Blockchain for Network Slicing in 5G and Beyond: Survey and Challenges

Shihan Bao, Yacong Liang, Hui Xu

***Abstract*—Network slicing has gained popularity as a result of the advances in the fifth generation (5G) mobile network. Network slicing facilitates the support of different service types with varying requirements, which brings into light the slicing-aware next generation mobile network architecture. While allowing resource sharing among multiple stakeholders, there is a long list of administrative negotiations among parties that have not established mutual trust. Distributed ledger technology may be a solution to mitigate the above issues by taking its decentralized yet immutable and auditable ledger, which may help to ease administrative negotiations and build mutual trust among multi-stakeholders. There have been many research interests in this direction which focus on handling various problems in network slicing. This paper aims at constructing this area of knowledge by introducing network slice from a standardization point of view to start with, and presenting security, privacy, and trust challenges of network slicing in 5G and beyond networks. Furthermore, this paper covers distributed ledger technologies basics and related approaches that tackle security, privacy, and trust threats in network slicing for 5G and beyond networks. The various proposals proposed in the literature are compared and presented. Lastly, limitations of current work and open challenges are illustrated as well.**

***Keywords*—network slicing, blockchain, beyond 5G, security, privacy and trust**

I. Introduction

The fifth generation (5G) is rolling out around the world. One of the most critical features of the 5G mobile network is softwarization. 5G featured services can be summarized under 4 categories as enhanced mobile broadband (eMBB), mission critical communication (MCC), ultra-reliable and low-latency communications (URLLC) and massive machine-to-machine type communications (mMTC). The requirements for different services may vary considerably. Hence only dedicated networks could meet the needs specifically[1]. With the help of software defined network (SDN) and network function virtualization (NFV), the 5G network enables multiple services through network slicing with distinctive features[2]. A network slice is an isolated, end-to-end (E2E), logical network which runs on shared physical infrastructure and agrees to provide a distinct level of service based on the needs. It decouples network functions (NF) functionality from physical infrastructure and relocates NF from dedicated appliances to pools of resources. This significantly improves network efficiency and can adjust virtual networks without suspending the overall service operation. Most notably, network slicing enables flexibility and modularity to establish multiple sub-networks. Each sub-network can be specified for a distinct use-case from one sheared network to meet various network needs of diverse verticals.

One of the fundamental attributes of network slicing is the E2E nature, which contains both E2E services and corresponding E2E resources of this service. Creating on-demand E2E network slices based on different service requirements is a critical feature of the 5G network. An E2E network slice instances (NSI) could contain various sub-networks of many administrative domains. It is logically or physically isolated from other network slices[3]. Therefore network slicing enables an E2E ecosystem to provide a consistent experience for distinct services. Network slicing has also been in the spotlight of many standardization bodies (e.g., third generation partnership project (3GPP)), International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) and European Telecommunications Standards Institute (ETSI). The motivation of network slicing is to facilitate a new business ecosystem. The industry and standardization bodies are expecting 5G to enable innovative services and networking capabilities for consumers and industry stakeholders[4,5]. As one of the key enablers of 5G networks, network slicing can speed the development of network ser-

Manuscript received Sep. 12, 2022; revised Oct. 08, 2022; accepted Nov. 17, 2022. This work was supported by the National Key R&D Program of China under Grant 2022YFB2902201. The associate editor coordinating the review of this paper and approving it for publication was Y. M. Shi.

S. H. Bao, Y. C. Liang, H. Xu. Standards Department of CICT Mobile Communication Technology Co., Ltd., Beijing 100083, China (e-mail: baoshihan@cictmobile.com; liangyangcong@cictmobile.com; xuhui1@cictmobile.com).

vices by creating customized services for vertical industries, and could create partnerships among network operators and verticals. The objectives of network slicing are the provision of enhanced quality of services (QoS) for consumers and cost-effective approaches for network operators and vertical industries.

The concept of marginalization and distributed structure of mobile networks draws a lot of attention, while the current 5G mobile network still inherits the traditional network security system of external border protection. New security challenges are emerging and conventional external attached protection methods cannot keep the rising pace of new issues. With the upcoming network slicing deployment, security and privacy threats of network slicing still are not getting enough attention. It might hinder the development of the next generation mobile network. Hence International Mobile Telecommunications-2020 (IMT-2020) and 3GPP both have stated emerging requirements for enhanced security and privacy[6-8]. Researchers start to believe that independent and self-growing security capabilities could be a key enabler for the next generation mobile network. It is envisioned that next generation network systems will face more challenging security and privacy issues, while the network structure becomes more intelligent and enormous data transmits among more mature network slicing mechanisms. In particular, the most benefits of network slicing may come from the cost-effectiveness and efficiency of aggregating services on common public infrastructure and resources, but the security, privacy, and reliability of public networks are considerable concerns not just for network operators but also for consumers. Isolation is one of the most fundamental features of network slicing. The security level of a network slice depends on assuring a required level of isolation. Reliability concern is another threat to network slicing. Having a single point of failure at any life-cycle of network slicing could easily shut down the network slice and even affect the whole system.

Since the success of blockchain applications in various areas, more and more entities believe that distributed ledger technology (DLT) will become a fundamental technology for future telecommunication and the Internet. DLT has the characteristics of decentralization, distributed structure, immutability, robustness, traceability, and openness. These characteristics assist the network to construct a peer-to-peer (P2P) networks that efficiently manages all network participants without any single centralized authority. With the decentralized architecture, DLT could be the basis of a transparent platform where multiple stakeholders negotiate with. Moreover, DLT provides the capability of avoiding single-point failure, which assures reliability on an E2E NSI with multi-parties. Due to these properties, blockchain has the potential to be integrated with network slicing.

The main contributions of the paper can be summarized as follows:

- Provision an overview of network slicing, concepts and challenges based on the standardization background for network slicing through major global standardization institutions. The paper mainly focuses on the security standards of network slices.
- Analyze existing research about network slicing security, privacy, and trust issues in current 5G networks and beyond.
- Present a brief introduction and enabling technologies of DLT.
- Summarize the state-of-art blockchain-based solutions for network slice security and privacy-preserving. To our best knowledge, this is the first time in the literature investigated from this perspective.

The remainder of the paper is structured as follows: Section II discusses network slice standardization to date in terms of basics, provisioning, management, and security. Based on the standardization studies, network slicing basics are illustrated. Section III presents a detailed network slice security threat analysis including security principles and potential privacy and trust challenges beyond 5G networks. Section IV provides research solutions about distributed ledger technology enabling network slicing security protection and analyzes their aim and functionalities as they integrate DLT features in their network slicing frameworks. Section V follows open challenges that need more attention in the next generation mobile networks. Finally, section VI concludes this paper.

II. Network Slicing Standardization

A. Standardization Works

3GPP standards established the foundation of 5G network slicing. 3GPP SA2 Release 15 puts forward the basic concept of network slicing, and formulates the basic functions, schemes and procedures required for 5G networks to support network slicing in 3GPP TS 23.501[9]. A network slice was defined as a logical E2E network that could be dynamically created to serve a purpose or service category or customers. Standard network slices are mainly divided into five categories in terms of service type, including eMBB slices, V2X slices, URLLC slices, massive Internet of things (mIoT) slices and MCC slices. A network slice is defined within public land mobile network (PLMN). It contains the Core Network Control Plane and User Plane network functions and 5G access network. When a user accesses the network, network slices will be selected based on user subscription data, slice selection strategies, user requests, etc. While the access and mobility management (AMF) instance logically belongs to all network slices, other network functions, such as the session management function (SMF) and user plane function, can be specific to a single network slice. In Release 16, the network slicing

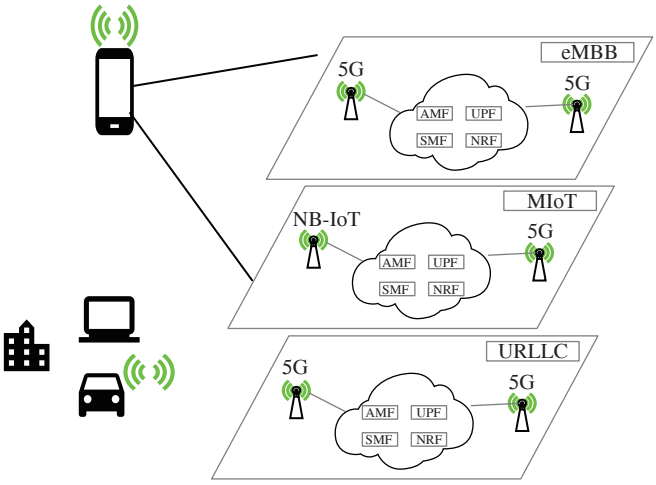

Fig. 1 A simplified networks slicing example based on TS 23.501

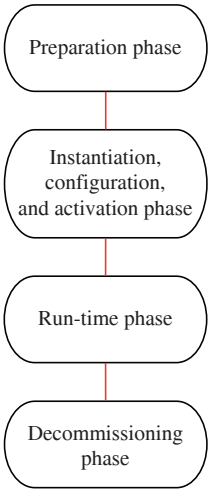

Fig. 2 Lifecycle of network slicing

security mechanism has been further enhanced in TS 23.501. It mainly focuses on supporting third parties to authenticate and authorize terminal access to network slicing. Network slicing specific authentication and authorization mechanisms have been formulated. In Release 17, a part of the generic network slicing template (GST) is studied and standardized within the scope of 3GPP, including the control of the number of access User Equipment (UE) in the slice, the number of protocol data unit (PDU) sessions, and the data rate. A simplified networks slicing example based on TS 23.501 as shown in Fig. 1. As it can be seen from the figure, each slice has dedicated AMF, SMF, network repository function (NRF) and user plane function (UPF) as its core network. End users, such as mobile phones, connected vehicles, and smart IoT devices, will have options to access various network slices based on the needs and scenarios.

The work group 3GPP SA5 has studied the management and orchestration of network slicing in TR 28.801[10] and normative specification works for Release 15 upon the report. Network slice concepts, use cases, and requirements were presented in TS 28.530[11]. In addition, provisioning, management and orchestration for network slice were presented in TS 28.531[12]. In terms of management, a complete network slice should include all network function instances and supporting resources to provide specific services for certain business purposes or operational efficiencies purposes. TR 28.801 has studied a general network slice lifecycle, from the preparation phase, then the configuration and activation phase, to run time phase and decommissioning phase when the slice is no longer needed. Fig. 2 depicts the lifecycle for the general network slicing procedure. 3GPP in TR 28.804[13] studied network slice performance and fault monitoring in multiple tenants environments.

The research work of 3GPP for network slicing security is mainly carried out in SA3. In Release 14, 3GPP SA3 TR 33.899[14] studied the security isolation of network slices, security mechanism differentiation for network slices, the access security of network slices, and security architecture for network slices. Isolation requirements were defined to have limited influence on other slices. The technical report also pointed out that the lack of security isolation could cause denial of service (DoS) attacks from one to another slice. In Release 15, SA3 launched the research and standardization work for the management security of network slicing in TS 33.501[15]. The slice management requester needs to be authenticated and authorized based on transport layer security (TLS) on the slice management interface. Different network slices could have different security policies, in terms of various types of authentication needs on different nodes (e.g., limited resources IoT devices vs. mobile equipment). Release 16 mainly focus on open security issues to conduct security enhancement research, including network slice specific authentication and authorization, network slicing specific re-authentication and re-authorization, and authorization revocation process. In single network slice selection assistance information (S-NSSAI), it has subscription information states whether the network slices requires re-authentication for a different level of security. In the Rel-16 stage, 3GPP SA3 began research work on TR 33.813 in 2018[7]. The enhanced network slicing security mainly studies the open issues left from the previous stage, including the authentication of access to specific network slices, key isolation, security features for network slice as a service (NSaaS), and privacy protection. The report is concerned about the security and privacy of device access. Forged slice selection information and original selection information eavesdropping may lead to further damage to the network. In addition, slice management functions may expose through application programming interfaces (APIs) that are vulnerable and need to be secured.

ETSI has set up a special security subgroup under NFV

to conduct in-depth research on NFV security. Currently, it has established standards for the execution architecture of sensitive NFV components, NFV security management and monitoring, management and orchestration (MANO) component and interface security, and NFV security enhancement architecture[16,17]. In Ref. [18], ETSI studied the reliability and availability of network slicing. The allocated resources concerned to isolated during network slice instance creation and management operations from a security point view. Moreover, Ref. [19] states the E2E network slicing management solutions including provisioning, performance, and fault management of a network slice instance across multiple management domains.

ITU-T describes security threats and potential attacks for IMT-2020 network management and orchestration, such as destruction of information, loss of information, disclosure of information and interruption of service. ITU-T also proposes security requirements for IMT-2020 network management and orchestration, i.e., protecting signaling exchange in support of resource requests and responses, protecting the information contained in all IMT-2020 network management and orchestration functional components. These requirements are mainly about information protection, performance assurance, and supporting measures to counter relevant attacks. In addition, ITU-T specifies a slice lifecycle management and orchestration procedure, the slice life-cycle management and orchestration functional architecture, and an IMT-2020 network management and orchestration procedure and implementation scenarios[20].

B. Research Projects

Research projects have worked on extending or envisioning standardization landscapes into various schemes and proposals. Industry programs like Horizon 2020 (H2020) and 5G infrastructure public private partnership (5GPPP) focus on the network slicing with diverse scenarios.

The 5G exchange (5GEx) funding EU project[21] has proposed a bottom-up architecture further extending the concept of ETSI NFV architecture, on condition that physical and virtual resources of a network slice are instantiated over multiple domains or parties. The proposed architecture has 3 layers, including the resource domain at the bottom, the single domain orchestration at the middle, and the multi-domain orchestration at the top. Each multi-domain orchestration controller inter-connects with one or multiple single domain orchestrators via the orchestrator administrative domain.

5G-Transformer (5GT), which is an H2020 project, proposes an E2E composite NFV network services architecture based the combination technology between SDN and NFV. Multiple administrative domains help to manage the E2E deployment, requiring network slice federation functionalities[22]. The relevant project [23] proposes the service federation functionality of the 5GT service orchestrator and covers gaps that were identified in the ETSI NFV reports on the relevance of multi-domain resource orchestration. Based on the 5GT, the 5Growth project aims to enhance the 5GT architecture to achieve better performance, flexibility, automation, and security[24].

III. Network Slicing Security, Privacy and Trust Threats for 5G and Beyond

Network slicing, as a network resource sharing mechanism, refers to dividing physical network resources into virtual networks. Each slice is tailored and optimized for a specific use, and can be managed completely by the slice owner. According to Ref. [25], an NFV framework of network slice management is shown in Fig. 3. The communication service management function is responsible for translating the communication service-related requirement to network slice-related requirements, and the network slice management function or network slice subnet management function is responsible for implementing the network slice related requirements by using virtual network functions (VNFs) or the connectivity to the physical network function (PNFs) to create network slices. The network functions virtualization orchestration (NFVO), VNFM and VIM are all management functions in the NFV framework, which manage the life cycle and resource allocation of the VNF and network functions virtualization instance (NFVI).

Because network slices that serve different types of services may have different levels of security and privacy policy requirements[26]. Combining the evolution of network architecture[27], the SDN and NFV are the main enablers for network slicing. Network softwarization consists in running network functions as software components to be hosted in the cloud, inside the virtual machines or containers. The management between network slices and inter-slices access in the 5G network is more complicated than previous one-fit-all mobile networks because of the E2E slicing approach. The access management to slices, securing mutual access between the radio access network and the core network resources in 5G network, and securing the connection between UE and network slice instances are the main challenges for a secure E2E network slicing management. Security threats can be caused by the concept of sharing resources among network slices. In Ref. [28] and Ref. [29], the authors state that the main types of security risks which associated with network softwarization are the availability of controllers or orchestrators, isolation failure, compromised insider and NFV instances, and unauthorized data access. The centralized slice manager also brings security issues such as network slice template, APIs, unauthorized access, trust etc[30]. In addition,

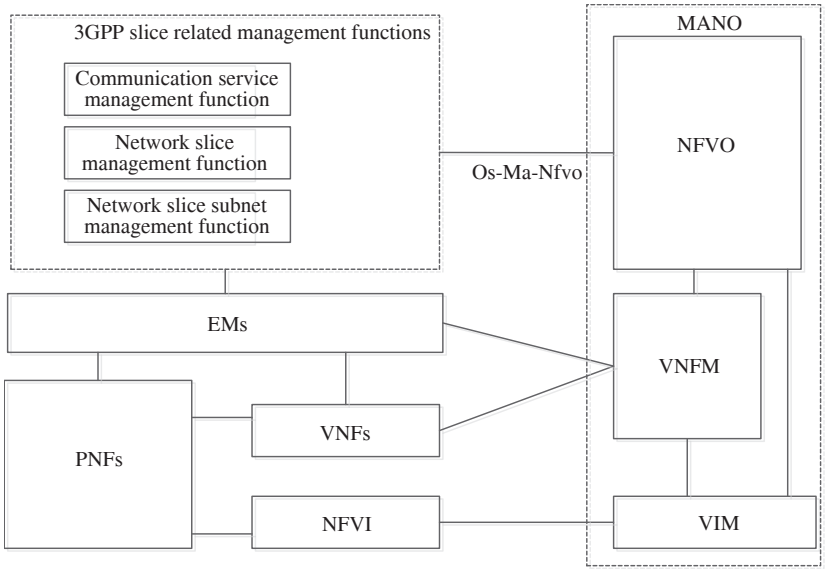

Fig. 3 Network slice management in a NFV framework

the next generation mobile network may face more security and privacy challenges when the network slicing is associated with multi-domain infrastructures or multi-tenants. The authors in Ref. [26] believe that the network slice security should follow traditional security principles including confidentiality, integrity, authenticity, availability, and authorization.

For confidentiality threats, a compromised slice manager could monitor the traffic through both northbound and southbound interfaces, which may leak the slice configurations. A vulnerable point of attack in the configuration phase is the API. A compromised API could allow adversaries to interfere in the installation, configuration, or activation of a slice[14]. Similar to the slice manager, NFVO also may breach confidentiality through interfaces. The confidentiality of inter-slice communications should be considered as well.

For integrity threats, a poorly designed, or improperly implemented network slice template may damage the integrity of the template in the network slice preparation phase[31]. Injecting or forging traffic into slice manager's interfaces could break the integrity. Data exchange between slices may expose vulnerability as well. Another integrity threat is that an attack could change network slice configuration, which leads to new threats such as slice deactivation at run time phase[32]. In addition, the service level agreement (SLA) of network slicing faces the threat of being tampered or spoofed. Conventional SLA monitoring methods rely on the third party auditors which still could temper the report for benefits[33].

For authenticity threats, a compromised network function where credentials are locally-stored would breach the system's authenticity. In addition, unauthorized access to the network slice may cause data leakage and lead to further damage to the network. In Ref. [34], the authors believe that rapid authentication needs to be innovated and rapidly adopted into the upcoming mobile communication network system since the network slice development requires UE more frequently change in different slices.

For availability threats, the availability issue of network slice may directly affect network capabilities and performance. Hence the availability of a network slice is a major challenge. Launching DoS or distributed denial of service (DDoS) could break the availability of the network and delay the communication between entities. In addition, the attackers tend to launch DDoS attacks on a large number of UEs[34]. Compared with conventional single-user devices, beyond 5G networks which will support extreme massive machine type communication and extremely high capacity communication may suffer this threat more serious than before.

Apart from the above security threats, privacy and trust issues are other critical concerns that have not been addressed well in current 5G networks[35]. Network slice providers may have incentives to misbehave against user privacy. Therefore, the interested services of users through the access of slice could be learned by the slice providers[36].

IV. DLT Enabled Secure Network Slicing

A. Distributed Ledger Technology

Bitcoin attracts a lot of attention along with its blockchain concept, which was proposed in 2008[37]. In simple terms, a blockchain is a synchronized and distributed ledger that stores a list of blocks. Each block records a set of validated transactions (e.g. user information and a receipt) and securely links to the previous block. Central authorities are removed from the blockchain structure and the public ledger is maintained by all

the network participants instead. This is realized by a protocol that achieves a trustworthy consensus about the chain of blocks created. In other words, network nodes can agree (deterministically) on the history and order of blocks that were created, and on which node is allowed to add the next block to the chain.

The network will reach eventual consistency since some regions may temporarily diverge in their opinion of who won the next block. Since nodes hold an entire block tree, such disputes get resolved eventually as all nodes consider the path in the local tree with the "biggest overall work" to be the genuine chain (and this choice may vary over time).

Despite the fact that blockchain has received a lot of attention from the banking industry, authors from Ref. [38] find that the use of blockchain can also improve other systems such as insurance, electric vehicle charging, and car sharing services. In addition, blockchain was used to facilitate the authentication and privacy preserving in the connected vehicle system. In Refs. [39,40], they propose cost efficient pseudonym certificate management schemes based on the blockchain technology for connected vehicles so that vehicles could reuse pseudonym certificates to protect anonymity in the vehicle-to-everything communication. Ref. [41] states that there are some concerns about blockchain, namely, majority attack, selfish mining, identity disclosure, and abuse of blockchain. In addition, blockchains based applications (e.g. Bitcoin and Ethereum) are facing big challenges in real life due to blockchain's low scalability and low amount of transactions per second. Hence, some studies from Ref. [42] proposed a new generation public digital ledger technique, namely IOTA[43]. It makes use of a small notation called tangle at its core, a directed acyclic graph (DAG), to eliminate huge transaction power consumption and the concept of mining.

The smart contract, a programmable script, plays a vital role in the blockchain system. While traditional contract tends to have a centralized authority to operate and supervise, the smart contract does not need any central authorities and operates by itself once certain conditions were met. Smart contract was first introduced by Nick Szabo in 1997[44]. The author believes that smart contracts could emerge protocols, user interfaces and promises to formalize and secure relationships over computer networks. Szabo thinks the smart contract can be seen as a vending machine, in which there is a pre-defined program that contract and agreement have set in advance. When certain conditions are met or parameters are reached, the smart contract, like a vending machine, will act correspondingly followed by the agreement. Close to vending machines that can replace sales in the vendor, the smart contract is able to substitute agencies and third parties in many fields. The first generation blockchain application, such as Bitcoin, is not much of programmable or Turing complete. Therefore, Bitcoin is not fully capable of operating the smart contract. The smart contract is often referred to in the second generation blockchain platforms, such as Ethereum and Hyperledger. In Ethereum, the smart contract was defined as an account which has a unique address and balance[45]. This account is also referred to as contract account. Users could initiate transactions with the contract account to interact with smart contract functions. As long as one's account has enough cryptocurrency ether to pay transaction fees, any account can write up and publish smart contracts.

B. Integration of DLT with Network Slicing

Recent studies have included DLT, the key technology to assist automation and management beyond 5G and future 6G networks[46-48]. Network slice could benefit from a promising technology, namely the DLT. Because DLT can provide a distributed framework, a secure and accountable digital ledger, and a fine-grained security indicator. It is a possible solution to resolve network slicing security challenges and keep the confidentiality, integrity, and availability of the system. The authors in Ref. [49] believe that blockchain suits scenarios with multiple partners in the E2E value chain of any ecosystem. Multiple partners can not only be a horizontal chain between companies, suppliers, and end users, but also a vertical chain among internal entities. In addition, many studies show that merging DLT/blockchain and network slicing could achieve multiple purposes. Firstly, since the DLT with smart contract could create an automated marketplace or auction platform, network slices and corresponding services can be negotiated among consumers, network operators, and industrial vertical players[50,51]. Secondly, another challenge raised by multi-tenant and multi-domain network slicing scenarios is much higher chances of attacks inside the network. The use of DLT can be a solution to establish a trust mechanism among network slicing parties, and could also build an authentication layer for the multiple administrative domains to meet security requirements[52,53]. Moreover, the distributed nature of DLT provides the capability of avoiding single-point failure, because the system has high robustness even one or a few nodes are out of reach. It assures reliability and availability on an E2E NSI with multi-parties. Due to these properties, blockchain has the potential to be integrated with network slicing[54,55].

C. DLT Powered Network Slicing In Verticals

Since the DLT could provide trust and secure solutions, it is noticeable that research has considered using DLT to tackle existing security, privacy, and trust challenges in network slicing. The authors in Ref. [56] proposed a blockchain based privacy preserved network slicing SLA audit scheme, aiming to preserve data privacy and integrity. Conventional SLA audit process faces threats of data leakage and alterations in the

audit report. This scheme introduces a blockchain-based audit strategy which can preserve data privacy in the audit process and the smart contract inside is designed to operate audit tasks and carry out punishments. The blockchain in this model is a platform to provide a public and transparent way to store immutable data across multiple parties. Then a data encryption scheme called order-revealing encryption (TORE) is introduced and implemented in the smart contract of the proposed blockchain-based SLA auditing scheme. In their more recent research[57], this TORE scheme is more refined to be able to encrypt monitored parameters in the SLA and realize the comparison over auditing ciphertexts, resulting in the prevention of data leakage in SLA auditing. In addition to the integrity, an order-revealing encryption algorithm is used for encrypting the monitored data and parameters in SLA audit. The smart contract in the blockchain can be also used for providing fine-grained security[49]. Future smart contracts could monitor security indicator and conduct in-depth analysis once any attack detected in a given slice. The paper presents a SDN and DLT based framework to provide secure, automatic, and distributed data[58]. It uses Hyperledger Fabric platform to show a secure and fast transaction performance through blockchain.

D. Multiple Participants Coordination and Trust Management by DLT for Network Slicing

Orchestration across multiple infrastructure providers can help to simplify infrastructural operations, and enable better scaling and faster deployment of network services. For the implementation of certain network services, it is required to create E2E NSI across multiple participants. In 3GPP TR 28.801[10], if an participant wants to create an E2E NSI across multiple participants, this participant should decompose the service request of the E2E network slice and provide its management data to the other participants. Pre-conditions of this connection are trust relationships that are assumed to exist between operators. This trust relationship makes the coordination between participants transparent and visible. However, the majority of participants worries whether sensitive management data could be exposed and other participants might not follow the agreement of network slicing. With this kind of concern, stakeholders could not trust each other. Since the immutable feature of blockchain and undeniable automated operations powered by smart contract, the blockchain becomes a feasible tool to build trust relationship among multiple stakeholders. Hence participants in the blockchain network can decide what to share and how to follow network slice operation agreements in the smart contract. Researchers such as Ref. [59] believe blockchain can be deployed to ensure trustworthiness between different telecom operators for multiple participants, coordination management in network slicing.

The authors of Ref. [60] propose an architecture comprising multi-domain edge orchestration to achieve SLA autonomy management by smart contracts. And the Hyperledger Fabric blockchain is used to improve the trustworthiness of the system by storing records in orchestrators. Ref. [61] introduces the concept of the 5G Network Slice Broker, which can facilitate on-demand resource allocation and perform admission control based on traffic monitoring and forecasting. The authors in Ref. [62] and Ref. [63] propose to use the blockchain to deploy the brokering mechanism by smart contracts. An example of network slice broker using the blockchain system was shown in Fig. 4. Mobile virtual network operators (MVNOs), over-the-top (OTT) providers and infrastructure providers (InPs) all participate in the blockchain network, and the slice broker mechanism would handle multiple traders in both selling and buying. Service and infrastructure providers can benefit from this auction mechanism by having real-time assets offers, requests, and automated payment settlements, while end consumers have options, in terms of infrastructure, resources, and prices, based on their demands. So the P2P system is able to replace conventional centralized approach to slice brokering. In Ref. [64], a multi-layer blockchain based secure network slicing architecture was designed to be used in the medical field. The paper states that using decentralized storage platforms to perform as slice broker could secure the network slicing. In addition, the authors[65] propose an automated resource allocation based on deep reinforcement learning (DRL) and blockchain, which can ensure the security of transactions. However, these papers provide only a qualitative analysis of the security performance of the dynamic slicing endowed by the blockchain, and have no mention of how to use the blockchain to establish a trust relationship.

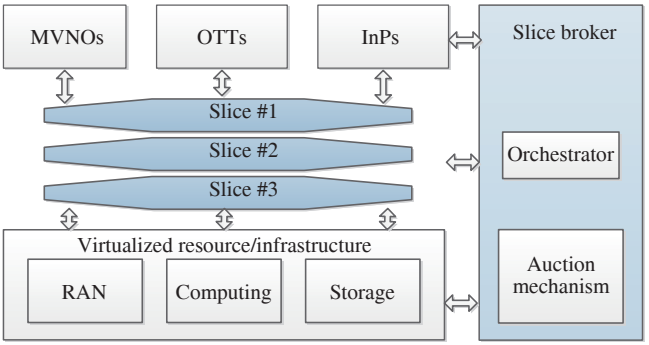

Fig. 4 An example of blockchain-based slice brokering system

The combination of network slicing and blockchain has become an inevitable trend, and it will be expected to establish trust relationship between multiple participants by DLT. Steward is a blockchain-based trust assessment framework, providing automated risk management in IoT devices[66]. The blockchain system will store trust scores of all devices, so that the network controllers could leverage these information and then allow devices which meet the expected trust levels to con-

Tab. 1 Taxonomy of blockchain-based solutions for threats in network slice

Category of threats	The role of blockchain	Ref.
Integrity	Realize SLA trust automation management	[60], [64], [68], [69], [70]
Authenticity	Control the access to network slices	[66]
Availability	Resist DoS attacks	[67]
Trust	Establish trust relationship between multiple	[60], [62], [63], [65], [68], [69]
Privacy	Ensure privacy between network slices	[67], [56]

nect with the network slice. The authors in Ref. [67] develop a blockchain-based secure and isolated software infrastructure of virtual functions. In order to isolate these slices and avoid common attacks in shared infrastructures, they provide different categories of blockchain for different slice requirements, while all slices share the same infrastructure. Ref. [68] proposes that DLT can be used to solve the trust problem. In addition, the authors of Ref. [69] present a zero-touch approach in cross-domain network slicing based on enterprise blockchain and AI-driven closed-loop automation architecture. It can detect or predict SLA violations with immediate action for mitigation without disrupting the service. A blockchain-based trusted architecture was proposed in Ref. [70] to provide an E2E security by utilizing smart contract for SLA management.

A taxonomy of blockchain-based solutions for security, privacy and trust threats in network slicing are summarized in Tab. 1. Threats of network slicing are categorized into integrity, authenticity, availability, trust, and privacy. The role of blockchain points to what benefits the blockchain system provides above solutions.

V. Open Challenges

Beyond 5G and future 6G networks, the trios of trust, security, and privacy are interconnected to some extent. The challenges remain in multidisciplinary technologies, standardization, techno-economics etc.[71]. Despite the fact that blockchain technology facilitates the security of network slicing, there are open challenges in terms of security, privacy, and trust. In this section, potential issues and challenges of endogenous security in network slicing beyond 5G networks will be reviewed.

A. RAN Slicing

The next generation radio access network (NG-RAN) would support a great number of RAN slice subnets[72]. To satisfy the advanced service requirements of E2E slicing in the next generation network, the future radio base stations are supposed to be more customizable and more capable of dynamic. Maintaining a significant level of isolation will be a key to provision security and privacy on the E2E slicing. Hence, more reliable and resilience slice isolation technologies require further study. Moreover, the open RAN (O-RAN) draws a lot of attention recently. The main concept of the openness and smartness in this new RAN framework is to let all participants build an open source, open hardware, software-driven, slicing-aware, and resource efficient innovated radio network together. However, O-RAN is still at the early stage and needs further research to fully realize in the next generation mobile networks. Major problems, especially security related, can be summarized as the hijacking attack of open networking, the doubt of trustworthy O-RAN, inter-operability, and standardization[73,74].

B. Edge Intelligence in Network Slicing

A popular use case for edge intelligence is the automation of virtual resource management and orchestration beyond 5G network[72]. The management procedures of the RAN network slice subnet management function will be automated by the edge intelligence to decrease the management and orchestration complexity. Therefore, the processed data among slices and users could be exposed or lack of protection. Secure and lightweight data preserving technologies can be further investigated, aiming to handle data confidentiality and privacy for the future scalable and fast changing next generation mobile networks. While the edge intelligence brings benefits for network slicing, the artificial intelligence itself will be a major concern in terms of data poisoning and data evasion[75]. In addition, the standardization and international recommendation also play key roles in the development of automated network slicing.

Moreover, the state-of-the-art security approaches for network slices as above stated are mostly human or machine-centric. For instance, even automated anomaly detection still needs human intervention to address false negatives[76]. Since the promising advanced telecommunication technologies and artificial intelligence techniques, the next generation mobile networks are inevitably facing more and more automated and advanced attacks. So more sophisticated and intelligent security mechanisms are essential to overcome future massive scale and automated related attacks. Machine learning could play a crucial role to design intelligent security solutions for network slicing. Machine learning algorithms and models, such as Markov models, neural networks, deep reinforcement learning, and genetic algorithms, could be utilized to find configuration errors to limit human intervention.

C. Post-Quantum Security

Apart from conventional threats, many believe that the upcoming quantum computing will bring serious challenges on network security. The current cryptography systems are mainly under two categories: symmetric and asymmetric[77]. However, mathematicians state that either symmetric algo-

rithms or asymmetric algorithms will be breakable once quantum computers come. Because the quantum computing is significantly more powerful than current computing capacity. The research and development of quantum resistant cryptography algorithms will be a big milestone for the next generation mobile networks. Future quantum-resistant cryptography algorithms should be secure enough against both quantum computing threats and classic cryptography threats.

D. Blockchain Scalability

In blockchain, there is a triangle, namely, decentralisation, security, and scalability. In this triangle, most blockchain-based systems can only meet two subjects. Both generations of blockchain (Bitcoin and Ethereum) have similar drawbacks, low transaction throughputs, small block size, and huge energy consumption. In terms of low transaction throughputs, bitcoin can do 3-5 transactions per second (TPS) and Etherum can do 25 tps, while Visa can do 1 500 tps. As a fundamental technology for future networks, distributed ledger technology is eager to seek solutions and innovations to meet the trio of decentralization, security, and scalability together. Novel blockchain architectures, sharding techniques, block size increase, and consensus algorithms are being researched to increase the throughput of today's blockchain networks.

VI. Conclusion

This article presents a review of DLT solutions for network slicing security, privacy, and trust challenges for the next generation mobile networks. It reviews current standardization efforts from multiple institutions, including the ITU, 3GPP, and ETSI, to provide a basic introduction to the concept of network slicing. The exploration of the next generation mobile network has led academia and industry to focus on enhancing the security of the system. Network slicing security concerns beyond 5G and potential DLT-based solutions are presented and discussed. Lastly, several open research challenges and potential issues of security and privacy threats of network slicing in the next generation mobile networks are identified.

References

[1] FOUKAS X, PATOUNAS G, ELMOKASHFI A, et al. Network slicing in 5G: survey and challenges[J]. IEEE Communications Magazine, 2017, 55(5): 94-100.

[2] BARAKABITZE A A, AHMAD A, MIJUMBI R, et al. 5G network slicing using SDN and NFV-a survey of taxonomy, architectures and future challenges[J]. Computer Networks, 2020, 167.

[3] AFOLABI I, KSENTINI A, BAGAA M, et al. Towards 5G network slicing over multiple-domains[J]. IEICE Transactions on Communications, 2017, 100(11): 1992-2006.

[4] ETSI G. Zero-touch network and service management (ZSM); reference architecture[J]. Group Specification (GS) ETSI GS ZSM, 2019, 2.

[5] ETSI G. Zero-touch network and service management (ZSM); closed-loop automation; Part 1: enablers[J]. Group Specification (GS) ETSI GS ZSM, 2021.

[6] ČOLAKOVIĆ A, HADŽIALIĆ M. Internet of things (IoT): a review of enabling technologies, challenges, and open research issues[J]. Computer Networks, 2018, 144: 17-39.

[7] 3GPP. Study on security aspects of network slicing enhancement[K]. 2020.

[8] 3GPP. Study on enhanced security for network slicing phase 2[K]. 2022.

[9] 3GPP. System architecture for the 5G system[K]. 2018.

[10] 3GPP. Study on management and orchestration of network slicing for next generation network[K]. 2017.

[11] 3GPP. Management and orchestration; Concepts, use cases and requirements[K]. 2022.

[12] 3GPP. Management and orchestration; Provisioning[K]. 2022.

[13] 3GPP. Study on tenancy concept in 5G networks and network slicing management V16.0.0[K]. 2019.

[14] 3GPP. Study on the security aspects of the next generation system[K]. 2017.

[15] 3GPP. Security architecture and procedures for 5G system[K]. 2018.

[16] ETSI. Network functions virtualisation (NFV) Release 4; Management and orchestration; Functional requirements specification: GS NFV-IFA 010[R]. [S.l.]: European Telecommunications Standards Institute(ETSI), 2022.

[17] Q. Y. Analysis on technologies and developments of 5G network slicing security[J]. Mobile Communication, 2019(10): 26-30.

[18] ETSI. Network functions virtualisation (NFV) Release 3; Reliability; report on NFV resiliency for the support of network slicing: GR NFV-REL 010[R]. [S.l.]: European Telecommunications Standards Institute(ETSI), 2019.

[19] ETSI. Zero-touch network and service management (ZSM); End-to-end management and orchestration of network slicing: GS ZSM 003[R]. [S.l.]: European Telecommunications Standards Institute(ETSI), 2021.

[20] ITU-T. IMT-2020 network management and orchestration framework[K]. 2017.

[21] GUERZONI R, PÉREZ-CAPARRÓS D, MONTI P, et al. Multi-domain orchestration and management of software defined infrastructures: a bottom-up approach[C]//2016.

[22] DE LA OLIVA A, LI X, COSTA-PEREZ X, et al. 5G-transformer: slicing and orchestrating transport networks for industry verticals[J]. IEEE Communications Magazine, 2018, 56(8): 78-84.

[23] BARANDA HORTIGUELA J, MANGUES-BAFALLUY J, MARTINEZ R, et al. Realizing the network service federation vision: enabling automated multidomain orchestration of network services[J]. IEEE Vehicular Technology Magazine, 2020, 15(2): 48-57.

[24] LI X, GARCIA-SAAVEDRA A, COSTA-PEREZ X, et al. 5Growth: an end-to-end service platform for automated deployment and management of vertical services over 5G networks[J]. IEEE Communications Magazine, 2021, 59(3): 84-90.

[25] ETSI. Network functions virtualisation (NFV) Release 3; Evolution and ecosystem; Report on network slicing support with ETSI NFV architecture framework: GR NFV-EVE012[R]. [S.l.]: European Telecommunications Standards Institute (ETSI), 2017.

[26] CUNHA V A, SILVA E D, CARVALHO M, et al. Network slicing security: challenges and directions[J]. Internet Technology Letters, 2(5): 1-6.

[27] AFOLABI I, TALEB T, SAMDANIS K, et al. Network slicing and softwarization: a survey on principles, enabling technologies and solutions[J]. IEEE Communications Surveys and Tutorials, 2018, 20(3): 2429-2453.

[28] REYNAUD F, AGUESSY F-X, BETTAN O, et al. Attacks against network functions virtualization and software-defined networking: state-of-the-art[C]//Proceedings of Workshop on Security in Virtualized Networks (Sec-Virtnet 2016), Workshop of 2nd IEEE Conference on Network Softwarization (NetSoft 2016). Piscataway: IEEE Press, 2016: 471-476.

[29] SATHI V N, SRINIVASAN M, THIRUVASAGAM P K, et al. A novel protocol for securing network slice component association and slice isolation in 5G networks[C]//Proceedings of the 21st ACM International Conference on Modeling, Analysis, and Simulation of Wireless and Mobile Systems. New York: Association for Computing Machinery, 2018: 249-253.

[30] ALLIANCE N. Security aspects of network capabilities exposure in 5G[J]. Final deliverable (approved-P Public), 2018.

[31] OLIMID R F, NENCIONI G. 5G network slicing: a security overview[J]. IEEE Access, 2020, 8: 99999-100009.

[32] KHAN R, KUMAR P, JAYAKODY D N K, et al. A survey on security and privacy of 5G technologies: potential solutions, recent advancements, and future directions[J]. IEEE Communications Surveys and Tutorials, 2019, 22(1): 196-248.

[33] ZHOU S, WU L, JIN C. A privacy-based SLA violation detection model for the security of cloud computing[J]. China Communications, 2017.

[34] FAN C-I, SHIH Y-T, HUANG J-J, et al. Cross-network-slice authentication scheme for the 5th generation mobile communication system[J]. IEEE Transactions on Network and Service Management, 2021, 18(1): 701-712.

[35] NI J, LIN X, SHEN X S. Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(3): 644-657.

[36] NI J, ZHANG K, LIN X, et al. Securing fog computing for Internet of things applications: challenges and solutions[J]. IEEE Communications Surveys and Tutorials, 2017, 20(1): 601-628.

[37] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB]. 2008.

[38] DORRI A, STEGER M, KANHERE S S, et al. Blockchain: a distributed solution to automotive security and privacy[J]. IEEE Communications Magazine, 2017, 55(12): 119-125.

[39] BAO S, CAO Y, LEI A, et al. Pseudonym management through blockchain: cost-efficient privacy preservation on intelligent transportation systems[J]. IEEE Access, 2019, 7: 80390-80403.

[40] BAO S, LEI A, CRUICKSHANK H, et al. A pseudonym certificate management scheme based on blockchain for Internet of vehicles[C]//Proceedings of 2019 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech). Piscataway: IEEE Press, 2019: 28-35.

[41] GAO W, HATCHER W G, YU W. A survey of blockchain: techniques, applications, and challenges[C]//Proceedings of 2018 27th International Conference on Computer Communication and Networks (ICCCN). [S.l.:s.n.], 2018: 1-11.

[42] DIVYA M, BIRADAR N B. IOTA-next generation blockchain[J]. International Journal of Engineering and Computer Science, 2018, 7: 23823-23826.

[43] SHABANDRI B, MAHESHWARI P. Enhancing IoT security and privacy using distributed ledgers with IOTA and the Tangle[C]//Proceedings of 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN). [S.l.:s.n.], 2019: 1069-1075.

[44] SZABO N. Formalizing and securing relationships on public networks[J]. First Monday, 1997, 2(9).

[45] BUTERIN V. A next-generation smart contract and decentralized application platform-Ethereum whitepaper[J]. consulted, 2014.

[46] AKHTAR M W, HASSAN S A, GHAFFAR R, et al. The shift to 6G communications: vision and requirements[J]. Human-Centric Computing and Information Sciences, 2020, 10(1): 1-27.

[47] 6GANA. Data service concepts and requirements for 6G networks (in Chinese)[R]. [S.l.]: 6GANA TG3, 2021.

[48] GUO F, YU F R, ZHANG H, et al. Enabling massive IoT toward 6G: a comprehensive survey[J]. IEEE Internet of Things Journal, 2021, 8(15): 11891-11915.

[49] BIHANNIC N, LEJKIN T, FINKLER I, et al. Network slicing and blockchain to support the transformation of connectivity services in the manufacturing industry[J], 2018.

[50] KAPASSA E, TOULOUPOS M, KYRIAZIS D, et al. A smart distributed marketplace[C]//Proceedings of European, Mediterranean, and Middle Eastern Conference on Information Systems. [S.l.:s.n.], 2019: 458-468.

[51] KABI O R, FRANQUEIRA V N. Blockchain-based distributed marketplace[C]//Proceedings of International Conference on Business Information Systems. [S.l.:s.n.], 2018: 197-210.

[52] CHAER A, SALAH K, LIMA C, et al. Blockchain for 5G: opportunities and challenges[C]//Proceedings of 2019 IEEE GLOBECOM Workshops (GC Wkshps). Piscataway: IEEE Press, 2019: 1-6.

[53] DE FILIPPI P, MANNAN M, REIJERS W. Blockchain as a confidence machine: the problem of trust and challenges of governance[J]. Technology in Society, 2020, 62: 101284.

[54] HEWA T, KALLA A, PORAMBAGE P, et al. How DoS attacks can be mounted on Network Slice Broker and can they be mitigated using blockchain?[C]//Proceedings of 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). Piscataway: IEEE Press, 2021: 1525-1531.

[55] HE G, SU W, GAO S, et al. NetChain: a blockchain-enabled privacy-preserving multi-domain network slice orchestration architecture[J]. IEEE Transactions on Network and Service Management, 2021, 19(1): 188-202.

[56] XIAO K, GENG Z, HE Y, et al. A blockchain-based privacy-preserving cloud service level agreement auditing scheme[C]//Proceedings of International Conference on Wireless Algorithms, Systems, and Applications. [S.l.:s.n.], 2020.

[57] XIAO K, GENG Z, HE Y, et al. A blockchain-based privacy-preserving 5G network slicing service level agreement audit scheme[J]. EURASIP Journal on Wireless Communications and Networking, 2021, 2021: 1-16.

[58] CAMILO G F, REBELLO G A F, de SOUZA L A C, et al. AutAvailChain: automatic and secure data availability through blockchain[C]//Proceedings of 2020 IEEE Global Communications Conference. Piscataway: IEEE Press, 2020: 1-6.

[59] GORLA P, CHAMOLA V, HASSIJA V, et al. Network slicing for 5G with UE state-based allocation and blockchain approach[J]. IEEE Network, 2021, 35(3): 184-190.

[60] RATHI V K, CHAUDHARY V, RAJPUT N K, et al. A blockchain-enabled multi-domain edge computing orchestrator[J]. IEEE Internet of Things Magazine, 2020, 3(2): 30-36.

[61] SAMDANIS K, COSTA-PEREZ X, SCIANCALEPORE V. From network sharing to multi-tenancy: the 5G network slice broker[J]. IEEE Communications Magazine, 2016, 54(7): 32-39.

[62] NOUR B, KSENTINI A, HERBAUT N, et al. A blockchain-based network slice broker for 5G services[J]. IEEE Networking Letters, 2019, 1(3): 99-102.

[63] ZANZI L, ALBANESE A, SCIANCALEPORE V, et al. NS-

Bchain: a secure blockchain framework for network slicing brokerage[C]//Proceedings of 2020 IEEE International Conference on Communications (ICC). Piscataway: IEEE Press, 2020: 1-7.

[64] CHENDEB N, KHALED N, AGOULMINE N. Integrating blockchain with iot for a secure healthcare digital system[C]//Proceedings of 8th International Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE 2020). [S.l.:s.n.], 2020: 1-8.

[65] GONG Y, SUN S, WEI Y, et al. Deep reinforcement learning for edge computing resource allocation in blockchain network slicing broker framework[C]//Proceedings of 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring). Piscataway: IEEE Press, 2021: 1-6.

[66] BOUSSARD M, PAPILLON S, PELOSO P, et al. STewARD: SDN and blockchain-based trust evaluation for automated risk management on IoT devices[C]//Proceedings of IEEE Conference on Computer Communications Workshops. Piscataway: IEEE Press, 2019.

[67] REBELLO G, CAMILO G F, SILVA L, et al. Providing a sliced, secure, and isolated software infrastructure of virtual functions through blockchain technology[C]//Proceedings of 2019 IEEE 20th International Conference on High Performance Switching and Routing (HPSR). Piscataway: IEEE Press, 2019.

[68] SAAD S B, KSENTINI A, BRIK B. A trust architecture for the SLA management in 5G networks[C]//Proceedings of IEEE International Conference on Communications. Piscataway: IEEE Press, 2021.

[69] THEODOROU V, LEKIDIS A, BOZIOS T, et al. Blockchain-based zero touch service assurance in cross-domain network slicing[C]//Proceedings of 2021 Joint European Conference on Networks and Communications 6G Summit. [S.l.:s.n.], 2021: 395-400.

[70] SCHEID E J, RODRIGUES B B, GRANVILLE L Z, et al. Enabling dynamic SLA compensation using blockchain-based smart contracts[C]//Proceedings of 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). Piscataway: IEEE Press, 2019: 53-61.

[71] YLIANTTILA M, KANTOLA R, GURTOV A, et al. 6G white paper: research challenges for trust, security, and privacy[J]. arXiv e-prints, arXiv:2004.11665, 2020.

[72] JIANG W, HAN B, HABIBI M A, et al. The road towards 6G: a comprehensive survey[J]. IEEE Open Journal of the Communications Society, 2021, 2: 334-366.

[73] PLANTIN J C. The political hijacking of open networking. The case of open radio access network[J]. LSE Research Online Documents on Economics, 2021.

[74] SINGH S K, SINGH R, KUMBHANI B. The evolution of radio access network towards Open-RAN: challenges and opportunities[C]//Proceedings of 2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW). Piscataway: IEEE Press, 2020: 1-6.

[75] PORAMBAGE P, GÜR G, MOYA OSORIO D P, et al. The roadmap to 6G security and privacy[J]. IEEE Open Journal of the Communications Society, 2021, 22: 1094-1122.

[76] PORAMBAGE P, LIYANAGE M. Security in network slicing[J]. Wiley 5G Ref: The Essential 5G Reference Online, 2019: 1-12.

[77] CHENG C, LU R, PETZOLDT A, et al. Securing the Internet of things in a quantum world[J]. IEEE Communications Magazine, 2017, 55(2): 116-120.

About the Authors

Shihan Bao [corresponding author] received the B.Sc. degree in Telecommunication Engineering from Northumbria University, Newcastle upon Tyne, UK, in 2014, the M.Sc. degree and the Ph.D. degree from the Institute for Communication Systems (ICS), University of Surrey, Guildford, UK, in 2015 and 2020 respectively. Further to his Ph.D. study, he had conducted research fellow at University of Surrey, Guildford, UK, from 2020 to 2021; and he is a standard engineer in the Standards Department of CICT Mobile Communication Technology Co., Ltd., Beijing, China. His research interest includes the privacy and security in Internet of things (IoT) and intelligent transportation systems (ITS).

Yacong Liang received the M.Sc. degree from Beijing University of Posts and Telecommunications, Beijing, China. Now she is a standard engineer in the Standards Department of CICT Mobile Communication Technology Co., Ltd., Beijing, China. Her research interests are in 6G security and distributed trusted in 6G network.

Hui Xu received the Ph.D. degree from Xian Jiaotong University, Xi'an, China, in 1999. She is a professor-level senior engineer in the Standards Department of CICT Mobile Communication Technology Co., Ltd., Beijing, China. She has long been engaged in the research and standardization of mobile communication core networks, communication security, and vehicle network security