Integration of Blockchain and Network Softwarisation for Space-Air-Ground-Sea Integrated Networks

Hong-Ning Dai, *Senior Member, IEEE,* Yulei Wu, *Senior Member, IEEE,* Muhammad Imran, *Senior Member, IEEE,* Nidal Nasser, *Senior Member, IEEE*

***Abstract*—Space-air-ground-sea integrated networks (SAGSINs) are promising to offer ubiquitous Internet services across the globe while confronting research challenges such as security vulnerabilities, privacy-leakage concerns, and difficulty in resource sharing. On the one hand, emerging network slicing and network softwarisation technologies can fulfill diverse requirements with the provision of various services on top of heterogeneous SAGSIN hardware and software resources. On the other hand, blockchain and smart contracts can compensate for network slicing and softwarisation to offer secure and automatic network services. This article presents an investigation on the convergence of blockchains with network slicing and network softwarisation technologies for SAGSINs from the perspectives of network management and brokerage services of SAGSINs. In contrast to existing studies, this article is the first to incorporate blockchains into network slicing and network softwarisation dedicated for SAGSINs. This article starts with a summary of key characteristics and challenges of SAGSINs. Then, a review on network slicing and network softwarisation is given in the context of SAGSINs. This article next presents an integrated framework of network slicing, network softwarisation, and blockchain for SAGSINs. Moreover, this article outlines a set of open issues and research challenges that would be useful to guide future research in this area.**

I. Introduction

Despite the rapid development of the fifth generation of cellular networks (5G) and the future sixth-generation (6G) networks, there is still a long way to go before achieving the ubiquitous Internet connection across the globe, especially for those sparsely populated areas (like deserts and the sea). Besides the coverage gap in rural areas, airplanes and high-speed trains are also absent from full coverage of 5G networks. The emergence of various satellite systems, high altitude platforms (HAPs), and autonomous flying vehicles (AFVs) brings opportunities to achieve the full coverage of the future Internet anywhere and anytime. It is expected to establish a space-air-ground-sea integrated network (SAGSIN) across the globe to offer ubiquitous Internet services [1].

H.-N. Dai is with the Department of Computing and Decision Sciences, Lingnan University, Hong Kong. Email: hndai@ieee.org.

Y. Wu is with the College of Engineering, Mathematics and Physical Sciences, University of Exeter, Exeter, EX4 4QF, U.K. Email: y.l.wu@exeter.ac.uk.

M. Imran is with the School of Engineering, Information Technology & Physical Sciences, Federation University Australia, Brisbane, Australia. Email: dr.m.imran@ieee.org.

N. Nasser is with the College of Engineering, Alfaisal University, Riyadh, Saudi Arabia. Email: nnasser@alfaisal.edu.

However, SAGSINs pose many challenges including security vulnerabilities, privacy-leakage concerns, and difficulties in resource sharing among SAGSINs. In particular, security vulnerabilities can be ascribed to difficulties in authenticating and authorizing SAGSINs as well as various malicious attacks. Moreover, the data privacy of SAGSINs can be intentionally or mistakenly leaked to untrusted service providers (e.g., cloud service providers). Furthermore, the heterogeneity and complexity of SAGSINs can lead to challenges in resource sharing among different stakeholders of SAGSINs.

Recent advances in network slicing and softwarisation as well as blockchain technologies bring opportunities in tackling the above challenges of SAGSINs. Firstly, network slicing and softwarisation is a promising technology to accommodate various services with different requirements. In particular, various network slices can be created to fulfill diversified requirements of specific services while network softwarisation can design, orchestrate, and manage diverse software-based network/computing resources (i.e., hardware) as well as virtualized resources. Secondly, blockchains and smart contracts are an ideal compensation for network slicing and softwarisation to offer secure and automatic network services. Integrating with network slicing and softwarisation, blockchains can achieve effective network management of SAGSINs.

This article investigates the integration of the blockchain with network slicing and softwarisation in SAGSINs. We first give an overview of SAGSINs and outline the characteristics and challenges of SAGSINs. Following the review of network slicing and softwarisation technologies in SAGSINs, we elaborate on the integration of the blockchain with network slicing and softwarisation in SAGSINs and illustrate the solutions to network management and brokerage services of SAGSINs. We also outline open issues and research challenges in this promising area. Different from existing studies on SAGSINs such as [1], [2], [3], [4], this article originally considers incorporating blockchains into SAGSINs with the integration of network slicing and network softwarisation.

The major contributions of this article are summarized as follows.

- We present an overview of of SAGSINs with a summary of key characteristics and challenges of SAGSINs.
- We then review network slicing and network softwarisation for SAGSINs.
- We next present an integrated framework of network slicing, network softwarisation and blockchain. This frame-

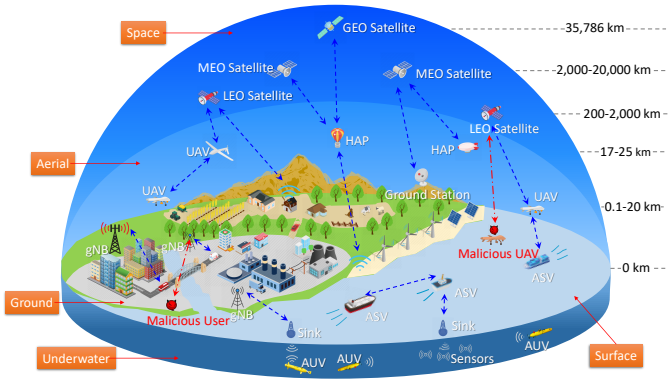

Fig. 1. An overview of space-air-ground-sea integrated networking.

work can address challenges of SAGSINs.

- We also discuss research issues and open challenges, which outline the future directions.

II. Overview of Space-Air-Ground-Sea Integrated Networks

SAGSINs have the vision to connect space networks, aerial/air networks, terrestrial/ground networks, and maritime/sea networks to form a ubiquitous networking infrastructure with the provision of uninterrupted Internet services, as shown in Fig. 1. The SAGSIN infrastructure consists of diverse platforms with varied communication and computing capacities [2].

Regarding space networks, there are different types of satellites deployed at different altitudes. Geosynchronous earth orbit (GEO) satellites are deployed at the highest altitude with about 35,786 km [3]. The high-altitude deployment of GEO satellites achieves wide coverage while it also causes a high propagation delay. Both medium earth orbit (MEO) satellites and low earth orbit (LEO) satellites are deployed at lower altitudes than GEO satellites. In particular, MEO satellites are usually deployed at altitudes about 2,000 km to 20,000 km while LEO satellites are deployed at altitudes about 200 km to 2,000 km. Different from GEO satellites with the fixed altitude, MEO/LEO satellites are launched and positioned at different altitudes depending on the coverage, operational cost, and capacity requirements [4]. Due to the lower launching expenditure than GEO satellites, MEO/LEO satellites can be even launched by companies such as SpaceX[1] and OneWeb[2]. Moreover, MEO/LEO satellites have a shorter propagation delay than GEO satellites.

Below space networks, various HAPs and AFVs construct aerial networks. HAPs include diverse aircraft, airships, and high-altitude balloons, which are either crewed or uncrewed. Compared with satellites, HAPs can be rapidly and flexibly deployed at varied altitudes from 17 to 25 km. Harvesting energy via solar panels or other ambience energy sources, HAPs can persist in the air for several days and even weeks. AFVs are often referred to unmanned aerial vehicles (UAV), which are fixed-wing or rotary-wing can be rapidly deployed at an even lower altitude (0.1 km to 20 km) than HAPs. AFVs that are equipped with gasoline engines or electric engines can usually persist in the air for several minutes to hours to offer an elastic while a narrow coverage. Aerial networks have a much lower propagation delay than space networks.

Ground (or terrestrial) networks consist of diverse infrastructure nodes, such as gNode B (gNB) in 5G networks, evolved Node B (eNB) in 4G networks, WiFi access point (AP), and the Internet of Things (IoT) gateway, which are connected by backhaul networks with the core network. Terrestrial networks offer ubiquitous Internet services to users in areas where infrastructure nodes are deployed. Compared with space networks and aerial networks, terrestrial networks can achieve much higher bandwidth and ultra-lower latency while having a limited coverage (usually in urban areas). Regarding rural areas where infrastructure nodes are difficult to be deployed, both space and aerial networks can offer the Internet services in a compensative way.

The proliferation of maritime and deep-sea exploration activities leads to the emergence of sea-based mobile networks, interconnecting both underwater networks and surface networks. In particular, underwater networks consist of autonomous underwater vehicles (AUVs), underwater sensors, and other underwater devices. Due to the high attenuation in the underwater environment, electromagnetic (EM) wave communications are not widely used for underwater communications. Acoustic communications have been typically used for underwater communications while only supporting a low throughput (e.g., 30 to 40 kbps in shallow water). Underwater optical communications [5] can achieve much higher throughput (in Gbps) than acoustic communications while having a limited communication range (from 10 meters to 100 meters). With respect to surface networks, EM waves are widely adopted for communications between autonomous surface vehicles (ASVs), offshore nodes, UAVs, HAPs, and satellites.

A. Characteristics of SAGSIN

The SAGSIN system consists of diverse infrastructure nodes across different types of networks. In summary, SAGSINs have the following key characteristics.

- *Heterogeneity.* The SAGSIN system consists of diverse infrastructure nodes (e.g., satellites, HAPs, UAVs, gNBs, eNBs, AUVs, etc.), user equipment, and IoT devices. Moreover, the heterogeneity also exhibits in different types of communications and networking protocols across space, aerial, terrestrial, and sea networks.
- *Complexity.* The heterogeneity of SAGSINs consequently leads to high system complexity. For example, space networks adopt radio spectrum and communication protocols different from aerial networks. Moreover, the complexity also exhibits in even the same type of networks, e.g., space networks need to consider inter-satellite links, radio resource management, and handover management.
- *Asymmetricity.* Asymmetricity mainly refers to asymmetric computing and communications resources at different types of networks in the SAGSIN system [2]. In particular, space networks often have limited communications

[1]https://www.spacex.com/
[2]https://www.oneweb.world/

and computing resources, e.g., scarce radio spectrum and limited computing capacity, while terrestrial networks usually have abundant radio spectrum, computing, and storage resources (offered by cloud computing facilities).

B. Challenges of SAGSINs

The unique characteristics of SAGSINs bring many challenges. Firstly, SAGSINs confront a number of security vulnerabilities exhibiting in the entire network stack, covering the physical layer, link layer, and network layer. For example, legitimate satellite-ground communications can be eavesdropped (wiretapped) by malicious users at ground or in the air (e.g., malicious UAVs), as shown in Fig. 1. Moreover, the handoff process between different satellite links also undergoes distributed denial of service (DDoS) attacks, thereby resulting in communication interruptions. Furthermore, both the heterogeneity and the complexity of SAGSINs lead to difficulty of key management, authentication, and authorization, consequently causing security vulnerabilities of SAGSINs [6].

Secondly, there are arising privacy concerns with SAGSINs. In particular, massive data generated from space, aerial, ground, sea mobile networks have usually been collected and transferred to the ground data centers. During data transmission, caching (temporary storage), and processing, data privacy can be intentionally or mistakenly leaked to untrusted third parties (e.g., the Internet and cloud service providers). Moreover, the trajectory privacy of UAVs, HAPs, and satellites can also be leaked to malicious users due to the authorized access or malicious intrusion to SAGSINs due to the security vulnerabilities of SAGSINs.

Thirdly, both heterogeneity and complexity of SAGSINs can result in the challenge of resource sharing among different types of networks in SAGSINs. For example, it is difficult to share the collected data between sea networks, ground networks, and space networks, consequently forming information silos. As a result, the quality of services (QoS) is lowered since it is hard to accurately predict and recommend service providers without analyzing information across different networks. Moreover, the asymmetricity of SAGSINs requires the orchestration of diverse computing and communication resources across different networks while it is challenging to achieve this goal with consideration of multiple stakeholders.

III. Network slicing and softwarisation for SAGSINs

Network slicing and softwarisation have been widely agreed as a promising technology to accommodate diversified services for the future Internet such as SAGSINs. Network softwarisation refers to the design, architecture, orchestration, and management of software-based hardware and software resources of a network infrastructure. With network softwarisation, a slice of network resources can be created according to the demands and requirements of a specific service. This slice of network resources is referred to as network slicing. The concept of network slicing has been first introduced in 3GPP Release 15[3], and then it is discussed more extensively in 3GPP Release 16[4] focusing on mobility, authentication and authorization, multiple tenant environment, and performance assurance for 5G networks. It has also been mentioned in a number of other standardization bodies, including NGMN[5], ETSI NFV[6], and ITU[7].

Network functions virtualization (NFV) and software-defined networking (SDN) are two of the most important enabling technologies of network slicing and softwarisation. NFV provides a way of enabling software-based network functions (also known as virtual network functions [VNFs]) which were available in the dedicated hardware form. It also provides a management and orchestration (MANO) framework to orchestrate and manage VNFs into a service chain according to the service needs. SDN facilitates the network control by separating the control plane from the data plane. It works with NFV to instantiate the service chain into the physical network infrastructure. This is performed by 1) VNF instantiation in the virtual machines (VMs) or containers of the standard servers in the physical network, and 2) the network connection between VMs or containers performed by SDN to meet the service chain requirement. The virtualization technology is another key enabling technology of network slicing and softwarisation to ensure the security and isolation of virtualized resources e.g., VMs. In what follows, we will first briefly review how network slicing and softwarisation is enabled in space, air, ground and sea mobile networks separately. Then, we will focus on three important issues of network slicing and softwarisation in the emerging SAGSINs, including cross-domain slicing, inter-slice scaling, and network economy. Table I summarizes the enabling technologies of network slicing and softwarisation for SAGSINS and its sub-networks.

A. Network slicing and softwarisation of ground-based mobile networks

Network slicing and softwarisation of ground-based mobile networks has been well supported by 5G networks including 5G radio access networks (RAN) and 5G core networks. Existing works include RAN slicing, core network slicing, and E2E network slicing including both RAN and core network slicing. RAN slicing and core network slicing are essentially separate, but in order to make E2E network slicing, the resources at the core network need to be reserved based on the demands from RAN slicing [7]. With the advent of Industry 4.0, in addition to the RAN and core network slicing, more "private" networks like industry networks need to be considered in this E2E network slicing. One of the key characteristics of network slicing is to meet service requirements in terms of e.g., packet delay and loss. However, many industry networks were using the connectivity technologies that do not have the QoS guarantee. In order to meet network slicing requirements, time-sensitive networking (TSN) and deterministic networking

[3]https://www.3gpp.org/release-15

[4]https://www.3gpp.org/release-16

[5]https://www.ngmn.org/wp-content/uploads/NGMN-5G-White-Paper-2.pdf

[6]https://www.etsi.org/committee/nfv

[7]https://www.itu.int/rec/T-REC-Y.3112/en

TABLE I
ENABLING TECHNOLOGIES OF NETWORK SLICING AND SOFTWARISATION FOR SAGSINS AND ITS SUB-NETWORKS.

Types of Networks	Enabling technologies for network slicing and softwarisation
Ground-based mobile networks	5G RAN, 5G core networks, TSN, DetNet
Air-based mobile networks	5G RAN, wireless network virtualization
Space-based mobile networks	Resource allocation at satellite terminals, satellites, satellite gateways
Sea-based mobile networks	5G RAN, wireless network virtualization
SAGSINs	The above technologies, cross-domain slicing, inter-slice scaling

(DetNet) technologies have received increasing attention in industry networks [8].

B. Network slicing and softwarisation of air-based mobile networks

Air-based mobile networks are usually established by HAPs and AFVs such as UAVs. Essentially, such AFVs have two roles in air-based mobile networks: 5G base station and wireless transport connectivity. Modern AFVs are equipped with lightweight 5G-enabled base stations, and they can provide 5G RAN services. Like a normal 5G RAN, such an AFV has network slicing and softwarisation capabilities in nature. Alternatively, an AFV can support a wireless transport connectivity towards a 5G base station, or from 5G RAN to a 5G core network. In order to allow network slicing for such a wireless transport connectivity, wireless network virtualization needs to be enabled [9].

C. Network slicing and softwarisation of space-based mobile networks

Space-based mobile networks are usually provided by satellite systems. Slightly different from the AFVs, due to their wider coverage, satellite systems serve more as a wireless transport connectivity towards a 5G base station, or between 5G RAN and a 5G core network as a transport network. The architecture of a satellite system is composed of ground, space, and user segments. The satellite terminal in the user segment communicates with the satellite gateways in the ground segment through one or multiple satellites (e.g., LEO satellites, GEO satellites, and MEO satellites) in the space segment. In order to allow network slicing for satellite systems, resource allocation needs to be enabled at satellite terminals, satellites, and satellite gateways, respectively.

D. Network slicing and softwarisation of sea-based mobile networks

Sea-based mobile networks are usually provided by AUVs and ASVs [10]. With the fast development of 5G technologies, ASVs are equipped with 5G modules that can be used to communicate with satellites and modern AFVs. AUVs essentially use the sink nodes as refer nodes to communicate with other entities such as a base station and an ASV. Depending on the distance of ASV from the land, satellites and AFVs are usually involved to facilitate the communication between a sea-based mobile network and the base station on the land. Therefore, network slicing for a sea-based mobile network may refer to a slice of resources of an ASV, an AFV, a satellite system, a 5G RAN, and a 5G core network.

E. Cross-domain slicing in SAGSINs

A SAGSIN essentially consists of multiple administrative network domains. E2E network slicing for a SAGSIN thus needs a slice of resources across multiple network domains. Different administrative domains have different types of resources and different optimization strategies for resource management and data control. For example, ground-based mobile networks aim to provide high bandwidth and low latency services, while satellite systems were originally designed to provide connectivity services in rural areas or military fields. However, the request of an E2E network slice has its unique application requirements such as high reliability and low latency. The cross-domain network slicing needs to provide adequate resources at different domains to meet the application needs in an E2E manner. The resource reallocation due to the changes of application demands needs to be incorporated in a cross-domain manner so that the E2E performance can be guaranteed.

The cross-domain slicing is usually handled in two ways: hierarchical manner and distributed manner. In the hierarchical fashion, there are two levels of slice orchestration, one is for the E2E cross-domain slice, and the other is for the domain-specific orchestration [11]. SDN is usually involved in slice management. The domain-specific SDN controller and NFV MANO can be adopted for the management and orchestration of resources at each administrative network domain. The higher level SDN controller and NFV MANO can be adopted for the life-cycle management of the E2E slice across multiple domains. The domain-specific SDN controllers can enable the abstraction of each administrative domain, and the higher level SDN controller allows the interaction of multiple administrative domains. In the distributed fashion, there is no centralized controller to coordinate distinctive management and control strategies from different domains, where the SDN controller at each domain works in a decentralized manner. Therefore, there must be a communication protocol that allows the information exchange between administrative domains [12]. The SDN controller at each domain needs to work out a slicing solution for its own domain according to the collected

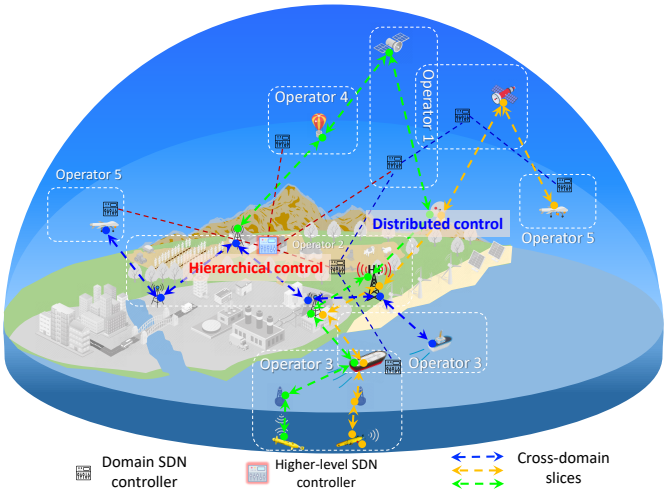

Fig. 2. Cross-domain slicing with both hierarchical and distributed ways of management and orchestration.

information from neighboring domains, so that the E2E slicing can meet the application requirements. Fig. 2 shows the cross-domain slicing with both hierarchical and distributed ways of management and orchestration.

F. Inter-slice scaling in SAGSINs

One of the characteristics of network slicing is to allow elastic and automatic resource scaling (i.e., resource reallocation) depending on the application needs. The resource here refers to both network resources (e.g., computing, networking, and storage resources) and the VNFs in the event of reallocating between VMs and/or servers. Given the limited resources of a physical infrastructure, resources are usually reallocated between slices, in the actual way of releasing back to the physical infrastructure (from one slice) and reallocating to another slice. Existing works have been performed for real-time and online resource scaling of network slicing, by virtue of optimization theory, game theory, and machine learning [7], [13].

The intrinsic cross-domain nature of SAGSINs brings additional *challenges* and *benefits* to the resource scaling of network slicing. The challenges come from the distinct types of resources, and the management and control strategies, between different domains. This brings an additional requirement for the communication protocol design that needs to allow a unified resource measurement across network domains. With the help of such a communication protocol, the network slice broker would carry out the management and orchestration of a slice in an E2E manner. On the other hand, the benefits come from the additional capabilities of different domains (e.g., computing, networking, and storage). Such additional resource capabilities could compensate for the resource limitation of a single network domain by virtue of the resource federation among multiple domains. Both abstraction and unification of resources across domains are needed to allow inter-slice scaling in SAGSINs.

G. Network economy in SAGSINs

The cross-domain nature of SAGSINs brings a significant problem to the network economy. From a user's (slice brokers) point of view, they shall minimize the cost of building a slice. From the perspective of network operators, they shall maximize their revenue, which comes from the profit from network slice brokers subtracting the resource renting cost from other administrative domains (in order to build an E2E slice that meets the application requirements). Game theory has been widely adopted to solve network economy issues. A two-stage game might be considered to address the issue in SAGSINs. The first stage is to find an equilibrium between different domains in order to build an E2E slice, and the second stage is to find an equilibrium between slice brokers and network operators in terms of an optimal pricing scheme. In terms of solving game theory models, neural networks can be considered, which can significantly mitigate the uncertainties caused by the cross-domain environment. In addition, new business models need to be considered to maximize the benefits of SAGSINs. For example, incentive mechanisms might need to be considered to stimulate the cooperation between different domains, e.g., sharing resources. In addition, new services, e.g., cross-domain-slicing-as-a-service and inter-slice-scaling-as-a-service, could be introduced.

IV. Integration of Blockchain, Network Slicing and Softwarisation for SAGSINs

A. Overview of blockchain technologies

Blockchain technologies have received growing interest recently. A blockchain is essentially a chain of data records, each of which is named as a block. Each block in a blockchain consists of the cryptographic hash value of its previous block, a timestamp, and historical transactional data. A blockchain keeps growing when new transactions are being committed and confirmed. The validation of a block is achieved by distributed consensus mechanisms. Since each node in the blockchain network keeps the entire blockchain, any modification on the blockchain needs to be approved by all the nodes in the network. The blockchain can essentially assure the immutability, auditability, and traceability of blockchain data.

The advent of blockchain technologies also fosters the development of smart contracts, which are essentially computerized contractual clauses or terms in programming languages. Being compiled into machine codes (or byte codes), smart contracts are stored in the blockchain so as to assure the immutability of smart contracts. When a certain event triggers the contractual statement (e.g., the date to update IoT firmware reaches or the tenancy period expires), a smart contract will automatically be executed at a VM deployed in a blockchain node. Smart contracts can automate business processes, e.g., maintenance, tenancy, and brokerage. Smart contracts can simplify traditional administrative processes, save cost, and shorten the turnaround time.

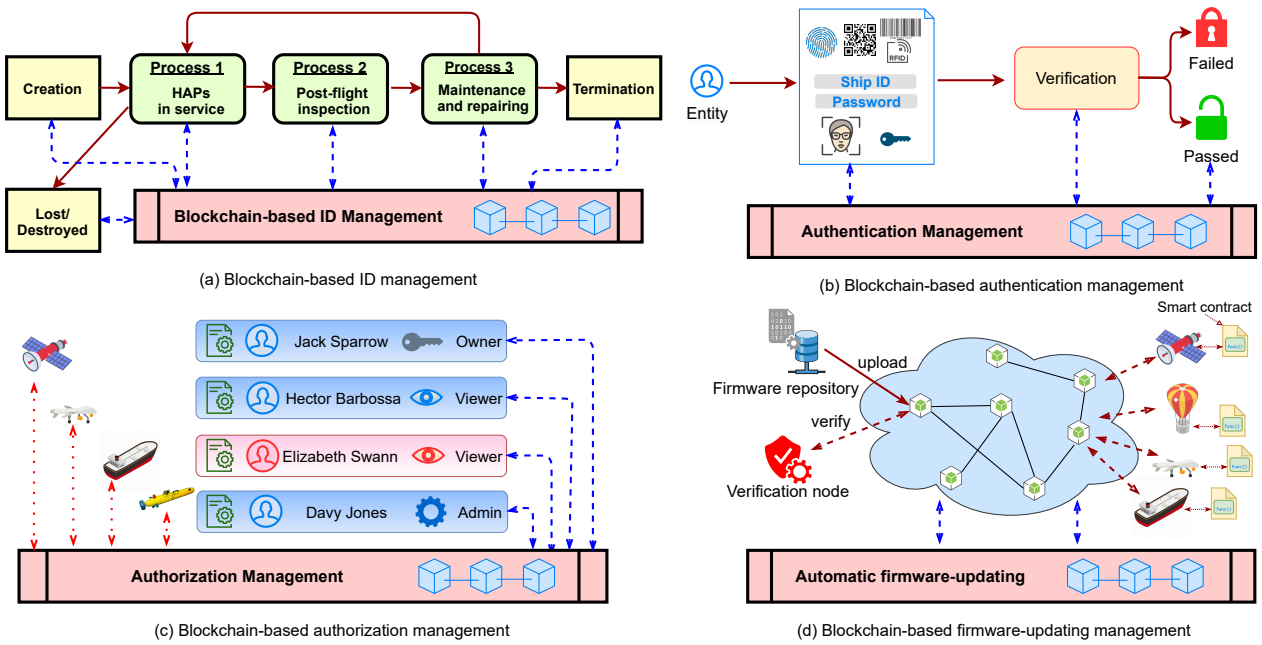

Fig. 3. Blockchain-enabled network management for SAGSINs.

B. Convergence of blockchain with network slicing and softwarisation

Blockchain technologies are an ideal catalyser to the full realization of network slicing and softwarisation. Blockchains can enable the network management of SAGSINs and brokerage services of diverse resources. We next elaborate on them in detail.

1) Network management of SAGSINs: Both heterogeneity and complexity of SAGSINs lead to the difficulty of network management in SAGSINs. On the one hand, it is challenging to manage massive heterogeneous network nodes, including satellites, HAPs, UAVs, ground gNBs, user equipment, surface nodes, and underwater nodes. Moreover, the dynamicity of SAGSINs (e.g., nodes may arbitrarily join and leave the network) makes it even worse. On the other hand, the complexity of SAGSINs also leads to the difficulty in identity and access management. The inappropriate access control or unauthorized access is often the root cause of security vulnerabilities and privacy leakages.

The adoption of blockchains to SAGSINs can facilitate the network management in aspects of ID management, authentication, authorization, and firmware-updating management, as shown in Fig. 3. In particular, blockchains can decentralize existing centralized network management systems. Nodes in SAGSINs can register, modify, revoke, and expire their IDs in blockchain-enabled ID management systems as shown in Fig. 3(a). Meanwhile, the whole life cycle of SAGSIN nodes is essentially traceable due to the traceability of the blockchain since every event is stored in the blockchain. Moreover, blockchain-based network management can also facilitate the authentication process as shown in Fig. 3(b).

Furthermore, blockchain-based authorization management can enhance authorization and access control of SAGSIN nodes since fine-grained access control policies saved in blockchains can enforce effective network authorization, as shown in Fig. 3(c). Furthermore, smart contracts on top of blockchains can also automate firmware upgrade processes of SAGSIN nodes, as shown in Fig. 3(d). For example, smart contracts deployed at SAGSIN nodes trigger automatic firmware-upgrading processes. The firmware-upgrading processes first scan firmware patches to avoid malicious codes and then automatically install firmware patches at nodes [14].

2) Brokerage services of SAGSINs: The built-in smart contracts can enable brokerage services of SAGSINs [15]. Running on top of blockchains, smart contracts can assure the trust of brokerage services throughout the entire SAGSINs. Fig. 4 presents blockchain-enabled brokerage services of SAGSINs.

There are multiple stakeholders in SAGSINs, as shown in Fig. 4. Infrastructure providers own different types of resources, such as RAN, network/computing sources, VMs, containers, and VNFs. Network brokers and managers can then orchestrate the underlying infrastructure resources and provide other stakeholders with diverse network slices. In particular, mobile network operators (MNOs) mainly maintain physical resources while mobile virtual network operators (MVNOs) lease virtual resources from MNOs. Meanwhile, over-the-top (OTT) service providers need to sign predefined service level agreements (SLAs) with MVNOs/MNOs so as to obtain the predefined network slices. SLAs also specify QoS and other requirements. Moreover, vertical industries are a number of applications across different industrial sectors, such as manufacturing, transportation, and agriculture.

During the interactions of multiple stakeholders, blockchains and smart contracts play a crucial role in offering a trustworthy brokerage service. Firstly, blockchains store the identification of every stakeholder as well as other properties, such as access control lists. Secondly, network slicing subscriptions and SLAs can be implemented by

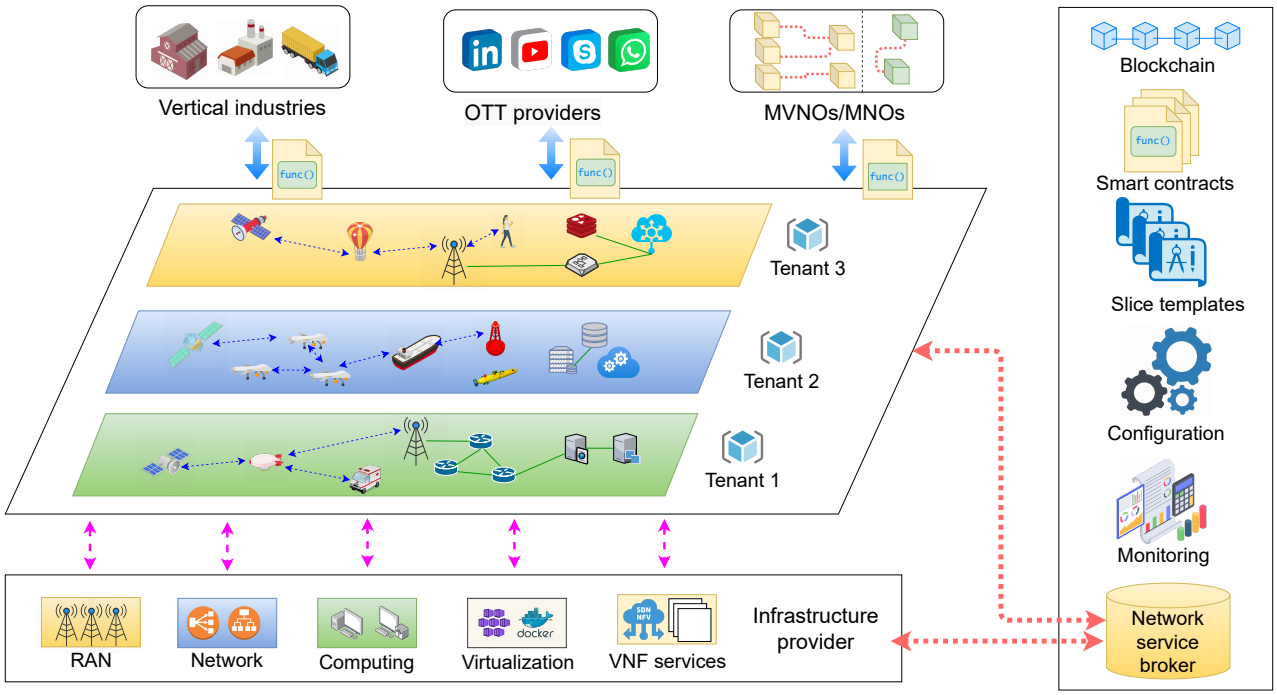

Fig. 4. Blockchain-enabled brokerage services of SAGSINs.

smart contracts. Moreover, blockchains can also automate the settlement and the payment process among multiple parties. Thirdly, unlike conventional centralized systems, the distributed nature of blockchains also prevents the system from a single point of failure and other malicious attacks.

C. Summary of solutions to the challenges of SAGSINs

As mentioned in Section II-B, SAGSINs face several challenges, such as security vulnerabilities, privacy concerns, and difficulties in resource sharing. We now troubleshoot the solutions to these challenges when blockchain, network slicing, and network softwarisation are integrated into SAGSINs. Table II summarizes the solutions to the challenges brought by the integration of blockchain, network softwarisation, and network slicing. It is worth mentioning that we just list the major technologies used for solutions in Table II though they should be integrated in the proposed framework.

V. Research Issues and Open Challenges

Existing research works have been conducted to address blockchain issues and network slicing and softwarisation issues of a ground-based mobile network, an air-based mobile network, a space-based mobile network, and a sea-based mobile network separately. There is little research carried out on the integration of blockchain and network softwarisation for SAGSINs. In order to move forward in this important research direction, the following research challenges shall be considered.

- One of the critical issues that hinder the efficiency of cross-domain slicing is that different administrative domains have different security and privacy considerations and strategies. SAGSINs bring additional challenges to the cross-domain slicing in the dimension that different administrative domains have distinct types of resources with different connectivity purposes and computation capacities. For example, satellite systems in the space-based mobile networks usually focus on a wider coverage, while AFVs in the air-based mobile networks usually aim for bridging different domains. Blockchain is able to address this issue due to its privacy protection and security mechanisms but with the challenge of a unification mechanism across multiple domains. In addition, a joint optimization considering the resource capacities of SAGSINs and the computation needs of blockchain systems is necessary to enhance the system utility of SAGSINs.
- As we mentioned in Section III-E, the control of different domains can be carried out in either a hierarchical manner or a distributed manner. The hierarchical manner is easier to implement and has been widely adopted. But from the security point of view, e.g., single point of failure, the distributed and decentralized manner is more effective and practical. The actual implementation of a purely distributed control of cross-domain slicing is challenging. The decentralized working principle of blockchain systems is a good candidate to achieve this implementation. However, the scale of SAGSINs challenges the efficiency of blockchain systems. How to optimize the large-scale blockchain systems with practical considerations, e.g., the storage of partial and complete transaction records and the computing resource allocations across domains, is still a hard research problem.
- SAGSINs work in a way with the contribution from multiple domains to build E2E network slices. However,

TABLE II
SUMMARY OF SOLUTIONS TO CHALLENGES OF SAGSINS.

Challenges	Solutions
Security vulnerabilities	Blockchain-enabled network management (e.g., ID and authentication management, automatic firmware-updating)
Privacy concerns	Blockchain-based authorization management
Difficulty in data sharing	Network softwarisation, network slicing, blockchain-enabled brokerage services

selfish nature exists in this cross-domain environment. An adequate incentive mechanism is needed to build a collaborative SAGSIN so that resources would be available for making an E2E slice across multiple domains. Game theory is a promising tool to address network economy issues. However, a game model needs to be solved each time when a network situation changes. Due to the complexity and dynamic nature of SAGSINs, the computational efforts that are needed to frequently solve a game theory model would be impractical. Recent research works are trying to make an equivalent machine learning model with the game model. As the machine learning model does not need to be solved each time when a network situation changes, the computation efforts can be reduced. However, on the other hand, in the process of building the equivalent machine learning model, a considerable amount of constraints due to the cross-domain nature of SAGSINs and the built-in blockchain systems need to be integrated into the model, which increases the model complexity. How to reduce the complexity of the equivalent machine learning model while maintaining a good matching between the built machine learning model and the actual game model is still a challenge.

- The scalability of blockchains should be considered when they are integrated into SAGSINs. On the one hand, the adoption of private or consortium blockchains is expected instead of public blockchains in SAGSINs since private or consortium blockchains are usually more scalable than public blockchains. On the other hand, other technologies such as sharding and hybrid of off-chain and on-chain storage can be considered to improve the scalability of blockchains when they are used in SAGSINs.

VI. CONCLUSION

As a promising technology for the future Internet, SAGSINs have received extensive attention though there are many challenges to be addressed before the full realization. This article investigates the adoption of blockchain, network slicing, and network softwarisation technologies to address the emerging challenges of SAGSINs. In particular, the characteristics as well as challenges of SAGSINs have been introduced. After reviewing network slicing and softwarisation technologies, the integration of the blockchain with network slicing and softwarisation has been thoroughly investigated with a focus on network management and brokerage services of SAGSINs. This article also outlines the open issues and research challenges as the future research directions.

REFERENCES

[1] J. Li, K. Xue, J. Liu, Y. Zhang, and Y. Fang, "An ICN/SDN-Based Network Architecture and Efficient Content Retrieval for Future Satellite-Terrestrial Integrated Networks," *IEEE Network*, vol. 34, no. 1, pp. 188–195, 2020.

[2] S. Zhou, G. Wang, S. Zhang, Z. Niu, and X. S. Shen, "Bidirectional Mission Offloading for Agile Space-Air-Ground Integrated Networks," *IEEE Wireless Communications*, vol. 26, no. 2, pp. 38–45, 2019.

[3] M. Bacco, L. Boero, P. Cassara, M. Colucci, A. Gotta, M. Marchese, and F. Patrone, "IoT Applications and Services in Space Information Networks," *IEEE Wireless Communications*, vol. 26, no. 2, pp. 31–37, 2019.

[4] B. Di, L. Song, Y. Li, and H. V. Poor, "Ultra-Dense LEO: Integration of Satellite Access Networks into 5G and Beyond," *IEEE Wireless Communications*, vol. 26, no. 2, pp. 62–69, 2019.

[5] N. Saeed, A. Celik, T. Y. Al-Naffouri, and M.-S. Alouini, "Underwater optical wireless communications, networking, and localization: A survey," *Ad Hoc Networks*, vol. 94, p. 101935, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870518309776

[6] T. Alladi, V. Kohli, V. Chamola, F. R. Yu, and M. Guizani, "Artificial Intelligence (AI)-Empowered Intrusion Detection Architecture for the Internet of Vehicles," *IEEE Wireless Communications*, vol. 28, no. 3, pp. 144–149, 2021.

[7] X. Cheng, Y. Wu, G. Min, A. Y. Zomaya, and X. Fang, "Safeguard Network Slicing in 5G: A Learning Augmented Optimization Approach," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 7, pp. 1600–1613, 2020.

[8] A. Nasrallah, A. S. Thyagaturu, Z. Alharbi, C. Wang, X. Shao, M. Reisslein, and H. ElBakoury, "Ultra-Low Latency (ULL) Networks: The IEEE TSN and IETF DetNet Standards and Related 5G ULL Research," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 88–145, 2019.

[9] Y. K. Tun, N. H. Tran, D. T. Ngo, S. R. Pandey, Z. Han, and C. S. Hong, "Wireless network slicing: Generalized kelly mechanism-based resource allocation," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 8, pp. 1794–1807, 2019.

[10] Y. Wu, Y. Ma, H.-N. Dai, and H. Wang, "Deep learning for privacy preservation in autonomous moving platforms enhanced 5G heterogeneous networks," *Computer Networks*, vol. 185, p. 107743, 2021. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S138912862031327X

[11] S. Dräxler, H. Karl, H. R. Kouchaksaraei, A. Machwe, C. Dent-Young, K. Katsalis, and K. Samdanis, "5G OS: Control and Orchestration of Services on Multi-Domain Heterogeneous 5G Infrastructures," in *2018 European Conference on Networks and Communications (EuCNC)*, 2018, pp. 1–9.

[12] Z. Kotulski, T. W. Nowak, M. Sepczuk, M. Tunia, R. Artych, K. Bocianiak, T. Osko, and J.-P. Wary, "Towards constructive approach to end-to-end slice isolation in 5G networks," *EURASIP Journal on Information Security*, vol. 2018, no. 1, p. 2, Mar 2018. [Online]. Available: https://doi.org/10.1186/s13635-018-0072-0

[13] H. Wang, Y. Wu, G. Min, and W. Miao, "A graph neural network-based digital twin for network slicing management," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 10.1109/TII.2020.3047843, 2020.

[14] J.-W. Hu, L.-Y. Yeh, S.-W. Liao, and C.-S. Yang, "Autonomous and malware-proof blockchain-based firmware update platform with efficient batch verification for internet of things devices," *Computers & Security*, vol. 86, pp. 238 – 252, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S016740481831438X

[15] B. Nour, A. Ksentini, N. Herbaut, P. A. Frangoudis, and H. Moungla, "A Blockchain-Based Network Slice Broker for 5G Services," *IEEE Networking Letters*, vol. 1, no. 3, pp. 99–102, 2019.

Hong-Ning Dai [SM'16] is currently with the Department of Computing and Decision Sciences, Lingnan University, Hong Kong, as an associate professor. He obtained the Ph.D. degree in Computer Science and Engineering from Department of Computer Science and Engineering at the Chinese University of Hong Kong. His current research interests include the Internet of Things and blockchain technology. He has served as associate editors of IEEE Transactions on Industrial Informatics, IEEE Systems Journal, and IEEE Access. He is also a senior member of the ACM.

Yulei Wu [SM'18] is a Senior Lecturer with the Department of Computer Science, College of Engineering, Mathematics and Physical Sciences, University of Exeter, United Kingdom. He received the B.Sc. degree (First Class Honours) in Computer Science and the Ph.D. degree in Computing and Mathematics from the University of Bradford, United Kingdom, in 2006 and 2010, respectively. His expertise is on intelligent networking and networked systems, and his main research interests include connected vehicles, autonomous systems, Internet of Things, mobile edge computing, privacy and trust. He is an Associate Editor of IEEE Transactions on Network and Service Management and IEEE Transactions on Network Science and Engineering, as well as an Editorial Board Member of Computer Networks and Future Generation Computer Systems. He is a Senior Member of the IEEE and the ACM, and a Fellow of the HEA (Higher Education Academy).

Muhammad Imran [SM] is working as a senior lecturer in the School of Engineering, Information Technology & Physical Sciences, Federation University, Australia. His research interests include mobile and wireless networks, Internet of Things, cloud and edge computing, and information security. He has published more than 200 research articles in reputable international conferences and journals. His research is supported by several grants. He serves as an associate editor for many top ranked international journals. He has received various awards.

Nidal Nasser [SM] completed his Ph.D. at the School of Computing, Queen's University, Kingston, Ontario, Canada, in 2004. He is currently a professor of software engineering at the College of Engineering, Alfaisal University, Saudi Arabia. He worked in the School of Computer Science at the University of Guelph, Guelph, Ontario, Canada. He was the Founder and Director of the Wireless Networking and Mobile Computing Research Lab @ Guelph. He is currently the Founder and Director of the Telecommunications Computing Research Lab @ Alfaisal University. He has authored 180 journal publications, refereed conference publications and book chapters in the area of wireless communication networks and systems. He is currently serving as an associate editor for IEEE Wireless Communications Magazine, Wiley's International Journal on Communication Systems, and IEEE Systems Journal. He has been a member of the technical program and organizing committees of several international IEEE conferences and workshops. He has received several outstanding research awards as well as a number of best paper awards.