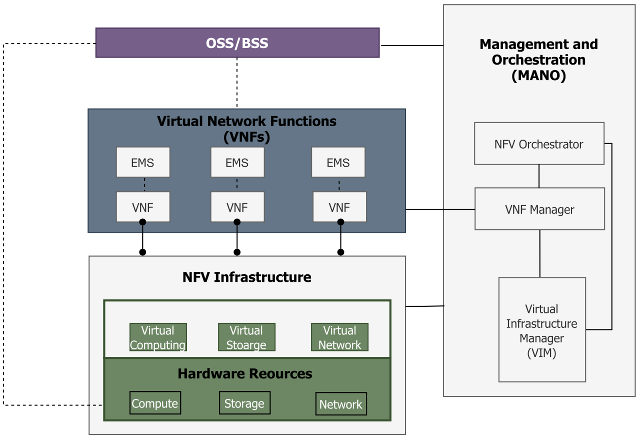

FIGURE 2. ETSI NFV reference architectural framework.

D. THE ETSI ARCHITECTURAL FRAMEWORK AND ITS MAJOR COMPONENTS: AN OVERVIEW

The technical framework enabling network slice offerings is that of European Telecommunications Standards Institute (ETSI)-NFV [40] and associated technologies (e.g., SDN). Figure 2 illustrates the ETSI NFV architectural framework.

NFV allows virtualizing network nodes and services (e.g., routers, firewalls, and load balancers) that have traditionally been run on proprietary hardware. Thus, the software and hardware, which have traditionally been tightly integrated in telecom scenarios, are now split [41]. These services are implemented with the help of virtual machines (VMs) or containers on commodity hardware, which permits service providers to run their network on conventional servers rather than proprietary ones, hence bringing to the telecom's world the economies of scale of cloud computing. This is even more important in a context with increasingly demanding and diverse services.

The ETSI NFV specifications define an operational framework for orchestrating and automating [42] VNF software appliances on virtualized infrastructure on commercial off-the-shelf (COTS) hardware and managing them through their life-cycle [43].

The functional blocks defined in the NFV architectural framework are:

- Virtualized Network Function (VNF)
- Element Management System (EMS)
- NFV Infrastructure (NFVI)
- NFV Management and Orchestration (MANO), including
  - NFV Orchestrator
  - VNF Manager (VNFM)
  - Virtualized Infrastructure Manager (VIM)
- Operations and Business Support Systems (OSS/BSS)

These major functional blocks of the framework are illustrated and explained in detail in the ETSI framework [44].

Thus, the NFV architectural framework specifies the interaction across different functional blocks by a set of well-defined reference points. The major components of an NFV architecture, i.e., the functional blocks, are discussed below. We start by explaining VNFs and EM. Then, we explain the role of NFVI and NFV MANO. And, lastly, we discuss OSS/BSS. We also illustrate these functional blocks in Figure 2.

1) VIRTUALIZED NETWORK FUNCTION (VNF) AND ELEMENT MANAGEMENT SYSTEM (EMS)

The functionality assigned to a given VNF can be deployed in one or more VMs (or containers) on top of general purpose hardware infrastructure. VNFs can embed routers, switches, firewalls, or a number of other network services available from various vendors that are run as software processes.

Therefore, VNFs replace dedicated hardware devices by virtualizing essential network functions previously in the domain of dedicated hardware appliances. As a result, operators can deploy novel services, improve security and tailor network performance at scale. Moreover, [44] provides several use-cases of targeted network functions (NFs) for virtualization.

The EMS, in the NFV context, is responsible for the functional management of the VNF, i.e., Fault, Configuration, Accounting, Performance and Security Management (FCAPS). An EMS may manage the VNFs through proprietary interfaces. Also, there may be one EMS per VNF, or an EMS can manage multiple VNFs [45].

2) NFV INFRASTRUCTURE (NFVI)

The NVFI is built on general purpose networking, computing, and storage hardware. The NFVI also includes the "virtualization layer", which sits on top of the hardware and abstracts hardware resources to expose them as virtual resources and to allow them to be logically partitioned and provisioned to serve VNFs. In other words, the NFVI combines the necessary software and hardware components to supply the computation, storage, network, and software resources on which VNFs are deployed and managed.

3) NFV-MANO FUNCTIONAL BLOCKS

The NFV management and network orchestration (NFV-MANO) [42], [46] enables the coordinated management and orchestration of services and resources over a virtualized shared infrastructure, including computation, networking, storage, transport network, and Radio Access Network (RAN). The NFV-MANO defined by ETSI, envisions direct mapping of network slices to NFV network services. According to [47], the NFV network service is a resource-centric view of a network slice.

The NFV MANO framework traditionally features three functional blocks: the Virtualized Infrastructure Manager (VIM), Virtualized Network Function Manager (VNFM), and NFV Orchestrator (NFVO). Below we summarize their scope:

- *NFV Orchestrator*: It offers two main functionalities: network service orchestration and resource orchestration. As for the former, it is in charge of the lifecycle management of the deployed services. For instance, this includes making the services available to customers, managing their instantiation/deployment, automatically reacting to service-related events (e.g., scaling if more resources are needed), or network service termination. Resource orchestration is in charge of the interaction with the underlying infrastructure (e.g., through its VIM. This includes the reservation/allocation of resources according to the service needs, the monitoring of their operation and the placement of VNFs in the right resources to fulfill service requirements.
- *VNF manager (VNFM)*: It is in charge of individual VNF lifecycle management. For this purpose, each VNF is associated with its VNFM. This includes instantiation (including not just deployment but configuration of the VNF itself), VNF instance software upgrade, VNF instance scale in/out/up/down, VNF instance termination.
- *Virtualized infrastructure manager (VIM) and WAN Infrastructure Manager (WIM)*: The VIM and the WIM control and manage NFV Infrastructure NFVI) physical and virtual resources in a single domain. These are the building blocks that interacts with the actual infrastructure for deploying the virtual machines or containers (VIM) and for setting up the paths in the transport network (WIM). Therefore, they interface with a variety of hypervisors and network controllers. In an NFV architecture, there may be more than one VIM/WIM, with each of them managing or controlling NFVI resources from a given infrastructure provider. Generally, a VIM/WIM may be concentrated in supervising a particular type of NFVI resource (e.g., computer-only or storage-only) or could operate various kinds of NFVI resources.

To these building blocks, a *network slice manager* is often added on top to manage network slices that are requested in the form of NFV network services to the NFVO, as for instance in [38]. This building block is in charge of the lifecycle management of the slices. In this sense, they are closer to the service actually requested by the vertical, and so, of its business priorities. This may include slice instantiation according to the types defined by the 3GPP, translation of vertical service requests into slice requests, and finally, into NFV network service requests sent to the NFVO, or arbitration among slices according to priorities.

4) OPERATION SUPPORT SYSTEM/BUSINESS SUPPORT SYSTEM (OSS/BSS))

The OSS of an operator tackles network management, as well as fault, service and configuration management. In contrast, BSS is in charge of customer, product and order management. In other words, in the ETSI NFV architectural framework, the OSS supports network operations and services while the

BSS supports business operations. In the NFV architecture, an operator's current OSS/BSS can be connected with the NFV MANO to perform various actions, such as requesting network or VNF lifecycle management or forwarding NFV related information. Further, [40] describes how this reference point can be used.

E. RELATED EFFORTS

Several initiatives from industry and academia have been defining network architectures that feature network slicing. Below we highlight some of these efforts;

1) STANDARDIZATION AND INDUSTRY GROUPS

Multiple organizations have adopted the network slicing concept and defined the architectures and frameworks to realize it.

- The *NGMN Alliance* elaborated some high level documents describing the network slicing concept and its potential for mobile network operators [39].
- *The 3GPP* is the one the significant standards organization involved in architecture definition for 5G. Numerous iterations of standards releases have placed a foundation for the current phase of slice-specific activity. The pathway to network slicing functionality has been paved by DÉCOR (eDÉCOR) in Release 14 standards and fully accomplished with the work on network slicing within the Release 15 system architecture for the 5G System (3GPP TS 23.501) [48]. In this architecture, various types of slices to serve widely different traffic types have been specified (mMTC, URLLC, and eMBB).
- The *ETSI NFV* [41] industry specification group is defining an open architecture that serves as framework for dealing with virtual networks in general, and so, network slices. This architecture separates the software from the hardware functionality and defines the building blocks to enable flexible deployment and management of virtual functions and virtual links over heterogeneous infrastructures. In this way, the flexibility required by operators to adapt to increasing and changing demands can be offered.

2) RESEARCH PROJECTS

There are multiple projects dealing with the concept of network slicing in general and also focusing on specific aspects in each of them. For instance, most projects in the Horizon 2020, the 5G Infrastructure Public Private Partnership (5GPPP) program deal in one way or another with network slicing [49]. In the following we focus on those that explore some of the concepts that set the framework for what is discussed in this survey paper:

- The *5G Novel Radio Multiservice Adaptive Network Architecture (5GNorma) project* [50] defines a new programmable and flexible mobile architecture. The intention is to enable multi-tenancy over a shared physical infrastructure. To this end, 5GNorma includes three enabling operational blocks, namely Software Defined for Mobile networks (SDM)-Orchestrator(O), SDM-Control(C), and SDM-X (Coordinator).
- The *5G Exchange (5GEx)* [51] has introduced an architecture further extending the concept of ETSI NFV architecture for multiple domains. The proposed architecture is composed of three layers: resource domain, single domain resource, and multi-domain resources. The resource domain illustrates the lower layer of the architecture. It presents domain resources to the single domain orchestration layer via specific interfaces. According to 5GEx, a domain may lead to a technological domain or operator domain. The middle layer, the single-domain orchestration layer, constitutes the domain-specific orchestrator, which performs resource and service orchestration of a specific domain managing the interfaces exposed by the domain resource layer. The domain-specific orchestrator is utilizing interfaces for communication and coordination. Additionally, the top layer of the architecture is the multi-domain orchestration, which involves the multi-domain orchestrator. Each multi-domain orchestrator is connected with one or multiple single-domain orchestrators, and managed by the orchestrator administrative domain via business-to-business (B2B) interface.
- *5G Transformer (5GT)* [37] aims to integrate network slicing concept into mobile transport networks by managing slices tailored to the needs of different vertical industries. The presented technical approach is: (i) enabling vertical industries to reach their service requirements within customized slices and (ii) federating transport networking from the edge up to the core, and cloud, specifically to create and manage slices throughout a federated virtualized infrastructure. It has been built on three main modules, namely; vertical slicer (VS), service orchestrator (SO), and mobile transport platform (MTP). The VS is a logical entry point for verticals to support easy creation and management of the slices. The SO deals with end-to-end service orchestration, the federation of transport networking and computing resources from multiple domains, and their allocation to slices [52]. Furthermore, the MTP is the underlying unified transport layer for integrated front-haul and back-haul networks [53].
- *The 5Growth* [38], [54] architecture is an evolution of the 5GT architecture. The purpose is to enhance performance, adaptability, automation, and security. It facilitates automated deployment and uniform operation of slices, customized to support the requirements of the various vertical industries, spanning from Industry 4.0 to the transportation industry and energy sectors, to name a few. In this direction, the basic core building blocks are those of 5GT, though they are extended to enable additional functionality. For instance, multiple options for multi-administrative domain interactions are possible,

including the request of segment of vertical services, of subslices, of segments of NFV network services, or of resources. The monitoring platform is improved to be able to better monitor those metrics that are needed to better deal with the adaptability requirements of slices and services. And talking about adaptability, an Artificial Intelligence/Machine Learning Platform (AIMLP) is integrated in the framework allowing to dynamically load models that automate management decisions to trigger some of the lifecycle management operations when the service/slice requires it.

This section has mostly described the technical characteristics and mechanisms for offering network slices. However, when discussing the inter-stakeholder interactions it was also clear that to realize the E2E network slicing concept to its full extent there are administrative aspects that must be integrated in such technical framework, and this is where Blockchain or Blockchain as a DLT comes into play.

There are two kinds of interactions in a network slicing context that are already assumed to negotiate administrative constraints. First, in addition to their variety, vertical industries are, in general, organizations with very different scopes from those of communication service providers. Therefore, different organization will have to negotiate the vertical service business conditions. And second, the E2E nature of slices in a general case will require the interaction between different communication service providers (sometimes referred to as service/resource federation [52]) in order to deploy the slice in all spots where a given vertical industry wants to deploy its service. For instance, service provider A, with service offering restricted to a given geographic region, may have to interact with service provider B to deploy a segment of the E2E slice that the vertical requested to be deployed in another region. Therefore, an administrative/business relationship must be negotiated.

The dynamicity brought by NFV provides the basic building blocks to adapt to demands and to locate slice resources in the appropriate network spots to fulfill slice requirements. However, this framework must be augmented with components that allow automating the above administrative relationships in the same way technical relationships between different architectural entities are. It is only in this way that generic E2E slices can be offered. It is precisely in this context that Blockchain is expected to play a key role.

III. BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGIES

This section provides a background on the DLT and Blockchain. This will allow better understanding in the following sections how these technologies are able to extend the support and the facilitation of B5G networks and services. Moreover, we also provide a summarized conclusion of all the key aspects which we will be discussed in this section.

a: WHAT IS A DLT?

A distributed ledger is a type of distributed database that by default assumes presence of malicious nodes. The DLT enables the realization of distributed ledgers through a shared consensus mechanism to establish immutable records of transactions despite failures [55].

b: WHAT IS BLOCKCHAIN?

Blockchain is a DLT realization that enables creation of cryptographically linked and chronologically ordered blocks, containing a certain number of transactions. Bitcoin is the first Blockchain, designed as a public, immutable, append-only, distributed ledger.

Blockchain is regarded as a disruptive powerful technology that has potential to radically reshape the society and the world economy through decentralized governing structures [56], [57]. The Blockchain idea is captivating because for the first time in human history people from distant locations can securely transact within a massive peer-to-peer network with decentralized/distributed management (i.e., no central authority).

According to [58]–[60], Blockchain is going to be the driving force for the next generation of Internet (i.e. 5G and 6G) and network slicing is fundamental part of it. To fully elaborate the Blockchain as a DLT integration with network slicing in later sections, this section first presents the Blockchain's history, fundamentals, taxonomy, consensus mechanisms. Later, we unfold the application smart contracts and the Distributed Applications (DApp) paradigm. Finally, we go through the leading openly available platforms.

A. HISTORY OF BLOCKCHAIN: AN OVERVIEW

In 2009, after the Financial Crisis of 2008 [61], Satoshi Nakamoto published the Bitcoin paper [62]. Despite the initial idea of creating an open source peer-to-peer electronic cash system that would avoid double-spending attacks, the outcome produced a disruptive technology [63]. Satoshi Nakamoto combined encryption and distributed computing in a unique way to assist a network of computers in collaborating towards maintaining a shared and secured database. Nakamoto generated the genesis block and mined the initial bitcoins, giving birth to the cryptocurrency era. Satoshi Nakamoto is a pseudonym for the person or group of people that design and built the Bitcoin. The identity of Satoshi is a mystery to date [64]–[66].

Bitcoin's popularity began to increase in 2011. Soon, technologists realized that Blockchains could be used to track other things besides money. In 2013, 19-year-old *Vitalik Buterin* proposed Ethereum. The idea of smart contracts was initially introduced by Nick Szabo [67]. This marks a new milestone in the evolution of Blockchain technology, often referred to as Blockchain 2.0 [68].

B. FUNDAMENTALS OF BLOCKCHAIN AND ITS WORKING PRINCIPLE

The key strengths of Blockchain are founded on its verifiability and tamper-proofness. To understand how Blockchain achieves its key characteristics, in this section we describe its building blocks and how the Blockchain works.

1) BLOCKCHAIN BUILDING BLOCKS

The main components to implement a Blockchain are:

- *Peer-to-peer network*: A Blockchain is constituted by *Blockchain nodes* that are inter-connected in a peer-to-peer network. When a new Blockchain node is setup and initiated, first connects to the peer-to-peer network, and once it has established a connection to at least one node, it starts the syncing process. This consists of downloading all the blocks of the Blockchain, till the latest block. Once a node is in full-sync, it can actively participate in the Blockchain.

  The Peer-to-Peer network is critical for Blockchain technology, as a base layer (similar to IP layer for Internet). In a *centralized* system, there is a high risk of single-point failures (SPOF) or denial of service cyber-attacks [69]. In a Blockchain instead there is no central authority to set the rules making it a *decentralized* network. Information is continuously recorded in append-only fashion, and an identical copy is transferred and stored between the nodes.
- *Blockchain address*: Each user of the Blockchain needs a unique Blockchain address. A Blockchain address is a password protected and has asymmetric keys (private and public key-pair). Users issue and authorize transactions by signing them with the private key. The public key is used for receiving transactions. More precisely, the Blockchain address represents a hash (SHA-256) of the public key. In Bitcoin, a pay-to-public-key-hash (P2PKH) script is used, where the Bitcoin address is a unique 27-34 alphanumeric characters long hash identifier [70].
- *Transaction*: Every transaction is a new and unique record exchanging value or data between two Blockchain addresses or entities. It has an origin and recipient Blockchain address. The issued transaction is added to a pool of unconfirmed transactions - a collection of signed transactions ready to be added in a block [71].
- *Block*: A block is a structured collection of multiple transactions. Each block contains a block header and a list of transactions. The block header contains: (*i*) a hash of the previous block, (*ii*) a hash of all listed transactions in the block, (*iii*) a nonce, (*iv*) a timestamp, (*v*) the difficulty, as explained in detail below. The list of transactions in a new block is populated from the pool of unconfirmed transactions. The miner is in charge of the process of block creation, and blocks are appended to the Blockchain after consensus is achieved, as it will be better described later. It is important to note that participants can explore the Blockchain data/transactions back in time to the genesis block (Block 0) thanks to the hash of the previous block. In this way each block points back to the preceding block creating a chain of blocks.
- *Consensus mechanism*: To append a new generated block to a Blockchain a miner needs to follow a consensus mechanism. This is a key procedure that enables immutability, security, and integrity to a Blockchain. A consensus mechanism includes a diversity of advanced cryptographic techniques and mathematical models that define a strict procedure for (*i*) generating the necessary block headers, and (*ii*) validating the new block. The consensus mechanism is run by all (peer-to-peer) nodes participating in a Blockchain network [72]. Satoshi Nakamoto proposed a Proof-of-Work (PoW) consensus mechanism to regulate nodes/participants in Bitcoin [62]. The consensus algorithms dictate the overall performance of a Blockchain (We discuss them in more details in Section III-D1.).
- *Hashing and hash functions*: A hash function takes any (data) input and produces a finite output of a specific size. The process of applying a hash function to data is called *hashing*, and the output of a hash function is called a *hash*. The essential feature of a particular hash function is the size of the output it produces. Essential for preserving structured, manageable and secure Blockchain data is through a hash algorithm with a data structure known as a *Merkle Tree*. This is a method to structure data that enables a large body of information to be verified accurately and efficiently [73].
- *Timestamp*: Each block in Blockchain is timestamped. Timestamps prove chronological order of blocks and transactions, representing the time of each recorded transaction. These tamper-proof timestamps serve as a notary service that prevent occurrence of double-spending transactions [74].
- *Nonce*: It is the number that a miner node has to *guess* in order to successfully *mine* a block. It is mainly used in a PoW-based Blockchains, such as Bitcoin. A nonce is an arbitrary whole number, which is 4 bytes field. The combined hash of the desired Nonce and the block header of a new block should produce a result with leading "zeros", depending on the difficulty. For example, if the difficulty is 1, the combined hash *(block header* + *nonce) should produce a result of single zero leading hash* $(0 \times 0\ldots)$*. In case that the difficulty was 2, the combined hash should be double zero leading hash* $(0 \times 00\ldots)$*, and so on. Thus this result is easy verifiable by the rest of miners, running the consensus algorithm. The found hash is* added to the hashed block [74].
- *Smart contracts*: At the most basic level, smart contracts are programs that run independently on top of a Blockchain. They have been introduced by Nick Szabo [67] and contain immutable deterministic code, the creator's Blockchain address and cannot be modified by anybody, not even by their creator. The benefits of smart contracts are most apparent in business collaborations, in which they are typically used to enforce some agreement so that all participants can be sure of the outcome without any intermediary's involvement [75].

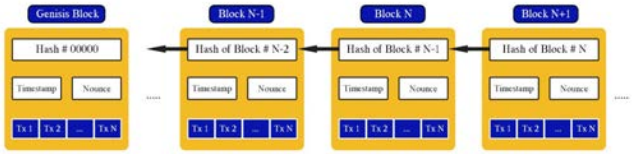

FIGURE 3. Blocks are chained together using the previous block's hash to form a Blockchain.

This concept is essential for designing frameworks or distributed applications, thus we discuss it in detail in Section III-D2.

2) HOW BLOCKCHAIN WORKS

Since we introduced the basic building blocks, in the rest of the section we focus on how a Blockchain generates a new block, and how the new block is appended or *mined*.

a: HOW BLOCKS ARE CREATED

Figure 3 shows how Blocks are chained together and the information they contain. The figure represents a chain of three blocks. The first block is different as it can not contain the previous block's hash, and is called the *Genesis block*. Every Blockchain is instantiated or starts with a genesis block. A genesis block is created or mined by a single node, usually the node of the Blockchain's creator.

Once a genesis block is created, all nodes of the Blockchain start to *compete* for a block creation. The rules of the competition are defined by the consensus mechanism. A Bitcoin block creation, can be summarized as follows:

- A node collects limited number of transactions from the pool of (pending) transactions
- A node populates all the necessary block headers, especially the hash pointer to a previous block and the hash of all included transactions (or the Merkle root).
- A node competes to win the consensus. If it wins, the generated block is appended to the Blockchain. In case it does not win the consensus, the transactions are released (or unlocked) back into the pending transactions pool.

Tampering the information in the second or any of the following blocks (in Figure 3), modifies the resulting hash. As a consequence, there would be no match in the following blocks, making all the subsequent blocks invalid. As a result, all nodes in the Blockchain can not validate the modified block and discard it. An attacker can only succeed if it controls at least 51% of nodes in the Blockchain network.

The data that is stored inside a block depends on the type of Blockchain. For instance, in Bitcoin, a transaction contains: *Sender A* sends bitcoins to *Receiver B*. Hence the transaction data consists of information regarding the sender, the receiver, and the amount of transferred bitcoins (tokens). Note that Bitcoin-capitalized refers to the first Blockchain technology created by Satoshi Nakamoto [62]. While bitcoin-lowercase refers to the token or (cryptocurrency) used to transfer different amounts between users.

The continuous creation of new blocks in Bitcoin using the PoW consensus mechanism is called *mining*.

b: HOW MINING WORKS

The active nodes in a Blockchain such as Bitcoin are referred as *miners*. They are accountants which record every transaction to the Blockchain. Mining involves creating a hash of a block of transactions that can not be easily forged, protecting the entire Blockchain's integrity without the need for a central system [76]. From a high-level (user) perspective, the concept is simple; a proof of payment is essential if a person wants the payment to be valid. The miners are the ones who keep the record of all the payments. Mining is typically done on a dedicated computer [77], as it requires a fast CPU and higher electricity usage, and more heat generated than typical computer operations [76].

To *mine* a block, the miner collects a batch of transactions, creates a block and generates all block headers, as mentioned previously. The last step for the miner is to guess or find the proper nonce. The *mining* process is a simple brute-force generation of random nonce. The right nonce hashed with the block header hash should produce a result with a specific number of leading zeros. The *mining difficulty* or the number of expected leading zeros is modified by the consensus algorithm. In this way the consensus algorithm can control the block creation time when new powerful computing devices are joining the Blockchain network as miners. For example, in Bitcoin the block creation time is around 10 minutes, and in Ethereum is around 13 seconds [78].

Once the miner brute-forced a proper nonce, records it in the block header and broadcasts the block on the Blockchain network. Note that multiple miners may generate a block at the same time, but only a single block is elected as the winning block that is appended to the Blockchain. The winning block is the block that is first validated by at least 51% of the miners/nodes in the Blockchain network [62].

The miner that *mined* the winning block is awarded with bitcoins to the miner's coinbase address. The amount of bitcoins or the *mining reward* depends on the block height. The mining reward is reduced by half every 210 000 blocks. For example, on 11th of May 2020 for the 629 999 block, the miner received 12.5 bitcoins, whereas for the next block (630 000), the miner received 6.25 bitcoins. The reduction of mining reward for Bitcoin is known as *bitcoin halving* [79]. According to calculations, it is expected miners to receive rewards up until year 2140 [79].

C. TAXONOMY OF BLOCKCHAIN

Different types of Blockchain are available. We focus on the three major types: (i) public, (ii) private, and (iii) consortium. We take a closer look at each of them, discussing their features and mapping them on Table 2.

1) PUBLIC/PERMISSIONLESS BLOCKCHAIN

Public Blockchains are highly decentralized, are accessible to everyone and rely on active network nodes.

The first Blockchain in the form of Bitcoin, created in 2009 by Satoshi Nakamoto [62], it is a public Permissionless Blockchain. Facilitating auditability is one of the benefits of using Blockchain technology and permissionless Blockchain allows public auditability. Nowadays, most public Blockchains run PoW consensus mechanism to maintain trust, immutability and security. We discuss consensus mechanisms in-depth in Section III-D. To encourage users in participating as active nodes (e.g., miners in Bitcoin or Ethereum), the network rewards block creators with a finite amount of tokens (e.g., bitcoins, ethers) for each block created.

An utterly public Blockchain with open-source community models is designed to leverage expertise from many diverse people worldwide and use a broad-ranging user base to have supreme decentralization. Public Blockchains are criticized for the vast amount of computational power required to support a distributed ledger at a massive scale. Other concerns are associated to the transaction approval frequency and to the confirmation delay [80]. The performance of other consensus than PoW, like Delegated Proof-of-Stake (DPoS) or Proof-of-Staked Authority (PoSA), running on public Blockchains is significantly higher. For example, they produce 1 block every second, compared to 1 block every 10 minutes [24] provided by PoW.

2) PRIVATE/PERMISSIONED BLOCKCHAIN

Private Blockchain or permissioned Blockchains are only accessible by a limited number of admitted participants as it follows a partial decentralization technique. A private Blockchain has a organization entity (e.g., the Blockchain creator or several members) which manages the Blockchain. Every new user requires an access invitation issued by the governmental entity. Frequently, enterprises or companies deploy private permissioned Blockchains. In this way they are able to define specific access and operating constraints to the user, making the auditability restricted. Enterprises or companies using private Blockchain can keep the autonomy limited. Additionally, the private Blockchains come with the possibility of immutability. Implicitly, these systems are not highly centralized, and often employ less computational demanding consensus mechanism (e.g., Proof-of-Stake), allowing for higher transaction throughput or more frequent block creation [81], [82], which leads to better performance compared to public Blockchain. [82].

3) FEDERATED/CONSORTIUM

A federated or consortium Blockchain is a permissioned and group-owned system where individual autonomy is removed, and instead, permissions are vested in a group of companies or individuals. In other words, the consortium Blockchain is a system that is "semi-private" and has a controlled user group (as in a company); however, it works beyond various organizations. Moreover, consortium Blockchain vs. private Blockchain is a sweet-spot between fully open, decentralized and fully centrally-controlled systems. There is more likely to be a trusted consensus, as multiple organizations have a stake in the outcome [83]. Consortium Blockchains have restricted audibility and only selected nodes have autonomy to validate new blocks, which makes them not completely immutable. Moreover, the transaction approval frequency is shorter than that of public Blockchain and offers a higher performance level [84].

TABLE 2. Taxonomy of blockchain.

Type Property	Public [80]	Consortium [84]	Private [83]
Decentralization	Yes	Partial	No
Auditability	Public	Public and restricted	Public and restricted
Autonomy	All nodes	Selected nodes	One organization
Immutability	Nearly impossible	Possibility	Possibility
Transaction approval frequency	Long	Short	Short
Performance	Low	High	High

In conclusion, federated/consortium Blockchain offers the same benefits provided by private Blockchain: productivity and privacy of transactions. However, it gives the combined advantage of separating the consolidation of power only to a single company. This realization of a Blockchain network is ideal for an organizational collaboration.

Table 2 summarizes the type of decentralization, suitability, autonomy, immutability, transaction approval frequency, and overall performance.

D. EXISTING TECHNOLOGIES TO ENABLE BLOCKCHAIN-BASED INTEGRATION

In this part of the section, we highlight the existing Blockchain-based solutions for integration, including supporting platforms, consensus algorithms, smart contracts, and other solutions currently available.

1) CONSENSUS MECHANISMS

We have established that a Blockchain is a decentralized peer-to-peer system of nodes with no central authority figure. The decision about what node to add next is achieved by reaching a consensus among all Blockchain nodes for the next block to be added. The procedure of reaching a consensus is referred to as "consensus mechanisms". It is a key element that provides immutability, trust, transparency and security of a Blockchain. We already discussed how consensus is reached through mining in Bitcoin (Section III-B2.b).

A consensus is a compelling way of getting an agreement in a group. Here, we strive to highlight some of the consensus mechanisms including which are being used by some of the frameworks including PoW, Practical Byzantine Fault Tolerance (PBFT) and RAFT. We also discuss other popular consensus mechanisms i.e., Proof-of-Stake (PoS) and Delegated

TABLE 3. Consensus algorithms.

Algorithm	Node Management	Transmission rate	Energy consumption	Scalability	Transaction Finality	Fault Tolerance	Throughput (Transactions/sec)
PoW [85]	Public	Low	High	Strong	Probabilistic-finality	50%	<100
PoS [86]	Partial	Medium	Medium	Strong	Probabilistic-finality	50%	<1000
DPoS [87]	Partial	High	Medium	Strong	Probabilistic-finality	50%	<1000
PBFT [88]	Private	High	Low	Weak	Absolute finality (Immediate)	33%	<2000
RAFT [89]	Private	Medium	Medium	Weak	N/A	N/A	<10k
PoA [90]	Public	Medium	High	Strong	Immediate finality	51%	<1000
PoB [91]	Public	Medium	Medium	Weak	N/A	51%	N/A
PoET [92]	Private	Medium	Low	Strong	N/A	N/A	N/A
PoA [93]	Private	High	Low	Strong	N/A	N/A	N/A
PoC [94]	Public	Low	Low	Strong	N/A	N/A	N/A

Proof-of-Stake (DPoS) as well. In the following, we discuss their potential and their drawbacks. Moreover, we draw a conclusion based on the power they consume, their fault tolerance, scalability, transmission rate, node management, transaction finality, and throughput.

In Table 3, we compare these algorithms based on *node management* (i.e. the need to know each node/miner in the network), *transmission rate*, *energy consumption*, *scalability*, *transaction finality* (i.e., a guarantee that past transactions can never change) and *fault tolerance*.

a: PROOF-OF-WORK (PoW)

A PoW is a consensus algorithm in which it is costly and time-consuming to produce a piece of data. The most famous cryptocurrency, Bitcoin is using the *Hashcash proof of work* system.

Although the original Hashcash idea was to battle against email spammers, Satoshi applied this idea to bitcoin transactions. To add a new block into the chain, miners have to complete a PoW to verify all the block transactions, as already described in Section III-B2.b.

A miner has to finish around 10^{21} computations to find the correct number, and it takes approximately 10 minutes to find the valid number. For a hash function, Bitcoin is using the *SHA-256* hash algorithm [90]. The *SHA-256* gives a distinctive result if anything changes in a block of text validated. If any transaction is modified, the result will not be the same, and everyone will be aware that the modified transaction is not valid.

However, PoW has its limitations. It has low transaction rate and (currently) consumes tremendous amounts of electricity and computer power. PoW is stated to have 50% fault tolerance with 100 transaction per second. Furthermore, now, roughly 50% of Bitcoin hash power is originating from a few mining pools. This means that only a few people have to meet at the same desk to agree on the 51% attack [85].

b: BYZANTINE FAULT TOLERANCE (BFT) AND PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT)

BFT is the property of a system that can resist the failures derived from the *Byzantine Generals' Problem* [95]. This means that a BFT system can continue operating nominal even if some of the participating nodes fail or act maliciously. Applied to Blockchain, this approach rules out validations from malicious nodes in the Blockchain network [16].

PBFT aims for high performance (e.g., high transactional throughput, low latency, etc.), and high execution time. The nodes in a PBFT permitted distributed system are sequentially ordered, with one node being the primary/leader, and others the secondary or the backup nodes. The purpose behind PBFT's technique is that all legitimate nodes assist in attaining a consensus concerning the nature of the system employing the majority rule. The rational of the operation is that the maximum number of malicious nodes must not be more than or equivalent to one-third of all the nodes in the system.

As the amount of nodes increases, the course shifts to a more secure state. For this, there are four phases; sending a request, broadcasting, performing the request, and finally, the request is sub-served successfully when the client receives *m+1* responses from separate nodes in the network with the corresponding result, where *m* is the highest number of faulty nodes allowed [88].

Table 3 shows that PBFT has private node management and has a high transmission rate with approximately <2000 transaction/sec. PBFT also consumes lower energy. However, its scalability is weaker. It suffers from <33% voting power attack, follows absolute finality and faults tolerance rate of 33%.

c: RAFT [89]

Raft aims to make a model that is easier to understand. In Raft's states model, each node can stay in any of the three states: leader, candidate, or follower. The distributed system will remain operational, even if one of the servers fails. The employed leader-election mechanism is the *remote procedure calls (RPC)* to request votes and sync-up the cluster (using Append Entries).

Consequently, the load of the calls does not fall upon the leader node in the cluster. It has a certain degree of fairness i.e, any node can be a leader. However, there is a high possibility that Raft is strictly a single Leader protocol, and in case of extreme traffic, the system can become overwhelmed. RAFT has private node management and has overall a medium transmission rate and energy consumption. However, it has weak scalability and fault tolerance of 50% with the throughput of <10k transactions/sec.

d: PROOF-OF-STAKE (PoS)

A PoS validator can generate (mint) or validate a new block with a probability equal to the Blockchain tokens/coins it holds. PoS minimizes PoW's rivalry by granting authority to upgrade the Blockchain to a randomly chosen stakeholder. PoS, like PoW, pays validators a clear monetary incentive, known as a *block reward*, for updating the Blockchain. However, unlike PoW, PoS does not require validators to pay a direct monetary cost (such as the one incurred by solving PoW's puzzle) to obtain the authority to update the Blockchain. In particular, PoS algorithm makes a pseudo-random-selection process to pick a node to be the validator of the subsequent block, based on a combination of various Blockchain specific variables or processes (e.g., token staking) [96].

Blockchain peers who desire to compete in the forging process are expected to secure a certain number of coins into the network as their stake. The size of the stake defines the possibilities for a node to be elected as the next validator to produce the next block - the more significant the stake, the higher the chances [86].

However, to prevent favoring the wealthiest nodes, multiple strategies are available, among them two most commonly used methods are ''Randomized Block Selection'', and ''Coin Age Selection''. In the Randomized Block Selection scheme, the validators are chosen by studying for nodes combined with the most profound hash-value and the most eminent stake. The *Coin Age Selection* method determines nodes based on how long their tokens have been staked [72]. Many people, however, are suspicious of PoS's long-term sustainability because they believe it would struggle to achieve consensus.

PoS has partial node management. However, it has a medium transmission rate. Table 3 compares PoS with PoW and other consensus algorithms and shows that PoS has lower energy consumption. Also, it offers strong scalability. However, it comes with <51% stake tolerated power. PoS follows probabilistic-finality, 50% fault tolerance and performs <1000 transaction/sec.

e: THE DELEGATED PROOF-OF-STAKE (DPoS)

DPoS) is a consensus algorithm developed in 2014. In DPoS, the consensus is achieved through an electoral process. In this process coin holders choose their delegates by votes, and these delegates are responsible for validating new blocks. Additionally, these delegates are also called *witnesses*. The witnesses or delegates are rewarded for adding blocks to the Blockchain. In DPoS, each participant has several votes depending on the number of parts it has. Or they can choose to delegate the value of their stake in favor of another participant in the network. Moreover, under reasonable conditions and depending on the implementation, delegates usually take a turn in block production every few seconds [72].

In comparison to PoW, DPoS offers better performance. As 3 illustrates that DPoS follows partial node management and has higher transmission rate. Moreover, by eliminating intense competition between miners, DPoS is energy efficient. This solution also promotes decentralization; however, the higher the delegated, the lower the network speed [87]. It also depicts strong stability features, although it comes with the possibility of <51% validator attack. DPoS follows Probabilistic-finality and fault tolerance of 50% and can perform <1000 transactions/sec.

f: PROOF OF ACTIVITY (PoA)

The idea of Proof of Activity (PoA) stems from the combination of PoW and PoS. PoA aims to use this hybrid approach to generate new blocks to take advantage of PoS and PoW and tries to provide a more efficient algorithm [97]. The mechanism of PoA goes through two phases before a completely new block is added to the Blockchain. The first phase uses the practice already known from PoW in which miners compete against each other to solve a complex task to generate a new block for the Blockchain. Once that block is generated, the system moves to the second phase, i.e., PoS., where participants are randomly selected from the network. Once all the selected validators sign or confirm the block, the process will complete, and a new block is added to the Blockchain [98].

PoA can offer a good security level and low overhead. It does not require much storage space, either. However, it suffers from a computationally-intensive process. Also, PoA based networks may lack decentralization. A PoA-based Blockchain can have only a limited number of validators, which may not be democratically selected [99]. Table 3 provides a comparison of PoA with others. PoA has private node management with a medium transmission rate. However, it suffers from high energy consumption but it has strong scalability. Also, PoA has immediate transaction finality with 51% fault tolerance.

g: PROOF OF BURN (PoB)

Participants burn their currencies to generate new blocks in the Proof of Burn (PoB) consensus technique. PoB validators burn coins by sending them to an irretrievable address [91]. Miners may burn the native currency or Bitcoin, depending on how the PoB is implemented. The more coin a validator burns, the more chances it will be selected.

PoB is an alternative consensus algorithm that attempts to address the high energy consumption issue of a PoW system. PoB is often called a PoW system without energy waste. While PoB is an alternative to PoW, the protocol still wastes resources. Also, it is questionable that mining power goes to those who are willing to burn more coins [100]. Table 3 illustrates a comparison of PoB. The node management of PoB is public. The transaction rate is high, but PoB does have high energy consumption. The scalability is medium and has a fault tolerance of 51%.

h: PROOF OF ELAPSED TIME (PoET)

Proof of Elapsed Time (PoET) is an Intel Corporation-developed consensus technique for permissioned Blockchain networks. PoET uses a lottery method that distributes winning possibilities evenly among network participants, ensuring that every node has an equal chance of winning [101]. The PoET algorithm assigns each node in the Blockchain network a random wait time, and each node must sleep for that duration. The first node to wake up will add a new block to the Blockchain.

The PoET workflow is similar to Bitcoin's PoW. However, it consumes less power. Nevertheless, PoET is highly dependent on Intel technology and suffers from interoperability issues [102]. Table 3 shows a comparison of PoET with other consensus algorithms. The node management of PoET is permissioned. The transaction rate is medium for PoET and also consumes less energy. Lastly, as it follows the PoW, the scalability is strong.

i: PROOF OF AUTHORITY (PoA)

Proof of Authority (PoA) is a reputation-based consensus algorithm. The expression "*Proof of Authority*" was proposed in 2017 by Ethereum co-founder and former CTO Gavin Wood. In the PoA consensus algorithm, block validators are staking their reputation. For this purpose, PoAth-based Blockchains are secured by the validating nodes randomly selected as trustworthy entities.

The PoA is scalable, as it relies on a limited number of block validators. Further, blocks and transactions are verified by moderators, pre-approved network participants. Therefore, PoA can be a solution for corporations as it can support private Blockchain applications with higher throughput [93]. Table 3 shows the comparison of PoA with the rest of the consensus algorithms. PoA can be private, with high transmission rate and throughput. PoA is also has good scalability and less power intensive.

j: PROOF OF CAPACITY

Proof of capacity (PoC) allows mining devices in the network to use their available hard-drive space to validate transactions. This is different from using the mining device's computational power (as in the PoW) or the miner's stake (as in the PoS). Instead, PoC authentication systems use leftover space on a device's hard-drive to keep solutions to a cryptocurrency hashing problem [94].

In PoC, a larger hard-drive equals more possible solution values to be stored. In simple words, it will result in a higher chance that a miner has to match the required hash value from its list, consequently in more chances of winning the mining reward. However, PoC has adaptability issues, and it is vulnerable to malware attacks [103]. Table 3 illustrates the comparison of PoC where it shows that it is public and decentralized. Also, the transmission rate is lower, although it has strong scalability.

2) DECENTRALIZED APPLICATIONS (DApps) AND SMART CONTRACTS

Besides the tools used in Bitcoin, a Blockchain can also use other tools, such as smart contracts and DApps.

a: WHAT IS A SMART CONTRACT

Smart contracts are self-executing, deterministic and Turing-complete code that runs on top of a Blockchain. The smart contracts self-execute predefined and deterministic actions when specific conditions correlated with negotiated transactions are met [104]. The smart contract idea was introduced by Nick Sazbo in 1994 [67].

The input parameters and the execution of a smart contract is precise and objective. In other words, if "x" happens, then execute "z". Smart contracts are stored on the Blockchain with an assigned Blockchain address. A smart contract execution is automatically triggered whenever a transaction is sent to a smart contract's Blockchain address. The called function is executed on every node of the Blockchain. The output is recorded as a state-transition (e.g., new value assignment to a smart contract variable). Additionally smart-contracts can issue transactions towards users' Blockchain addresses or other smart contracts. Note that the smart contract function execution is atomic, which means it is either executed fully or not executed at all. The most emblematic Blockchain supporting smart contracts is Ethereum. In the context of Ethereum, smart contracts run on top of the Ethereum Virtual Machine (EVM) as part of the Ethereum network protocol (i.e., on the decentralized Ethereum world computer). In Ethereum, Solidity is a JavaScript-like language developed for writing Ethereum smart contracts. Solidity compiles this code into bytecode, which is deployed on the Ethereum Blockchain as a special contract creation transaction. A successfully deployed smart contract is assigned with a unique Ethereum address.

To prevent mis-usage (e.g., spamming, infinite loops, etc.), for every function executed, a finite amount of *gas* is spent. In Ethereum, a *gas* is calculated as the product of *gas* usage and *gas* price. The *gas* price follows free-market policy based on the network activity (e.g., busy network, higher gas prices), expressed as a small fraction of the main token - ether. *Gas* usage is unknown prior to execution [105]. A user must specify the maximum amount of *gas*, it is willing to pay for a full-execution of a smart contract function. The more complex the smart contract, the more *gas* is used to execute it. If during execution the maximum amount of *gas* is exceeded, the execution is reverted, without affecting the state of the smart contract. As a result, *gas* currently acts as an essential gate to prevent overly complicated or numerous smart contracts from overwhelming the EVM [106]. Smart contracts allow for various agreements' terms and conditions to be fully accessible and visible to all the relevant parties. Once a deal is established, there is no way to dispute it.

Additionally, automated contracts attempt to sidestep the pitfalls associated with manually filling out heaps of forms, and the speed can save countless working hours compared to traditional business methods [104].

b: WHAT ARE DApps

DApps are applications that can be mostly or entirely decentralized. There are various advantages of DApps over a centralized architecture. Centralized applications operate on a central server, which implies a single point of failure and a single government & management entity. On the other hand, the decentralized applications distribute the risk to different entities, which favours resiliency, transparency, and censorship resistance. A DApp is usually a web application using an open-source software platform, which interacts with a smart contract on a decentralized Blockchain. A fully decentralized DApp is structured similarly to a common web application, based on front-end and backend code. The main difference is that the backend is minimal, containing an application API. Smart contracts are used to store the business logic and the application state. The design of DApps aims to lower the smart contract execution or the application state transitions, manly due to the fact that the computation executed in a smart contract is expensive [107]. Previously, DApps were referred to as applications used as media sharing protocols like BitTorrent. Later new DApps have been built on top of BitTorrent. Ethereum, as the first Blockchain offering smart contracts, allowed the emergence of the first DApps interacting with EVM. Another example is EOS.

- *Ethereum for DApps:* The Ethereum platform along with the Web3 Javascript API libraries,[1] allows for simple development of DApps and integration within most of the open source web platforms. The first step in creating a DApp is to develop a smart contract using the Solidity language.[2] The smart contract is uploaded on the EVM, and later executed by the decentralized Ethereum network. Finally a front-end web application is enabled to interact with the uploaded smart contract through the web3.js library. Numerous DApps have been created using Ethereum, including games, gambling apps, exchanges, marketplaces, and many more [108].
- *EOS for DApps:* The other platform which is competing with Ethereum is EOS. EOS offers a virtual machine and authorizes the execution of any deterministic language inside the VM sandbox. EOS gives the DApps developers the freedom to use the preferred development stack inside the VM and ensures the network's flexibility. Moreover, the EOS platform aims to address the scalability and flexibility concerns faced on Ethereum. EOS's capability to freeze and rollback transactions have decreased the community's confidence lately and gained high criticism [109].

3) PLATFORMS

The demand for Blockchain development platforms increases, as different sectors are exploring numerous applications based on Blockchain. Some of the widely used Blockchain platforms are further discussed. We also discuss new Blockchain platforms as well.

a: ETHEREUM

Ethereum is a wide-ranging, open-source Blockchain platform for DApps, powered by smart contracts and implanted with a congenital digital currency, called ether *ETH*. Ethereum is decentralized, open-source, public, secure, transparent, and Pseudo-anonymous [108]. Ethereum allows the code to be written to control the transmission of numeric values based on programmable conditions. Ethereum was conceptualized through a white paper published in November 2013 by Vitalik Buterin, and with additional contributions from his seven co-founders and other developers. The network was launched in June 2015 to extend the use-cases supported by Bitcoin [110].

b: HYPERLEDGER FABRIC

Hyperledger is an open-source collaborative effort designed to advance cross-industry Blockchain technologies, and it is a permissioned Blockchain. The architecture of Hyperledger is modular and it enables components, i.e., ledger, consensus mechanism, and membership services, to be plug-and-play. [111], [112]. The permissioned nature of Hyperledger allows organizations to define specific peer isolation through the use of *channels*. The smart contracts referred as *chaincode* run in a separate container at a specific channel. The workflow is not common as in Ethereum. Unlike Ethereum, the nature of Hyperledger opens a risk for execution of a non-deterministic chaincode [113].

c: CORDA

Corda is a, open-source, permissioned and private enterprise Blockchain. It has been supported by important companies like Amazon, Intel and Microsoft. Lately, it has opened its gate to nearly every industry by providing a private network for enterprises as well [114]. Corda does not allow peers to share information like Ethereum. Corda introduces legal footing and assured identity feature as well. Moreover, this is a massive performance boost, as linear horizontal scalability can be achieved due to not having all data shared with all network members.

d: QUORUM

Quorum is a private/permissioned, Blockchain-based implementation of the Ethereum protocol. It uses a voting-based consensus algorithm and obtains data privacy by introducing a new "private" transaction identifier. Compared to Ethereum, it adds improved permission management and better privacy. One of the most significant benefits of using Quorum is its high performance. Quorum can carry out more

[1] Web3.js: https://web3js.readthedocs.io/en/v1.3.4/
[2] Solidity: https://docs.soliditylang.org/en/latest/

TABLE 4. Summary of features with respect to platforms.

Features	Ethereum	Hyperledger Fabric	Corda	Quorum	MultiChain	EOS	Tendermint	Cosmos	Polkadot
Initial release	2015 July	2018 Sep	2016 April	2016 Oct	2015	2018 Jan		2016	2020
Type	Public Blockchain	Enterprises	Enterprises	Enterprises	Enterprises	Enterprises	Private	Private/Public	Private/Public
Language	Go, C++, Java	Go, Java	Kotlin	Go, Java	C++	C++	Go	Go	Rust, javascript, Substrate
Consensus	PoW	PBFT	BFT	RAFT, Istanbul BFT	round-robin	DPoS + BFT	BFT and DPoS	PoS	NPoS
Smart contract	Yes	Yes	Yes	Yes	Smart filters	Yes	No / App-based	Emulated or App-based	No / Parachains enable SC
Crypto currency	Ether (ETH)	Constructing using chaincode	none	Ether (ETH)	Bitcoin	EOS token	none	Cosmos (ATOM)	Polkadot (DOT)
Block creation/sec	15	not available	not available	not available	60	500 ms	1	6	60
Block Reward	2 Eth	none	none	none	50 native currency	318 EOS		3.81 ATOMs	re-calculated %
Contract language	Solidity	Golang, Java	Kotlin, Java	Solidity	V8	C++, Java	none	Solidity (for emulated)	none
Ledger type	Public /Permissionless	Permissioned	Permissioned	Permissioned	Permissioned	Public /Permissionless	Permissioned	Permissioned /Permissionless	Permissioned /Permissionless
Transaction cost	21000 Gas	not available	not available	not available	not available	Free	none	fees adjustable	fees adjustable
DApps	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Token creation	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Hash function	Keccak SHA-3	SHA-256	SHA-256	SHA-3	SHA-256	SHA-256	SHA256	SHA256	Blake2b
Smart contract execution	EVM	Dockers	JVM	EVM	Streams	EOS Virtual Machine	App-based	App-based	App-based
Throughput (Tps)	>20	>2000	>2000	>=100	7	>2000	10000	1000-4000	1500
Latency/sec	30	not available	not available	not available	not available	1.5	1	6	60-3600
Governance	Ethereum developers	Linux foundation	R3	Ethereum/Jp Morgan	MultiChain	Block.one	Interchain Foundation	Interchain Foundation	Web3 Foundation
Preferred use-cases	Wide ranging /general	Wide ranging/modular	Financial	Financial	Financial	Financial	High-throughput permissioned Apps	Wide-ranging	Wide-ranging
Focus on Industry	Cross-Industry	Cross-Industry	Financial	Cross-Industry	Financial	Cross-Industry	Cross-industry	Cross-industry	Cross-industry
Code repository	github.com/ ethereum	github.com/ hyperledger	github.com/ corda	github.com/ jpmorgan-chase/quorum	github.com/ MultiChain	github.com/ EOSIO/eos	github.com /tendermint	github.com /cosmos	github.com /paritytech

than 100 transactions per second, which outperform both Bitcoin and Ethereum [115].

e: MULTICHAIN

MultiChain is an open-source platform for private Blockchain, based on Bitcoin [116]. MultiChain allows users to customize many parameters, including chain anonymity, maximum block size, and mining incentive. A group of identified block validators performs the mining. Each block has only one validator, scheduled in a round-robin fashion. The latest MultiChain 2.0, introduces *Smart Filters*, a feature that allows custom rule coding for transaction validation [117].

f: EOS.IO

EOS is a BFT and DPoS consensus based Blockchain which offers smart contracts implementation. In comparison to Ethereum, EOS performs higher transaction rate [118], producing a block every 05 sec. The DPoS is based on 21 unique block producers that agree on strict block order creation [119], the producers are voted by token holders. The chosen 21 block producers remain for at least 126 rounds or blocks, where each elected producer generates at least 6 blocks for the elected period. The collaborative nature of the block producers is positive for avoiding potential forks, but it reduces the decentralization of the Blockchain.

g: TENDERMINT

Tendermint is an application-based Blockchain with a default BFT consensus [120], [121], which enables users to turn any deterministic application into a Blockchain application through the use of the Tendermint BFT state-machine replication. In particular, an application is adapted to use an Application BlockChain Interface (ABCI) in order to communicate any state-transition in the form of transactions to the Tendermint Blockchain. Unlike Bitcoin, Tendermint adds blocks through voting of validator nodes.

h: COSMOS

Cosmos is a network of many Tendermint Blockchains joined in a single Blockchain with a global transaction ordering [122]. It is an upgrade of Tendermint with the goal of enabling inter-operability between different applications realized as Tenderemint Blockchains [123]. It is useful for specific use-cases such as Decentralized Exchange (DEX) [124]. The mechanism for enabling the inter-communication is referred as Inter-Blockchain Communication (IBC).

i: POLKADOT

Polkadot is a Blockchain framework created by one of the Ethereum co-founders - Gavin Wood [125], which aims to tackle the scalability issues of common Blockchains (e.g., Bitcoin, Ethereum) [126]. Its framework is organized into a scalable multichain. The organization of nodes is hierarchical and is based on (*i*) a single relay-chain, and (*ii*) a large number of *parallelised* sidechains - parachains - able to communicate among themselves through the relay chain. Polkadot uses Nominated Proof-of-Stake (NPoS) consensus mechanism [127]. At the time of writing, Polkadot has not been fully rolled out for performance evaluation.

To conclude this section, Table 4 summarizes all the key aspects we have discussed so far for the different presented platforms.

IV. INTEGRATION OF DLT/BLOCKCHAIN WITH NETWORK SLICING: MOTIVATION AND PROPOSED ARCHITECTURES

B5G and future 6G networks are expected to be increasingly complex and will need an adaptive and intelligent architecture based on improved SDN, NFV and network slicing concepts in order to facilitate the network management operations [128]. On the other hand, a recent report discussing 6G vision and requirements [129] includes Blockchain as a DLT as one of the key technology to facilitate automation and management in future networks. Specifically, recent studies have proposed to merge the network slicing and Blockchain concepts for multiple purposes, since the Blockchain offers the opportunity to create an automated marketplace, where the network slices and their services can be negotiated. Additionally, Blockchain also offers E2E performance auditing opportunities among all involved actors in various complex scenarios, e.g., multi-tenancy or multi-administrative domain. In this section, we summarize the motivation behind the current research to use Blockchain platforms to handle the management of network slicing, in order to foster automation, organize/configure networking or computational resources, while delivering trust, privacy, and transparency.

A. MOTIVATION: THE ROLE OF BLOCKCHAIN/DLT AND SMART CONTRACT IN THE MANAGEMENT OF NETWORK SLICING

Network slicing success strongly depends on the involved provider's capability to offer an adequate set of solutions tailored to specific needs/requests of various sectors, including but not limited to verticals end-user, tenants and other MNOs. The different industrial verticals are characterized by specific challenges, which the provider needs to fulfill in order to support their clients. In this subsection we go through the different motivations that generate new opportunities for the merge of network slicing and Blockchain concepts.

1) OPEN MARKETPLACE

With the introduction of virtualization technologies, NFV has generated a new market focused on the offer and distribution of VNFs. The notion of an open and decentralized marketplace where to store, advertise, purchase and compare services or resource offers is absent in the 5G concept, but has appeared in many new NFV related contributions. An open marketplace is a significant component of the advertisement and publication of the developed services from different service providers, adding diversity in network services and virtualization. Service and infrastructure providers can benefit from this open market by having real-time assets offers, requests and automated payment settlements [130]. Service and infrastructure providers can also take advantage of the open market by providing their infrastructure, resources, VNFs, to fulfil end user's demands. The demand for the marketplace to be more flexible is increasing, and it is expected to be able to support on-demand agile businesses [131].

Similarly, in network slicing, any network request can be served by combining available VNFs as network slices. A marketplace for network slicing enables end-users like Mobile virtual network operator (MVNOs), Over the Top Provider (OTTP), industrial vertical players to request and lease resources from infrastructure providers that create predefined, differing levels of services for different clients by customizing their requirements. Solutions that promote the competition between providers can reduce prices while increasing network performance to accommodate specific user's demands.

In this context, the need for trust/security between buyer and providers drives the need to integrate DLT because it can redefine the interaction and provide a safe environment for negotiation of resources with its features like consensus and immutability [132]. Ultimately, a decentralized marketplace's role is to introduce an economic plane for exchange of services, VNFs, or resources among service providers by promoting trust and transparency. Therefore, to create telecom infrastructure marketplaces, efforts towards Blockchain-based marketplace are on the rise [133]. For example, IOTA[3] is one of the participant working on ''Blockchain-based Telecom Infrastructure Marketplace'' catalyst project with TM Forum.[4]

2) DISCOVERY AND SELECTION FOR OFFERED SERVICES

An NFV market, which includes the offering, distribution, and execution of VNFs, opens up opportunities for service providers to offer VNF. However, the research on models to efficiently host, audit and improve revenue by introducing market competition can be improved. An auction mechanism can help choose the right infrastructure candidate to host a requested service. Auction mechanisms from economics are transferred and applied in network slicing, and resource allocation [134]. In this direction, a Blockchain-enabled system based on smart contracts helps address the challenge of discovering and selecting offered VNFs and services. As it can be employed to provide immutable and permanent records that allow interested parties to audit and trust in the data,this has motivated some of the proposed studies, which will be discussed later.

3) SECURITY

We have already discussed how 5G (through network slicing) supports a wide range of new network services from heterogeneous VNFs. In NFV, security weaknesses have been identified in the integrity of VNFs and network services; new challenges have been identified about incorporating trust among end-users. Similarly, network slicing solutions must ensure the main security principles, traditionally categorized into confidentiality, authentication, authorization, availability, and integrity [135]. Ensuring isolation between network slices is essential to avoid common attacks in shared infrastructures. The multi-tenant and multi-domain environment increases the possibility of attacks inside the cloud. The use of Blockchain as a DLT can implement security for building a trust mechanism between different infrastructure providers. DLT can be a reasonable solution to establish an authentication layer for the multi-administrative domain to satisfy the security principles [21]. For instance, DApps for multi-administrative domains enables transparency on identity and permission management for NFVIaaS providers and consumers [12]. Furthermore, Smart Contracts may be used as a mechanism for *access control* when they execute all the access information (e.g. user credentials) and record it in a distributed ledger. This is elaborated in the latest publication by ETSI PDL [136], which may serve as a guide to prevent future disputes.

4) SMART RESOURCE MANAGEMENT

The complexity of network management with an increase in users and the lack of spectrum in 5G/6G networks requires capabilities to automate the critical processes involved in network operation. Hewa *et al.* mentioned that the resource management operations require to be compatible with the large infrastructures [58]. Blockchain technology aims to offer advantages to enable decentralized solutions that ensure the integrity and immutability of the information stored and traded. For instance, [137] presented a Blockchain-based solution that allows providers to trade their processing and networking resources. Also, [138] depicts a smart resource management where a Smart Contract is triggered whenever there is a request for resource allocation.

5) QoS MONITORING

Smart Contracts can provide mechanisms for network service provisioning or service allocation, including accountability. The service contracts and their SLAs and QoS can be deployed in the Blockchain through Smart Contracts. This can prevent future disputes and provides audibility. For instance, [139] present a distributed SLA management with Smart Contracts and Blockchain creating distributed cloud offering dynamic services and promoting reduced costs for cloud consumers. Additionally, the service contracts from all operators can be advertised on DApps backed by Smart Contracts and stored in a distributed ledger. The publication on *Permissioned Distributed Ledgers (PDL) Smart Contracts System Architecture and Functional Specification* by ETSI [136] discusses the complete possible scenario in detail.

6) AUTOMATION OF OPERATIONAL SAVINGS

Another advantage of applying a Blockchain to network slicing is the savings in coordination among consumers and providers for transaction costs. Since a Blockchain provides a platform for negotiations that is trustworthy, it enables automatic agreements so that the slice negotiation process is accelerated, and consequently, the cost of the individual network slicing agreement is reduced [59].

7) NEW BUSINESS-MODEL-DRIVEN NETWORK SERVICES

Network slicing naturally involves interactions among stakeholders. As a result, it is essential to create network services able to co-exist with the new business models to improve profit for providers and better experience and cost-effective solutions for the consumers. SLAs between users and network slice providers are required for these business-model-driven network services. For this purpose, *record-keeping Blockchain* is used as an authoritative log mechanism for recording and keeping track of final transactions. This allows reduction of conflicts among involved parties [56].

B. REVIEW OF PROPOSED ARCHITECTURES

In the literature, the integration of Blockchain and network slicing concepts has already been explored in different

[3] https://www.iota.org/
[4] https://www.tmforum.org/

contributions [140]–[150]. In this section we analyze the literature. We aim to spotlight the main features that enable and enhance the integration of Blockchain with network slicing.

We divide the proposed works that interact with network slice stakeholders (as consumers or providers) via NFV MANO frameworks or a Blockchain. These frameworks, can be divided into two main groups as follow:

- Blockchain and smart contract-based network slice broker, where we discuss the frameworks integrating Blockchain using network slice broker. A network slice broker act as an enabler for MVNOs, OTTPs or vertical market players to request and lease resources from service providers. We further discussed with details about its components in IV-B2
- Blockchain and smart contract based, where the proposed works introduce Blockchain-based components in their frameworks which are further discussed in IV-B3.

Additionally, for clarity the different types of interactions that can happen between stakeholders can be further categorized. The interactions are grouped in:

- Vertical-to-provider
- Provider-to-provider

We start by introducing the network slice stakeholders, i.e., providers or consumers. Then, we go through the architecture summarizing the different contributions in literature, and finally, we elaborate on the different interactions.

1) STAKEHOLDERS

We have introduced in Section II-C different stakeholders that interact, negotiate or exchange information in order to deploy E2E network slices. They can be divided into two roles:

- Providers
- Consumers

A single stakeholder may have both roles.

a: PROVIDERS

According to 3GPP [151] the *Communication Service Provider* (CSP) is an entity that provides communication services, and the CSP consumes *Network Slice Provider* (NSP) services. In the same manner, a *provider* refers to any entity that provides a service to another entity in terms of infrastructure (e.g., network resources) or Network-as-a-Service (NaaS). According to [152] Infrastructure providers (InP) are able to provide computational and network resources to external entities (or consumers) in order to be used by different network slices. In [145], [147], [149], the term InP is used in similar manner, while Nour *et al.*, in [148] use the term ''resource provider''. MNOs can take both the InP and NaaS providers roles for example in [146]. Furthermore, the works in [143] and [141] describe interactions between different service providers (e.g., MNOs) to exchange services where they can have both roles, consumer and provider roles.

b: CONSUMERS

The term consumers refers to several entities that consume network slices, or VNFs, for example in terms of a marketplace for VNFs. In [153] the *Communication Service Customers* is defined as a consumer of services offered by a service provider. Keller defines in [140] the consumer as a customer which acquires VNFs via a web application portal (the *front-end*), to a *Blockchain-based Trusted VNF Package Repository*. The authors in [145] also use the concept of *generic marketplace* where a provider can list their services and the consumer can access this marketplace via the user-interface. Authors in [147] use the term *tenants* for the consumers of network slices [154]. The concept of a tenant is defined by [152] as that of ''consumers acquiring a slice to orchestrate and run network functions within it to provide a certain service to their customers''. To accommodate the needs of growing industrial vertical tenants, the authors introduce a Blockchain-based Intermediate Broker (IB), enabling InPs to allocate network resources among tenants.

The ETSI Permissioned Distributed Ledger Industry Specification Group (PDL ISG) has recently released several reports [136], [155], [156] specifying different applications of permissioned DLT to networking. The group categorizes different stakeholders (e.g., end-users, platform operators, infrastructure vendors, regulatory and governance authorities) in [155]. Additionally, it defines three different ICT vertical families: 1) compute vertical, 2) connectivity vertical and 3) storage vertical. Each vertical family leverages on Permissioned Distributed ledger - PDL or permissioned Blockchain to consume or provide different network services or slices.

2) BLOCKCHAIN AND SMART CONTRACT-BASED NETWORK SLICE BROKER

According to [157] the business interactions among stakeholders are mainly focused on (i) support of business-to-customer (B2C) model, where the consumer acquires customized network resources based on its requirements without considering which provider provides the requested resources, (ii) support of business-to-business (B2B) model, where the provider sells customized network resources to enterprises which control their resources and (iii) support of Business-to-Business-to-Customer (B2B2C) model, where a *network slice broker* plays an intermediate role and engages with the consumer. In this manner the broker gets more control of the network.

Currently, in the literature the works in [145]–[150] introduce the idea of a Blockchain-based broker, which facilitates the trading of network slices, by benefiting from the introduction of Blockchain. Among the possible tasks of the network slice broker there is to create a generic marketplace to trade VNFs, to lease network slices, the billing management, or the management of auctions to choose the appropriate service providers. This brokering layer is referred to *intermediate broker* and *distributed blockchain-based broker* in [147] and [150], respectively.

In this direction authors in [145], implement a *generic marketplace* for VNFs trading between consumer and InPs. The *generic marketplace* is linked to a *smart contract creator* and *Blockchain Adapter* by means of a broker, so that the proposed solution can be used to supply a large variety of services based on VNFaaS. This approach presents a transparent solution via Blockchain in which InPs can compete to host VNFs for each consumer. Hence, it brings fairness and trust to some degree where an auditable auction is performed as there are transparent records about each interaction between provider marketplace and consumer.

The *Slice Leasing Ledger*, is another concept based on Blockchain is introduced by [146]. In the proposed system, every involved stakeholder (consumer or provider) has its own unique digital keys which can be used to sign and verify transactions. These keys are tightly interconnected to each stakeholder's identity. The aim behind introducing *Slice Leasing Ledger* is to create the possibility for verifiable transactions which can be used for charging, billing and SLA agreements between consumer and provider. Moreover, with the help of Blockchain, the time decreases during service creation, and it facilitates to perform operations dynamically. Also, the concept for *Monitoring and Billing Management* is introduced in [147] to handle the QoS monitoring and billing of services. Together with Blockchain technology, the proposed solution can record the various exchanges of resources.

Similarly, the concept of *Sub-Slice Brokering* is introduced in [148] to manage all the information related to the subslice deployment brokering mechanism in a permissioned Blockchain. The authors introduce a new business entity called ''Slice Provider'', which aims to select the resources from different resource providers to create E2E slices. The proposed framework integrates smart contracts to deploy the sub-slices. The process starts when the consumer requests to create a network slice using a template or a blueprint. The Slice Provider translates the template to specific slice resource requirements (VNFs, storage, or memory) and generates a contract. Consequently, the integration of Blockchain allows leasing resources from various providers in a secure manner.

Moreover, the determination of the trading price of resources or services is one of the crucial challenges when it comes to network resource leasing [158]. Also, it is not fair to the consumer if the price is solely determined by the service providers, as consumers need a fair and transparent algorithm for pricing in transactions of services. Auction mechanisms traditionally studied in economics, have been proposed for network resource allocation as one potential solution to the pricing selection problem [159]. The auction helps the consumers choose the best provider according to its own utility, while facilitating that service providers increase their efficiency. In this regard, [145], [147], [149] and [150] use smart contracts-based to perform *auction mechanisms*. The objective of these approaches is to motivate the providers to bid honestly, which helps the consumers understand the information provided on services and prices to achieve more desirable results. Hence, Blockchain can guarantee reliable auditing and enforces policies through smart contracts in a secure and automated manner.

Also, authors in [150] introduce *Service Management* and *Blockchain Entity*. The authors propose a bidding scheme through a Distributed Blockchain-based Broker (DBB) to help operators place their bids for resource provisioning to offer the requested service. The above mentioned components (*Service Management* and *Blockchain Entity*) are added inside the broker to perform the process of bidding and resource provisioning. The DBB relies on a Blockchain-based system to request resources, evaluate resource provisioning offers, and propose a service management entity. The proposed system, via a Blockchain-based bidding system, aims to provide admission control for incoming requests and minimize the tedious process of setting up a memorandum of understanding.

3) BLOCKCHAIN AND SMART CONTRACT-BASED

The works presented in [140]–[144] propose Blockchain-based solutions to achieve different purposes, like the incorporation of trust, the automation of SLA definition and management, or security provisioning to the network slicing management.

The authors in [140] propose a Blockchain-based trusted VNF repository, which uses smart contracts to incorporate trust. This Blockchain-based solution aim to tackle the challenge of VNF integrity verification by leveraging smart contracts properties of immutability and accessibility, where it is possible for a consumer to verify the integrity of VNF packages running on a local virtualization platform and allowing the the provider to automatically receive any payments once a VNF is acquired.

In [141] the authors talk about the concept of *Network Slice Manager* referred as *Slicer*. This work presents a multi-domain NFV/SDN network, in which each domain has its own NFV/SDN architecture managed with the support of a *Slicer* on top. In such a scenario when a vertical in a domain needs a service controlled by a different domain *Slicer*, it can request an E2E slice to its own domain *Slicer*, and it takes care of the whole slice deployment with the collaboration of other *Slicers* in different domains through the support of the Blockchain. The authors aim to minimize the deployment time of the E2E network slice, and hence they illustrate through results that the Blockchain can be a solution. Also, authors state that the Blockchain can bring a fair collaboration among various domain owners to deploy different services.

In [142], the idea of allocation of network resources through an *Accountable Just-in-Time* to support QoS levels is proposed. This module is specifically designed to handle services that can dynamically change, in both time and location. The proposed architecture achieves billing and accountability through smart contracts solution based on SLA with the aim to provide transparency, immutability and automation. The study also suggests that failure to maintain the SLA may result in penalties that can be automatically imposed through the smart contracts.

Furthermore, to enable service federation for service providers to provide network services across multiple domains, in [143], authors encourage the integration of i.e., Blockchain and smart contracts. The idea is proposed to use Blockchain as an opportunity for secure, distributed and scalable federation solution. This solution also involves a single-blinded reverse auction mechanism to help the consumer domain select a provider administrative domain.

Lastly, the work in [144] proposes the Blockchain technology to register all commands that create, modify, configure, and destroy the network functions of each network slice in the form of signed transactions. The authors propose a Blockchain architecture for creating secure network slices tailored for various E2E use case (i.e., eMBB, mMTC, or Industry 4.0). The consumer interacts with the system to acquire a slice and defines the requested slice features, including desired VNFs and the corresponding Blockchain category for desired use-case to address different slice requirements through different categories of Blockchains. The consumer accesses to the system with a *user-interface* and interacts with the *Management Blockchain Server* and a *Blockchain Creation Server* to create secure network slices for various E2E use cases.

We conclude and summarize the above mentioned discussion with the help of Table 5, where we discuss each framework and its details including stakeholders involved, components, mechanisms, Blockchain platform used, smart contract implemented or not, consensus mechanism used.

4) INTERACTIONS AMONG STAKEHOLDERS

As mentioned, the stakeholders can have different interactions among themselves mainly grouped as: (*i*) vertical-to-provider and (*ii*) provider-to-provider. Specifically, the vertical-to-provider interactions that are using Blockchain can be further grouped into:

- OSS/BSS interactions - in this group, the vertical customers are using Blockchain to communicate and exchange information with the OSS/BSS of the service providers. In the evaluated literature, the authors are using OSS/BSS endpoint (e.g., web portal) to request networking services through *auction and bidding* process [145], [147], [149], [150]. Although some of the works [143], [148] does not directly use the auction and bidding to interact with customers, they do implement the negotiation process. On top of that, in [140], [142] the authors envision the use of Blockchain in order to perform *billing and accountability* operations between vertical customers and service providers. In short, it means that customers are charged for all the networking services through the Blockchain, enabling the customers for more transparent and extended choice of providers.
- Slice-related interactions - verticals use Blockchain or DApps to request to perform *slice creation and leasing*. In the works [144], [146], [148], [149] the authors elaborate the process where the verticals are envisioned to request end-to-end slices directly through DApps, specifying the slice requirements. Although they focus on conceptual realization [146], others evaluate the solution through Hyperledger [144], [149], and a custom PoW based prototype [148].

On the other hand, the provider-to-provider interactions involve interactions among provider domains via Blockchain, with a common goal to establish end-to-end network slices across multiple domains. These interactions can be grouped into:

- Service related interactions - The work in [143] elaborates how NFV MANO administrative domains negotiate and perform federation of network services using Ethereum Blockchain. In [145], the authors discuss how VNFaaS can be achieved with the support of the Blockchain technology.
- Resource-related interactions - Besides network services, providers may exchange network resources. In [141] the authors elaborate how different providers may exchange NFVI resources in order to achieve end-to-end network slices.

V. APPLICATION OF DLT/BLOCKCHAIN IN VERTICALS

In the previous sections, we have analyzed how Blockchain can be integrated in the network slicing provisioning process, either between verticals and providers or between two providers exchanging services/resources in peering relationships.

In this section, we analyze a number of vertical industries by focusing on how the Blockchain as a technology is currently used to improve their business logic. At the end of the section we explore how some works have already integrated a Blockchain solution into a network slice. In our view, the application of network slicing with Blockchain will improve current solutions. The goal is for the reader to understand how specific vertical-related problems can be solved through Blockchain technology, which in most cases is deployed within a vertical network slice.

a: MEDIA AND ENTERTAINMENT

The emergence of the Blockchain technology is significantly affecting *media and entertainment*. As mentioned in Section III, Blockchain brings novelty in the media and entertainment ecosystem. It provides added value to media publishers and content creators, thus shifting the economical benefits more towards the copyright-owners (e.g., the creator can be the copyright-owner of the content, or the publisher has the full ownership) [160]. The impact is measured as disruptive and sustainable [161].

The micropayment channels [162] disrupt the configuration of the ecosystem by allowing content providers and

TABLE 5. Review of proposed frameworks in literature.

Ref	Stakeholders		Vertical-to-Provider		Provider-to-Provider		Components	Mechanisms	Blockchain Platform	Smart Contract	Consensus
	Consumer	Provider	OSS/BSS	Slice	Service	Resource					
[140]	Vertical	InPs	✓				Front-end and Package Repository[a]	Consumer can register a new VNF or delete VNF using Blockchain-based repository	Ethereum	✓	PoW
[141]	Multi-domain & Vertical	Multi-domain				✓	Slicer[b], NFVO	Each slicer shares its own network resources in its domain with other domains. The Slicers are members of a private Blockchain.	Ethereum	✓	PoW
[143]	Multi-domain	Multi-domain			✓		5Growth-based[c]	A domain(consumer) creates an offer and the rest of the provider domain bid for it. Each received, offer is mapped and recorded via smart contracts.	Ethereum	✓	PoW
[144]	Vertical	InPs		✓			Global Manger[d] and User-interface	To create slices specified for each user-case using Blockchain	Hyperledger Fabric	✓	BFT
[145]	Vertical/ OTTP	InPs	✓		✓		NFV-Broker[e], NFV-enabled architecture	The bid manager allows InPs to start biding to provide resources to end-users. The auctioneer finalizes the best bid to buy VNFaas	Ethereum	✓	PoW
[146]	Tenants & Vertical	InPs & MNOs	✓	✓			Slice leasing ledger, NFV MANO & Broker	Consumer requests slice and accepts SLA and the Slice Leasing Ledger (SLL) helps lease a slice from the network slice broker	Not implemented	✓	Not implemented
[147]	Tenants, OTTP	InPs	✓				Intermediate Broker & Blockchain domain	InPs sell resources to tenants with the help of the Blockchain-based broker	Hyperledger Fabric	✓	RAFT
[148]	Vertical	InPs		✓			Slice provider[f]	An end-to-end slice is seen as a series of sub-slices, established by a smart contract's chain	Permissionless		PoW
[149]	Vertical	InPs, MVNO	✓				Slice broker, Virtualized Resource/Infrastructure	Providing end-user to find the best price (i.e. lowest) and for InPs sell their idle resource for the highest price possible using Blockchain-based distributed marketplace.	Hyperledger Fabric	✓	RAFT
[150]	MNO	MVNO, OTTP	✓				Broker[g], Network slice management system	OTTP request a service for service management which I then sent to broker. Broker creates a bid and forward it to Blockchain entity	Quorum	✓	RAFT

[a] Blockchain-based
[b] In a multi-domain NFV/SDN network, in which each domain has its own NFV/SDN architecture with a Slicer on the top
[c] Consisting of 5Growth Vertical Slicer (5Gr-VS), the 5Growth Service Orchestrator (5Gr-SO) and the 5Growth Resource Layer (5Gr-RL)
[d] Consisting of NFV-MANO, Management Blockchain Server, Blockchain Creation Server
[e] NFV broker has generic marketplaces, smart contract creator linked with Auctioneer and Blockchain Adapter
[f] Consisting of business slice orchestrator and resource broker
[g] Consisting of service management, Blockchain entity and resource provisioning broker

aggregators to be bypassed and shift the power to content creators. Each art piece, song or movie is published on Blockchain-based platforms by the creators/owners and directly sold to the consumers. This disruptive concept referred to as "one-stop shop" model enhances the relationships between the content creators and the consumers. Through the application of Smart Contracts, each created content can be tokenized and its ownership fairly distributed [163]. The distribution of royalty payments is automatized and fairly distributed to each musician.

Also, in the gaming industry, the in-game assets are registered on public Blockchain (e.g., Bitcoin, BitCrystals [164]). Users can trade or exchange in-game assets outside the game.

b: AR/VR

Vibehub [165] is a combination of a VR and Blockchain platform for creating virtual spaces where a variety of activities can be conducted, from marketplaces to virtual business meetings. Vibehub has 3D photo-realistic in-house holograms (Holoportation) technology that is used for body scanning of musicians and educators. These holograms can be placed in a custom VR or AR environments where users can take part of the experience.

Decentraland [166] is an open-source and a community-driven platform that simulates a virtual world where users can access with VR devices through a web browser. Decentraland uses a distributed storage paired with Blockchain that holds all the information to recreate the virtual space in the users' devices. Decentraland users can explore the world, consume user-generated content or create their own experiences and offer it to peering users on the platform.

c: DRONES

In the Unmanned Aerial Vehicles (UAVs) industry, Blockchain solves issues and challenges related to cyber-security, air-traffic control and insurance. With drone technology advancements, the information gathered by drone-control systems and the drones becomes an attractive target for cyber-attacks. Blockchain can then be used as a defense against the growing threat of cyber-attacks. In [167], the authors focus on the application of Hyperledger fabric to increase the security of networked swarms of UAVs. More specifically, the authors in [168] analyze the current 5G network security solutions and open issues, and propose an application of Blockchain to solve most security challenges. Air traffic control is essential to prevent drones colliding with an aircraft and/or other drones. The increasing number of active drones may lead to potential mid-air collisions. In this context, Blockchain has been proposed to resolve the issue through an air traffic management system based on Blockchain [169].

d: AVIATION

Currently, the radar-based air traffic service providers can preserve the privacy of flight plans and position of airplanes, mainly for military and corporate operations. In the US, the Federal Aviation Administration (FAA) adopted in 2020 the Automatic Dependent Surveillance Broadcast (ADS-B), which does not include privacy features, with corresponding implications in terms of potential security issues (e.g., spoofing, denial of service, etc.). In [169], the National Aeronautics and Space Administration (NASA) proposes a Blockchain-based prototype for air traffic management with the goal to mitigate the ADS-B security issues. The framework envisions the use of Hyperledger fabric, as permissioned Blockchain, which would provide a framework that includes certificate authority, use of smart contracts and high bandwidth communication channels for secure communication channels between entities (e.g., aircraft, authorized members).

In [170], the authors propose to replace paper records through the use of Blockchain-based distributed ledgers. The work provides ideas for improving the aviation record management systems through the example of a record flow using a paper record and the advantage of the use of the Blockchain technology. These records present all the logs that are kept regarding flights (e.g., crewmembers records, airplane maintenance records).

e: eHEALTH

The application of Blockchain technology to the healthcare industry has been subject of numerous reviews in the last years [171]–[175]. The maintenance of medical records using Blockchain is the most anticipated use-case [176]–[179]. The MedRec [180] is one of the early proof-of-concepts that demonstrate the usability of the Ethereum smart contracts to maintain the patients' records over the years or even for future generations. The feasibility study in [181] confirms that permissioned Blockchain can be successfully used for exchange of personal health records. However, its generalized practical use requires numerous modifications (e.g., reduction in records data size) and reduced operational cost.

The work in [182] proposes a light-weight Blockchain implementation for healthcare data management. The work uses customized Blockchain implementation where the adopted consensus approach is PBFT and the main network regulator is the Head Blockchain Manager (HBCM), which acts as a Certificate Authority (CA). The concept relies on the usage of channels, referred to as canal(s), similar to the Hyperledger network. The results show at least 67% increased efficiency or speed in ledger updates.

The healthcare industry is looking forward to the application of Blockchain to battle drug counterfeit. Numerous studies evaluate the Blockchain benefit for tackling drug counterfeit [183]–[186].

f: AUTOMOTIVE

The automotive industry is going to be revolutionized by the next generation of communication technologies [187]. The introduction of vehicular-to-vehicular communications introduces a number of security and privacy issues [188]. The application of Blockchain has been proposed as a solution to the security and privacy issues [189]–[191], as well as a solution for trustful collection of vehicle's data [192]. Specifically, to protect trust among all involved parties, Blockchain technology can be applied to counter fraud. Companies, like Bosch, have committed to build a framework to counter fraudulent actors targeting the manipulation of car odometers [193], [194].

The work in [195] explores the application of Hyperledger fabric as a proof of concept to verify and record reports for vehicle-to-vehicle (V2V) messages exchanged in multiple areas. Thanks to the implementation of the Hyperledger solution, the proposed system manages to collect individual reports of received messages from each vehicle in a certain area and to join them in a single distributed ledger for all areas. To improve the authentication, trust and validation in the vehicle-to-infrastructure (V2I) or V2V communication, the work in [196] proposes a new Blockchain algorithm that uses local dynamic Blockchain for keeping local information of the events that are happening in a given region, and a main Blockchain that keeps track of the global events. Each vehicle in a certain region is authenticated through a unique ID. If an unusual event occurs with a vehicle, the event is directly reported to the main Blockchain.

g: LOGISTICS & SUPPLY CHAIN

From the logistics and supply chain perspective, the Blockchain technology is seen as a disruptive technology that will change the way industry operates. Stakeholders in the supply chain eco-system expect a major impact in increased efficiency, transparency and reliability. The authors of the work in [197] conducted a survey on social media to measure the acceptance of the Blockchain technology applied to the logistics and supply chain industry. The findings reveal that most of the companies understand the positive impact of Blockchain over the logistics industry. However, companies are more hesitant to devote significant resources in developing Blockchain applications.

The work in [198] aims to overcome the adoption fear and to design a strategy to design, develop, validate and integrate a Blockchain solution in a logistic and supply chain business strategy. The authors present a case study of fresh food supply chain deployed with Hyperledger Fabric. The results show that the implementation of Blockchain solutions is highly sustainable and is completely covered by the savings. The most critical issue is that the Blockchain should be adopted by all involved actors. The work in [199] proposes a decision framework for the logistics industry based on using a quantitative approach. The framework is applied on a large-scale logistics company where the findings suggest a range of important criteria for Blockchain applications (e.g., security, visibility and audit) and a range of feasible logistics operations where the Blockchain can be applied (e.g., transportation, materials handling, warehousing, order processing).

VI. CHALLENGES AND RESEARCH OPPORTUNITIES

A. LIMITATIONS OF CURRENT WORK

1) APPLICABILITY

Blockchain is a technology which offers many opportunities, but also at a high implementation cost. As a result of that, it is important to identify the areas of applicability which obtain the highest benefits for the costs that are to be paid. Not to pay attention to this initial design phase may make Blockchain more a source of problems rather than a solution. The authors of [200] provide a step-by-step chart of how one should evaluate if a Blockchain would be an appropriate solution to a given problem or use-case. Consequently, while implementing Blockchain applications, the decisions need to be well planned, and Blockchain applications must keep in mind the network effects it will have while delivering value to consumers. Furthermore, identifying the business case and primary drivers cost of implementation are some of the issues that need to be considered beforehand [201].

2) ADOPTION AND COMPLEXITY

According to [202], there are three categories of factors that abate the adoption of the Blockchain technology: (*i*) technological factors; (*ii*) organizational factors; and (*iii*) environmental factors. The study conducted in [202] focuses on the organizational factors and argues that the biggest adoption factors for a company are the top management, the organizational readiness and the size of the company. Other studies suggest that the Blockchain makes positive adoption steps in the business and industry sector. According to Deloitte's annual report on Blockchain [203] around 55% of the companies included in the survey study confirm that Blockchain technology is in their top-five strategic priorities. Around 80% of the respondents believe that the Blockchain technology will be widely used in the future.

3) BLOCKCHAIN SCALABILITY

The Blockchain scalability is a known problem [204]. With increasing number of users or full-nodes in the Blockchain network, the activity and transactions grow drastically. Each new added node, needs to synchronize the Blockchain (e.g., download all the transaction history - more than 1 terabyte (TB) in the Ethereum Blockchain) and start actively participating in the Blockchain network. When a Blockchain grows significantly, the synchronization process is slow and newly joined nodes take time to start actively participating in the network, which results in poor scalability performance. In [126], the authors evaluate these limitations and explore the current solutions to solve the scalability problem in the most widely adopted Blockchains, as Bitcoin and Ethereum.

For the network slicing application, the scalability issue should not be a problem. With the assumption that the number of operators is not more than few thousands (e.g. 3 to 5 operators per country) [205], any Blockchain network (permissioned or permissionless) is not expected to expand as much as the Bitcoin or the Ethereum network. However, if many new stakeholders emerge in the eco-system, beside the mobile operators, the use of a public or a widely adopted permissioned Blockchain may be at risk run into the well known scalability issues, which then need to be taken into account in the design of the network.

4) ENERGY EFFICIENCY

The mainstream view is that Blockchain is one of the major existing energy consuming technology [206], and the numbers are still growing [207]. The analysis in [208] suggest that even maintaining a private or permissioned enterprise Blockchain is significantly more energy inefficient than a non-Blockchain (e.g. centralized) solution for enterprise. The same study suggests that the sustainability of the Blockchain application mainly depends of the design solution. For example, minimizing the on-chain activity can significantly increase the energy efficiency of the Blockchain application. From a networking operator or service provider perspective, depending on the number of nodes running over the local infrastructure, the application of Blockchain technology for network slicing might increase the impact on the operational expenditures (OPEX). At the same time, the automation introduced by the Blockchain can reduce the OPEX on other aspects.

5) STORAGE

Once a Blockchain is set up and running, the ledger begins to grow recording all the transactions and verified blocks. The storage of a Blockchain can significantly increase if the Blockchain itself allows for big files to be stored on-chain. The overall recommendation is not to store any data on-chain (e.g., size in the order of megabytes) [209]. For this reason, significant effort has been recently put to provide distributed off-chain solutions in projects such as Storj [210] and Sia [211]. Recently, with the emergence of the Interplanetary File System (IPFS) [212] in combination with the Blockchain technology promising solutions have been proposed in the area of P2P sharing systems for storing off-chain data [92], [213]–[216]. In network slicing applications, the storage issue mainly depends on the design solution. Specifically, it is important to keep low the on-chain data shared among all participants in the Blockchain network.

B. FUTURE RESEARCH DIRECTIONS

1) GLOBAL SERVICE FOOTPRINT

The implementation of the Service federation and resource sharing (described in Sec. IV-B) opens a range of opportunities for global collaborations between different service providers and/or stakeholders. Potentially, all operators and service providers can be interconnected in a single permissioned Blockchain. Through the use of service federation feature, the operators and service providers can offer a new range of on-demand services to vertical industries on global scale. With the use of Blockchain technology, the full potential of the network slicing may be extended from a single domain to a global scale, in an automatic and agile manner. By enforcing the SLAs through smart contracts, the reliability of the offered global services can be significantly increased, as well as Blockchain-powered integrated pay-as-you go charging. Research on how to automate these federated scenarios through the use of Blockchain and the combination with Artificial Intelligent is overall and exciting new area of research.

2) MARKETPLACE FOR NETWORK SLICE AS A SERVICE (NSaaS)

Projects such as 5G-Transformer [37] and 5Growth [54] have studied the possibility to provide mobile network operators the capability to offer Network Slice as a Service (NSaaS). The work in [217] breaks down the NSaaS business model, orchestration and management. From a customer point of view, the NSaaS feature allows the customer to request an on-demand network slice to satisfy the network requirements to monitor an agricultural area [218], or to provide connectivity for a big sporting event [219]. Usually, the customer chooses a template from a catalog of offered *slices*, that are adjusted according to the needs of the customer. Each mobile network operator has its own catalog of *slices* that is offered to customers. Joining the catalogs of all mobile operators would create a single-point of access or a *marketplace* for NSaaS [220]–[222]. By deploying the marketplace on a Blockchain [223] (e.g., as a DApp), the marketplace can have a distributed nature that can potentially overcome all the challenges mentioned in [221]. Research in this area is still widely open and require significant efforts also at implementation levels.

3) DApps WIDESPREAD

According to [224] there are around 3750 deployed DApps on all the platforms (e.g., Etheruem, Tron, EOS, etc.) with around 200 000 users per month. By mid-2020 [225], the major increase of Decentralized Finance (DeFi) projects emerge along with a new smart contract token standards (e.g. ERC 1155), and these standards help ensure that the smart contract achieves composability. For instance, newly issued token remains compatible with decentralized exchanges already existing. This indicates that the DApps usability and user adoption is slowly increasing. With the introduction of Digital Asset Modeling Language (DAML) [226], [227], a user-friendly programming language for creation of DApps and DLT solutions that is enabling simple set-up of a private Blockchain network without entailing all the setup complexity over certain infrastructure. In our view, the combination of DAML and network slicing (platforms) may open a range of opportunities for research and application of DApps as part of network services or increase the general public usage of DApps.

4) BLOCKCHAIN AND AI

The Blockchain technology can enhance the AI or vice-versa, the AI can enhance the Blockchain applications [16], [17]. From a network slicing perspective, the deployment of distributed AI applications is beneficial for life-cycle management of deployed network slices. Combined with monitoring information, the distributed AI applications can decide per slice different strategies to maintain the SLAs and employ different strategies [228].

5) THEORETICAL CHARACTERIZATION OF THE BLOCKCHAIN IN NETWORK SLICING SCENARIOS

Blockchain operation has been modeled in the literature in multiple ways at analytical level. In this area, tools that are gaining importance are the batch service queuing and the Markov processes [229], [230]. It is important to study the scenario and application of interest also at theoretical level (in our case, the network slicing one) in order to properly design the Blockchain network so that all the limitations previously discussed can be successfully handled. Aspects which can be theoretically evaluated are the design of the Blockchain in terms of optimal block size, optimal dimension, optimal distribution of information to reduce fork events, etc. An example of this kind of studies, to analyze the stability of the Blockchain and the delays introduced in the provision of service in telecom scenario is the work presented in [231], where a batch queue model allows the analysis of the delay introduced by the Blockchain as a function of the block size, the forks and the timeouts. More work in this area to further understand the theoretical models of the Blockchain in network slicing scenario are of great interest.

6) INTRODUCTION OF BLOCKCHAIN IN NEXT GENERATION ARCHITECTURE

With the purpose to pursue openness and automation in mobile networks, novel architectures for the RAN, based on NFV capabilities are being standardized and require further enhancements in the area of Blockchain to promote its inclusion for automation of procedures like RAN sharing and security purposes. Some preliminary works in this area can be found in [232], [233].

C. LESSONS LEARNED

The above discussion lists the current literature, including applicability issues lack of adaption factors including technological, organizational, and environmental. We also discuss the scalability challenges of Blockchain and high energy consumption and storage limitations.

Lastly, many potential research directions were then identified, including global on-demand service offers and novel business models such as NSaaS. We also highlight that DAML integration with a network slicing platform can open various opportunities for research and applications of DLT-based applications. In addition, we have mentioned that Blockchain and other domains such as AI can benefit from each other specifically for the life-cycle management of deployed network slices. We also discuss the theoretical models of the Blockchain in network slicing scenario, and Blockchain introduction in next-generation architecture (novel architecture for RAN based on NFV capabilities) are potential research directions.

Finally, realizing the potential of Blockchain technology, specifically in network slicing or generally in future networks, requires a framework for design and implementation that begins by thinking first about areas where there is a need to improve security, transparency, or trust among the stakeholders—then followed by consideration of the Blockchain architectures, protocols and other technical considerations to deliver the necessary capabilities.

VII. CONCLUSION

In this paper, we have reviewed the current state-of-the-art related to the use and applicability of Blockchain features for network slicing. In particular, we have started by introducing the network slicing concept and important related literature, and then we have introduced the main concepts in a tutorial fashion in the areas of Blockchain, DLT and smart contracts. We have discussed how we believe that Blockchain technology can enhance and solve key issues related to network slicing. In this context, we have surveyed the available literature in the area of Blockchain integration with network slicing and also how vertical industries are using it on top of the deployed slices.

Our literature review shows that adopting DLT for network slicing is still in its infancy.

Overall, this analysis has shown that Blockchain holds a lot of promise in contexts where multiple stakeholders (or administrative domains) are involved, such as when deploying an End-to-End (E2E) network slice. And this is increasingly relevant in 6G networks, given their increasing complexity.

REFERENCES

[1] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," *Comput. Netw.*, vol. 167, Feb. 2020, Art. no. 106984.

[2] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2429–2453, 3rd Quart., 2018.

[3] I. Afolabi, A. Ksentini, M. Bagaa, T. Taleb, M. Corici, and A. Nakao, "Towards 5G network slicing over multiple-domains," *IEICE Trans. Commun.*, vol. 100, no. 11, pp. 1992–2006, 2017.

[4] 5GPPP. *View on 5G Architecture*. Accessed: Sep. 9, 2020. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2021/08/Architecture-WP-v4.0_forPublicConsultation.pdf

[5] X. Cheng, C. Chen, W. Zhang, and Y. Yang, "5G-enabled cooperative intelligent vehicular (5GenCIV) framework: When Benz meets Marconi," *IEEE Intell. Syst.*, vol. 32, no. 3, pp. 53–59, May/Jun. 2017.

[6] S. K. Rao and R. Prasad, "Impact of 5G technologies on industry 4.0," *Wireless Pers. Commun.*, vol. 100, no. 1, pp. 145–159, May 2018.

[7] H. Ullah, N. G. Nair, A. Moore, C. Nugent, P. Muschamp, and M. Cuevas, "5G communication: An overview of vehicle-to-everything, drones, and healthcare use-cases," *IEEE Access*, vol. 7, pp. 37251–37268, 2019.

[8] G. Caruso, F. Nucci, O. P. Gordo, S. Rizou, J. Magen, G. Agapiou, and P. Trakadas, "Embedding 5G solutions enabling new business scenarios in media and entertainment industry," in *Proc. IEEE 2nd 5G World Forum (5GWF)*, Sep. 2019, pp. 460–464.

[9] S. Li, L. Da Xu, and S. Zhao, "5G Internet of Things: A survey," *J. Ind. Inf. Integr.*, vol. 10, pp. 1–9, Jun. 2018.

[10] Y. Zhuang, T. Qu, J. Wong, W. Wan, M. C. T. Dieck, and T. Jung, "Using 5G mobile to enable the growing slate of VR and AR applications," in *Augmented Reality and Virtual Reality*. New York, NY, USA: Springer, 2020, pp. 185–194.

[11] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, "Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 80–87, May 2017.

[12] R. 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, Oct. 2018.

[13] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and beyond networks: A state of the art survey," *J. Netw. Comput. Appl.*, vol. 166, Sep. 2020, Art. no. 102693.

[14] I. Bashir, *Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained*. Birmingham, U.K.: Packt, 2018.

[15] L. Hughes, Y. K. Dwivedi, S. K. Misra, N. P. Rana, V. Raghavan, and V. Akella, "Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda," *Int. J. Inf. Manage.*, vol. 49, pp. 114–129, Dec. 2019.

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

[17] T. N. Dinh and M. T. Thai, "AI and blockchain: A disruptive integration," *Computer*, vol. 51, no. 9, pp. 48–53, Sep. 2018.

[18] 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.

[19] 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.

[20] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, "Blockchain and machine learning for communications and networking systems," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1392–1431, 2nd Quart., 2020.

[21] 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.

[22] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, 2018.

[23] 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.

[24] S. M. H. Bamakan, A. Motavali, and A. B. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Syst. Appl.*, vol. 154, Sep. 2020, Art. no. 113385.

[25] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, ''Blockchain for 5G and beyond networks: A state of the art survey,'' *J. Netw. Comput. Appl.*, vol. 166, Sep. 2020, Art. no. 102693.

[26] 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.

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

[28] 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.

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

[30] *5G-Transformer Initial System Design*, 5G-Transformer, Deliverable D1.2, New York, NY, USA, 2018.

[31] X. Li, M. Samaka, H. A. Chan, D. Bhamare, L. Gupta, C. Guo, and R. Jain, ''Network slicing for 5G: Challenges and opportunities,'' *IEEE Internet Comput.*, vol. 21, no. 5, pp. 20–27, Sep. 2017.

[32] P. Caballero, A. Banchs, G. De Veciana, and X. Costa-Pérez, ''Network slicing games: Enabling customization in multi-tenant mobile networks,'' *IEEE/ACM Trans. Netw.*, vol. 27, no. 2, pp. 662–675, Apr. 2019.

[33] R. Peter, C. Mannweiler, D. S. Michalopoulos, C. Sartori, V. Sciancalepore, N. Sastry, O. Holland, S. Tayade, B. Han, D. Bega, D. Aziz, and H. Bakker, ''Network slicing to enable scalability and flexibility in 5G mobile networks,'' *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 72–79, May 2017.

[34] GSM Association. *E2E Network Slicing Architecture*. Accessed: Sep. 15, 2020. [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads//NG.127-v1.0-2.pdf

[35] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, ''Network slicing in 5G: Survey and challenges,'' *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 94–100, May 2017.

[36] *Study on Management and Orchestration of Network Slicing for Next Generation Network (Release 15)*, document 3GPP TR 28.801, 3GPP, Jan. 2018.

[37] A. de la Oliva, X. Li, X. Costa-Perez, C. J. Bernardos, P. Bertin, P. Iovanna, T. Deiss, J. Mangues, A. Mourad, C. Casetti, J. E. Gonzalez, and A. Azcorra, ''5G-TRANSFORMER: Slicing and orchestrating transport networks for industry verticals,'' *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 78–84, Aug. 2018.

[38] X. Li, A. Garcia-Saavedra, X. Costa-Perez, C. J. Bernardos, C. Guimaraes, K. Antevski, J. Mangues-Bafalluy, J. Baranda, E. Zeydan, D. Corujo, P. Iovanna, G. Landi, J. Alonso, P. Paixao, H. Martins, M. Lorenzo, J. Ordoñez-Lucena, and D. R. López, ''5Growth: An end-to-end service platform for automated deployment and management of vertical services over 5G networks,'' *IEEE Commun. Mag.*, vol. 59, no. 3, pp. 84–90, Mar. 2021.

[39] *Description of Network Slicing Concept*, NGMN 5GP, NGMN Alliance, Frankfurt, Germany, 2016, vol. 1, no. 1.

[40] *ETSI Network Function Virtualization Industry Specification Group*. Accessed: Oct. 10, 2020. [Online]. Available: https://www.etsi.org/technologies/nfv

[41] M. Ersue, ''ETSI NFV management and orchestration—An overview,'' presented at the IETF, vol. 88, 2013.

[42] *Network Functions Virtualisation (NFV)*, NFV, ETSI, Manage. Orchestration, Sophia Antipolis, France, 2014, vol. 1.

[43] B. Yi, X. Wang, S. K. Das, K. Li, and M. Huang, ''A comprehensive survey of network function virtualization,'' *Comput. Netw.*, vol. 133, pp. 212–262, Mar. 2018.

[44] ETSI. *Network Functions Virtualisation (NFV), Architectural Framework*. Accessed: Oct. 10, 2020. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf#

[45] *Network Functions Virtualisation (NFV) Release 3, ETSI GR NFV-IFA 021 V3.1.1 (2018-01)*. Accessed: Oct. 10, 2020. [Online]. Available: https://docbox.etsi.org/ISG/NFV/open/Publications_pdf/Specs-Reports/NFV-IFA

[46] R. Mijumbi, J. Serrat, J.-L. Gorricho, S. Latré, M. Charalambides, and D. Lopez, ''Management and orchestration challenges in network functions virtualization,'' *IEEE Commun. Mag.*, vol. 54, no. 1, pp. 98–105, Jan. 2016.

[47] ETSI. (2017). *GR NFV-EVE 012—V3.1.1—Network Functions Virtualisation (NFV) Release 3; Evolution and Ecosystem; Report on Network Slicing Support With ETSI NFV Architecture Framework*. [Online]. Available: https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

[48] *Enhancements of Dedicated Core Networks Selection Mechanism (Release 14)*, document, 3GPP, 2016. Accessed: Sep. 20, 2020. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=296

[49] *European Union Horizon 2020 5G Public Private Partnership (5GPPP)*. Accessed: Oct. 10, 2020. [Online]. Available: https://5g-ppp.eu/

[50] B. Sayadi, M. Gramaglia, V. Friderikos, D. von Hugo, P. Arnold, M.-L. Alberi-Morel, M. A. Puente, V. Sciancalepore, I. Digon, and M. R. Crippa, ''SDN for 5G mobile networks: NORMA perspective,'' in *Proc. Int. Conf. Cogn. Radio Oriented Wireless Netw.* New York, NY, USA: Springer, 2016, pp. 741–753.

[51] R. Guerzoni, D. Perez-Caparros, P. Monti, G. Giuliani, J. Melian, and G. Biczók, ''Multi-domain orchestration and management of software defined infrastructures: A bottom-up approach,'' IEEE Commun. Soc., New York, NY, USA, Tech. Rep., 2016.

[52] J. Baranda, J. Mangues, R. Martínez, L. Vettori, K. Antevski, C. J. Bernardos, and X. Li, ''Realizing the network service federation vision: Enabling automated multidomain orchestration of network services,'' *IEEE Veh. Technol. Mag.*, vol. 15, no. 2, pp. 48–57, Jun. 2020.

[53] J. Baranda, L. Vettori, R. Martínez, and J. Mangues, ''A mobile transport platform interconnecting VNFs over a multi-domain optical/wireless network: Design and implementation,'' in *Proc. 24th Int. Conf. Opt. Netw. Design Modeling (ONDM)*, Castelldefels, Spain, May 2020.

[54] C. Papagianni, J. Mangues-Bafalluy, P. Bermudez, S. Barmpounakis, D. De Vleeschauwer, J. Brenes, E. Zeydan, C. Casetti, C. Guimaraes, P. Murillo, A. Garcia-Saavedra, D. Corujo, and T. Pepe, ''5Growth: AI-driven 5G for automation in vertical industries,'' in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2020, pp. 17–22.

[55] A. Sunyaev, ''Distributed ledger technology,'' in *Internet Computing*. New York, NY, USA: Springer, 2020, pp. 265–299.

[56] S. Yrjölä, ''How could blockchain transform 6G towards open ecosystemic business models?'' in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2020, pp. 1–6.

[57] Y. Du, Z. Wang, and V. C. M. Leung, ''Blockchain-enabled edge intelligence for IoT: Background, emerging trends and open issues,'' *Future Internet*, vol. 13, no. 2, p. 48, Feb. 2021.

[58] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, ''The role of blockchain in 6G: Challenges, opportunities and research directions,'' in *Proc. 2nd 6G Wireless Summit (6G SUMMIT)*, Mar. 2020, pp. 1–5.

[59] H. Xu, P. V. Klaine, O. Onireti, B. Cao, M. Imran, and L. Zhang, ''Blockchain-enabled resource management and sharing for 6G communications,'' 2020, *arXiv:2003.13083*.

[60] T. Nguyen, N. Tran, L. Loven, J. Partala, M.-T. Kechadi, and S. Pirttikangas, ''Privacy-aware blockchain innovation for 6G: Challenges and opportunities,'' in *Proc. 2nd 6G Wireless Summit (6G SUMMIT)*, Mar. 2020, pp. 1–5.

[61] A. Murphy, ''An analysis of the financial crisis of 2008: Causes and solutions,'' Elsevier, Amsterdam, The Netherlands, Tech. Rep., 2008.

[62] S. Nakamoto, ''Bitcoin: A peer-to-peer electronic cash system,'' Manubot, Tech. Rep., 2019.

[63] Satoshi Nakamoto Institute. *Bitcoin Open Source Implementation of P2P Currency*. Accessed: Apr. 26, 2021. [Online]. Available: https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/1/

[64] N. Popper, ''Decoding the enigma of Satoshi Nakamoto and the birth of Bitcoin,'' New York Times, 2015.

[65] P. Lemieux, ''Who is Satoshi Nakamoto?'' *Regulation*, vol. 36, no. 3, pp. 14–16, 2013.

[66] *Bitcoin's Origin Story Remains Shrouded in Mystery. Here's Why it Matters*. Accessed: Apr. 26, 2021. [Online]. Available: https://www.cnbc.com

[67] N. Szabo, ''The idea of smart contracts,'' Nick Szabo's Papers Concise Tuts., Tech. Rep., 1997, vol. 6.

[68] D. Efanov and P. Roschin, ''The all-pervasiveness of the blockchain technology,'' *Proc. Comput. Sci.*, vol. 123, pp. 116–121, Jan. 2018.

[69] N. Abdullah, A. Hakansson, and E. Moradian, ''Blockchain based approach to enhance big data authentication in distributed environment,'' in *Proc. 9th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2017, pp. 887–892.

[70] K. Okupski, ''Bitcoin developer reference,'' Enetium, Eindhoven, The Netherlands, Tech. Rep., 2014. [Online]. Available: https://enetium.com/ and https://enetium.com/resources/Bitcoin.pdf

[71] P. T. Duy, D. T. T. Hien, D. H. Hien, and V.-H. Pham, "A survey on opportunities and challenges of blockchain technology adoption for revolutionary innovation," in *Proc. 9th Int. Symp. Inf. Commun. Technol.*, 2018, pp. 200–207.

[72] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2017, pp. 2567–2572.

[73] J. P. Conley, "Encryption, hashing, PPK, and blockchain: A simple introduction," Dept. Econ., Vanderbilt Univ., Nashville, TN, USA, Tech. Rep., 2019.

[74] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, Jun. 2017, pp. 557–564.

[75] L. W. Cong and Z. He, "Blockchain disruption and smart contracts," *Rev. Financial Stud.*, vol. 32, no. 5, pp. 1754–1797, Apr. 2019.

[76] S. S. Gupta, *Blockchain*. Hoboken, NJ, USA: Wiley, 2017.

[77] M. B. Taylor, "The evolution of Bitcoin hardware," *Computer*, vol. 50, no. 9, pp. 58–66, 2017.

[78] *Ethereum (ETH) Blockchain Explorer*. Accessed: May 6, 2021. [Online]. Available: https://etherscan.io/

[79] *Bitcoin Block Reward Halving Countdown*. Accessed: May 6, 2021. [Online]. Available: https://www.bitcoinblockhalf.com/

[80] D. Guegan, "Public blockchain versus private blockhain," Centre d'Economie de la Sorbonne, Paris, France, Tech. Rep., Apr. 2017. [Online]. Available: https://halshs.archives-ouvertes.fr/halshs-01524440

[81] P. Tasca and C. J. Tessone, "Taxonomy of blockchain Technologies. Principles of identification and classification," 2017, *arXiv:1708.04872*.

[82] S. Perera, S. Nanayakkara, M. N. N. Rodrigo, S. Senaratne, and R. Weinand, "Blockchain technology: Is it hype or real in the construction industry?" *J. Ind. Inf. Integr.*, vol. 17, Mar. 2020, Art. no. 100125.

[83] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics Informat.*, vol. 36, pp. 55–81, Mar. 2019.

[84] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Dec. 2017.

[85] J. Golosova and A. Romanovs, "The advantages and disadvantages of the blockchain technology," in *Proc. IEEE 6th Workshop Adv. Inf., Electron. Electr. Eng. (AIEEE)*, Nov. 2018, pp. 1–6.

[86] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *Proc. 41st Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, May 2018, pp. 1545–1550.

[87] H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi, and A. Rindos, "Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric)," in *Proc. IEEE 36th Symp. Reliable Distrib. Syst. (SRDS)*, Sep. 2017, pp. 253–255.

[88] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 398–461, 2002.

[89] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in *Proc. Annu. Tech. Conf.*, 2014, pp. 305–319.

[90] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending Bitcoin's proof of work via proof of stake [extended abstract] Y," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 3, pp. 34–37, 2014.

[91] K. Karantias, A. Kiayias, and D. Zindros, "Proof-of-burn," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* San Francisco, CA, USA: Springer, 2020, pp. 523–540.

[92] Y. Chen, H. Li, K. Li, and J. Zhang, "An improved P2P file system scheme based on IPFS and blockchain," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2017, pp. 2652–2657.

[93] S. Alrubei, E. Ball, and J. Rigelsford, "HDPoA: Honesty-based distributed proof of authority via scalable work consensus protocol for IoT-blockchain applications," Elsevier, Amsterdam, The Netherlands, Tech. Rep.

[94] S. Latif, Z. Idrees, Z. E. Huma, and J. Ahmad, "Blockchain technology for the industrial Internet of Things: A comprehensive survey on security challenges, architectures, applications, and future research directions," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 11, Nov. 2021, Art. no. e4337.

[95] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," in *Concurrency: The Works of Leslie Lamport*. New York, NY, USA: ACM, 2019, pp. 203–226.

[96] F. Saleh, "Blockchain without waste: Proof-of-stake," *Rev. Financial Stud.*, vol. 34, no. 3, pp. 1156–1190, 2021.

[97] C. N. Samuel, S. Glock, F. Verdier, and P. Guitton-Ouhamou, "Choice of Ethereum clients for private blockchain: Assessment from proof of authority perspective," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2021, pp. 1–5.

[98] L. Wiesflecker. *What is Proof of Activity?* Accessed: Jan. 8, 2022. [Online]. Available: https://medium.datadriveninvestor.com/what-is-proof-of-activity-1dc176db213

[99] S. J. Alsunaidi and F. A. Alhaidari, "A survey of consensus algorithms for blockchain technology," in *Proc. Int. Conf. Comput. Inf. Sci. (ICCIS)*, Apr. 2019, pp. 1–6.

[100] L. Wiesflecker. *What is Proof of Burn (PoB)?* Accessed: Jan. 8, 2022. [Online]. Available: https://medium.datadriveninvestor.com/what-is-proof-of-burn-pob-e8f7e7dfbbfa

[101] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (PoET)," in *Proc. Int. Symp. Stabilization, Saf., Secur. Distrib. Syst.* New York, NY, USA: Springer, 2017, pp. 282–297.

[102] A. Corso, "Performance analysis of proof-of-elapsed-time (PoET) consensus in the Sawtooth blockchain framework," Ph.D. dissertation, Dept. Comput. Inf. Sci., Univ. Oregon, Eugene, OR, USA, 2019.

[103] A. Hayes. *Proof of Capacity*. Accessed: Jan. 8, 2022. [Online]. Available: https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp

[104] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," *Future Gener. Comput. Syst.*, vol. 105, pp. 475–491, Apr. 2020.

[105] A. A. Zarir, G. A. Oliva, Z. M. Jiang, and A. E. Hassan, "Developing cost-effective blockchain-powered applications: A case study of the gas usage of smart contract transactions in the Ethereum blockchain platform," *ACM Trans. Softw. Eng. Methodol.*, vol. 30, no. 3, pp. 1–38, May 2021.

[106] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts (SoK)," in *Proc. Int. Conf. Princ. Secur. Trust*. New York, NY, USA: Springer, 2017, pp. 164–186.

[107] A. M. Antonopoulos and G. Wood, *Mastering Ethereum: Building Smart Contracts and DApps*. Sebastopol, CA, USA: O'Reilly Media, 2018.

[108] C. Dannen, *Introducing Ethereum and Solidity*, vol. 1. New York, NY, USA: Springer, 2017.

[109] Y. Huang, H. Wang, L. Wu, G. Tyson, X. Luo, R. Zhang, X. Liu, G. Huang, and X. Jiang, "Characterizing EOSIO blockchain," 2020, *arXiv:2002.05369*.

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

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

[112] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers*, 2016, vol. 310, no. 4, pp. 1–4.

[113] S. Zhang, E. Zhou, B. Pi, J. Sun, K. Yamashita, and Y. Nomura, "A solution for the risk of non-deterministic transactions in hyperledger fabric," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2019, pp. 253–261.

[114] R. G. Brown, J. Carlyle, I. Grigg, and M. Hearn, "Corda: An introduction," *R3 CEV*, vol. 1, p. 15, Aug. 2016.

[115] J. M. Chase, "A permissioned implementation of ethereum," Quorum, Tech. Rep. Accessed Feb. 20, 2018.

[116] T.-T. Kuo, H. Z. Rojas, and L. Ohno-Machado, "Comparison of blockchain platforms: A systematic review and healthcare examples," *J. Amer. Med. Inform. Assoc.*, vol. 26, no. 5, pp. 462–478, 2019.

[117] J. Polge, J. Robert, and Y. Le Traon, "Permissioned blockchain frameworks in the industry: A comparison," *ICT Exp.*, vol. 7, no. 2, pp. 229–233, Jun. 2021.

[118] E. Elrom, "EOS.IO wallets and smart contracts," in *The Blockchain Developer*. New York, NY, USA: Springer, 2019, pp. 213–256.

[119] (Mar. 2018). *EOS.IO Technical White Paper V2*. Accessed: Jun. 16, 2021. [Online]. Available: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

[120] J. Kwon, "TenderMint: Consensus without mining," Tendermint, Fall, Draft Version 0.6, Tech. Rep., 2014, vol. 1, no. 11.

[121] A. Amoordon and H. Rocha, "Presenting TenderMint: Idiosyncrasies, weaknesses, and good practices," in *Proc. IEEE Int. Workshop Blockchain Oriented Softw. Eng. (IWBOSE)*, Feb. 2019, pp. 44–49.

[122] COSMOS. *COSMOS/WHITEPAPER.md at Master*. Accessed: Apr. 20, 2021. [Online]. Available: https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md

[123] S. Schulte, M. Sigwart, P. Frauenthaler, and M. Borkowski, "Towards blockchain interoperability," in *Proc. Int. Conf. Bus. Process Manage.* New York, NY, USA: Springer, 2019, pp. 3–10.

[124] L. X. Lin, "Deconstructing decentralized exchanges," *Stanford J. Blockchain Law Policy*, vol. 2, Jan. 2019.

[125] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," Polkadot, Switzerland, White Paper, 2016.

[126] A. Chauhan, O. P. Malviya, M. Verma, and T. S. Mor, "Blockchain and scalability," in *Proc. IEEE Int. Conf. Softw. Quality, Rel. Secur. Companion (QRS-C)*, Jul. 2018, pp. 122–128.

[127] A. Cevallos and A. Stewart, "A verifiably secure and proportional committee election rule," 2020, *arXiv:2004.12990*.

[128] A. Shahraki, M. Abbasi, M. J. Piran, and A. Taherkordi, "A comprehensive survey on 6G networks: Applications, core services, enabling technologies, and future challenges," 2021, *arXiv:2101.12475*.

[129] M. W. Akhtar, S. A. Hassan, R. Ghaffar, H. Jung, S. Garg, and M. S. Hossain, "The shift to 6G communications: Vision and requirements," *Hum.-Centric Comput. Inf. Sci.*, vol. 10, no. 1, pp. 1–27, Dec. 2020.

[130] A. Adhiappan, A. Chernetsov, M. Fenomenov, U. Karabudak, A. Korabanova, S. Kislyakov, L. Beller, M. Nati, B. Radier, A. Sushkov, A. Ustimenko, A. Vedin, O. Yurlov, T. Meriem, V. Messié, and N. L. Omnes, "Federated CSPs marketplace: A DLT-based data trust enabling business assurance for CSPs platforms federation," TMForum, USA, Tech. Rep., Nov. 2020.

[131] *Blockchain-Based Telecom Infrastructure Marketplace Enables 'Pop-Up' Networks and on-the-Fly Business Models*. Accessed: Oct. 6, 2021. [Online]. Available: https://inform.tmforum.org/

[132] E. Kapassa, M. Touloupos, D. Kyriazis, and M. Themistocleous, "A smart distributed marketplace," in *Proc. Eur., Medit., Middle Eastern Conf. Inf. Syst.* New York, NY, USA: Springer, 2019, pp. 458–468.

[133] *Blockchain-Based Telecom Infrastructure Marketplace*. Accessed: Oct. 6, 2021. [Online]. Available: https://www.tmforum.org/blockchain-based-telecom-infrastructure-marketplace/

[134] M. Jiang, M. Condoluci, and T. Mahmoodi, "Network slicing in 5G: An auction-based model," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[135] V. A. Cunha, E. da Silva, M. B. de Carvalho, D. Corujo, J. P. Barraca, D. Gomes, L. Z. Granville, and R. L. Aguiar, "Network slicing security: Challenges and directions," *Internet Technol. Lett.*, vol. 2, no. 5, p. e125, Sep. 2019.

[136] PDL and ETSI. (2021). *GR PDL 004—V1.1.1—Permissioned Distributed Ledgers (PDL) Smart Contracts System Architecture and Functional Specification*. [Online]. Available: https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

[137] M. Xevgenis, D. G. Kogias, P. Karkazis, H. C. Leligou, and C. Patrikakis, "Application of blockchain technology in dynamic resource management of next generation networks," *Information*, vol. 11, no. 12, p. 570, Dec. 2020.

[138] 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./Dec. 2017.

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

[140] M. Keller, "Design and implementation of a blockchain-based trusted VNF package repository," Ph.D. dissertation, CSG@IFI, Univ. Zürich, Zürich, Switzerland, 2019.

[141] P. Alemany, R. Vilalta, R. Muñoz, R. Casellas, and R. Marínez, "Peer-to-peer blockchain-based NFV service platform for end-to-end network slice orchestration across multiple NFVI domains," in *Proc. IEEE 3rd 5G World Forum (5GWF)*, Sep. 2020, pp. 151–156.

[142] T. Faisal, D. D. F. Maesa, N. Sastry, and S. Mangiante, "AJIT: Accountable just-in-time network resource allocation with smart contracts," in *Proc. ACM MobiArch 15th Workshop Mobility Evolving Internet Archit.*, Sep. 2020, pp. 48–53.

[143] K. Antevski and C. J. Bernardos, "Federation of 5G services using distributed ledger technologies," *Internet Technol. Lett.*, vol. 3, no. 6, Nov. 2020, Art. no. e193.

[144] G. A. F. Rebello, G. F. Camilo, L. G. C. Silva, L. C. B. Guimaraes, L. A. C. de Souza, I. D. Alvarenga, and O. C. M. B. Duarte, "Providing a sliced, secure, and isolated software infrastructure of virtual functions through blockchain technology," in *Proc. IEEE 20th Int. Conf. High Perform. Switching Routing (HPSR)*, May 2019, pp. 1–6.

[145] 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 Networking)*, May 2019, pp. 1–9.

[146] J. Backman, S. Yrjölä, K. Valtanen, and O. Mämmelä, "Blockchain network slice broker in 5G: Slice leasing in factory of the future use case," in *Proc. Internet Things Bus. Models, Users, Netw.*, Nov. 2017, pp. 1–8.

[147] L. Zanzi, A. Albanese, V. Sciancalepore, and X. Costa-Pérez, "NSBchain: A secure blockchain framework for network slicing brokerage," 2020, *arXiv:2003.07748*.

[148] B. Nour, A. Ksentini, N. Herbaut, P. A. Frangoudis, and H. Moungla, "A blockchain-based network slice broker for 5G services," *IEEE Netw. Lett.*, vol. 1, no. 3, pp. 99–102, Sep. 2019.

[149] N. Afraz and M. Ruffini, "5G network slice brokering: A distributed blockchain-based market," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2020, pp. 23–27.

[150] M. A. Togou, T. Bi, K. Dev, K. McDonnell, A. Milenovic, H. Tewari, and G.-M. Muntean, "A distributed blockchain-based broker for efficient resource provisioning in 5G networks," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2020, pp. 1485–1490.

[151] *5G; Management and Orchestration; Concepts, Use Cases and Requirements*, document TS 128 530, 3GPP TS 28.530, Version 15.3.0, ETSI, 2020. [Online]. Available: https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

[152] D. Bega, M. Gramaglia, A. Banchs, V. Sciancalepore, K. Samdanis, and X. Costa-Perez, "Optimising 5G infrastructure markets: The business of network slicing," in *Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM)*, May 2017, pp. 1–9.

[153] *5G; Management and Orchestration; Concepts, Use Cases and Requirements*, document TS 128 530, 3GPP TS 28.530, Version 15.1.0, Release 15, ETSI, 2019. [Online]. Available: https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

[154] A. Devlic, A. Hamidian, D. Liang, M. Eriksson, A. Consoli, and J. Lundstedt, "NESMO: Network slicing management and orchestration framework," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*. Piscataway, NJ, USA: Institute of Electrical and Electronics Engineers, May 2017, pp. 1202–1208.

[155] *Permissioned Distributed Ledger (PDL); Application Scenarios*, Standard ETSI GR PDL 003, Version 1.1.1, PDL, 2020. [Online]. Available: https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

[156] *Enhanced Reader*, Standard ETSI GR PDL 001, Version 0.0.9, ETSI, 2020.

[157] I. P. Chochliouros, A. S. Spiliopoulou, P. Lazaridis, A. Dardamanis, Z. Zaharis, and A. Kostopoulos, "Dynamic network slicing: Challenges and opportunities," in *Proc. IFIP Int. Conf. Artif. Intell. Appl. Innov.* New York, NY, USA: Springer, 2020, pp. 47–60.

[158] S. Fan, H. Zhang, Y. Zeng, and W. Cai, "Hybrid blockchain-based resource trading system for federated learning in edge computing," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2252–2264, Feb. 2021.

[159] I. Koutsopoulos and G. Iosifidis, "Auction mechanisms for network resource allocation," in *Proc. 8th Int. Symp. Modeling Optim. Mobile, Ad Hoc, Wireless Netw.*, May/Jun. 2010, pp. 554–563.

[160] M. Deloitte, "Blockchain@Media: A new game changer for the media industry," Blockchain Inst., Toronto, ON, Canada, Tech. Rep., 2017.

[161] A. Dutra, A. Tumasjan, and I. M. Welpe, "Blockchain is changing how media and entertainment companies compete," *MIT Sloan Manage. Rev.*, vol. 60, no. 1, pp. 39–45, Fall 2018. [Online]. Available: https://search.proquest.com/docview/2131141868?accountid=14501

[162] H. S. Galal, M. ElSheikh, and A. M. Youssef, "An efficient micropayment channel on Ethereum," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. New York, NY, USA: Springer, 2019, pp. 211–218.

[163] R. Matulionyte, "Can copyright be tokenized?" Elsevier, Amsterdam, The Netherlands, Tech. Rep., 2019.

[164] *Everdreamsoft*. Accessed: Aug. 1, 2022. [Online]. Available: https://www.everdreamsoft.com/

[165] *VIBEHub.io*. Accessed: Aug. 1, 2022. [Online]. Available: https://www.vibehub.io/

[166] O. Esteban, M. Ariel, J. Yemel, and A. Manuel, "Decentraland white paper," Decentraland, Tech. Rep., 2017.

[167] I. J. Jensen, D. F. Selvaraj, and P. Ranganathan, "Blockchain technology for networked swarms of unmanned aerial vehicles (UAVs)," in *Proc. IEEE 20th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2019, pp. 1–7.

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

[169] *AIAA SciTech Forum*, NTRS, San Diego, CA, USA, 2019.

[170] S. Kar, V. Kasimsetty, S. Barlow, and S. Rao, "Risk analysis of blockchain application for aerospace records management," SAE Tech. Paper 2019-01-1344, Mar. 2019, doi: 10.4271/2019-01-1344.

[171] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *J. Amer. Med. Inform. Assoc.*, vol. 24, no. 6, pp. 1211–1220, 2017, doi: 10.1093/jamia/ocx068.

[172] M. Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, p. 470, Oct. 2018.

[173] J. M. Roman-Belmonte, H. de la Corte-Rodriguez, and E. C. Rodriguez-Merchan, "How blockchain technology can change medicine," *Postgraduate Med.*, vol. 130, no. 4, pp. 420–427, May 2018, doi: 10.1080/00325481.2018.1472996.

[174] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 135, pp. 62–75, Jun. 2019.

[175] A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, "Blockchain in healthcare and health sciences—A scoping review," *Int. J. Med. Informat.*, vol. 134, Feb. 2020, Art. no. 104040.

[176] C. Pirtle and J. Ehrenfeld, "Blockchain for healthcare: The next generation of medical records?" Springer, New York, NY, USA, Tech. Rep., 2018.

[177] A. F. Hussein, N. Arunkumar, G. Ramírez-González, E. Abdulhay, J. M. R. Tavares, and V. H. C. de Albuquerque, "A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform," *Cogn. Syst. Res.*, vol. 52, pp. 1–11, Dec. 2018.

[178] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-based medical records secure storage and medical service framework," *J. Med. Syst.*, vol. 43, no. 1, p. 5, Jan. 2019.

[179] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in *Proc. AMIA Annu. Symp.* Bethesda, MD, USA: American Medical Informatics Association, 2017, p. 650.

[180] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare: 'MedRec' prototype for electronic health records and medical research data," in *Proc. IEEE Open Big Data Conf.*, vol. 13, Aug. 2016, p. 13.

[181] Y. R. Park, E. Lee, W. Na, S. Park, Y. Lee, and J.-H. Lee, "Is blockchain technology suitable for managing personal health records? Mixed-methods study to test feasibility," *J. Med. Internet Res.*, vol. 21, no. 2, Feb. 2019, Art. no. e12533.

[182] L. Ismail, H. Materwala, and S. Zeadally, "Lightweight blockchain for healthcare," *IEEE Access*, vol. 7, pp. 149935–149951, 2019.

[183] F. Jamil, L. Hang, K. Kim, and D. Kim, "A novel medical blockchain model for drug supply chain integrity management in a smart hospital," *Electronics*, vol. 8, no. 5, p. 505, Apr. 2019.

[184] R. Kumar and R. Tripathi, "Traceability of counterfeit medicine supply chain through blockchain," in *Proc. 11th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2019, pp. 568–570.

[185] M. Sahoo, S. S. Singhar, and S. S. Sahoo, "A blockchain based model to eliminate drug counterfeiting," in *Machine Learning and Information Processing*. New York, NY, USA: Springer, 2020, pp. 213–222.

[186] R. Anand, K. Niyas, S. Gupta, and S. Revathy, "Anti-counterfeit on medicine detection using blockchain technology," in *Inventive Communication and Computational Technologies*. New York, NY, USA: Springer, 2020, pp. 1223–1232.

[187] M. Malinverno, J. Mangues-Bafalluy, C. E. Casetti, C. F. Chiasserini, M. Requena-Esteso, and J. Baranda, "An edge-based framework for enhanced road safety of connected cars," *IEEE Access*, vol. 8, pp. 58018–58031, 2020.

[188] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, p. 91, Aug. 2015.

[189] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.

[190] D. Lu, P. Moreno-Sanchez, A. Zeryihun, S. Bajpayi, S. Yin, K. Feldman, J. Kosofsky, P. Mitra, and A. Kate, "Reducing automotive counterfeiting using blockchain: Benefits and challenges," in *Proc. IEEE Int. Conf. Decentralized Appl. Infrastruct. (DAPPCON)*, Apr. 2019, pp. 39–48.

[191] S.-K. Kim, C. Y. Yeun, E. Damiani, Y. Al-Hammadi, and N.-W. Lo, "New blockchain adoptation for automotive security by using systematic innovation," in *Proc. IEEE Transp. Electrific. Conf. Expo, Asia–Pacific (ITEC Asia-Pacific)*, May 2019, pp. 1–4.

[192] S.-O. Lee, H. Jung, and B. Han, "Security assured vehicle data collection platform by blockchain: Service provider's perspective," in *Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2019, pp. 265–268.

[193] Bosch Media Service. *Artificial Intelligence: Bosch Teaches Cars How to Learn and Take Appropriate Action*. Accessed: Sep. 9, 2020. [Online]. Available: https://www.boschpresse.de

[194] *How Blockchain Can Help to Prevent Odometer Fraud*. Accessed: Sep. 9, 2020. [Online]. Available: https://blog.bosch-si.com

[195] C. F. Chiasserini, P. Giaccone, G. Malnati, M. Macagno, and G. Sviridov, "Blockchain-based mobility verification of connected cars," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2020, pp. 1–6.

[196] M. Singh and S. Kim, "Branch based blockchain technology in intelligent vehicle," *Comput. Netw.*, vol. 145, pp. 219–231, Nov. 2018.

[197] N. Hackius and M. Petersen, "Blockchain in logistics and supply chain: Trick or treat?" in *Proc. Hamburg Int. Conf. Logistics (HICL)*, vol. 23. Berlin, Germany: Epubli GmbH, 2017, pp. 3–18.

[198] G. Perboli, S. Musso, and M. Rosano, "Blockchain in logistics and supply chain: A lean approach for designing real-world use cases," *IEEE Access*, vol. 6, pp. 62018–62028, 2018.

[199] I. M. Ar, I. Erol, I. Peker, A. I. Ozdemir, T. D. Medeni, and I. T. Medeni, "Evaluating the feasibility of blockchain in logistics operations: A decision framework," *Expert Syst. Appl.*, vol. 158, Nov. 2020, Art. no. 113543. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0957417420303675

[200] K. Wüst and A. Gervais, "Do you need a blockchain?" in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Jun. 2018, pp. 45–54.

[201] T. Swanson. *Blockchain Key Challenges*. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-key-challenges.pdf

[202] T. Clohessy and T. Acton, "Investigating the influence of organizational factors on blockchain adoption," *Ind. Manage. Data Syst.*, vol. 119, no. 7, pp. 1457–1491, Aug. 2019.

[203] *2020 Global Blockchain Survey*. Accessed: Oct. 2, 2020. [Online]. Available: https://www2.deloitte.com

[204] G. Karame, "On the security and scalability of Bitcoin's blockchain," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 1861–1862.

[205] *Mobile Network Codes (MNC) for the International Identification Plan for Public Networks and Subscriptions (According to Recommendation ITU-T E.212 (09/2016))*. Accessed: Sep. 30, 2020. [Online]. Available: https://www.itu.int/pub/T-SP-E.212B-2018

[206] *Bitcoin Consumes More Energy Than Switzerland, According to New Estimate—The Verge*. Accessed: Oct. 1, 2020. [Online]. Available: https://www.theverge.com

[207] P. Fairley, "Blockchain world—Feeding the blockchain beast if Bitcoin ever does go mainstream, the electricity needed to sustain it will be enormous," *IEEE Spectr.*, vol. 54, no. 10, pp. 36–59, Oct. 2017.

[208] J. Sedlmeir, H. U. Buhl, G. Fridgen, and R. Keller, "The energy consumption of blockchain technology: Beyond myth," *Bus. Inf. Syst. Eng.*, vol. 62, pp. 599–608, Jun. 2020.

[209] T. Hepp, M. Sharinghousen, P. Ehret, A. Schoenhals, and B. Gipp, "On-chain vs. off-chain storage for supply- and blockchain integration," *Inf. Technol.*, vol. 60, nos. 5–6, pp. 283–291, Dec. 2018.

[210] S. Wilkinson, T. Boshevski, J. Brandoff, and V. Buterin, "Storj a peer-to-peer cloud storage network," Storj (storj.io), USA, Tech. Rep., 2014.

[211] D. Vorick and L. Champine, "Sia: Simple decentralized storage," Nebulous, Boston, MA, USA, Tech. Rep., 2014.

[212] J. Benet, "IPFS—Content addressed, versioned, P2P file system," 2014, *arXiv:1407.3561*.

[213] R. Kumar, N. Marchang, and R. Tripathi, "Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and blockchain," in *Proc. Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2020, pp. 1–5.

[214] H.-S. Huang, T.-S. Chang, and J.-Y. Wu, "A secure file sharing system based on IPFS and blockchain," in *Proc. 2nd Int. Electron. Commun. Conf.*, Jul. 2020, pp. 96–100.

[215] S. Vimal and S. K. Srivatsa, "A new cluster P2P file sharing system based on IPFS and blockchain technology," *J. Ambient Intell. Hum. Comput.*, pp. 1–7, Sep. 2019.

[216] S. S. Hasan, N. H. Sultan, and F. A. Barbhuiya, "Cloud data provenance using IPFS and blockchain technology," in *Proc. 7th Int. Workshop Secur. Cloud Comput.*, 2019, pp. 5–12.

[217] X. Zhou, R. Li, T. Chen, and H. Zhang, "Network slicing as a service: Enabling enterprises' own software-defined cellular networks," *IEEE Commun. Mag.*, vol. 54, no. 7, pp. 146–153, Jul. 2016.

[218] M. Ayaz, M. Ammad-Uddin, Z. Sharif, A. Mansour, and E. M. Aggoune, "Internet-of-Things (IoT)-based smart agriculture: Toward making the fields talk," *IEEE Access*, vol. 7, pp. 129551–129583, 2019.

[219] V. Frascolla, F. Miatton, G. K. Tran, K. Takinami, A. De Domenico, E. C. Strinati, K. Koslowski, T. Haustein, K. Sakaguchi, S. Barbarossa, and S. Barberis, "5G-MiEdge: Design, standardization and deployment of 5G phase II technologies: MEC and mmWaves joint development for Tokyo 2020 Olympic games," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Sep. 2017, pp. 54–59.

[220] P. D. Maciel, F. L. Verdi, P. Valsamas, I. Sakellariou, L. Mamatas, S. Petridou, P. Papadimitriou, D. Moura, A. I. Swapna, B. Pinheiro, and S. Clayman, "A marketplace-based approach to cloud network slice composition across multiple domains," in *Proc. IEEE Conf. Netw. Softw. (NetSoft)*, Jun. 2019, pp. 480–488.

[221] A. I. Swapna, R. V. Rosa, C. E. Rothenberg, I. Sakellariou, L. Mamatas, and P. Papadimitriou, "Towards a marketplace for multi-domain cloud network slicing: Use cases," in *Proc. ACM/IEEE Symp. Architectures Netw. Commun. Syst. (ANCS)*, Sep. 2019, pp. 1–4.

[222] C. J. Bernardos, B. P. Gerö, M. Di Girolamo, A. Kern, B. Martini, and I. Vaishnavi, "5GEx: Realising a Europe-wide multi-domain framework for software-defined infrastructures," *Trans. Emerg. Telecommun. Technol.*, vol. 27, no. 9, pp. 1271–1280, Sep. 2016.

[223] D. Nasonov, A. A. Visheratin, and A. Boukhanovsky, "Blockchain-based transaction integrity in distributed big data marketplace," in *Proc. Int. Conf. Comput. Sci.* New York, NY, USA: Springer, 2018, pp. 569–577.

[224] *DApp Statistics—State of the DApps*. Accessed: Oct. 6, 2020. [Online]. Available: https://www.stateofthedapps.com/stats

[225] DappReview. *2020 Q2 Dapp Market Report by DappReview*. Accessed: Oct. 6, 2020. [Online]. Available: https://dapp.review/article/274/2020-Q2-Dapp-Market-Report-by-DappReview

[226] S. Kfir and C. Fournier, "DAML: The contract language of distributed ledgers," *Commun. ACM*, vol. 62, no. 9, pp. 48–54, Aug. 2019.

[227] *Digital-Asset/DAML: The DAML Smart Contract Language*. Accessed: Oct. 2, 2020. [Online]. Available: https://github.com/digital-asset/daml

[228] M. H. U. Rehman, A. Batool, C. S. Liew, Y.-W. Teh, and A. U. R. Khan, "Execution models for mobile data analytics," *IT Prof.*, vol. 19, no. 3, pp. 24–30, 2017.

[229] Q.-L. Li, J.-Y. Ma, Y.-X. Chang, F.-Q. Ma, and H.-B. Yu, "Markov processes in blockchain systems," *Comput. Social Netw.*, vol. 6, no. 1, pp. 1–28, Dec. 2019.

[230] Q.-L. Li, J.-Y. Ma, and Y.-X. Chang, "Blockchain queue theory," in *Proc. Int. Conf. Comput. Social Netw.* New York, NY, USA: Springer, 2018, pp. 25–40.

[231] F. Wilhelmi and L. Giupponi, "Discrete-time analysis of wireless blockchain networks," in *Proc. IEEE PIMRC*, Sep. 2021, pp. 1011–1017.

[232] H. Xu, L. Zhang, Y. Sun, and I. Chih-Lin, "BE-RAN: Blockchain-enabled open RAN with decentralized identity management and privacy-preserving communication," 2021, *arXiv:2101.10856*. Accessed: Jun. 30, 2021.

[233] L. Giupponi and F. Wilhelmi, "Blockchain-enabled network sharing for O-RAN in 5G and beyond," 2021, *arXiv:2107.02005*. Accessed: Jun. 30, 2021.

FARHANA JAVED received the bachelor's degree from COMSATS University, in 2016, and the master's degree in computer applied technology from the Huazhong University of Science and Technology (HUST), Wuhan, China, in 2019. She is currently pursuing the Ph.D. degree with the Communication Networks Division, Centre Tecnològic de Telecomunicacions de Catalunya (CTTC/CERCA). She is also a Research Assistant with the Communication Networks Division, Centre Tecnològic de Telecomunicacions de Catalunya (CTTC/CERCA). She joined CTTC, in December 2019, as a Formación Personal Investigador (FPI) which is a fellowship funded by Spanish MINECO Grant, to carry out fundamental and applied research on the project 5G-REFINE (Resource Efficient 5G Networks).

KIRIL ANTEVSKI received the B.S. degree in telecommunication engineering from Ss. Cyril and Methodius University in Skopje, Macedonia, in 2012, and the M.S. degree in telecommunication engineering from the Politecnico di Milano, Milan, Italy, in 2016. He is currently pursuing the Ph.D. degree in telematics engineering with University Carlos III Madrid (UC3M), Spain. His research interests include the development of mechanisms to integrate and enhance NFV and MEC for 5G networks in dynamic and heterogeneous environments.

JOSEP MANGUES-BAFALLUY received the Graduate and Ph.D. degrees in telecommunications engineering from the Technical University of Catalunya (UPC), in 1996 and 2003, respectively. He has over 20 years of experience in the networking field. He was also a Researcher and an Assistant Professor at UPC, from 1996 to 2003. He has been the Research Director and the Head of the Communication Networks Division, Telecommunications Technological Center of Catalunya (CTTC), since 2013. He held various roles in several public funded and industrial research projects (e.g., EU 5Growth and 5G-REFINE (PI)) on virtualization and automated network management, also involving verticals (e.g., automotive and eHealth). His research interests include mobile networks, machine learning for network optimization, and network function virtualization. He was the Vice-Chair of IEEE WCNC 2018, in Barcelona.

LORENZA GIUPPONI received the Ph.D. degree from UPC, Barcelona, Spain, in 2007. In 2003, she joined the Radio Communications Group, UPC, with a grant of the Spanish Ministry of Education, where she was an Assistant Professor, from 2006 to 2007. In September 2007, she joined the CTTC, where she was a Research Director with the Communication Networks Division, Mobile Networks Department. Since 2007, she has been a member of the Executive Committee of CTTC, where she acts as the Director of Institutional Relations. She was a co-recipient of the IEEE CCNC 2010, the IEEE 3rd International Workshop on Indoor and Outdoor Femto Cells 2011, and the IEEE WCNC 2018 Best Paper Award. Since 2015, she has been a member of the Executive Committee of ns-3 Consortium.

CARLOS J. BERNARDOS received the degree in telecommunication engineering and the Ph.D. degree in telematics from the University Carlos III of Madrid, in 2003 and 2006, respectively. He worked as a Research Assistant and Teaching Assistant with the University Carlos III of Madrid, from 2003 to 2008 and, since then, he has worked as an Associate Professor. He has published over 70 scientific papers in international journals and conferences. His research interests include IP mobility management, network virtualization, cloud computing, vehicular communications, and experimental evaluation of mobile wireless networks. He has participated in several EU funded projects, being the project coordinator of 5G-TRANSFORMER and 5Growth.