electronics

MDPI

Article

State-of-the-Art and New Challenges in 5G Networks with Blockchain Technology

Serhii Onopa and Zbigniew Kotulski *

Institute of Telecommunications of WUT, Nowowiejska 15/19, 00-665 Warsaw, Poland; serhii.onopa.dokt@pw.edu.pl
* Correspondence: zbigniew.kotulski@pw.edu.pl

Abstract: As mobile communications transform, 5G technology can potentially change many industries and businesses. The change will have a great influence across many fields, such as the automotive, healthcare, and manufacturing sectors. This paper aims to review the existing applications of blockchain technology in providing 5G network security and identify new possibilities for such security solutions. We consider different aspects of blockchain in 5G, particularly data transmission, access control, and applications including vertical industry-oriented applications and specific solutions supporting such sectors of economic activity. The paper briefly describes modern technologies in 5G networks and introduces blockchain's properties and different aspects of using such technology in practical applications. It also presents access control management with blockchain applied in 5G and related problems, reviews other blockchain-enforced network technologies, and shows how blockchain can help in services dedicated to vertical industries. Finally, it presents our vision of new blockchain applications in modern 5G networks and beyond. The new-generation networks use two fundamental technologies, slicing and virtualization, and attackers attempt to execute new types of attacks on them. In the paper, we discuss one of the possible scenarios exhibiting the shortcomings of the slicing technology architecture. We propose using blockchain technology to create new slices and to connect new or existing subscribers to slices in the 5G core network. Blockchain technology should solve these architectural shortcomings.

Keywords: 5G mobile networks; network slicing; multi-access edge computing; blockchain; access management

Citation: Onopa, S.; Kotulski, Z. State-of-the-Art and New Challenges in 5G Networks with Blockchain Technology. *Electronics* **2024**, *13*, 974. https://doi.org/10.3390/electronics13050974

Academic Editor: Christos J. Bouras

Received: 31 January 2024
Revised: 22 February 2024
Accepted: 1 March 2024
Published: 3 March 2024

1. Introduction

Fifth-generation mobile networks (5G) are designed to meet high communication requirements regarding the bandwidth, delay, device density in the area, reliability, availability, etc. The expected values of the relevant parameters (called IMT-2020 requirements, ref. [1]) characterizing the network are defined in document M.2083 of the ITU-R (International Telecommunication Union—Radiocommunication Sector); see [2]. The needs of the services provided do not justify the simultaneous achievement of the maximum values of all network parameters. It is also contrary to the economic conditions of the network operator's activity. Therefore, three types of 5G mobile networks with high utility values have been proposed, which meet the requirements of access to different network services with expected performance and quality. The predefined types of networks are as follows.

- Enhanced Mobile Broadband (eMBB), which supports large data rates and high bandwidths. It is suitable for real-time and other Fixed Wireless Access (FWA) services with high quality and a strong user experience; see [3].
- Ultra-Reliable and Low-Latency Communication (URLLC), which supports use cases with very low latency for services requiring quick response times. It is useful for autonomous vehicles and telesurgery; see [4].

- Massive Machine Type Communication (mMTC), designed to support many devices in a base station. It is suitable for machine-to-machine (M2M) communication, Internet of Things (IoT), or supporting mass events; see [5,6].

The 5G mobile networks have created a technical and business innovation ecosystem involving vertical markets with performance, scalability, availability, and reliability requirements [7]. They serve a comprehensive portfolio of use cases and offer applications with a corresponding diversity of conditions being a choice or a combination of these three pre-defined types of networks: the high-bandwidth eMBB, the low-latency uRLLC, and the mMTC, able to support many devices. The 5G Infrastructure Association (5G-IA), representing the private side in 5G-PPP, with its 5G-PPP Vertical Engagement Task Force (VTF), proposed to consider the seven 5G vertical industries [8]: automotives, manufacturing, media, energy, e-health, public safety, and smart cities. This proposition is similar to the recommended verticals of the survey by Mobile World Live [9], conducted on 345 people from the mobile industry and vertical enterprise sectors who answered the question, "Which industries will benefit most from 5G in the next two years?".

The primary spectrum of 5G vertical industries with their specific network use cases can consist of the following twelve verticals [10]:

- Agriculture and Food Industry;
- Automotives and Logistics;
- Authorities and Public Administration;
- Banking, Financial Services, and Insurance (BFSI);
- Critical Infrastructure Sectors;
- Education, Culture, and Science;
- Healthcare and Telemedicine;
- Manufacturing Industry;
- Media and Entertainment;
- Retail;
- Smart Cities;
- Telecommunications.

The modern 5G mobile networks are based on three technological pillars, which are software-defined networking (SDN), network function virtualization (NFV), and multi-access edge computing (MEC) [11], as is presented in Figure 1. Each technology helps in constituting and managing a mobile network optimally. The SDN technology enables shifting the network management from hardware devices to software-based solutions. It separates the control and data traffic into a control plane and data planes, respectively; see [12]. Covering all management aspects, SDN is widespread in contemporary networks (system architecture, resource management, mobility, interference, etc.); see [13]. NFV allows the decoupling of network functions from physical devices and moving them to a virtualized space (see [14]). Virtual network function-based (VNF-based) services provide flexibility and scalability in 5G and reduce expenses [15]. NFV and SDN technologies are beneficial in constructing slices in 5G networks—see [16]—and in providing integrated, complete 5G network security solutions—see [17,18]. The MEC technology intends to shift an IT service environment and computing capabilities to the edge of the cloud, near mobile subscribers, to reduce latency, and to improve network operation and service delivery (see [19]). It supports the VNFs with applications running at the network's edge.

In addition to high performance requirements, security is a critical expectation in the 5G network. A contemporary mobile network experiences many threats [20,21]. Several articles have already considered the security problem and presented specific security models and approaches to protecting 5G networks. For example, ref. [22] analyzes security problems in mobile network deployment and proposes mitigation mechanisms for cloud layers. Ref. [23] presents new treatments for network threats in 5G with SDN, NFV, and MEC technologies. Ref. [24] surveys machine learning approaches supporting 5G security. Generally speaking, all security solutions currently used and designed for future use should find

their place in protecting 5G verticals and slices. Examples include automated security and orchestration for slices dedicated to different stakeholders operating in MEC architectures: network, service, and application providers; tenants; and end users. It leads to end-to-end (E2E) security solutions guaranteeing complete service protection, e.g., [25,26].

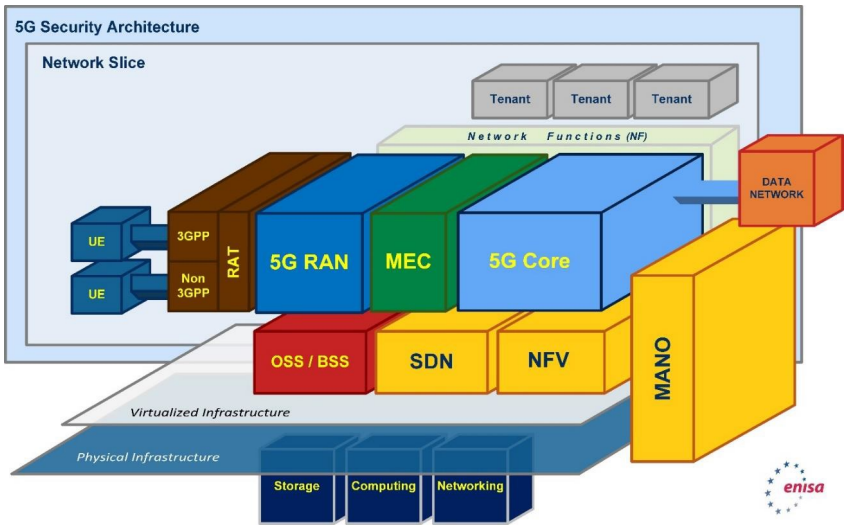

Figure 1. The 5G high-level technical architecture [20].

In our studies, we concentrate on 5G security solutions using blockchain technology. This paper aims to review the existing applications of blockchain technology in providing 5G network security and identify new possibilities for such security solutions [27]. We consider different aspects of blockchain in the 5G mobile network, particularly network transmission, access control, and applications, including vertical industry-oriented applications and specific solutions supporting such sectors of economic activity.

The rest of the paper is organized as follows. Section 2 presents the characteristics of modern network technologies and security solutions applied in 5G mobile networks. Section 3 introduces blockchain, its properties, and different aspects of using such technology in practical applications. Section 4 presents access control management with blockchain applied in 5G and related problems. Section 5 overviews different blockchain-enforced network technologies. Section 6 shows how blockchain can help in services dedicated to vertical industries. Section 7 presents our vision of new blockchain applications in modern mobile networks of the fifth generation and beyond. In Section 8, we give an overview of some methods of slice management and propose a new protocol for slice access with blockchain security. Section 9 compares several slice access protocols, while Section 10 concludes the paper and proposes future research.

2. 5G Mobile Networks

2.1. Introduction

The need to use the network for different services requires the creation of many use cases with numerous requirements, including availability, reliability, security, performance, etc. One can achieve such conditions by using programmable networks. Network softwarization technology can create virtual networks with different properties, such as Quality of Service (QoS) and Quality of Experience (QoE). Moreover, it can provide virtualization, modularity, dynamism, and flexibility; see ref. [12]. A specific form of such a solution is network slicing, which allows multiple virtual networks of different properties to run on a shared physical network infrastructure; see Figure 2. A slice separates part of the network by building a virtual subnet with properties tailored to the user's needs and allocating it to the necessary common physical resources [28]. Slice isolation establishes the security and proper provision of services in 5G networks [29].

Figure 2. The 5G network slicing services [30].

Historically, the isolation in computer networks started from isolated tunnels [31]. Different approaches exist to configure private networks in existing infrastructure. One can classify virtual private networks (VPN) according to the tunneling protocol, the tunnel termination point location, the type of connection topology, the ISO OSI layer that they present to the connecting network, etc. However, the present markets have created new business and technological demands. Therefore, the use of programmable IP networks has been widely accepted. This approach is also used in 5G slicing concepts. It is reasonable to provide specific parts of the network with specific requirements. Otherwise, implementing these requirements for the entire network will be complex and expensive. It is advisable to give groups of requirements for the operator, who can implement them for specific network sections, defining new logical networks. Such logical networks have properties established based on the business requirements for each service provided over the web, e.g., real-time transmission (voice, video), IoT, telemedicine, etc. The whole network's characteristics will consist of a subset of common properties and the properties for a particular virtual network. Properly chosen parameters for a specific network can improve the services provided based on this network. The slice concept is based on logical networks with several parameters, where the available physical resources are partitioned into many slices designated for services with adequate requirements [32].

In this section, we present the modern network technologies used to implement 5G mobile networks, where blockchain-based solutions can slightly improve different aspects of network security.

2.2. Software-Defined Networking

SDN is a recently emerging technology simplifying network management and configuration. The technology should provide higher reliability and safety. SDN technology uses the centralization of the management function. In contrast, in conventional networks, the management function is distributed in routers and switches. The SDN architecture consists of three network planes: the user (data) plane, the control plane, and the application plane [33]. The user plane provides devices transmitting user data in the network with basic functionalities for the execution of commands from the SDN controller. The network logic and the SDN controller reside in the control plane, acting as a network operating system and providing a global view of the network to the application plane. The SDN controller is the central software application managing the network. It allows the network administrator to configure elements of this network from a single point [34]. For SDN-based networks, there are defined policies, such as Quality of Service and security services such as firewalls acting on the application plane [35]. The northbound interface enables information exchange between the control plane and the application plane.

On the one hand, SDN is more secure against some threats and provides centralized network monitoring and traffic protection tools. On the other hand, it introduces new vulnerabilities [36]. The main threats in SDN are fake traffic, vulnerabilities in switches and controllers, and the lack of a pre-defined trust mechanism between the controller and the application managing the network. Moreover, a possible single point of failure is an SDN controller. Including all the above, the solution could be decentralizing the controller (several controllers or a hierarchy of controllers) and some other SDN services. Establishing trust between network components could also support the improvement of the reliability and security of the SDN technology. Blockchain is a good candidate for such a solution [37].

2.3. Network Function Virtualization

Network function virtualization allows the installation, control, and manipulation of network functions as software and running on typical compute nodes [38]. NFV allows 5G service providers to simplify a broad line of network functions, increase efficiency, deliver services faster, and offer new services more quickly and easily [39]. The application of network slicing allows the creation of multiple virtual networks in a physical network infrastructure and NFV helps to deploy virtual applications quickly. As an effect, mobile applications will be implemented rapidly and have high values of users' QoE [40].

Three main components of NFV are the Network Function Virtualization Infrastructure (NFVI), Virtualized Network Functions (VNF), and Management and Network Orchestration (MANO). It has several advantages: higher flexibility and scalability of deployments and connections, the optimization of resource provision, and more. However, NFV is fraught with new security challenges [41]. Since service functions can be deployed in a multi-provider environment, this can lead to data leaks. Moreover, one cloud infrastructure is often used for several service providers—the likelihood of attacks inside the cloud increases in such a case. In addition, communication between orchestrators and physical machines is an urgent security issue.

NFV technology can be beneficial in device-to-device (D2D) connections. D2D communication assumes that devices close to each other exchange data via a direct channel without additional central nodes. As a result, mobile devices will communicate within a short distance, significantly reducing the network latency [42]. Using NFV technology allows network functions to be dynamically allocated and easily deployed. NFV in 5G ensures the optimization of resource delivery to end-users and guarantees the high performance of VNF work. VNFs have three differences from traditional network functions (NF) [16,43].

- The separation of software from the hardware platform.
- High flexibility over short distances, which significantly reduces the latency in the operation of the network functions. The hardware and software can perform different tasks at different times, allowing the use and implementation of various modern services on the joint hardware infrastructure.
- Network operation and service provision in a dynamic manner.

2.4. Multi-Access Edge Computing

Multi-access edge computing (MEC), initially called mobile edge computing, is a highly flexible element in communication networks. The delivery technology and the MEC platform hardware remain open and can be adapted to the chosen scenario. The MEC framework developed by ETSI was initially treated as a complete edge computing solution, with strictly defined components and relations and rigorously specified communication at the interfaces [44]. Recent concepts of MEC are open to the specifications of other standardization organizations and research groups; see [45]. MEC is a technology that provides a cloud computing and IT service environment at the edge of the mobile network, within the radio access network (RAN) near the mobile subscribers. This scenario reduces the network latency, ensures efficient network operation, and improves the user experience of services. Based on data from 5G PPP, technologies such as MEC, NFV, and SDN are crucial for 5G networks. These 5G networks will use advanced air interface technologies, programmable

software networking approaches, and virtualization technology in infrastructure and applications. Thus, MEC technology is critical in 5G because it helps to transform the mobile broadband network into a programmable network and helps to improve indicators such as throughput, latency, scalability, and automation. The infrastructure that hosts MEC and NFV is quite similar [43]. The environment of MEC enables low latency, a high bandwidth, and real-time insights into radio network information and locations. It offers new possibilities for network operators, content, and application providers. It also leads to many new business opportunities and applications across multiple 5G vertical industries, which will contribute to the growth of the global market [10]. For this reason, a new open environment should be created and standardized to enable efficient integration across multi-vendor MEC platforms [46].

2.5. Network Slicing in 5G

The expected use of 5G networks imposes requirements that include flexible management, orchestration, and efficient data transfer [47]. Such conditions can be met using an SDN planar architecture, primarily using its two network planes—control and data. The 5G network uses the IaaS cloud model with fixed elements of the radio access network (RAN), an access network for end-users to provide mobile access to resources, and a core network (CN) that provides access to cloud services. The second element divides the network into slices with specific properties. Usually, each slice meets the quality requirements of one of the predefined 5G networks, i.e., eMBB, URRLC, mMTC [48]. However, it is a hard-to-solve problem with the optimal and secure separation of network slices [49]. Slicing is a method to ensure an appropriate level of quality and proper security on the network; this is called performance isolation and security isolation. Slicing makes it possible to provide isolated sets of resources. Providing slice isolation affects the traffic and operations in a shared environment [32]. The slices in a 5G architecture are like virtual sub-networks with specific properties. The open problem for network slicing is the optimal allocation of resources assigned for slices. Three already presented basic concepts are used to achieve this functionality: SDN, NFV, and MEC. SDN's programmable network technology is the basis for resource virtualization, which then enables the virtualization of network services and edge server sharing. NFV technology allows the design of network services in slices. It realizes operations that guarantee resource scaling (dynamic allocation), the migration of virtual resources between physical devices, disaster recovery, and the relocation of resources in the case of their insufficient size [50] for different models of slices; see [51]. The MEC technology supports various slicing concepts expected by external organizations to provide edge services [52]. As graphically presented in Figure 2, a slice is an element connecting (via RAN and CN) the user equipment (UE) with the cloud, in which the applications and their resources as used by users are located. Such a connection requires a number of security measures, the most important of which is isolating slices, discussed in Section 2.6, as well as ensuring proper access control [53].

2.6. Isolation Techniques in 5G Areas

Isolation is a good security measure. It is essential in 5G networks with slices to provide QoS and information security, where some network functions must be shared with different slices. The isolation techniques in SDN networks require the consideration of isolation in the SDN planes: the data plane, control plane, and application plane. Isolation in 5G networks raises concerns about the end-to-end isolation approach [25,32], which combines isolation in RAN and CN [54–56]. Isolation classification considers the infrastructure component and its tools [57]. In CN, we think of isolation in network nodes (servers) and the isolation of links. The techniques used in the nodes are language-based isolation, sandbox-based isolation, virtual machine-based isolation, operating system-based isolation, and hardware-based isolation [29,58]. Language-based isolation is a set of techniques that may provide a higher level of security by using the properties of programming languages. Language-based isolation enforces computer security on an application level [59]. The sandbox-based

methods isolate a program to prevent crashes or exploit vulnerabilities in host systems. Such scenarios can prevent unverified or untrustworthy programs from harming the host device [60]. Virtual machine-based isolation involves using virtual machines in which the operational functions of each VM are entirely isolated from the host and other VMs. Guest VMs provide isolation between virtual operating systems, leading to the isolation of tasks inside the VMs [61]. However, a critical aspect is that resources such as processors, storage, memory, and networks are shared between VMs. Isolation based on an operating system kernel is one of the most reliable and depends on the OS kernel's security. The OS kernel provides the primary isolation between the applications running on top [62]. Hardware-based isolation is provided by the processors or special devices that work with the processor. It is based on the specific assignments of the memory management unit (MMU) and input–output memory management unit (IOMMU), providing the isolation of processes [63].

Network links' isolation techniques can be of a physical or logical nature. Physical isolation means that a network is ideally disconnected from other networks. Logical isolation is a configuration that prevents virtual networks with the same physical infrastructure from interacting. Logical isolation techniques are strongly related to communication protocols [64]. Network protocols can operate in different network layers specified with the ISO OSI model. The logical network isolation methods can be considered as tunneling [65], where traffic isolation is carried out from other networks using a port, host, or subnetwork. In a virtual private network [66], traffic isolation is carried out from the outside environment by using particular virtual subnets over a physical network; multitenancy via tunneling or virtual networks, where the traffic is isolated within a tunnel.

In the CN physical layer, two types of media can be used on which the transmission depends: copper cables and optical fiber lines. OXC and ROADM virtualization, subwavelength switching virtualization, and link virtualization can be used to obtain virtually isolated slices in optical networks [67,68]. In the data link layer (layer 2), traffic separation can be considered as VLANs and MACsec [69]. In the network layer (layer 3), separations may depend on the routing technology used, such as MPLS, GMPLS, and VRF; see [70]. The second approach isolates a device under one tenant's control and includes a more complex case in which one device is shared between several tenants. Isolation in network devices is complicated because this device transforms information in different ways and switches the data streams between layers and nodes. The data plane uses the virtualization of network devices. The control plane must access three parties: the network provider, service provider, and users. Therefore, firewall technology must be used in the control plane [29].

In the RAN physical layer, isolation can be provided by multiplexing methods, classified into two groups. Complete isolation is when each channel has its own resources, while partial isolation is when each channel can share some available resources. Zero isolation occurs if all channels use the same set of available resources. These isolation techniques need proper resource management. RAN also implies special equipment for this part of the network, which should be considered part of the possible isolation. Antennas in RAN can use the TDMA method or FDMA. RAN technologies for the 5G physical layer can use the following techniques: OQAM/FBMC, QAM/FBMC, P-OFDM, F-OFDM, and OFDM enhancements [55,67]. In layer 2, the MAC protocol can be used, allowing the medium to be shared. Moreover, some collision avoidance protocols can be used. In layers 3–7, the CN and RAN domains in 5G networks generally use the same protocols [43,71].

Network slicing is resource isolation in which each slice is a set of resources with defined functions [54]. The isolation level depends on the requirements presented by the slice [48]. In some cases, such a connection between slices may be required, which affects the isolation level [25]. In 5G networks, isolation increases the security in many situations, e.g.,

- The isolation of each slice's assigned physical and operational resources (storage volume, processor cores, memory area);

- Ringfencing a security protocol's working space in the slices;
- The prohibition of uncontrolled direct communication between slices;
- Allowing the necessary exchange of data between slices according to strictly defined rules;
- Protecting slices from the hacking of one slice against another one;
- Secure communication between slices and orchestrators;
- Ensuring the reliable functioning of the physical equipment hosting slices;
- Providing secure management for slices;
- Protecting slices against side-channel attacks;
- Providing isolation in a hybrid environment for hardware network functions and virtual network functions;
- The enhanced isolation of slices served by the same hardware component.

Isolation assurance problems for slices may also be seen from the network protocols' points of view [48,72]:

- ISO OSI layer 2 tag-based isolation (MPLS);
- ISO OSI layer 2 VLAN-based isolation;
- ISO OSI layer 3 VPN-based isolation;
- SDN-based network slice isolation.

3. Blockchain

3.1. Beginnings

Blockchain, at present, is one of the most significant innovative technologies. It affects various sectors, such as finance, manufacturing, and education [73]. The blockchain construct refers to blocks or lists of records linked using cryptographic algorithms, or, in other words, blocks linked using hash pointers. Each block contains data from the previous blocks. Blockchains are distributed digital ledgers of blocks containing transactions signed digitally [74]. Each newly added block is cryptographically linked to the series of older blocks. After the validation procedure and a consensus decision, the new block is accepted, and the blockchain becomes tamper-evident. The updates are distributed across copies of the ledger within the network, and inconsistencies are resolved according to established rules [75]. In this way, we obtain a distributed database whose records are easy to recover thanks to the multiplication of the blockchain copies and secured against forgery thanks to digital signatures.

Haber and Stornetta were the first to describe the representation of a blockchain in 1991—see [76]—proposing the secure timestamping of digital documents, which included information about when the documents originated and the order of their creation. The pointer in this scheme links to a piece of data; it indicates any data changes. The timestamp server uses three elements: the current time, the hash pointer to the previous document, and the certificate. Keeping several certifications from clients enables the use of the scheme recursively. Blocking documents, chaining the blocks, and using a tree structure instead of a linear one improve the efficiency in linking and checking individual documents [77]. Lamport proposed Paxos [78], protocols for establishing consensus in an untrusted network. Consensus is the process of agreeing on one result among participants; when the participants or their communication medium fail, this problem becomes complicated [79]. Next, progress was made by Okamoto and Ohta [80], who described systems that use Merkle trees [81], enabling the subdivision of a balance into many parts. In 2008, Nakamoto [82] specified the protocol and published the initial code of Bitcoin. The concepts from earlier articles were combined and applied to construct the cryptocurrency using blockchain technology in a distributed architecture where no single user controls the system and no single point of failure exists. The scheme is without trusted intermediaries but exploits four critical characteristics of blockchain technology: ledgers, robust security, a shared infrastructure, and a distributed architecture [82].

3.2. Components and Technology

Blockchain networks can be categorized into two models based on their permission, determining who can maintain blocks. In a permissionless model, anyone can publish blocks. If only particular users can post blocks, it is a permissioned model. In a permissionless network, anyone can read the blockchain, create transactions, and write to the ledger, so a malicious user can publish blocks to subvert the system. Blockchain networks utilize a consensus system to protect the system against attackers. Examples of consensus protocols are Proof of Work [83] and Proof of Stake [84]. Only authorized users maintain the blockchain in permission blockchain networks, and some authority exists to authorize these users. The authority can restrict read access, issue transactions, or access authorized individuals. They also use consensus models, but this case does not require resources' expense or maintenance. These blockchains have a level of trust in each other, and authorization can be revoked if they misbehave. Consensus is usually a faster and less burdensome system in permissioned blockchains. A permissioned blockchain may be used if needed to control and protect a blockchain or if organizations work together but do not fully trust each other. These organizations decide on the consensus model based on their trust level. It can explicitly include auditing and oversight entities, making audits a constant event. Moreover, the ability exists to reveal transaction information selectively. For example, a blockchain records that a transaction between two users has taken place, but the actual contents of the transaction are only accessible to the involved parties [73].

Blockchain technology utilizes well-known computational and cryptographic algorithms (hash functions and digital signatures) with new distributed databases (ledgers). It uses the cryptographic hash function for many operations, such as address derivation, generating identifiers, protecting the block data, securing the block header, etc. Blockchain uses SHA-256, Keccak, RIPEMD-160, and many other functions. Such algorithms are extensively used, so optimizing their work to save energy is essential. For instance, implementations of hash functions can be optimized [85] to reduce the costs of their work. One can also modify hash algorithms to reduce the number of operations without decreasing the level of security; see, e.g., [86]. Hash functions with digital signatures enable trust between mutually untrusted users: transactions are signed with private keys; public keys allow the derivation of addresses and signature verification. Blockchain technology may use two approaches: distributed ledgers and a distributed physical architecture or central authority.

Blockchain can be classified into three categories: public, consortium, and private. In a public blockchain, everyone can check the transaction and verify it; see Figure 3. In a consortium (hybrid) case, a node (a set of privileged nodes) with authority that can be chosen in advance usually has partnerships in consensus establishment; see Figure 4. In a private blockchain means, all nodes are restricted. Nodes are strictly managed to obtain data access; see Figure 5 and ref. [75].

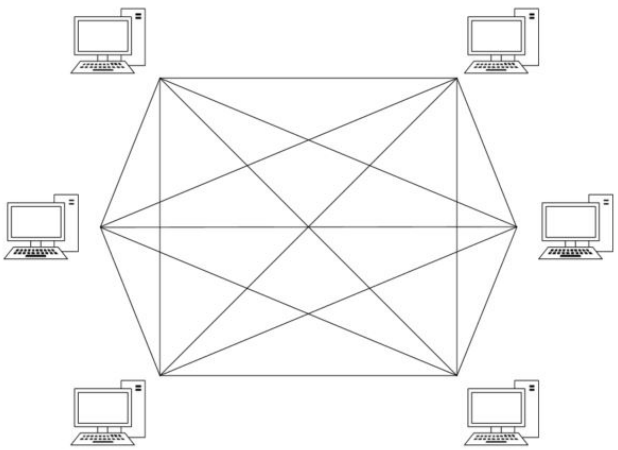

Figure 3. Public blockchain.

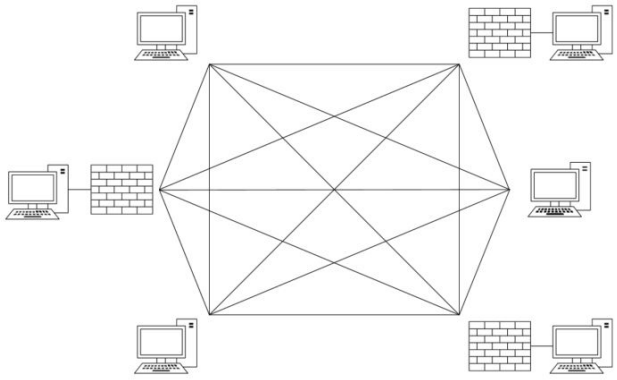

Figure 4. Consortium blockchain.

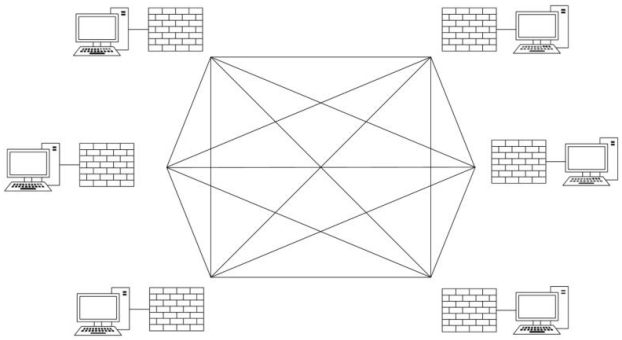

Figure 5. Private blockchain.

The root of blockchain technology is consensus algorithms. Consensus algorithms are a decision-making process. Consensus models define blockchain security by maintaining consistency across the shared state of the blockchain. Consensus models include Proof of Work [83], Proof of Stake [84], Round Robin [87], Proof of Authority [88], Proof of Elapsed Time [89], and others [90]. Fork is a word that describes changes to a blockchain network and data structure. There are two types of forks: soft and hard. A soft fork appears if the changes are backward and compatible with nodes that have not been updated. In the opposite case, the changes are not back-compatible; these are hard forks [73,74]. Blockchain technology creates a distributed ecosystem where no third-party organization controls the data. A blockchain is an increasing list of blocks that are linked using hashes and digital signatures. Such a list uses hash pointers; included in each block's data is a pointer to the previous block. The main feature of this structure is protection against tampering with prior records. This property results from the security features of the hash function: resistance against finding pre-images (first and second) and to finding collisions; see Figure 6.

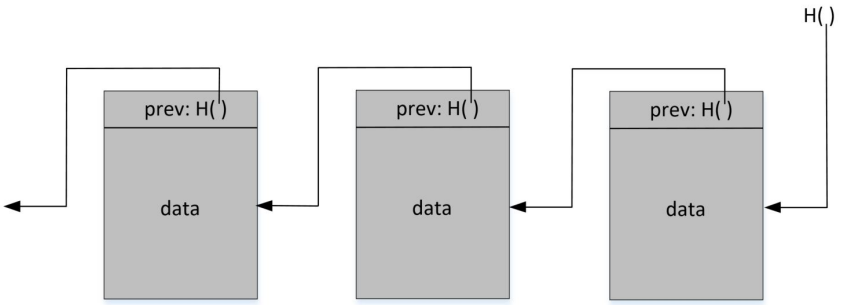

Figure 6. Blockchain.

Another data structure that can be built with a hash pointer is a binary tree (Merkle tree). All blocks contain data blocks; the procedure involves grouping these blocks into

pairs of two, and then, for each couple, building a data structure with two hash pointers, one for every block. These data constitute the next level of the tree. The grouping of blocks continues until they reach a single block that is the tree's root; see Figure 7.

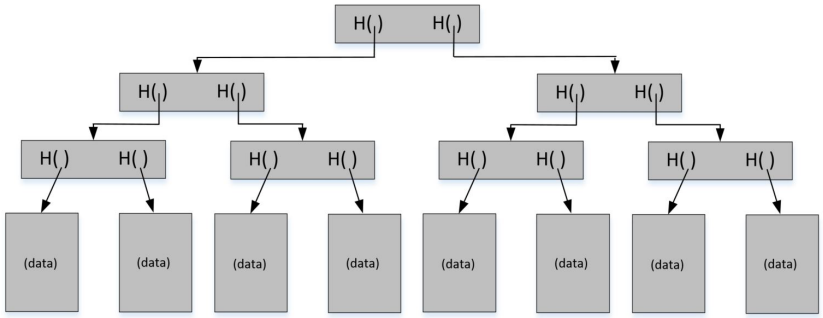

Figure 7. The Merkle tree.

3.3. Main Characteristics and Cybersecurity

The great popularity and versatility of blockchain technology result from its useful properties. The main properties are as follows [91].

- Decentralization: a decentralized network maintains data and executes a consensus algorithm.
- Persistence: transactions are validated quickly, invalid transactions are not admitted, and blocks with invalid transactions are discovered immediately.
- Anonymity: each user interacts with the blockchain using a generated address that does not disclose his/her identity; it does not guarantee complete confidentiality.
- Auditability: transactions are easily verified and tracked.

The blockchain is generated by adding new blocks to the chain of verified blocks containing previous transactions. The user's software sends a new transaction to a node. Next, the transactions propagate to other networks' nodes, and each new transaction must wait until it is added to the blockchain by a publishing node. The transaction is added to the blockchain only after the node publishes a block. The block consists of a block header and block data. The block header consists of the block number, the previous block header's hash value, a hash representation of the block data, a timestamp, the size of the block, and the nonce value. The block data contain a list of verified transactions submitted to the network. A valid and authentic transaction must be formatted and signed correctly. The node checks the validity of the private key. The other nodes check the validity and authenticity of all transactions in a published block [92–94].

Although cryptography is used to secure transactions, blockchain and related protocols may be subject to attacks. The classification of attacks is presented to reflect existing research that describes security incidents with cryptocurrencies such as Bitcoin, Ethereum, or other Altcoins. All incidents are classified into three main groups: OPSEC, smart contracts, and consensus protocol incentives [77]. OPSEC contains the most significant number of incidents, more than 60%. Incidents compromise an organization or individual's control of information and access to critical assets. Other sources also present incidents, such as financial losses, scams, and distributed denial of service (DDoS) attacks on exchanges and mining pools. Four types of Bitcoin scams have been investigated: Ponzi scams, mining scams, scam wallets, and fraudulent exchanges. According to other authors, many possible security breaches can occur, including DDoS attacks and private account hacking using Trojan horses or viruses. Other examples include the emergence of mining pools, potentially leading to 51% attacks.

Blockchain is not entirely secure by design, and only if data are committed to the blockchain can these data not be changed. The data that have not yet been included in a published block within the blockchain are vulnerable to several types of attacks. If blockchain networks have timestamps, time spoofing can occur. Moreover, denial of

service (DoS) attacks can be executed on the blockchain platform. Blockchain platforms also can be scanned by attackers and infiltrated to discover vulnerabilities and perform zero-day attacks [75,77].

Moreover, there are data malleability problems, which result in data integrity losses. Malleability means that the signatures proving the transfer of ownership do not have guaranteed integrity, so that the attacker can intercept, modify, and rebroadcast a transaction. At the same time, the issuer lacks confirmation of the original transaction. We may use the available standard cybersecurity solutions to prevent OPSEC class incidents. The smart contracts category makes up about 20% of incidents. These incidents occur when smart contracts are disrupted or improperly written, deployed, and executed on a blockchain. Hackers continuously look for vulnerabilities in the deployed smart contract because preventing such attacks on deployed code is complicated. When a new vulnerability is detected, fixing it requires deploying a new smart contract. Incidents arising from the malicious exploitation of consensus protocols are known as consensus protocol incentives. This property makes creating opportunities and benefits for blockchain participants possible. This class is more challenging to detect, as the effect usually involves the improper mining of a block or censorship of nodes. A formal framework can be used to evaluate this problem, e.g., the PREStO framework [95]. Security vulnerabilities are of the most interest in blockchain networks due to increasing financial losses. The identified vulnerabilities include 51% attacks, selfish mine attacks, transaction data malleability problems, and deanonymization by transaction linking. Identifying known issues requires the categorization of OPSEC, smart contracts, and consensus protocol incentives. One can prevent this problem using standard cybersecurity solutions, fixing and patching smart contracts, and using the framework for testing. Ref. [96] proposes PADVA—a next-generation notary system. Blockchain seems to be a suitable solution for conducting transactions using cryptocurrencies; however, it still has some technical challenges and limitations that must be studied. The high integrity of transactions and the security and privacy of nodes are needed to prevent attacks and attempted attacks from disturbing the transactions in the blockchain. Anonymity, data integrity, and security attributes raise a number of questions and problems that need to be solved and assessed with high-quality research [48,74,92,97,98].

Another critical issue with blockchain is performance. Blockchain performance has several quantitative measures. Centralized systems have higher performance because they do not need consensus mechanisms. Decentralized blockchain systems require message exchange and consensus protocols to verify each node, each adding some latency. The transactions per second (TPS) parameter is the best performance metric for blockchain networks. The TPS is the system's rate of processing a transaction. The TPS describes a node's time to verify and write a transaction to the local ledger. Another definition of the TPS is the time that most modes require to write transactions for each ledger. The relevant parameter is the maximum number of transactions that the system can process per second. The simplest definition of the TPS comprises the time at which the transaction was sent and the time at which the transaction was finally entered into the query record. This parameter is recommended for repeated use for several transactions, because decentralized systems often have different delays and noise levels in the network. The system developer must repeat this test for good representation depending on the context. Since the TPS estimate is random, it should be complemented by parameters characterizing its central value (mean value, median, mode) and dispersion (variance, standard deviation, quantiles, minimum–maximum) [93,99].

4. Blockchain for Access Management in 5G Networks

4.1. Access to the Services in MEC

4.1.1. Blockchain in Authentication

Authentication is a verification process that checks that the object is what it claims to be. There are three main authentication methods: knowledge-based, possession-based, and inheritance-based. A combination of these methods constitutes multi-factor au-

thentication. Knowledge-based methods use the user's knowledge—a PIN or a password. Possession-based methods use the user's possession—credentials or RFID [100]. Inheritance-based authentication uses biometric features like fingerprints. Multi-factor authentication combines the previous techniques. For example, the framework stores users' data in the blockchain and uses a smart contract for managing permissions. This framework keeps his/her identity in the blockchain and encrypted personal data in the off-chain storage. When a user tries to log in to a website, the service provider checks the identity and retrieves the user's private data from the off-chain storage.

Another example is an authentication method called SAMS. This authentication method for the cloud environment uses a master node, which manages the system's security. For user authentication, the master node creates its block for user authentication and stores it in the blockchain. When a new client node wishes to connect, another block will be created and the created block connects with the master node. The master node creates a block with this information from the client and checks the identity of the block. If the blocks are identical, the client block will be connected; see [101]. An interesting application has been proposed for home networks as an authentication method for door locking. This method uses supporting data such as fingerprints from a mobile phone. The fingerprint is converted into a hash and the hash is saved to the blockchain to be secure against forging, tampering, or leakage. The authentication protocol uses a consensus mechanism (Proof of Work) executed by a mobile phone; see [102]. There are many cases that involve using blockchain for IoT devices. In ref. [103], an authentication and authorization method to control the user's access to the resources of IoT has been proposed. The method consists of two smart contracts, one handling digital certificates and operation and another responsible for access control. It uses the Ethereum blockchain. An authentication system called bubbles of trust has been proposed in [104]. This system relies on Ethereum, creating virtual secure zones, in which parties can identify and trust each other. It is possible to create an authentication and access control (AAC) system for IoT in which the authentication part is based on users' credentials in token form. This method only supports token-based authorization. If a token is expired, the user should mine two tokens, to ensure that a token is available, and this token could be used; see [105]. An interesting authentication method is the CoinsShuffle protocol. During authentication, users install Auth-Wallet. The wallet allows users to obtain authorization exchanging coins instead of user information; see [106]. In the literature, one can find more original results and survey papers presenting authentication and authorization protocols using blockchain; see, e.g., [107–109].

4.1.2. Blockchain in Access Control

Access control is the process of granting or denying a subject's access to a specific object, such as data, an application, or a service. This means that access control regulates access rights—read, write, and execute. The most well-known methods are DAC, MAC, RBAC, and ABAC. In discretionary access control (DAC), the owner defines the rights to his/her object. DAC uses access control lists (ACL) or access matrices to represent access rights. In the mandatory access control (MAC) model, access rights are assigned to subjects by a central authority. The role-based access control (RBAC) method uses the concept of roles. The system of rules gives rights to roles and roles to subjects.

The recent attribute-based access control (ABAC) model grants access rights to users according to security policies combining attributes [108]. Blockchain can be used as a distributed database for rules and policies, and access control is carried out based on these policies. The resource owner defines the policies and rules and stores them in the blockchain. One can keep only a link to an external source containing the policy to avoid extra resource consumption. It also considers the possibility of using smart contracts to enforce policies. It is possible to improve privacy through blockchain in cognitive cellular networks [73]. Services use blockchain and smart contracts as access control and identity management mechanisms. First, users obtain a pseudo-anonymous unique blockchain IS

from the service when they register with this service. When the user wishes to access the network, they send a request to the service. This service sends the response to the network when the user confirms their rights. After the network accepts their access, the user will have access. BlendCAC is an access control mechanism based on smart contracts for IoT environments. Smart contracts store the access matrix. The remote procedure call interface checks the validity of the tokens or permission. Another access control (AC) mechanism for IoT is a method in which the user signs a contract in the registration process. The smart contract stores the user's hash and policies. In addition to the blockchain data, this method uses the PoW mechanism. In another solution for IoT and smart cities, administrators add attributes for users in the blockchain.

The ABAC method used in the cloud uses four subjects and the blockchain network. The subjects are the central authority (CA), data owner (DO), data user (DU), and cloud service provider (CSP). The certification authority (CA) is the manager of the security system. It performs attribute management and access control. The CA issues an attribute key and sets the validity period of the attributes in the smart contract. In the access control phase, the DO uploads the encrypted text to the CSP. The CSP obtains a valid attribute set from the contract. If the DU has the right to access the data, he/she can decrypt the desired information. The weak point is the single point of failure in the CA that serves the whole system. Another method for data sharing uses an attribute encryption mechanism. The DO encrypts the system master key, saves it to the blockchain, and then deploys a smart contract. The DO manages the DU's secret key and keeps it in the blockchain. Next is an attribute-based AC mechanism using Tangle. Owners define AC, define the security policies, and store them in the blockchain. If the DU has access rights, the DO sends the authorization token [108,110].

4.2. Authentication and Authorization in 5G

The 5G network claims to be a universal telecommunications and internet access channel. In particular, 5G should support voice calls and provide access to telecommunications services in all vertical industries [10]. A critical security service in a network is access control and authorization to the network and the services provided in it. The basic authentication and authorization service requirements are formulated in the ETSI standard [111]. The 5G system should satisfy the following requirements.

- Subscription authentication: The serving network should authenticate the subscription identifier in the authentication process and the key agreement between the UE and the network.
- Serving network authentication: The UE should authenticate the serving network identifier through implicit key authentication.
- UE authorization: The serving network should authorize the UE through the subscription profile obtained from the home network. UE authorization is based on the authenticated subscription permanent identifier (SUPI).
- Serving network authorization by the home network: Assurance should be provided to the UE that it is connected to an access network that is authorized by the serving network to provide services to the UE. This authorization is implicit in the sense that the successful establishment of access network security implies it. This authorization is applied to all access network types.
- Unauthenticated emergency service: Anonymous access to emergency services should be provided according to regional legal regulations.

4.3. Using Tokens in Blockchain with JSON

OAuth 2.0 is an industry-standard protocol for authorization. It is used in higher-security environments like IoT, open banking, e-health, e-government, and electronic signatures. OAuth 2.0 is the protocol through which clients obtain an access token to access a protected resource from the authorization server. However, the specification does not define how this token is generated, validated, or destroyed. OAuth 2.0 systems consist of

a resource server, the client who wishes access to this server, and an authorization server. The authorization server is responsible for generating access tokens. First, a client requests an authorization grant from the resource owner. Then, they use this grant to obtain an access token from the authorization server. The final client uses this token to access the resource stored in the server. In the standard OAuth 2.0, one may choose the type of token that it will use.

JWT is a compact, URL-safe means of representing claims. It consists of zero or more name–value pairs. It is transmitted encoded in Base64url. Standard claim names are defined in RFC 9068 [112]. Ethereum is a blockchain platform designed for smart contracts. Smart contracts allow for the creation of decentralized applications. The user signs the smart contract with a key, and this key's hash is used as the user address. All transactions are recorded in the blockchain. The Ethereum community is developing the Ethereum Request for Comments (ERC) [113]. These standards define a required set of functions for a token type that allows apps and smart contracts to interact with them.

The most popular token standards are ERC-20 and ERC-721. ERC-20 is a token standard created by Vitalik Buterin. It allows for the creation of tokens on Ethereum and can be reused by other applications. The ERC-20 standard contains six key functions: totalSupply(), balanceOf(), transfer(), transferFrom(), approve(), allowance(). The ERC-721 standard defines non-fungible tokens. Fungibility is a characteristic of a good whose units are identical and interchangeable. The ERC-721 standard allows anyone to create tokens that are unique. Another ERC standard is ERC-223, which defines a token type similar to ERC-20 with an added functionality: it contains a method called token fallback that ensures that tokens are only sent to contracts with the appropriate functionality. ERC-777 is a standard that improves ERC-20; it defines advanced features and offers more control over tokens. ERC-1155 allows smart contracts to manage multiple token types, and ERC-1337 is the standard for recurring subscriptions on the Ethereum blockchain [114].

5. Blockchain Technology for 5G Network Applications

5.1. Cloud Computing

Cloud computing enables resource sharing to efficiently manage increasing demands for resources and data storage management. The modern understanding of cloud computing is related to the concept of Continuum. Continuum is an environment unifying the continuum of resources and continuum of computing [115]. Continuum is a distributed, heterogeneous, and dynamic infrastructure covering a broad spectrum of resources like IoT devices, MEC, and the cloud, including private, public, hybrid, and multi-cloud. It is integrated with wireless and wireline connectivity, where modern mobile networks are crucial. Clouds often have functions distributed over many locations from central servers and managed by different vendors and providers. An edge server is usually a server where the connection to the user is relatively close. Further development should include the 5G needs due to the growing role of edge instances like edge clouds, mobile edges, and fog computing. Edge computing is considered to empower the capabilities of 5G. It provides services at the mobile network's edge, improving the performance and latency. Cloud computing can provide robust and efficient services with minimum effort and has unlimited storage and computing power resources. In effect, cloud computing is integrated with 5G networks, which require significant computing power and resources. The Cloud Radio Access Network (C-RAN) is an attractive model that manages many cells using a centralized cloud controller as a baseband unit (BBU). However, the cloud security, computer performance, and networking models remain unresolved. Many devices that transmit data to the cloud create new problems and challenges with privacy, integrity, and availability. For example, data exchange between the cloud and mobile users is vulnerable to sniffing and modification. It is also an internal problem of the organization due to the powers of certain employees. Distributing used resources between different owners and locations means that all Continuum (cloud) management systems, including security management,

should avoid centralized solutions. This is why blockchain and its consensus protocols are beneficial here.

Cloud resource providers have complete control over the data in the cloud. This creates a severe problem for data monitoring and verification in 5G because transparency is required to ensure fairness and openness. Blockchains have been integrated to solve this problem with security in the cloud. Blockchain is used as a platform between devices, BBU units, and manufacturers. The smart contract is also used for automatic user authentication. On one hand, a blockchain-based C-RAN is a distributed blockchain consensus platform that eliminates bottlenecks and improves system trust. On the other, a blockchain-based platform helps to optimize the use of resources. Smart contracts possess the following properties: transparency and immutability for data exchange [42,116].

5.2. Blockchain in MEC, Network Slicing, D2D Communication, and NFV

Blockchain can optimize networking in 5G MEC systems. Blockchain can be used for distributed and trusted authentication systems with reliable authentication and information sharing. Authentication of data and user access information will be assumed to be stored in the blockchain. Smart contracts can help to store trusted data in edge networks. Another issue is that vehicular edge computing seems to have a problem with latency and the privacy of users' information; therefore, blockchain technologies are appropriate. A ledger can keep information about the driver and car profile and other data from a car, like vehicle sensor data. There are also possible cases of using blockchain technologies to create a security mechanism for edge computing-based systems where smart contracts are used to access control schemes for energy sharing and distribution.

Further, blockchain can be used for anonymity and key management for authentication protocols. Blockchain can improve the security efficiency of data storage for edge systems [117]. Moreover, blockchain can maintain data and ensure secure communication between IoT devices in the smart city. An extensive data repository would be indispensable for data access in a distributed MEC-supported blockchain, such as ISFS, Filecoin, or Storij. Let us assume the integration of this platform with a dynamic MEC. Blockchain can support the computation processes in MEC, such as authentication capabilities, and monitor and verify all computing tasks transmitted to the MEC servers to prevent external attacks. It can be used to improve the efficiency of IoT computing and video processing and provide services without centralized authentication. Further, blockchain can provide data file safety [118–120].

Network slicing is a technology that separates multiple virtual networks running on the same physical hardware. This technology makes it possible to divide networks into specific services and applications. To implement this technology, one can use softwarization with virtual network functions. A network slice is a set of VNFs with physical network functions. This approach creates new security challenges, such as interslice security threats and resource harmonization between interdomain slice segments. All this can lead to resource abuse, data compromises, data leaks, and damage to the whole system. In such contexts, blockchains provide excellent security oversight and segmentation management opportunities in the 5G network [29,42,121,122].

Device-to-device communication is a technology that allows mobile devices to communicate directly without any access point or core network. This type of communication is possible if the devices are nearby. D2D communication improves the overall system throughput and reduces delays, energy consumption, and traffic loads. However, there is a threat of data leaks in untrusted D2D environments. Hence, such settings should provide authentication mechanisms to reduce the device computing load. Edge servers can perform mining tasks for the blockchain. The blockchain reward policy is also used to improve the reliability and security of the D2D network. For this, the consensus protocol is used. In such cases, blockchains record hashes of the information exchanged during user authorization. Smart contracts support concatenation if authorization is requested. The authentication mechanism also protects network resources against DoS attacks. Blockchain

registries enable secure mobile data transfer, while edge servers can perform computing offloading and content caching. Blockchain can support distributed security monitoring in D2D systems [123–125].

Using blockchain technology can provide a secure and isolated software infrastructure. Blockchain technology can provide the reliable, simple, and flexible orchestration of VNF services. Blockchain protects network functions and ensures system integrity under internal and external attacks. With blockchain technology, data auditing and system health monitoring can be performed. For example, it is possible to use blockchain technology for orchestration—all the instructions used by the NFV services are registered in the blockchain, guaranteeing instructions' authenticity, integrity, and invariability. Orchestration by blockchain-based virtual machines is also possible. It gives the ability to protect the NFV or cloud orchestration operations. Moreover, using blockchain, it is possible to audit network segment orchestration operations to protect VNF configuration updates. A smart contract can store access information for MANO components and use resources efficiently [42,47].

6. Blockchain Technology in 5G Vertical Industries

6.1. Blockchain in Crowdsourcing Systems

Crowdsourcing systems help to solve many problems through the participation of many people. It is used by companies, public institutions, and non-profit organizations, for which crowdsourcing replaces traditional employees. Examples are Wikipedia, Linux, and Yahoo. Among them are also the services of smart cities, where 5G technology significantly affects this trend. Most existing crowdsourcing systems rely on central servers as a trust center, and payment is made with the help of third parties. This creates additional risks that can lead to significant losses. This is also a problem that significantly affects the development of smart cities with 5G. The solution to this problem is to create a decentralized service based on the blockchain platform. A smart city means using innovative information technologies and applications to compose an integrated system for urban services, improving and optimizing management and resource utilization and increasing the quality of life in such cities. The 5G smart city centralizes and unifies public services like transportation and communication, utilities (water and energy), etc. The 5G technology has a high speed and low latency, necessary to ensure adequate network quality for smart cities. In the vertical framework, crowdsourcing contains three stakeholders—the requesters, the workers, and the crowdsourcing platform. The requesters are usually companies or individuals who need collaboration in solving their tasks. The workers are generally different internet users. The main task of the crowdsourcing platform is to connect requesters and workers. The work of the crowdsourcing platform is as follows.

- The requester submits a task to the crowdsourcing platform.
- The platform checks the task. If correct, it publishes the task in the library.
- The worker chooses a suitable task.
- The worker makes a scheme for the task.
- The worker submits the task to the crowdsourcing platform.
- The requester receives the scheme from the crowdsourcing platform.
- The requester checks the scheme.
  - If accepted, the worker receives a reward, and the platform charges the service fee.
  - If not accepted, the task returns to the library, and the cycle repeats.

Most existing crowdsourcing systems rely on central servers or trust centers, and payments depend on third-party financial institutions like banks. This model comprises two trust centers, crowdsourcing platforms and payment institutions. The disruption of these centers can lead to severe losses. Moreover, during attacks on these centers, the system's operation is disrupted. Using blockchain technology to avoid such problems and improve crowdsourcing systems is possible. The workers and the crowdsourcing platform will conduct blockchain-based transactions in such a system. Accordingly, the blockchain supports payments, and the entire crowdsourcing service uses the blockchain, an open and

transparent tool [126,127]. Ref. [128] offers such a platform with the additional functionality of multi-tier worker quality evaluation. Ref. [129] proposes a framework that involves assigning tasks and verifying solutions.

6.2. Blockchain for IoT and UAVs

Blockchain in 5G can improve IoT systems due to the improvement of such characteristics as security and performance. It will also enhance the serviceability of such networks. Implementing blockchain for healthcare and smart cities will help to ensure direct and secure connections between users, service providers, and network operators. It will allow safe and low-latency communication and resource-sharing methods. Data privacy is also critical in the healthcare system [117].

Integrating the blockchain into the unmanned aerial vehicle (UAV) network to solve critical problems is possible. UAVs can be a good solution for data transmission for air and ground communication systems. Blockchain can improve the characteristics of such networks, primarily in terms of security. It is assumed that the UAV will exchange information with IoT systems, reducing the load on the UAV's energy resources and prolonging the UAV's service life. Using the LECast protocol reduces the amount of energy consumed; see [130].

6.3. Blockchain for Machine Learning and Big Data

Machine learning (ML) provides data analytics capabilities for decision making or data prediction problems. ML will contribute to the development of blockchain in 5G networks. ML can provide a solution to simplify resource management. ML has predictive potential, making it possible to predict user behavior and the traffic that they will need. In turn, it influences control algorithms to prevent network congestion. Blockchain with ML can be used for secure and intelligent resource management and network orchestration.

It is assumed that in 5G networks, a large amount of data will be generated by IoT devices. These data can be used to create applications for data analysis using artificial intelligence. By using blockchain for big data, there is an opportunity to improve the security, privacy, and risks when processing big data.

7. Perspectives and Challenges

7.1. Security

Blockchain technology requires cybersecurity risk management. Cybersecurity standards and guidelines remain relevant to ensure the security of the systems that interact with blockchain technology. Some standards are related to blockchain technology cybersecurity. One of them, the NIST Cybersecurity Framework, is not universal or written for blockchain technology, because organizations will always have unique risks and threats. At the same time, the security standards are technology-neutral and can support blockchain technology, such as developing policies and processes that identify and control risks, implementing cryptographic algorithms, etc.

Blockchain technology is safe and tamper-proof. However, this is only true when the information is already recorded in the published block. Transactions not yet included in the published block are vulnerable to several types of attack. The first type is the time attack vector, because some blockchain networks have timestamps that affect the whole network. DoS attacks can also be used on the blockchain platform or smart contracts. Another case is network scanning and reconnaissance, which enable malicious users to discover unknown exploits and use zero-day vulnerabilities. Technology implementation errors may also bring known vulnerabilities and weaknesses.

Blockchain networks without access rights cannot guarantee how the user will behave on the network. Often, such networks provide rewards for users, but there can also be cases of malicious activity if beneficial. A malicious action can involve ignoring transactions from specific users or nodes or creating a modified alternative chain. If the chain is longer than the actual chain, private nodes switch to it, refusing to transfer blocks to other

nodes. Moreover, network administrators can act maliciously to block production, block users, spoof the history, engage in double spending, remove resources, or partially block the network.

The main point of trust for blockchain users is cryptographic algorithms or their correct implementation. For smart contracts, this is the assurance that there are no mistakes in the work. Moreover, in blockchains, one must ensure that most users do not conspire to control more than 50 percent of the network [73,131].

7.2. Blockchain in 5G-b and 6G Networks

Sixth-generation networks are expected to link terrestrial wireless and satellite communications. For the intelligent and flexible development of network services, 6G networks will use artificial intelligence, which is associated with processing large volumes of data. The centralized storage and management of AI applications used in 6G poses security threats. Data encryption is currently used to solve this problem. However, this solution is centralized as one cloud server processes these data. Therefore, the development of a new decentralized solution with secure data exchange is indispensable; this solution can be a blockchain [132].

In 6G wireless networks, critical parameters of the 5G network will be improved—reliability, speed, and bandwidth—which will make it possible to create new generations of applications, such as applications that use artificial intelligence or the ultra-reliable Internet of Things. It is also necessary to provide improved security in networks and applications in such networks; for example, using blockchain technology makes it possible to improve security and privacy. The 6G networks are expected to satisfy the Internet of Everything (IoE) paradigm and to support distributed AI solutions. The 6G network will have ultra-high reliability and ultra-low latency, and Key Performance Indicators (KPI) are enabling significant improvements over 5G. Using blockchain technology will enable the creation of advanced IoE applications for the 6G blockchain and improve trust and security for access control, authentication, key management, and audit evidence. Using blockchain 6G networks will improve security and trust in the following cases. Edge computing allows the offloading of computations to remote servers and mitigates the long latency and lack of privacy related to cloud offloading. This offloading may include sensitive information. Blockchain technology can securely connect user devices and edge servers. Leveraging blockchain in spectrum management will help to manage the spectrum more securely across multiple categories of users, but user privacy remains an issue. In 6G networks, a large amount of content can be cached on user devices, improving the service quality. Since content can contain sensitive information, blockchain can provide trust between requesters and providers. Some use blockchain in edge-based distributed machine learning to avoid the need for centralized control. It is possible to use blockchain technology to create a marketplace where users can exchange resources without violating their privacy; spectrum owners, infrastructure owners, and ISP owners can use it. Blockchain can improve the management of virtual network slices. Blockchain can also be used for optimal interference management [133–136].

8. Secure Access to Slices with Blockchain

Some papers describe the possible use cases of blockchain technology in 5G networks. One offers to use blockchain technology to create isolated networks—slices. It is supposed to create blockchain nodes for slice isolation. The authors also propose to log all VNF orchestration operations on a management blockchain. In the proposed architecture, blockchain is used for different networks—mobile network slices, Industry 4.0, and vehicular networks [137].

8.1. Service-Based Architecture

The 5G networks have new security features, such as

- A Secure Edge Protection Proxy (SEEP) to protect the network against attacks from roaming traffic;
- A unified authentication framework for many 5G access technologies that is independent of the network (3GPP access and non-3GPP access);
- The protection of user privacy on the air interface;
- Extended security control for users from roaming networks;
- NRF authorization functions.

8.2. Slice Management

A slice is a logical group of network functions, see Figure 8, and the business purpose defines the quality features of these dedicated pieces of networks. Each slice has its own single network slice selection assistance information (S-NSSAI); this identifier is unique in the core and RAN infrastructure and in the UE [54]. The same type of slice can be used by the operator for different verticals. The operator can use non-standard S-NSSAI.

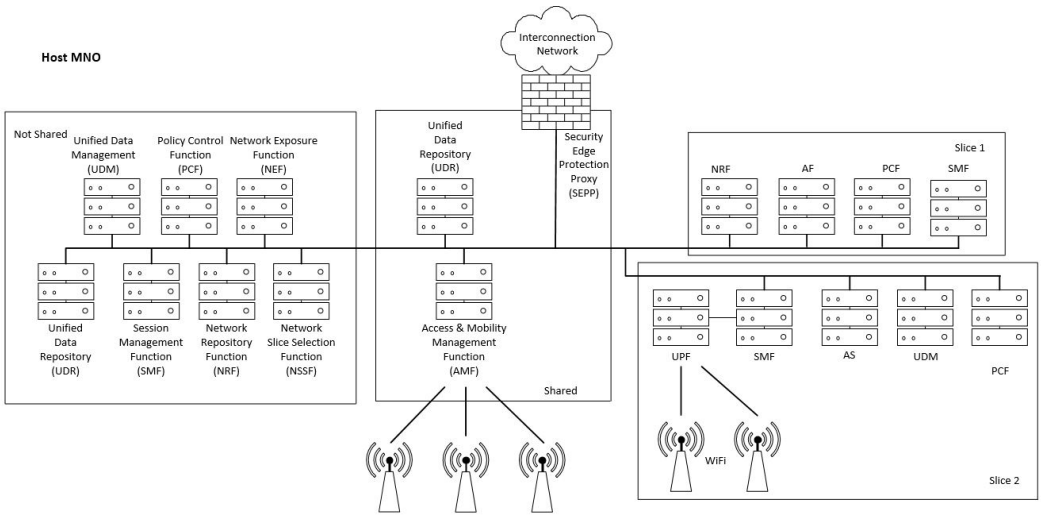

Figure 8. Shared network functions.

The expected use of 5G networks imposes requirements that include flexible management, orchestration, and efficient data transfer. Such conditions can be met using an SDN planar architecture with two network planes—the control and data planes. The 5G network uses the IaaS cloud model divided by the radio access network—the end-user access network to provide resources and the core network. The second element divides the network into slices with specific properties. However, at this point, there is an unsolved problem: the optimal separation of network slices. Using network slicing can control parameters such as the Quality of Service and the level of security required for the service. Slicing makes it possible to provide isolated sets of resources. Properly providing slice isolation affects the traffic and operations in a shared environment. Slices in 5G architectures are like sub-networks with specific properties. The open problem for network slicing is the optimal allocation of slices. Slicing is a method to ensure an appropriate level of quality and an appropriate required level of security on the network; this is called performance isolation and security isolation, respectively. Three basic concepts are used to achieve this functionality: software-defined networks, network function virtualization, and multi-access edge computing.

Network slicing is a technology that allows the separation of multiple virtual networks running on the same physical hardware. This technology makes it possible to divide networks into specific services and applications. To implement this technology, one can use softwarization with virtual network functions. One network slice is a set of VNFs with physical network functions. It brings new security challenges like interslice security threats or resource harmonization between interdomain slice segments. All this can

lead to resource abuse, data compromises, data leaks, and damage to the whole system. In such contexts, blockchains provide excellent opportunities for security oversight and segmentation management in the 5G network.

Slices are a logical separation in the 5G core network. This separation can create slices for private networks, streaming, automotives, or other purposes. For some purposes, details are specified, but a mobile network operator (MNO) can create non-standard slices. A slice consists of a group of functions or NFs. This NF can be used by different slices simultaneously. NFs can be categorized into virtual and physical. One hardware server can host several network functions. Slices would not be separated on the transport or network layer (layers 2 or 3). Some network functions might not belong to the hosting MNO, so the third side has access to the core network.

In this case, slice 1 and slice 2 are not entirely separated on the signaling plane. These functions are connected to the SBA, so these functions need to exchange signaling messages. This means that slices have interslice communication. Slicing allows the flexible customization of network functions and the rapid deployment of services. This group of network functions communicate with each other. The MNO aims to group NFs on the transport and signaling planes into security zones according to the requirements of this slice. Some NFs communicate in this group using TLS and IPSec, but others share the signaling plane. Thus, key areas must be protected: between the network and the internetwork, between slices, between shared and non-shared NFs, and between 5G and elements of previous generations.

Each slice is identified in the CN, RAN, and UE by a slice identifier called single network slice selection assistance information (S-NSSAI). S-NNSAI is composed of the slice service type (SST) and service differentiator (SD). The slice service type is a predefined value that refers to the expected network slice behavior, depending on the slice type. A slice differentiator is optional for the MNO for differentiation between the same types of slices. S-NSSAI can have standard values or non-standard values. A non-standard value identifies a single slice in the network associated with it. The UE can work in several slices; in this case, the MNO uses a group or list of slices called network slice selection assistance information (NSSAI). NSSAI is used for traffic control, QoS, authorization, policy enforcement, and routing in the core network. Network Slice Selection Assistance Information is a list of slices. There are different categories of NSSAI: allowed NSSAI, rejected NSSAI, configured NSSAI, or requested NSSAI.

The detailed management aspects of network slicing are described in [138]. Slice management starts with use cases and requirements. This information is then translated into an SLA. The MNO analyzes which network functions are needed. Some cases for templates for slices are provided by [47,139,140], e.g., 3GPP TS 28.531. Then, the templates are populated based on the SLA, and the templates, called network slice types (NESTs), are settled. The NEST defines the characteristics based on the use cases and requirements. The NEST is used to identify the resources and functions needed to create slices, see Figure 9.

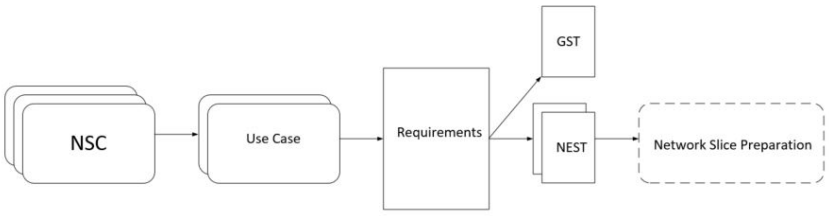

Figure 9. Preparation before slice creation.

Slice management consists of four steps: preparation, commissioning, operation, and decommissioning. The preparation phase is network slice design, which includes capacity planning, onboarding, network function planning, environment preparation, and other tasks to create a network slice instance. The commissioning phase consists of

the creation of the slice. All necessary resources are allocated and configured to fulfill the requirements in this phase. The operation phase consists of the activation, supervision, performance reporting, capacity planning, modification, and deactivation of the NSI. The decommissioning phase involves decommissioning NSI components and removing specific configurations from shared components. After the decommissioning phase, this NSI is terminated, see Figure 10.

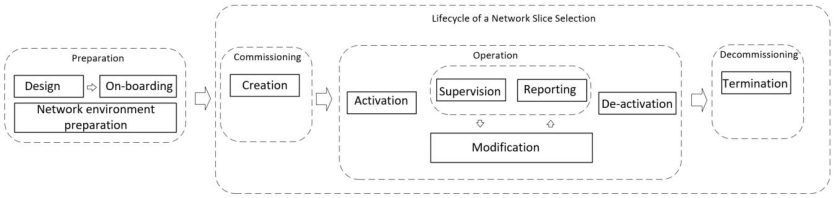

Figure 10. Management aspects of network slicing.

Blockchain in 5G can improve IoT systems due to the improvement of such characteristics as security and performance. It will also enhance the serviceability of such networks. Implementing blockchain for healthcare and smart cities will help to ensure direct and secure connections between users, service providers, and network operators. It will allow safe and low-latency communication and resource-sharing methods. Data privacy is essential in the healthcare system. Depending on the supported features and network function optimization, the MNO may offer different slice types. Each slice must have different S-NSSAI (e.g., eMBB for various streaming providers or mMTC for other IoT service providers). Slice creation is a part of the commissioning phase.

- The creation of slices starts with the vertical, which has its use cases and requirements. This requirement is converted into a Service Level Agreement;
- The MNO analyzes which network functions are needed and uses templates [47,139,140];
- A filled-in template is created, called a network slice type;
- The slice and the network functions are tested;
- The MNO enforces the QoS attributes for the slice.

The MNO acquires the information about the NSI using the network slice selection assistant information—NSSAI. NSSAI is not standardized.

8.3. Slice Selection

There are two different approaches to selecting a slice. First, the UE has the option to choose the appropriate NSI. The core network checks whether access to the selected instance can be granted. The CN selects a slice based on the device service request in the second solution. Slice selection can occur based on QoS class identifiers, security needs, or traffic routing [42,123,141].

8.4. Blockchain-Based Secure Slice Identification

It is assumed that improving or even making a mandatory field that provokes the above problems is possible. It involves an identifier, S-NSSAI. The general management aspects of network slicing will remain unchanged from 3GPP TS 28.530. However, after creating requirements, one step will be added. This step will use blockchain technology to create S-NSSAI. The SST parameter will remain unchanged, but the SD part will be created using a random algorithm, see Figure 11.

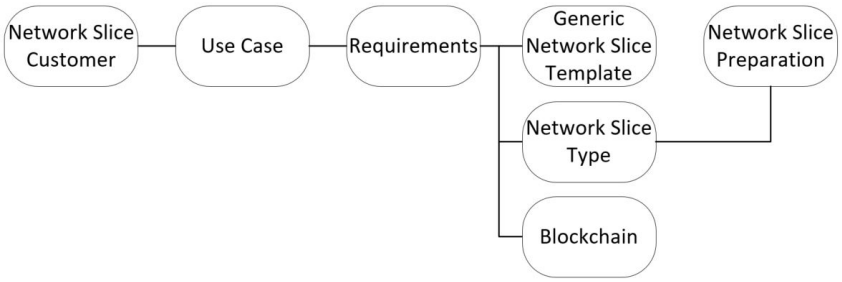

Figure 11. Slice creation with an additional step to create S-NSSAI.

An example of such a blockchain is given in Figure 12.

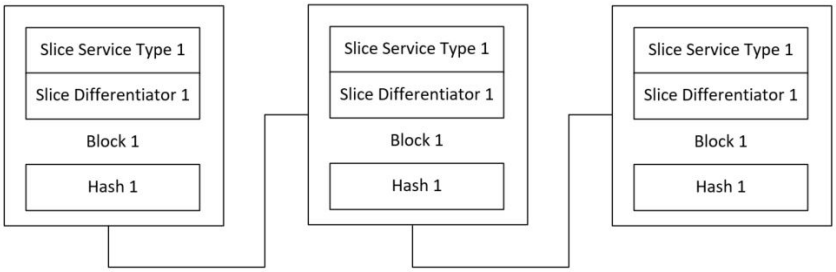

Figure 12. Blockchain scheme for S-NSSAI.

8.5. Simple Slice Access with Blockchain-Based S-NSSAI

The 3GPP standard deals with attack scenarios in which only authorized user equipment can access and use the services of a particular network slice. A network slice selection function (NSSF) is used for this, which holds the NSSAI [142]. The NSSAI is a list of slice identities—a list of S-NSSAIs. The usual use case is that the UE will have access to a specific private or corporate data network. Each UE has so-called subscription information. This subscription information has different data network names (DNNs) that this user equipment can access and that belong to specific slices. The DNNs in 5G are equivalent to access point names (APNs) in 4G, which could be a particular factory network or corporate network. The UE is pre-configured with default NSSAI. A UE can use services that use several slices—internet access and private networks. If the UE is roaming, the visited network can update the allowed NSSAI slices by mapping its corresponding S-NSSAI based on SST [143].

The S-NSSAI slice identity is critical for authenticating and authorizing the UE's access to a slice. There are two approaches to controlling UE access to a slice: simple slice access, which occurs during UE registration in the network, and slice-specific access, which requires an extra authentication step. This second step uses other authentication types with an extensible authentication protocol (EAP).

Gaining access to a slice is part of the standard procedure in 5G [54]. The proposed slice access scheme using blockchain technology consists of the following steps; see Figure 13.

1. The UE sends the RAN a list of S-NSSAI in the registration request to find the slice. It can also send a mapping of the requested NSSAI in the case of roaming. The RAN does not know the subscription data for this UE.
2. The RAN performs the initial selection of the access and mobility function (AMF). This choice can be based on an AMF address or RAT and the requested NSSAI. The RAN can also apply local configuration when the provided information is insufficient or invalid.
3. To perform the registration, the RAN sends a request to the AMF, and this information contains the requested NSSAI and mapping information (in the case of roaming).
4. The initial AMF checks whether access to this S-NSSAI is allowed. The AMF contacts the UDM to make a request for the UE's slice selection Subscription data.

5. The first UDM supplies the requested data to the first AMF.
6. The AMF now has information about the UE, i.e., which slices are subscribed to, from the information supplied by the UDM. The AMF now has the data to cross-check whether the UE is allowed to access the slices requested.
7. The first AMF may not be able to service all S-NSSAI on request. In this case, it sends a network slice selection request to the NSSF. This request can hold the requested NSSAI, mapping, subscribed S-NSSAI, and other parameters [54]. The NSSF may need to obtain data from the NRF to discover the target AMFs for this UE.
8. The NSSF must contact the NRF to request a list of AMF candidates and include the S-NSSAI that it considers suitable for the candidate AMF [54].
9. The NRF contacts the proper blockchain, which supplies a list of available identifiers.
10. The blockchain returns the candidate list to the NRF.
11. The NRF finds the AMF and returns a candidate list of AMFs to the NSSF.
12. The NSSF returns to the first AMF the allowed NSSAI and optionally maps the allowed NSSAI and the target set or the list of candidate AMFs.
13. The initial AMF receives the list of candidate AMFs. The stored AMF instance address must contact the NRF for discovery if it does not have the candidate. The first AMF now has two options: redirecting the UE to the new target AMF or informing the target AMF that the first AMF will serve the UE. An action is chosen based on the local configuration and subscription information.
14. The RAN sends the first UE message to the new target AMF and indicates the route change due to the slice information provided by the NSSF through the first AMF in the previous message.
15. The new AMF that services the UE executing the UE's requested slice now continues the standard registration procedure [144].

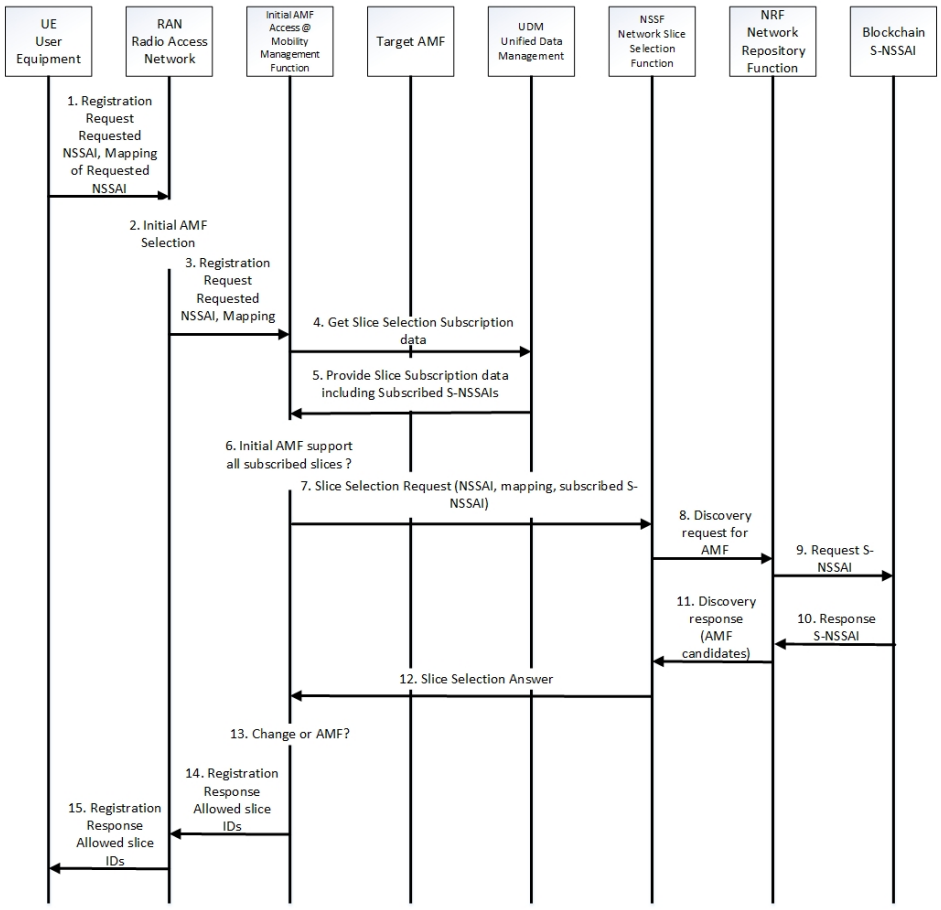

Figure 13. Simple slice access with blockchain security.

The overall basic concept is that the UE presents slices configured for use, and then the network cross-checks this with the subscription database during registration. If the information is correct, it runs the necessary NF to configure access. Once the AMF has verified the identity of the UE fragment, no further cross-checks are performed by the NRF or other network functions. The use of blockchain technologies in the above procedure means that the NRF will store a modified S-NSSAI identifier, part of which is stored in the blockchain ledger.

9. Protocols' Analysis

The 5G network architecture includes new technologies developed and standardized after implementing previous-generation networks. It introduces many improvements, but the use of new technologies and the openness of the network, including the inclusion of a significant number of partners and operators, leads to new security challenges.

Mobile networks continue to develop. Even when MNOs switch to the 5G core, they will continue to support interactions with older-generation networks for several reasons. Firstly, it should be considered that the transition will occur at different rates for different MNOs. The mixed architecture should support the interaction of 5G networks with 4G networks. However, the standards do not specify security issues related to the interaction of a 4G network with slices in 5G networks. We expect that such a network interaction will entail security problems.

The development of internetworks also brings an increase in the complexity of setting up these structures. It should be assumed that several mistakes will be made when creating such networks. In addition, 5G networks have increased protocol complexity compared to 4G networks. Approximately five times more types of commands are sent between MNOs, and around four times more information elements can be transmitted compared to 4G networks. These implications are evident for security issues since every command and element must be verified before being sent to the network. The complexity further continues to increase as the network develops. Moreover, each hosting operator will manage the slices, and ensuring secure access to these slices for clients is necessary. All this will lead to setting problems, omissions, and the following issues.

Slicing is a necessary element in 5G networks. The S-NSSAI slice identity is used to supply the correct features to the UE since the UE will receive the required functions by connecting to the proper slice. S-NSSAI has two parts: the mandatory SST (a predefined value depending on the use case) and the SD. When the MNO starts to deploy a slice, the SD value is set every time. The SD value can be placed at the operator's discretion; the standard does not describe this requirement. This means that the attacker can guess the differentiator. Let us assume that the differentiator is not given or that it can be supposed. In this case, this means that a rogue NF or rogue slice from the compromised partner can use it to obtain unauthorized information or access resources. The main problem is that the specifications do not provide for layer matching. Since there is no overlap between the layers, the NRF will only see, at the lower transport/network layer, the "authenticated partner". At the upper signaling plane, it can see the actual slice ID and service request. There is no cross-checking of whether the slice ID in the request matches the slice ID used for the TLS tunnel. If two slices in the network interact with the NRF, one slice is fraudulent. A rogue slice can take advantage of such flaws and, through interaction with the NRF and another slice, gain access to the information of another slice. The roaming procedure also has potential security issues because a fraudulent slice in one MNO can obtain a token to service its slice in another MNO.

Another problem is confirming elements in messages passed between network functions. In particular, 3GPP has the congestion control indicator header information, which is part of the HTTP header and should be used to show the overload of one network function to another during service operations [145]. Using this feature, a fraudulent slice in the network can attack another slice by creating HTTP messages with a service request that includes an overload of header information, 3GPP-SBI-OSI, and the slice identifier (S-NSSAI). Currently, 3GPP does not include a requirement to check whether the slice identity in the

3GPP-SBI-OSI header matches the slice identifier in the token for the use of the service API. The slice identifier in the token requires an added field, AuthenticationTokenClaims, which is not defined in detail and does not provide interoperability between the network functions of different providers. The improper use of congestion control features can potentially lead to partial network delays or outages.

The next problem is network zoning, which depends on the subscriber's interaction with the network. This situation may arise if a subscriber simultaneously uses several slices with different service quality levels (e.g., fixed by SLA [146]). The situation becomes more complicated when the subscriber uses slices migrating between operators. the 5G standard uses the security edge proxy (SEPP), but this solution seems insufficient for more complex network usage scenarios.

As a solution to the security issues presented above, we propose using blockchain to protect access to the slices and prevent mistakes at network and slice interfaces. In Tables 1 and 2, we summarize these issues for six types of connection procedures: simple slice access, slice-specific access that requires extra authentication, interworking procedures without an N26 interface, untrusted non-3GPP access, trusted non-3GPP access [147], and simple slice access with blockchain technology.

Table 1. Security aspects of slice access: Part I.

Security Aspect	Simple Slice Access [147]	Slice-Specific Access That Requires Extra Authentication [147]	Simple Slice Access with Blockchain Technology
Security issues at slice level	1. Issues with misconfigured, misbehaving, malfunctioning, or compromised slices. 2. Leakage of information from a rogue slice to another slice or through shared elements. 3. Communication security issues between slices. 4. Interaction with legacy networks. 5. Interaction and cross-validation between network layers. 6. Attacks between different protocols.		
Security challenges	1. Legacy interworking. 2. Increased complexity. 3. Configuration mistakes and missing layer matching. 4. Missing security zones.		
Vulnerabilities	1. SDS in HTTP header for DoS. 2. Malicious access to different slices by modifying slice differentiator.		SDS in HTTP header for DoS.
Extra security check	No validation of whether a network function is presenting the correct S-NSSAI.		S-NSSAI is requested via trusted blockchain technology.

Table 2. Security aspects of slice access: Part II.

Security Aspect	Interworking Procedures without N26 Interface [147]	Untrusted Non-3GPP Access [147]	Trusted Non-3GPP Access [147]
Security challenges	1. Improper integration with older networks. 2. Vulnerabilities in 3GPP LTE protocols. 3. Vulnerabilities in LTE system architecture, security architecture, security mechanism, access procedure, and handover procedure. 4. 4G network configuration and implementation vulnerabilities.	1. Improper integration with non-3GPP networks. 2. Vulnerabilities in non-3GPP networks (WiFi, WiMAX, fixed networks, CDMA networks).	
Vulnerabilities	1. Authentication and authorization. 2. Key management. 3. Encryption. 4. Physical layer (layer 1) vulnerabilities. 5. Denial of service. 6. Bandwidth stealing [148].	Vulnerabilities in non-3GPP networks (WiFi, WiMAX, fixed networks, CDMA networks).	

10. Conclusions and Future Work

In this paper, we present the impact of modern technologies used in fifth-generation (5G) networks on their security. In particular, we consider the effect of using slicing and virtualization techniques. The recent approach to building 5G networks assumes that many partners (network owners, service providers, and end-users of different competencies) will connect to the networks. In such a new network ecosystem, attackers are expected to use new types of attacks. Our analysis shows that there are security problems that are not considered by the 5G-related standards. The study reveals that attacks on new technology approaches used in 5G networks are possible. Using slicing technology, in addition to the apparent advantages, also leads to security problems. The security issues that cannot be solved only with the help of the present standards used are access to a network function and the related information of other vertical industries, internal network problems against network functions, user data, and user data extraction (e.g., geolocation).

The access of user devices to a specific slice is well protected, but some core network security aspects are not covered. How the slice access information is protected is at the discretion of slice owners, and the configuration and deployment requirements do not cover this problem. In the present network slicing model, information can potentially be revealed. Accordingly, it is possible to abuse the services and carry out an attack on the network elements. Using firewalls and TLS encryption will not provide complete protection against this attack. This countermeasure does not protect against partner attacks or unreliable network functions. In the model, authentication and authorization at the slice level exist. However, there are also problems: misconfigured or compromised slices, information extraction via shared elements between slices, interslice communication security, interactions with legacy networks, cross-validation between layers, and attacks between protocols. Some authors suggest solving these problems using enhanced filtering and validation approaches. This is an excellent approach to some extent because it allows the network to be divided into security zones to protect the core network, but this approach does not resolve the essence of the problem. In this paper, a new protection method is proposed as a solution.

We suggest solving the configuration security issues in slices and establishing trust between slices using blockchain technology. Depending on the needs, a private or consortium-type blockchain can be used. The approach involves using blockchain technology at the slice creation stage. It will allow us to control the necessary parameters of the slices and safely save them. Blockchain is also proposed in the simple slice access procedures and slice-specific access procedures. The approach with blockchain increases the control over the identifiers of the S-NSSAI type. In future work, we plan to consider applying blockchain technology in other core network aspects. This should reduce the necessary further checks using enhanced filtering and validation.

Making the procedure for managing access to slices using blockchain proposed in this paper practically feasible requires many experiments. In addition to estimating the efficiency of generating identifiers and the appropriate optimization of calculations, methods of providing compatibility between different types of networks and procedures of efficient data transfer should be developed. These tasks will be the next step in our activities.

It is necessary to simulate the operation of the 5G network and the influence of the slice configuration parameters on the procedure when connecting to the core network. In this simulation, it is necessary to create a 5G CN and create several slices. Then, we need to analyze the influence of the slice parameters and network configuration on the UE that will connect to the slices and, accordingly, to the network core. It is also assumed that the UE can connect to several slices simultaneously. To determine the dependence, it is necessary to create additional delays and additional network interference, between the subscriber and the network core. All these experiments will make it possible to determine more precise characteristics for the use of blockchain technology, which in turn will make it possible to avoid the problems specified in Section 9.

Author Contributions: Conceptualization, S.O.; methodology, S.O.; validation, S.O. and Z.K.; formal analysis, S.O. and Z.K.; investigation, S.O.; resources, S.O. and Z.K.; writing—original draft preparation, S.O.; writing—review and editing, S.O. and Z.K.; visualization, S.O.; supervision, Z.K.; project administration, Z.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

3GPP	Third-Generation Partnership Project
4G	Fourth-Generation Mobile Network
5G	Fifth-Generation Mobile Network
5G-b	Beyond Fifth-Generation Mobile Network
5G-IA	5G Infrastructure Association
5G PPP	5G Public–Private Partnership
5GS	5G System
5GU	5G for Ubiquitous Connectivity
6G	Sixth-Generation Mobile Network
AAC	Augmentative and Alternative Communication
ABAC	Attribute-Based Access Control
AC	Access Control
AMF	Access and Mobility Management Function
BBU	Baseband Unit
BFSI	Banking, Financial Services, and Insurance
CA	Certificate Authority
CAC	Capability-Based Access Control
CN	Core Network
C-RAN	Cloud Radio Access Network; Centralized Radio Access Network
CSP	Content Security Policy
D2D	Device-to-Device
DAC	Discretionary Access Control
DDoS	Distributed Denial of Service
DMA	Direct Memory Access
DoS	Denial of Service
E2E	End-to-End
ETSI	European Telecommunications Standards Institute
eMBB	Enhanced Mobile Broadband
ERC	Ethereum Request for Comments
FDMA	Frequency Division Multiple Access
F-OFDM	Filtered-Orthogonal Frequency-Division Multiplexing
FWA	Fixed Wireless Access
GMPLS	Generalized Multi-Protocol Label Switching
GSM	Global System for Mobile Communications
ID	Identity
IEEE	Institute of Electrical and Electronics Engineers
IMT-2020	International Mobile Telecommunications-2020
IOMMU	Input–Output Memory Management Unit
IoT	Internet of Things
IPsec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6

ISO OSI	International Organization for Standardization Open Systems Interconnection
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
JSON	JavaScript Object Notation
JWT	JSON Web Token
LTE	Long Term Evolution
M2M	Machine-to-Machine
MAC	Mandatory Access Control
MACsec	Media Access Control Security
MANO	Management and Orchestration
MEC	Multi-Access Edge Computing; Mobile Edge Computing
ML	Machine Learning
MNO	Mobile Network Operator
mMTC	Massive Machine Type Communication
MPLS	Multiprotocol Label Switching
NF	Network Function
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
NRF	Network Repository Function
NSI	Network Slice Instance
NSSAI	Network Slice Selection Assistance Information
OFDM	Orthogonal Frequency-Division Multiplexing
OPSEC	Operations Security
OQAM/FBMC	Offset QAM/Filter-Bank Multi-Carrier
OS	Operating System
OSI	Open Systems Interconnection
OXC	Optical Cross-Connect
PIN	Personal Identification Number
P-OFDM	Polar-Orthogonal Frequency-Division Multiplexing
PoW	Proof of Work
QAM	Quadrature amplitude modulation
QAM-FBMC	QAM Filter-Bank Multi-Carrier
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
RBAC	Role-Based Access Control
RFC	Request for Comments
RFID	Radio-Frequency Identifiier
ROADM	Reconfigurable Optical Add-Drop Multiplexer
SD	Service Differentiator
SDN	Software-Defined Networking
SEPP	Secure Edge Protection Proxy
SHA	Secure Hash Algorithm
S-NSSAI	Single Network Slice Selection Assistance Information
SST	Slice Service Type
SUPI	Subscription Permanent Identifier
TDMA	Time-Division Multiple Access
TLS	Transport Layer Security
TPS	Transactions Per Second
UAV	Unmanned Aerial Vehicle

UE	User Equipment
URL	Uniform Resource Locator
URLLC	Ultra-Reliable Low-Latency Communication
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNF	Virtual Network Function
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VTF	Vertical Engagement Task Force

References

1. *Minimum Requirements Related to Technical Performance for IMT-2020 Radio Interface(s)*; Report ITU-R M.2410-0; ITU: Geneva, Switzerland, 2017.
2. Why Do We Need 5G? Available online: https://www.etsi.org/technologies/ (accessed on 17 January 2024).
3. Spathoulas, G.; Katsikas, S. Towards a Secure Industrial Internet of Things. In *Security and Privacy Trends in the Industrial Internet of Things. Advanced Sciences and Technologies for Security Applications*; Alcaraz, C., Ed.; Springer: Cham, Switzerland, 2019. [CrossRef]
4. Jiang, Y.; Duan, H.; Zhu, X.; Wei, Z.; Wang, T.; Zheng, F.C.; Sun, S. Toward URLLC: A Full Duplex Relay System with Self-Interference Utilization or Cancellation. *IEEE Wirel. Commun.* **2021**, *28*, 74–81. [CrossRef]
5. Sefati, S.S.; Halunga, S. Ultra-reliability and low-latency communications on the internet of things based on 5G network: Literature review, classification, and future research view. *Trans. Emerg. Telecommun. Technol.* **2023**, *34*, e4770. [CrossRef]
6. Doukoglou, T.; Gezerlis, V.; Trichias, K.; Kostopoulos, N.; Vrakas, N.; Bougioukos, M.; Legouable, R. Vertical Industries Requirements Analysis and Targeted KPIs for Advanced 5G Trials. In Proceedings of the 2019 European Conference on Networks and Communications (EuCNC), Valencia, Spain, 18–21 June 2019. [CrossRef]
7. Vannithamby, R.; Soong, A.C.K. (Eds.) *5G Verticals: Customizing Applications, Technologies, and Deployment Techniques*; Wiley: New York, NY, USA, 2020. [CrossRef]
8. 5G Infrastructure Association Web Page. Available online: https://5g-ia.eu/verticals/ (accessed on 17 January 2024).
9. Great Expectations: Sizing the Opportunity for 5G in Vertical Industries. Survey Report, Insights Mobile World Live, 9 March 2020. Available online: https://www.gsma.com/iot/resources/great-expectations-sizing-theopportunity-for-5g-in-vertical-industries/ (accessed on 17 January 2024).
10. Nowak, T.W.; Sepczuk, M.; Kotulski, Z.; Niewolski, W.; Artych, R.; Bocianiak, K.; Osko, T.; Wary, J.P. Verticals in 5G MEC-Use Cases and Security Challenges. *IEEE Access* **2021**, *9*, 87251–87298. [CrossRef]
11. Blancoa, B.; Fajardo, J.O.; Giannoulakis, I.; Kafetzakis, E.; Peng, S.; Pérez-Romero, J.; Trajkovska, I.; Khodashenas, P.S.; Goratti, L.; Paolino, M.; et al. Technology pillars in the architecture of future 5G mobile networks: NFV, MEC and SDN. *Comput. Stand. Interfaces* **2017**, *54*, 216–228. [CrossRef]
12. Singh, S.; Jha, R.K. A Survey on Software-Defined Networking: Architecture for Next Generation Network. *J. Netw. Syst. Manag.* **2017**, *25*, 321–374. [CrossRef]
13. Long, Q.; Chen, Y.; Zhang, H.; Lei, X. Software-Defined 5G and 6G Networks: A Survey. *Mob. Netw. Appl.* **2019**, *27*, 1792–1812. [CrossRef]
14. Mijumbi, R.; Serrat, J.; Gorricho, J.L.; Bouten, N.; De Turck, F.; Boutaba, R. Network Function Virtualization: State-of-the-Art and Research Challenges. *IEEE. Commun. Surv. Tuts.* **2016**, *18*, 236–262. [CrossRef]
15. Chiaraviglio, L.; Salsano, S.; Melazzi, N.B.; Sidoretti, G.; Rossetti, S.; Chiasserini, C.F.; Malrino, F.; D'Andreagiovanni, F. Algorithms for the design of 5G networks with VNF-based Reusable Functional Blocks. *Ann. Telecommun.* **2019**, *74*, 559–574. [CrossRef]
16. Barakabitze, A.A.; Ahmad, A.; Mijumbi, R.; Hines, A. 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. *Comput. Netw.* **2020**, *167*, 106984. [CrossRef]
17. Sahay, R.; Meng, W.; Jensen, C.D. The application of Software Defined Networking on securing computer networks: A survey. *J. Netw. Comp. Appl.* **2019**, *131*, 89–108. [CrossRef]
18. Nife, F.; Kotulski, Z.; Reyad, O. New SDN-Oriented Distributed Network Security System. *Appl. Math. Inf. Sci.* **2018**, *12*, 673–683. [CrossRef]
19. Hu, Y.-C.; Patel, M.; Sabella, D.; Sprecher, N.; Young, V. Mobile Edge Computing. A key Technology towards 5G, ETSI White Paper No. 11, First Edition, September 2015. Available online: https://www.etsi.org/images/files/etsiwhitepapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf (accessed on 17 January 2024).
20. Enisa Threat Landscape for 5G Networks. Threat Assessment for the Fifth Generation of Mobile Telecommunications Networks (5G), November 2019. Available online: https://www.enisa.europa.eu/publications/ (accessed on 17 January 2024).
21. Enisa Threat Landscape for 5G Networks. Updated Threat Assessment for the Fifth Generation of Mobile Telecommunications Networks (5G), December 2020. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks (accessed on 17 January 2024).

22. Monshizadeh, M.; Khatri, V.; Adam, I. Security for Vertical Industries. In *Wiley 5G Ref: The Essential 5G Reference*; Wiley: New York, NY, USA, 2019. [CrossRef]
23. Krishnan, P.; Duttagupta, S.; Achuthan, K. SDNFV Based Threat Monitoring and Security Framework for Multi-Access Edge Computing Infrastructure. *Mob. Netw. Appl.* **2019**, *24*, 1896–1923. [CrossRef]
24. Fourati, H.; Maaloul, R.; Chaari, L. A survey of 5G network systems: Challenges and machine learning approaches. *Int. J. Mach. Learn. Cyber.* **2021**, *12*, 385–431. [CrossRef]
25. Kotulski, Z.; Nowak, T.W.; Sepczuk, M.; Tunia, M.; Artych, R.; Bocianiak, K.; Osko, T.; Wary, J.P. Towards constructive approach to end-to-end slice isolation in 5G networks. *EURASIP J. Inf. Sec.* **2018**, *2018*, 2. [CrossRef]
26. 5G E2E Technology to Support Verticals URLLC Requirements. NGMN Alliance. 2020. Available online: https://ngmn.org/wp-content/uploads/200210-NGMN_Verticals_URLLC_Requirements_v16.pdf (accessed on 17 January 2024).
27. Dai, H.-N.; Wu, Y.; Imran, M.; Nasser, N. Integration of Blockchain and Network Softwarization for Space-Air-Ground-Sea Integrated Networks. *IEEE Internet Things Mag.* **2022**, *5*, 166–172. [CrossRef]
28. ETSI GR NGP 011 V1.1.1 (2018-09) Next Generation Protocols (NGP); E2E Network Slicing Reference Framework and Information Model. Available online: https://www.etsi.org/deliver/etsi_gr/NGP/001_099/011/01.01.01_60/gr_ngp011v010101p.pdf (accessed on 17 January 2024).
29. Kotulski, Z.; Nowak, T.W.; Sepczuk, M.; Tunia, M.A. 5G networks: Types of isolation and their parameters in RAN and CN slices. *Comput. Netw.* **2020**, *171*, 107135. [CrossRef]
30. 5G Systems—Enabling Industry and Society Transformation, Ericsson White Paper, UEN 284 23-3244, Ericsson 2015. Available online: https://gsacom.com/paper/ericsson-mobility-report-mwc-2015-edition/ (accessed on 17 January 2024).
31. Gentile, A.F.; Fazio, P.; Miceli, G. A Survey on the Implementation and Management of Secure Virtual Private Networks (VPNs) and Virtual LANs (VLANs) in Static and Mobile Scenarios. *Telecom* **2021**, *2*, 430–445. [CrossRef]
32. Kotulski, Z.; Nowak, T.; Sepczuk, M.; Tunia, M.; Artych, R.; Bocianiak, K.; Osko, T.; Wary, J.P. On end-to-end approach for slice isolation in 5G networks. Fundamental challenges. In Proceedings of the 2017 Federated Conference on Computer Science and Information Systems (FedCSIS), Prague, Czech Republic, 3–6 September 2017. Available online: https://ieeexplore.ieee.org/abstract/document/8104638 (accessed on 17 January 2024).
33. ONF TR-521 SDN Architecture, Version 1.1, Open Networking Foundation. 2016. Available online: https://opennetworking.org/wp-content/uploads/2014/10/TR-521_SDN_Architecture_issue_1.1.pdf (accessed on 17 January 2024).
34. Guerzoni, R.; Trivisonno, R.; Soldani, D. SDN-based architecture and procedures for 5G networks. In Proceedings of the 1st International Conference on 5G for Ubiquitous Connectivity (5GU), Akaslompolo, Finland, 26–28 November 2014. [CrossRef]
35. Nife, F.N.; Kotulski, Z. Application-Aware Firewall Mechanism for Software Defined Networks. *J. Netw. Syst. Manag.* **2020**, *28*, 605–626. [CrossRef]
36. Deb, R.; Roy, S. A comprehensive survey of vulnerability and information security in SDN. *Comput. Netw.* **2022**, *206*, 108802. [CrossRef]
37. Alharbi, T. Deployment of Blockchain Technology in Software Defined Networks: A Survey. *IEEE Access* **2020**, *8*, 9146–9156. [CrossRef]
38. ETSI GS NFV-MAN 001 V1.2.1, Network Functions Virtualisation (NFV);Management and Orchestration; Report on Management and Orchestration Framework (2021-12). Available online: https://www.etsi.org/deliver/etsi_gr/NFV-MAN/001_099/001/01.02.01_60/gr_NFV-MAN001v010201p.pdf (accessed on 17 January 2024).
39. Chowdhury, N.M.K.; Boutaba, R. A survey of network virtualization. *Comput. Netw.* **2010**, *54*, 862–876. [CrossRef]
40. Boubendir, A.; Guillemin, F.; Le Toquin, C.; Alberi-Morel, M.L.; Faucheux, F.; Kerboeuf, S.; Lafragette, J.L.; Orlandi, B. Federation of Cross-Domain Edge Resources: A Brokering Architecture for Network Slicing. In Proceedings of the 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), Montreal, QC, Canada, 25–29 June 2018; pp. 415–423. [CrossRef]
41. NFV Security in 5G—Challenges and Best Practices, ENISA Report, 24 February 2022. Available online: https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices (accessed on 17 January 2024).
42. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for 5G and beyond networks: A state of the art survey. *J. Abbr.* **2008**, *10*, 142–149. [CrossRef]
43. Dighriri, M.; Alfoudi, A.S.D.; Lee, G.M.; Baker, T. Data Traffic Model in Machine to Machine Communications over 5G Network Slicing. In Proceedings of the 2016 9th International Conference on Developments in eSystems Engineering (DeSE), Liverpool, UK, 31 August–2 September 2016; pp. 239–244. [CrossRef]
44. ETSI GS MEC 003 V3.1.1 Multi-Access Edge Computing (MEC); Framework and Reference Architecture, (2022-03). Available online: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/03.01.01_60/gs_MEC003v030101p.pdf (accessed on 17 January 2024).
45. Harmonizing Standards for Edge Computing—A Synergized Architecture Leveraging ETSI ISG MEC and 3GPP Specifications, ETSI White Paper No. 36, July 2020. Available online: https://www.etsi.org/images/files/ETSIWhitePapers/ETSI_wp36_Harmonizing-standards-for-edge-computing.pdf (accessed on 17 January 2024).
46. Giust, F.; Verin, G.; Antevski, K.; Chou, J.; Fang, Y.; Featherstone, W.; Fontes, F.; Frydman, D.; Li, A.; Manzalini, A.; et al. MEC Deployments in 4G and Evolution towards 5G. ETSI White Paper No. 24, First Edition—February 2018. Available online: https://www.etsi.org/images/files/etsiwhitepapers/etsi_wp24_mec_deployment_in_4g_5g_final.pdf (accessed on 17 January 2024).

47. 3GPP, Telecommunication Management; Study on Management and Orchestration of Network Slicing for Next-Generation Network. Specification 28.801. 2018. Available online: https://www.3gpp.org/ftp/Specs/archive/28_series/28.801/ (accessed on 17 January 2024).
48. SLICENET: End-to-End Cognitive Network Slicing and Slice Management Framework in Virtualised Multi-Domain, Multi-Tenant 5G Networks. Available online: https://5g-ppp.eu/slicenet/ (accessed on 17 January 2024).
49. Rost, P.; Mannweiler, C.; Michalopoulos, D.S.; Sartori, C.; Sciancalepore, V.; Sastry, N.; Holl, O.; Tayade, S.; Han, B.; Bega, D.; et al. Network Slicing to Enable Scalability and Flexibility in 5G Mobile Network. *IEEE Commun. Mag.* **2017**, *55*, 72–79. [CrossRef]
50. ETSI GR NFV-REL 010 V3.1.1 (2019-06) Network Functions Virtualisation (NFV) Release 3; Reliability; Report on NFV Resiliency for the Support of Network Slicing. Available online: https://www.etsi.org/deliver/etsi_gr/NFV-REL/001_099/010/03.01.01_60/gr_NFV-REL010v030101p.pdf (accessed on 17 January 2024).
51. ETSI GR NFV-EVE 012 V3.1.1 (2017-12) Network Functions Virtualisation (NFV) Release 3; Evolution and Ecosystem; Report on Network Slicing Support with ETSI NFV Architecture Framework. Available online: https://www.etsi.org/deliver/etsi_gr/NFV-EVE/001_099/012/03.01.01_60/gr_nfv-eve012v030101p.pdf (accessed on 17 January 2024).
52. ETSI GR MEC 024 V2.1.1 (2019-11) Multi-Access Edge Computing (MEC); Support for Network Slicing. Available online: https://www.etsi.org/deliver/etsi_gr/MEC/001_099/024/02.01.01_60/gr_mec024v020101p.pdf (accessed on 17 January 2024).
53. Lu, Y.; Chen, X.; Xi, R.; Chen, Y. An access selection mechanism in 5G network slicing. In Proceedings of the 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), Beijing, China, 14–16 August 2020; pp. 72–78. [CrossRef]
54. ETSI TS 123 501 5G; System Architecture for the 5G System (5GS), V17.7.0 (2023-01). Available online: https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/17.07.00_60/ts_123501v170700p.pdf (accessed on 17 January 2024).
55. CHARISMA, Converged Heterogeneous Advanced 5G Cloud-RAN Architecture for Intelligent and Secure Media Access. 2016. Available online: https://www.charisma5g.eu/ (accessed on 17 January 2024).
56. Li, Q.; Wu, G.; Papathanassiou, A.; Mukherjee, U. An end-to-end network slicing framework for 5G wireless communication systems. *arXiv* **2016**, arXiv:1608.00572.
57. WWRF, White Paper 3: End to End Network Slicing. 2017. Available online: https://www.wwrf.ch/files/wwrf/content/files/publications/outlook/White%20Paper%203-End%20to%20End%20Network%20Slicing.pdf (accessed on 17 January 2024).
58. Viswanathan, A.; Neuman, B.C. *A Survey of Isolation Techniques*; Draft Copy; University of Southern California, Information Sciences Institute: Los Angeles, CA, USA, 2009.
59. Ankergård, S.F.J.J.; Dushku, E.; Dragoni, N. State-of-the-Art Software-Based Remote Attestation: Opportunities and Open Issues for Internet of Things. *Sensors* **2021**, *21*, 1598. [CrossRef]
60. Gama, K.; Donsez, D. A Self-healing Component Sandbox for Untrustworthy Third Party Code Execution. In *Component-Based Software Engineering CBSE 2010*; Grunske, L., Reussner, R., Plasil, F., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6092. [CrossRef]
61. Gupta, D.; Cherkasova, L.; Gardner, R.; Vahdat, A. Enforcing Performance Isolation Across Virtual Machines in Xen. In *Middleware 2006: ACM/IFIP/USENIX 7th International Middleware Conference, Melbourne, Australia, 27 November–1 December 2006*; van Steen, M.H., Ed.; Lecture Notes in Computer Science, 4290; Springer: Berlin/Heidelberg, Germany, 2006; pp. 342–362. [CrossRef]
62. Narayanan, V.; Huang, Y.; Tan, G.; Jaeger, T.; Burtsev, A. Lightweight kernel isolation with virtualization and VM functions. In Proceedings of the VEE '20 Proceedings of the 16th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments, Lausanne, Switzerland, 17 March 2020; pp. 157–171. [CrossRef]
63. Ehret, A.; Rosario, E.D.; Schwicking, C.; Gettings, K.; Kinsy, M.A. Reconfigurable Hardware Root-of-Trust for Secure Edge Processing. In Proceedings of the 2021 IEEE High-Performance Extreme Computing Conference (HPEC), Waltham, MA, USA, 20–24 September 2021; pp. 1–7. [CrossRef]
64. Farinacci, D.; Li, T.; Hanks, S.; Meyer, D.; Traina, P. Generic Routing Encapsulation (GRE), RFC 2784. 2000. Available online: https://www.rfc-editor.org/rfc/rfc2784.html (accessed on 17 January 2024).
65. Hamzeh, K.; Pall, G.; Verthein, W.; Taarud, J.; Little, W.; Zorn, G. Point-to-Point Tunneling Protocol (PPTP), RFC 2637. 1999. Available online: https://www.rfc-editor.org/rfc/rfc2637 (accessed on 17 January 2024).
66. Rosen, E. Rekhter, BGP/MPLS IP Virtual Private Networks (VPNs), RFC 4364, IETF, February 2006. Available online: https://www.rfc-editor.org/rfc/rfc4364 (accessed on 17 January 2024).
67. Benhaddou, D.; Alanqar W. Layer 1 virtual private networks in multidomain next-generation networks. *IEEE Commun. Mag.* **2007**, *45*, 52–58. [CrossRef]
68. Takeda, T. Framework and Requirements for Layer 1 Virtual Private Networks, RFC 4847. 2007. Available online: https://datatracker.ietf.org/doc/html/rfc4847 (accessed on 17 January 2024).
69. Konorski, J.; Pacyna, P.; Kolaczek, G.; Kotulski, Z.; Cabaj, K.; Szalachowski, P. A Virtualization-Level Future Internet Defense-in-Depth Architecture. In *Recent Trends in Computer Networks and Distributed Systems Security. SNDS 2012. Communications in Computer and Information Science*; Thampi, S.M., Zomaya, A.Y., Strufe, T., Alcaraz Calero, J.M., Thomas, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 335. [CrossRef]
70. Townsley, W.; Valencia, A.; Rubens, A.; Pall, G.; Zorn, G.; Palter, B. Layer Two Tunneling Protocol L2TP, RFC 2661. 1999. Available online: https://www.rfc-editor.org/rfc/rfc2661.html (accessed on 17 January 2024).
71. Kent, S.; Seo, K. Security Architecture for the Internet Protocol, RFC 4301, RFC. 2005. Available online: https://www.rfc-editor.org/rfc/rfc4301 (accessed on 17 January 2024).

72. Furuhashi, R.; Nakao, A. Opentag: Tag-based network slicing for wide-area coordinated in-network packet processing. In Proceedings of the 2011 IEEE International Conference on Communications Workshops (ICC), Kyoto, Japan, 5–9 June 2011. https://doi.org/10.1109/iccw.2011.5963588. [CrossRef]
73. Yaga, D.; Mell, P.; Roby, N.; Scarfon, K. NISTIR 8202, Blockchain Technology Overview. 2018. Available online: https://csrc.nist.gov/publications/detail/nistir/8202/final (accessed on 17 January 2024).
74. Natarajan, H.; Krause, S.; Gradstein, H. World Bank Group, Distributed Ledger Technology (DLT) and Blockchain. 2017. Available online: https://olc.worldbank.org/system/files/122140-WP-PUBLIC-Distributed-LedgerTechnology-and-Blockchain-Fintech-Notes.pdf (accessed on 17 January 2024).
75. Isnsiti, M.; Lakhani, K.R. The Truth about Blockchain. 2017. Available online: https://hbr.org/2017/01/the-truth-about-blockchain (accessed on 17 January 2024).
76. Haber, S.; Stornetta, W.S. How to time-stamp a digital document. *J. Cryptol.* **1991**, *3*, 99–111. [CrossRef]
77. Narayanan, A.; Bonneau, J.; Felten, E.; Miller, A.; Goldfeder, S. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*; Princeton University Press: Princeton, NJ, USA, 2016; ISBN 978-0-691-17169-2.
78. Lamport, L. The Part-Time Parliament. 1998. Available online: https://lamport.azurewebsites.net/pubs/lamport-paxos.pdf (accessed on 17 January 2024).
79. Zhou, S.; Li, K.; Xiao, L.; Cai, J.; Liang, W.; Castiglione, A. A Systematic Review of Consensus Mechanisms in Blockchain. Mathematics 2023, 11, 2248. [CrossRef]
80. Okamoto, T.; Ohta, K. Universal Electronic Cash. In *Advances in Cryptology—CRYPTO '91. CRYPTO 1991*; Feigenbaum, J., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1992; Volume 576. [CrossRef]
81. Merkle, R.C. A Digital Signature Based on a Conventional Encryption Function. In *Advances in Cryptology—CRYPTO '87. CRYPTO 1987*; Pomerance, C., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1988; Volume 293. [CrossRef]
82. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 17 January 2024).
83. Dwork, C.; Naor, M. Pricing via Processing or Combatting Junk Mail. In *Advances in Cryptology — CRYPTO' 92. CRYPTO 1992*; Brickell, E.F., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1993; Volume 740. [CrossRef]
84. Ge, L.; Wang, J.; Zhang, G. Survey of Consensus Algorithms for Proof of Stake in Blockchain. *Secur. Commun. Netw.* **2022**, *2022*, 2812526. [CrossRef]
85. Courtois, N.T.; Grajek, M.; Naik, R. Optimizing SHA256 in Bitcoin Mining. In *Cryptography and Security Systems. CSS 2014. Communications in Computer and Information Science*; Kotulski, Z., Księżopolski, B., Mazur, K., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; Volume 448. [CrossRef]
86. Onopa, S.; Kotulski, Z. Improving security of lightweith SHA-3 against preimage attacks. *Int. J. Electron. Telecommun.* **2018**, *64*, 159–166. [CrossRef]
87. Ahmed-Rengers, M.; Kostiainen, K. Don't Mine, Wait in Line: Fair and Efficient Blockchain Consensus with Robust Round Robin. *arXiv* **2018**, arXiv:1804.07391. [CrossRef]
88. Manolache, M.A.; Manolache, S.; Tapus, N. Decision Making using the Blockchain Proof of Authority Consensus. *Procedia Comput. Sci.* **2022**, *199*, 580–588. [CrossRef]
89. Chen, L.; Xu, L.; Shah, N.; Gao, Z.; Lu, Y.; Shi, W. On Security Analysis of Proof-of-Elapsed-Time (PoET). In *Stabilization, Safety, and Security of Distributed Systems*; SSS 2017; Spirakis, P., Tsigas, P., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2017; Volume 10616. [CrossRef]
90. Khan, D.; Jung, L.T.; Hashmani, M.A.; Waqas, A. A Critical Review of Blockchain Consensus Model. In Proceedings of the 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 29–30 January 2020; pp. 1–6. [CrossRef]
91. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 2017. Available online: https://ieeexplore.ieee.org/document/8029379 (accessed on 17 January 2024).
92. Shetty, S.S.; Kamhoua, C.A.; Njilla, L.L. *Blockchain for Distributed Systems Security*; Wiley: Hoboken, NJ, USA, 2019; ISBN 978-1-119-51958-4.
93. Nasir, Q.; Qasse, I.A.; Talib, M.A.; Nassif, A.B. Performance Analysis of Hyberledger Fabric Platforms. *Secur. Commun. Netw.* **2018**, *2018*, 3976093. [CrossRef]
94. Bayer, D.; Haber, S.; Stornetta, W.S. Improving the Efficiency and Reliability of Digital Time-Stamping. In *Sequences II*; Capocelli, R., De Santis, A., Vaccaro, U., Eds.; Springer: New York, NY, USA, 1993. [CrossRef]
95. Leonardos, S.; Reijsbergen, D.; Piliouras, G. PREStO: A Systematic Framework for Blockchain Consensus Protocols. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1028–1044. [CrossRef]
96. Szalachowski, P. Blockchain-based TLS Notary Service. *arXiv*, **2018**, arXiv:1804.00875v1.
97. Lin, I.-C.; Liao, T.-C. A Survey of Blockchain Security Issues and Challenges. 2017. Available online: https://www.semanticscholar.org/paper/A-Survey-of-Blockchain-Security-Issues-and-Lin-Liao/f61edb500c023c4c4ef665bd7ed2423170773340 (accessed on 17 January 2024).

98. Chia, V.; Hartel, P.; Hum, Q.; Ma, S.; Piliouras, G.; Reijsbergen, D.; van Staalduinen, M.; Szalachowski, P. Rethinking Blockchain Security: Position Paper. 2018. Available online: https://arxiv.org/pdf/1806.04358.pdf (accessed on 17 January 2024).
99. Kotulski, Z.; Szczepinski, W. *Error Analysis with Applications in Engineering*; Springer: Dordrecht, The Netherlands, 2010. [CrossRef]
100. Jangirala, S.; Das, A.K.; Vasilakos, V. Designing Secure Lightweight Blockchain-Enabled RFID-Based Authentication Protocol for Supply Chains in 5G Mobile Edge Computing Environment. *IEEE Trans. Ind. Inf.* **2020**, *16*, 7081–7093. [CrossRef]
101. Kim, H.W.; Jeong, Y.S. Secure Authentication-Management human-centric Scheme for trusting personal resource information on mobile cloud computing with blockchain. *Hum. Cent. Comput. Inf. Sci.* **2018**, *8*, 11. [CrossRef]
102. Huh, J.H.; Seo, K. Blockchain-based mobile fingerprint verification and automatic log-in platform for future computing. *J. Supercomput.* **2019**, *75*, 3123–3139. [CrossRef]
103. Widick, L.; Ranasinghe, I.; Dantu, R.; Jonnada, S. Blockchain Based Authentication and Authorization Framework for Remote Collaboration Systems. In Proceedings of the 2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Washington, DC, USA, 10–12 June 2019; pp. 1–7. [CrossRef]
104. Hammi, M.T.; Hammi, B.; Bellot, P.; Serhrouchni, A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Comput. Secur.* **2018**, *78*, 126–142. [CrossRef]
105. Ouaddah, A.; Abou Elkalam, A.; Ait Ouahman, A. FairAccess: A new Blockchain-based access control framework for the Internet of Things. *Secur. Commun. Netw.* **2016**, *9*, 5943–5964. [CrossRef]
106. Sanda, T.; Inaba, H. Proposal of new authentication method in Wi-Fi access using Bitcoin 2.0. In Proceedings of the 2016 IEEE 5th Global Conference on Consumer Electronics, Kyoto, Japan, 11–14 October 2016; pp. 1–5. [CrossRef]
107. Mohsin, A.H.; Zaidan, A.A.; Zaidan, B.B.; Albahri, O.S.; Albahri, A.S.; Alsalem, M.A.; Mohammed, K.I. Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions. *Comput. Stand. Interfaces* **2019**, *64*, 41–60. [CrossRef]
108. Ghaffari, F.; Bertin, E.; Hatin, J.; Crespi, N. Authentication and access control based on distributed ledger technology: A survey. In Proceedings of the BRAINS 2020: 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services, Paris, France, 28–30 September 2020; pp. 79–86. [CrossRef]
109. Thakker, J.; Park, Y. Resilient and Efficient Blockchain Consensus Protocol for Internet-of-Things. In Proceedings of the 2020 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 4–6 January 2020; pp. 1–6. [CrossRef]
110. Lesavre, L.; Varin, P.; Mell, P.; Davidson, M.; Shook, J. A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems. 2020. Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01142020.pdf (accessed on 17 January 2024).
111. ETSI TS 133 501 V17.7.0 (2022-09), 5G: Security Architecture and Procedures for 5G System. Available online: https://cdn.standards.iteh.ai/samples/67056/b6e5388b825a4a929d08f8f72a86676c/ETSI-TS-133-501-V17-7-0-2022-09-.pdf (accessed on 17 January 2024).
112. RFC 9068, JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens, Internet Engineering Task Force, October 2021. Available online: https://www.rfc-editor.org/info/rfc9068 (accessed on 17 January 2024).
113. Request for Comments (RFCs) for the COMIT Network. Available online: https://github.com/comit-network/RFCs (accessed on 17 January 2024).
114. Fotiou, N.; Pittaras, I.; Siris, V.A.; Voulgaris, S.; Polyzos, G.C. OAuth 2.0 authorization using blockchain-based tokens. *arXiv*, **2020**, arXiv:2001.10461. [CrossRef]
115. Moreschini, S.; Pecorelli, F.; Li, X.; Naz, S.; Hästbacka, D.; Taibi, D. Cloud Continuum: The Definition. *IEEE Access* **2022**, *10*, 131876–131886. [CrossRef]
116. Tong, W.; Dong, X.; Shen, Y.; Zheng, J. BC-RAN: Cloud radio access network enabled by blockchain for 5G. *Comput. Commun.* **2020**, *162*, 179-186. [CrossRef]
117. Al-Naji, F.H.; Zagrouba, R. A survey on continuous authentication methods in Internet of Things environment. *Comput. Commun.* **2020**, *163*, 109–133. [CrossRef]
118. Huawei Technologies Co., Ltd. 5G MEC IP Network White Paper. 2020. Available online: https://carrier.huawei.com/~/media/CNBGV2/download/program/5G-MEC-IP-Network-White-Paper-en-v2.pdf (accessed on 17 January 2024).
119. Zhang, S.; Lee, J.-H. A Group Signature and Authentication Scheme for Blockchain-Based Mobile-Edge Computing. *IEEE Internet Things J.* **2020**, *7*, 4557–4565. [CrossRef]
120. Queralta, J.P.; Qinqing, L.; Zou, Z.; Westerlund, T. Enhancing Autonomy with Blockchain and Multi-Access Edge Computing in Distributed Robotic Systems. In Proceedings of the 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC), Paris, France, 20–23 April 2020; pp. 180–187. [CrossRef]
121. Nokia, Dynamic End-to-End Network Slicing for 5G, White Paper. 2016. Available online: https://gsacom.com/paper/dynamic-end-end-network-slicing-5g/ (accessed on 17 January 2024).
122. Lin, W.; Xu, X.; Qi, L.; Zhang, X.; Dou, W.; Khosravi, M.R. A Proof-of-Majority Consensus Protocol for Blockchain-enabled Collaboration Infrastructure of 5G Network Slice Brokers. In Proceedings of the BSCI '20: Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure, Taipei, Taiwan, 6 October 2020; pp. 41–52. [CrossRef]
123. Sattar, D.; Matrawy, A. Optimal Slice Allocation in 5G Core Networks. *arXiv* **2018**, arXiv:1802.04655. [CrossRef]

124. Yang, D.; Yoo, S.; Doh, I.; Chae, K. Selective blockchain system for secure and efficient D2D communication. *J. Netw. Comput. Appl.* **2021**, *173*, 102817. [CrossRef]
125. Lee, H.; Ma, M. Blockchain-based mobility management for 5G. *Future Gener. Comput. Syst.* **2020**, *110*, 638–646. [CrossRef]
126. Tan, L.; Xiao, H.; Yu, K.; Aloqaily, M.; Jararweh, Y. A blockchain-empowered crowdsourcing system for 5G-enabled smart cities. *Comput. Stand. Interfaces* **2021**, *76*, 103517. [CrossRef]
127. Ericsson White Paper, 5G Systems. Enabling Industry and Society Transformation, UEN 284 23-3251 Rev B, January 2017. Available online: https://www.ericsson.com/49daeb/assets/local/reports-papers/white-papers/wp-5g-systems.pdf (accessed on 17 January 2024).
128. Kodjiku, S.L.; Han, T.; Fang, Y.; Stacy, E.; Aggrey, E.B.; Sey, C.; Asamoah, K.O.; Fiasam, L.D.; Aidoo, E.; Wang, X. WQCrowd: Secure blockchain-based crowdsourcing framework with multi-tier worker quality evaluation. *J. King Saud Univ.—Comput. Inf. Sci.* **2023**, *35*, 101843. [CrossRef]
129. Li, S.; Bai, X.; Wei, S. Blockchain-Based Crowdsourcing Framework with Distributed Task Assignment and Solution Verification. *Secur. Commun. Netw.* **2022**, *2022*, 9464308. [CrossRef]
130. Luo, H.; Liu, S.; Xu, S.; Luo, J. LECast: A Low-Energy-Consumption Broadcast Protocol for UAV Blockchain Networks. *Drones* **2023**, *7*, 76. [CrossRef]
131. Saad, M.; Spaulding, J.; Njilla, L.; Kamhoua, C.; Shetty, S.; Nyang, D.H.; Mohaisen, A. Exploring the Attack Surface of Blockchain: A Systematic Overview. *arXiv* **2019**. [CrossRef]
132. Li, W.; Su, Z.; Li, R.; Zhang, K.; Wang, Y. Blockchain-Based Data Security for Artificial Intelligence Applications in 6G Networks. *IEEE Netw.* **2020**, *34*, 31–37. [CrossRef]
133. Nguyen, T.; Tran, N.; Loven, L.; Partala, J.; Kechadi, M.T.; Pirttikangas, S. Privacy-Aware Blockchain Innovation for 6G: Challenges and Opportunities. In Proceedings of the 2020 2nd 6G Wireless Summit (6G SUMMIT), Levi, Finland, 17–20 March 2020; pp. 1–5. [CrossRef]
134. Vincenzi, M.; Antonopoulos, A.; Kartsakli, E.; Vardakas, J.; Alonso, L.; Verikoukis, C. Multi-tenant slicing for spectrum management on the road to 5G. *IEEE Wirel. Commun.* **2017**, *24*, 118–125. [CrossRef]
135. 5G ENSURE. 2016. Available online: www.5gensure.eu (accessed on 17 January 2024).
136. 5G PPP Architecture Working Group, "View on 5G Architecture", Version 3.0, February 2020. Available online: https://5g-ppp.eu/wp-content/uploads/2020/02/5G-PPP-5G-Architecture-White-Paper_final.pdf (accessed on 17 January 2024).
137. Rebello, G.A.F.; Camilo, G.F.; Silva, L.G.; Guimarães, L.C.; de Souza, L.A.C.; Alvarenga, I.D.; Duarte, O.C.M. Providing a Sliced, Secure, and Isolated Software Infrastructure of Virtual Functions Through Blockchain Technology. In Proceedings of the 2019 IEEE 20th International Conference on High Performance Switching and Routing (HPSR), Xi'an, China, 26–29 May 2019; pp. 1–6. [CrossRef]
138. ETSI TS 129 531 V17.6.0 (2022-10) 5G; 5G System; Network Slice Selection Services; Stage 3 (3GPP TS 29.531 Version 17.6.0 Release 17). Available online: https://cdn.standards.iteh.ai/samples/67165/acd783e5673b462db091226d86bc4f18/ETSI-TS-129-531-V17-6-0-2022-10-.pdf (accessed on 17 January 2024).
139. GSM Association Non-Confidential, Official Document NG.116. "Generic Network Slice Template". Version 7.0, 17 June 2022. Available online: https://www.gsma.com/newsroom/wp-content/uploads/NG.116-v7.0.pdf (accessed on 17 January 2024).
140. ETSI TS 128 531 V17.6.0 (2023-01) 5G; Management and Orchestration; Provisioning (3GPP TS 28.531 version 17.6.0 Release 17). Available online: https://cdn.standards.iteh.ai/samples/67729/72813a2923024b0c9fee02c788a420e1/ETSI-TS-128-531-V17-6-0-2023-01-.pdf (accessed on 17 January 2024).
141. Shurman, M.; Rawashdeh, J.; Jaradat, A. Slice Selection in 5G Networks: Novel Approach for Accessing Multiple Slices Simultaneously. In Proceedings of the 2020 11th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 7–9 April 2020; pp. 113–117. [CrossRef]
142. Diaz Rivera, J.J.; Khan, T.A.; Mehmood, A.; Song, W.-C. Network Slice Selection Function for Data Plane Slicing in a Mobile Network. In Proceedings of the 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), Matsue, Japan, 18–20 September 2019,; pp. 1–4. [CrossRef]
143. GSM Association Non-Confidential, Official Document NG.132—Report 5G Mobile Roaming Revisited (5GMRR) Phase 1, Version 2.0, 6 July 2022. Available online: https://www.gsma.com/newsroom/wp-content/uploads//NG.132-v2.0-1.pdf (accessed on 17 January 2024).
144. ETSI TS 123 502 V17.7.0 (2023-01), Procedures for the 5G System (5GS). Available online: https://cdn.standards.iteh.ai/samples/67681/0a0f2faededb4d0ab3fae55ae6ad6a2c/ETSI-TS-123-502-V17-7-0-2023-01-.pdf (accessed on 17 January 2024).
145. 3GPP TS 29.500 V18.4.0 (2024-01-02) 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 5G System; Technical Realization of Service Based Architecture; Stage 3 (Release 18). Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3338 (accessed on 29 January 2024).
146. Niewolski, W.; Nowak, T.W.; Sepczuk, M.; Kotulski, Z.; Artych, R.; Bocianiak, K.; Wary, J.-P. Security Context Migration in MEC: Challenges and Use Cases. *Electronics* **2022**, *11*, 3512. [CrossRef]

147. 3GPP TS 23.502 V16.18.0 (2023-12) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Procedures for the 5G System (5GS); Stage 2 (Release 16). Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3145 (accessed on 20 February 2024).
148. Seddigh, N.; Nandy, B.; Makkar, R.; Beaumont, J.F. Security advances and challenges in 4G wireless networks. In Proceedings of the 2010 Eighth International Conference on Privacy, Security and Trust, Ottawa, ON, Canada, 17–19 August 2010; pp. 62–71. [CrossRef]