Blockchain-Empowered Space-Air-Ground Integrated Networks: Opportunities, Challenges, and Solutions

Yuntao Wang, Zhou Su, *Senior Member, IEEE*, Jianbing Ni, *Member, IEEE*, Ning Zhang, *Senior Member, IEEE*, and Xuemin Shen, *Fellow, IEEE*

***Abstract*—The terrestrial networks face the challenges of severe cost inefficiency and low feasibility to provide seamless services anytime and anywhere, especially in the extreme or hotspot areas (e.g., disaster areas, mountains, and oceans) due to limited service coverage and capacity. The integration of multi-dimensional networks consisting of space, air, and ground layers is expected to provide solutions in delivering cost-effective and ubiquitous Internet of things (IoT) services for billions of users and interconnected smart devices. Autonomous data collection, exchange, and processing across different network segments with minimal human interventions in space-air-ground IoT (SAG-IoT) can bring great convenience to consumers, however, it also suffers new attacks from intruders. Severe privacy invasion, reliability issues, and security breaches of SAG-IoT can hinder its wide deployment. The emerging blockchain holds great potentials to address the security concerns in SAG-IoT, thanks to its prominent features of decentralization, transparency, immutability, traceability, and auditability. Despite of the benefits of blockchain-empowered SAG-IoT, there exist a series of fundamental challenges in terms of efficiency and regulation due to the intrinsic characteristics of SAG-IoT (e.g., heterogeneity, time-variability, and poor interoperability) and the limitations of existing blockchain approaches (e.g., capacity and scalability). This article presents a comprehensive survey of the integration of blockchain technologies for securing SAG-IoT applications. Specifically, we first discuss the architecture, characteristics, and security threats of SAG-IoT systems. Then, we concentrate on the promising blockchain-based solutions for SAG-IoT security. Next, we discuss the critical challenges when integrating blockchain in SAG-IoT security services and review the state-of-the-art solutions. We further investigate the opportunities of blockchain in artificial intelligence and beyond 5G networks and provide open research directions for building future blockchain-empowered SAG-IoT systems.**

***Index Terms*—Blockchain, space-air-ground integrated network (SAGIN), Internet of Things (IoT), security, privacy, trust, network optimization.**

Manuscript received August 19, 2021; revised October 28, 2021; accepted November 19, 2021. Date of publication December 1, 2021; date of current version February 24, 2022. This work was supported in part by NSFC under Grant U20A20175 and Grant U1808207, and in part by the Fundamental Research Funds for the Central Universities. *(Corresponding author: Zhou Su.)*

Yuntao Wang and Zhou Su are with the School of Cyber Science and Engineering, Xi'an Jiaotong University, Xi'an 710049, China (e-mail: zhousu@ieee.org).

Jianbing Ni is with the Department of Electrical and Computer Engineering, Queen's University, Kingston, ON K7L 3N6, Canada.

Ning Zhang is with the Department of Electrical and Computer Engineering, University of Windsor, Windsor, ON N9B 3P4, Canada.

Xuemin Shen is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada.

Digital Object Identifier 10.1109/COMST.2021.3131711

I. Introduction

RECENT decades have witnessed the rapid advances of terrestrial wireless communication technologies and the surge growth of low-cost smart devices. It is predicted that by 2025 the number of connected devices will reach up to 27 billion with a global market over $3 trillion, and the data volume produced by Internet of Things (IoT) devices will be more than 2 ZB [1]. The massive data produced by the explosively increasing number of IoT devices enables a large number of emerging applications in various domains including smart home, smart city, smart healthcare, intelligent transportation, and advanced manufacturing. To accommodate the diverse quality-of-service (QoS) requirements of a wide range of IoT services and applications in various scenarios (e.g., urban, crowded, and sparsely populated areas), future communication networks are envisioned to offer ubiquitous connectivity, low latency, high capacity, and high reliability [2]. Currently, limited by the network coverage and capacity, it is infeasible for existing terrestrial wireless networks (e.g., Wi-Fi, long-term evolution (LTE), and 5G) alone to offer reliable and cost-effective wireless services anytime and anywhere [3], especially for extreme areas such as disaster areas, mountains, and oceans. In particular, it can cause severe cost inefficiency in offering remote IoT services in rural areas by deploying terrestrial network infrastructures. Moreover, in environmentally harsh scenarios such as disaster sites, terrestrial communication networks can be destroyed or damaged functionally. On the other hand, traffic demands can vary dramatically in both time and space in urban or hotspot areas, while the fixed deployment of ground communication infrastructures lacks flexibility for on-demand applications such as virtual reality games, live sports, and city traffic monitoring.

The space-air-ground integrated networks (SAGINs) offer a promising solution for large-scale coverage and network performance enhancement for mobile and IoT devices [2]–[4]. SAGINs consist of three network segments, i.e., the communication satellites form the *space subnetwork*; aerial communication devices such as balloons, airships, and unmanned

aerial vehicles (UAVs) form the *aerial subnetwork*; and terrestrial communication networks form the *ground subnetwork*. In SAGINs, satellites can offer wide coverage and seamless access capability for most remote and sparsely populated areas and assist services such as public emergency rescue, earth observation, and navigation. Generally, a geostationary earth orbiting (GEO) satellite can cover about half of the Earth's area, and a low earth orbiting (LEO) satellite can cover nearly 7.95% of the Earth's surface area. Aerial subnetworks can be flexibly scheduled in an on-demand manner to temporally increase network capacity to meet the spatiotemporally dynamic traffic demands. For example, by harnessing the flexibility and controllable maneuverability of UAVs, a series of network functions (e.g., edge caching, rapid service recovery, and offloading) can be enabled for users and IoT devices in crowded areas. SAGINs have attracted wide attention from both academia and industry, and more and more worldwide projects are focused on SAGINs such as Google's Loon, AT&T's Flying COW, SpaceX, Global Information Grid (GIG), and OneWeb.

A. Challenges of Securing SAG-IoT Systems

Despite the promising advantages of space-air-ground IoT (SAG-IoT), the security, reliability, and privacy concerns are dominant factors that impede its success [5]–[7]. Firstly, intrinsic trust and data reliability issues may arise in SAG-IoT during multi-hop transmissions among distrustful entities within each segment or across segments. Secondly, the network topology of SAGIN can be highly dynamic and the devices in/across segments can be dramatically heterogeneous, which results in a critical challenge for large-scale, dynamic, and automated resource scheduling and orchestration toward efficient integration of different network segments. Thirdly, compared to traditional centralized architectures such as cloud-based IoT, in the large-scale SAG-IoT consisting of various heterogeneous network segments, a distributed approach tolerable to device failures and single point of failure (SPoF) may be more suitable for large-scale practical implementations. Furthermore, as the SAG-IoT employs various communication protocols in each network segment, it can cause poor interoperability especially for inter-operations across different segments. Moreover, due to the lack of fundamental and unified security provisioning, interconnected smart devices such as IP cameras, webcams, and UAVs can be vulnerable to a variety of cyber attacks, and it is also hard for traceable data provenance. For example, in 2016, Mirai, as one of the largest IoT botnets to date, attacked a huge part of the Internet including Twitter, Netflix, and Reddit using malicious traffic with Tbps level produced by tens of thousands of hacked smart devices [8]. In addition, the pervasive and invisible data collection of pervading devices for personalized services may track individuals' private behaviors and reveal the profiles of daily activities. Indeed, wearable devices contain our health information, smart meters know when we go back home, and surveillance UAVs know where we have gone. Thereby, it is urgent and significant to realize the reliable, intelligent, robust, and secure network design and system integration in SAG-IoT.

The emerging blockchain [9], [10] holds numerous potentials to enhance the security for SAG-IoT applications thanks to its prominent features of decentralization, transparency, immutability, traceability, and auditability. As a decentralized, tamper-resistant, and publicly shared ledger, the blockchain is a "secure by design" technology [11] to safeguard SAG-IoT with better robustness through the design of hash-chained blocks, consensus algorithms, and smart contracts. In particular, in the blockchain, data is organized into a growing list of hash-chained ledgers which have been time-stamped and verified by a majority of consensus nodes via consensus operations for ledger consistency. By building the cross-border trusted interactions among distrustful devices, any two entities in SAG-IoT can securely complete data and asset exchange without reliance on any trusted third party (TTP). As such, the operation cost can be greatly reduced while the performance bottleneck and SPoF risk can be alleviated. Moreover, the trust-free SAG-IoT services and applications instantiated by smart contracts (e.g., cross-layer resource management) can be constructed atop the blockchain in an automatic fashion. Besides, the device information, sensory data, processed data, and digital asset trading in SAG-IoT can be recorded in the format of transactions in the blockchain, which is guaranteed to be traceable, reliable, immutable, and undeniable. Furthermore, the blockchain can permanently track node behaviors and the use of personal data with cryptographic evidence, especially for supply chains, thereby promoting a fair, transparent, and auditable environment and preventing the misuse of personal data [12]. Hence, a surge growth of applications integrating blockchain with SAG-IoT can be seen; and over 20% of the IoT applications are expected to enable blockchain-based solutions by 2020 [13].

Nevertheless, existing blockchain solutions may still be inefficient for the wide deployment in SAG-IoT applications. Firstly, the intrinsic features of multi-dimensional SAG-IoT systems including heterogeneity, time-variability, and self-organization, may bring about a series of challenges in the efficient integration with blockchain. Compared with terrestrial networks, SAG-IoT integrates three different network segments and can be regarded as a multi-segment heterogeneous network (HetNet) [3], which is more complex to manage. For example, in SAG-IoT, different network segments are supported by different communication protocols (e.g., satellite links, air-to-air (A2A) links, vehicular ad hoc networks (VANETs)), while massive devices with distinct interfaces for communications and configurations coexist in each network segment. In particular, the blockchain operations in SAG-IoT should consider the collaborative control and management of vast heterogeneous devices, as well as the inter/intra-segment communications in various HetNets. The time-varying dynamic network topology may affect the block propagation modeling, network sharding, data routing, and mobility management. The self-organization feature brings challenging issues such as consensus node discovery, collusion prevention, and cross-layer optimization. As a result, the blockchain technologies need to be redesigned for SAG-IoT applications in terms of IoT-specific consensus mechanisms, mobility enhancement, on-chain and off-chain

cooperation [14], sidechain [15], sharding [16], blockchain pruning [17], and on-chain regulations. Meanwhile, new security threats originated from the conventional blockchain such as Eclipse attacks [18], long range attacks [19], and programming fraud may occur in blockchain-based SAG-IoT applications. Furthermore, the scalability and capacity of existing blockchain systems need to be improved to accommodate the massive data and devices in SAG-IoT, while making a better trade-off among security, efficiency, and decentralization. In addition, various revolutionary technologies such as artificial intelligence (AI), edge/cloud computing, and software-defined network (SDN) are rapidly becoming an integral part of the SAG-IoT fabric, thereby the incorporation with blockchain towards future SAG-IoT networks is non-trivial.

B. Contributions of the Survey and Comparison With Related Surveys

There have been several recent surveys on blockchain [11], [20], [21], and blockchain for IoT applications [22]–[26]. For example, Reyna *et al.* [22] investigated the research issues and possibilities, as well as different architectures, in the integration of blockchain and IoT. Dai *et al.* [23] presented a survey of generalized network architectures of the integrated blockchain-IoT systems. Yang *et al.* [24] reviewed the challenges and existing blockchain-enabled solutions for edge-centric IoT applications. Most recently, Ferrag *et al.* [25] discussed the recent research efforts of blockchain in securing intelligent transportation, smart grid, smart healthcare, etc. Ali *et al.* [26] reviewed the applications of blockchain technology in the IoT domain in terms of security, privacy, trust, identity and data management, and monetization. The above existing surveys mainly focus on the integration of blockchain for ground IoT applications. In comparison to them, this article gives a comprehensive survey of challenges and state-of-the-art advances in harnessing blockchain to safeguard the security of SAG-IoT by integrating the space, air, and ground layers. Moreover, we identify the potential blockchain-empowered applications in the SAG-IoT domain including trustworthy resource allocation, traceable data provenance, device management, personal data protection, resilient network design, and system regulations. Besides, different from existing surveys on the blockchain which mainly focus on the architecture design [20], consensus protocols [21], and security measures [11] of blockchain systems, we put an emphasis on the tailored blockchain solutions for securing SAG-IoT, as well as the security, privacy, and efficiency issues of integrating blockchain with SAG-IoT.

Therefore, it is very interesting and important to have a comprehensive survey on blockchain-empowered solutions for SAG-IoT applications. In this paper, we present an in-depth survey on the key challenges and solutions when applying blockchain technologies in SAG-IoT applications from the security perspective. A summary of contributions of this survey is listed as below:

- We investigate the security and privacy threats in the SAG-IoT domain from five aspects (i.e., data-related, identity-related, communication-related, service-related, and governance-related), and discuss the potentials of harnessing blockchain technologies to resolve them.
- We discuss the state-of-the-art blockchain-based solutions and identify potential blockchain-based SAG-IoT applications including trustworthy resource allocation, traceable data provenance, identity and device management, personal data management, secure communication and resilient network design, digital forensics, and system regulations in safeguarding SAG-IoT security.
- We present the challenges of deploying blockchain-empowered security services in practice and existing industrial and academic advances in designing tailored blockchain approaches for SAG-IoT from the data layer, network layer, consensus layer, incentive layer, contract layer, and application layer.
- We outline the open research issues of applying AI and beyond 5G (B5G) technologies (e.g., edge/cloud computing, SDN, and network slicing) for future blockchain-empowered SAG-IoT systems.

TABLE I
A COMPARISON OF CONTRIBUTION BETWEEN OUR SURVEY AND RELEVANT SURVEYS

Refs.	Contribution
[20] [21] [11]	Survey of blockchain systems in terms of architecture design, consensus protocols, and security measures, respectively.
[3]	Survey on system integration and resource management in SAGINs.
[22]	Discussions on research challenges, trends, and applications of blockchain-IoT systems.
[23]	Survey on generalized network architectures of integrated blockchain-IoT systems.
[24]	Discussions on challenges and existing blockchain solutions for edge-centric IoT applications.
[25]	Discussions on recent research efforts of blockchain in securing intelligent transportation, smart grid, smart healthcare.
[26]	Survey on blockchain-enabled applications in ground IoT including security, privacy, trust, identity&data management, and monetization.
Our work	Comprehensive survey of the integration of blockchain technologies for securing SAG-IoT systems from space, air, and ground layers, discussions about the architecture, characteristics, and security threats of SAG-IoT systems, discussions about potential applications, critical challenges, state-of-the-art solutions, and future research directions of blockchain-empowered SAG-IoT.

Table I summarizes the comparison between our work and previous relevant surveys.

C. Organization of the Survey

The remainder of this article is organized as follows. Section II presents the characteristics and threats of SAG-IoT applications. The potential blockchain-based applications to safeguard SAG-IoT security are summarized in Section III. Section IV discusses the tailored blockchain for SAG-IoT including the architecture, challenges, and existing/potential solutions that integrate blockchain and SAG-IoT. Finally, we discuss future research directions in Section V and draw the conclusion in Section VI. For the reader's convenience, the organization of this paper is illustrated in Fig. 1. Besides, all related acronyms are listed in Table II.

II. SAG-IoT SECURITY AND BLOCKCHAIN TECHNOLOGY

In this section, we first introduce the characteristics of SAG-IoT, and then discuss the threats to SAG-IoT. After that, we give an overview of the blockchain technology.

TABLE II
SUMMARY OF IMPORTANT ABBREVIATIONS IN ALPHABETICAL ORDER

Abbr.	Definition	Abbr.	Definition	Abbr.	Definition
ABE	Attribute-Based Encryption	HAP	High-Altitude Platform	PoET	Proof of Elapsed Time
AI	Artificial Intelligence	HetNet	Heterogeneous Network	PoL	Proof of Labor
AP	Access Point	H2H	Human-to-Human	PoI	Proof of Importance
BS	Base Station	IoT	Internet of Things	PoS	Proof of Stake
B5G	Beyond 5G	IoV	Internet of Vehicles	PoSpace	Proof of Space
BLE	Bluetooth Low Energy	IIoT	Industrial Internet of Things	PoW	Proof of Work
BFT	Byzantine Fault Tolerance	IDaaS	Identity-as-a-Service	PoX	Proof of X
BaaS	Blockchain-as-a-Service	IBE	Identity-Based Encryption	QoE	Quality-of-Experience
BaaI	Blockchain-as-a-Infrastructure	IPFS	InterPlanetary File System	QoS	Quality-of-Service
BGP	Border Gateway Protocol	LAP	Low-Altitude Platform	RBAC	Role-Based Access Control
CA	Certificate Authority	LEO	Low Earth Orbit	RFID	Radio Frequency IDentification
CoC	Chain of Custody	LoS	Line-of-Sight	SAG-IoT	Space-Air-Ground IoT
CP-ABE	Ciphertext Policy ABE	LTE	Long-Term Evolution	SAGIN	Space-Air-Ground Integrated Network
D2D	Device-to-Device	M2M	Machine-to-Machine	SBS	Small Base Station
dBFT	Delegated BFT	MANET	Mobile Ad hoc NETwork	SGX	Software Guard eXtensions
DNN	Deep Neural Network	MBS	Macro Base Station	SDN	Software-Defined Network
DoS	Denial of Service	MEC	Mobile Edge Computing	SPoF	Single Point of Failure
DPoS	Delegated Proof of Stake	MEO	Medium Earth Orbit	SPV	Simplified Payment Verification
DAG	Directed Acyclic Graph	NB-IoT	NarrowBand-IoT	SSI	Self-Sovereign Identity
DHT	Distributed Hash Table	NFC	Near Field Communication	TEE	Trusted Execution Environment
DAO	Decentralized Autonomous Organization	NFV	Network Function Virtualization	TTP	Trusted Third Party
EVM	Ethereum Virtual Machine	NOCC	Network Operation&Control Center	UAV	Unmanned Aerial Vehicle
FANET	Flying Ad hoc NETwork	P2P	Peer-to-Peer	VANET	Vehicular Ad hoc NETwork
FBA	Federated Byzantine Agreement	PBFT	Practical BFT	VLEO	Very Low Earth Orbit
FCC	Federal Communications Commission	PKI	Public Key Infrastructure	VNF	Virtual Network Function
GDPR	General Data Protection Regulation	PII	Personally Identifiable Information	WLAN	Wireless Local Area Network
GEO	Geostationary Earth Orbit	PoA	Proof of Authority	ZKP	Zero-Knowledge Proof
GUID	Global Unique IDentifier	PoB	Proof of Burn	ZB	Zettabyte

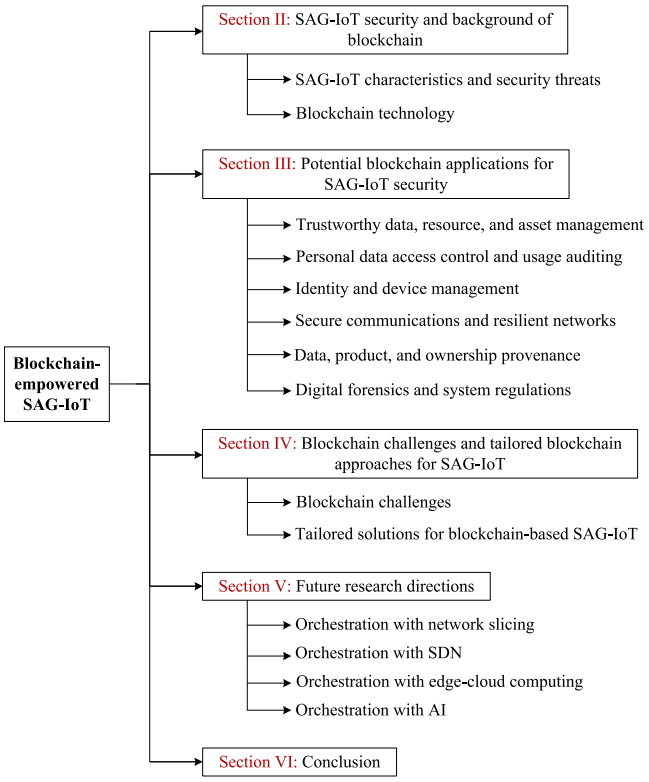


Fig. 1. Organization structure of this paper.

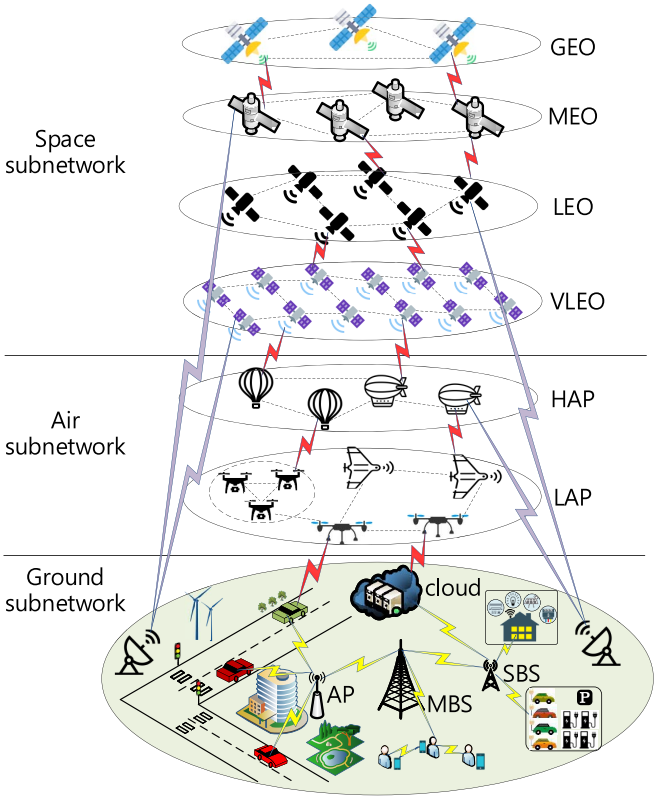


Fig. 2. Architecture of SAG-IoT.

A. SAG-IoT Characteristics and Security Threats

As shown in Fig. 2, a typical SAG-IoT is a hybrid network composed of the space, air, and ground subnetworks [27]. Table III shows the detailed comparison of the space, air, and ground layers in SAG-IoT.

- *Space Subnetwork:* The satellite network consists of a group of satellites and the corresponding terrestrial infrastructures such as ground stations and network operation&control centers (NOCCs). Based on the altitude,

TABLE III
COMPARISON OF SPACE, AIR, AND GROUND LAYERS IN SAG-IOT

Layer	Entities	Altitude	Mobility	One-way Latency	Pros	Cons
Space	GEO	35786km	Static to earth	about 270ms	Broadcast/multicast, global coverage, reliable access	Limited capacity, long propagation delay, costly, high mobility
	MEO	2000-35786km	Medium fast	about 110ms		
	LEO	less than 2000km	Fast	about 40ms		
	VLEO	approximately less than 450km	Fast	Medium		
Air	HAP	17-30km	Quasi-stationary	Medium	Wide coverage, low cost, easy deployment, infrastructure-free	Unstable links, limited capacity, high mobility
	LAP	less than 10km	Highly mobile			
Ground	Ad hoc	N.A.	Static/mobile	Lowest	High throughput	Limited coverage, unbalanced capacity, vulnerable to disaster
	Cellular WLAN	N.A.	Static			

the satellites located at different orbits can be categorized into four kinds: geostationary earth orbit (GEO), medium earth orbit (MEO), low earth orbit (LEO), and very low earth orbit (VLEO). Satellite networks can offer global coverage by using 3 GSO satellites or a constellation of LEO satellites (e.g., 77 LEO satellites in Iridium constellation). Moreover, satellite communications can benefit from broadcast and multicast services to support massive users simultaneously. In addition, it provides reliable access for emergency scenarios, e.g., disaster search and relief. The inter-satellite channel and satellite-to-ground channel follow the large free-space path loss and suffer from the tropospheric attenuation significantly [3]. Meanwhile, the channel of satellite-to-UAV links mainly depends on the line-of-sight (LoS) link and also suffers from the rain attenuation [3]. According to the channel bandwidth, satellite networks can be classified into broadband and narrowband. Broadband satellite networks can provide a high-speed data rate of 10 Gbps and are expected to attain the capacity of 1000 Gb/s by 2020, while narrowband satellite systems can primarily offer global voice and low-rate data services for users. Nevertheless, the round-trip latency between satellites and ground networks is relatively large (especially for GEO and MEO satellites) to support real-time services. Moreover, for satellite-to-UAV links, due to the continuous attitude variation of UAVs, UAVs need to constantly adjust their spatial beam to the target satellite to maintain the connection.

- *Air Subnetwork:* The air network is composed of low-altitude platforms (LAPs) and high-altitude platforms (HAPs). Due to the size, weight, and power (SWaP) constraints, a variety of aircraft platforms including UAVs, balloons, and airships are restricted to different operational altitudes. As a complement to terrestrial networks, air network is featured by wide coverage, low cost, easy deployment, and infrastructure-free to provide broadband wireless services. In particular, UAVs have attracted wide attention from academia to industry owing to the salient features of short-range LoS links, better signal-to-noise ratio (SNR), and additional design degrees of freedom with controlled maneuverability [28]. Specific UAVs equipped with heterogeneous radio interfaces, e.g., Wi-Fi or LTE, can communicate with satellites or ground infrastructures and offer flexible Internet access to ground users/devices. UAVs can either connect to satellites via the sky-haul link or connect to ground networks via the backhaul link [29]. In remote areas, compared with the high cost of satellite connections, a swarm of UAVs can economically and collaboratively form the flying ad hoc network (FANET) to offer information sensing, delivery, and processing services for IoT devices. In crowded places, they can serve as on-demand aerial access points (APs) to alleviate the congestion of macro cells and ensure the QoS of throughput- and latency-sensitive IoT applications, where the corresponding coverage area is called as *drone-cell*. Furthermore, when terrestrial Internet infrastructures go down in disasters, UAVs can assist to construct the emergency communication network and perform sensing and rescue missions (e.g., survivor detection) to benefit the disaster relief process. Nevertheless, air networks have shortcomings in terms of unstable links and limited capacity in practical deployment.
- *Ground Subnetwork:* The ground network consists of various heterogeneous communication systems, e.g., mobile ad hoc network (MANET), cellular network, wireless local area network (WLAN), etc., to support a variety of services. For cellular communications, the macro base stations (MBSs) and small base stations (SBSs) constitute the heterogeneous radio access networks to serve mobile users, IoT devices, autonomous vehicles, etc. As for standardization, the Third Generation Partnership Project (3GPP) aims to design a group of specifications for cellular/mobile environments. The terrestrial networks are able to offer services with high data rates to users, while the network coverage in remote and rural regions is limited and the capacity in hotspots remains to be improved. Moreover, they are vulnerable to man-made infrastructure damages and natural disasters. In the integration of air and ground networks, popular contents can be cached at UAVs or ground devices, and relayed or disseminated via drone-cells or device-to-device (D2D) links. Besides, mobile devices with high computing capability can be conceived as mobile edge computing (MEC) nodes to offload the heavy computation missions produced by UAVs or IoT devices.

A comparative summary of existing industrial projects for SAGIN applications is given in Table IV.

TABLE IV
A SUMMARY OF EXISTING REPRESENTATIVE PROJECTS FOR SAGIN APPLICATIONS

Project	Scenario	Main Components	Targets	Integrated Layers
GIG	Military	Ground, aerospace, near-space and satellite networks	Ubiquitous global communications	Space-air-ground
TSAT	Military	5 GEOs	Real-time optical and radar imagery access	Space-air-ground
Iridium	Telecommunication	66 LEOs	Global data and voice services	Space-ground
O3b	Telecommunication	12-20 MEOs	Seamless broadband Internet access for remote areas	Space-ground
Oneweb	Telecommunication	648 LEOs	Global Internet access with low cost	Space-ground
Google's Loon	Telecommunication	Highflying balloons	Using balloons to beam the Internet to rural areas	Air-ground
AT&T's Flying COW	Telecommunication	UAVs	Emergency connectivity to first responders in disasters	Air-ground

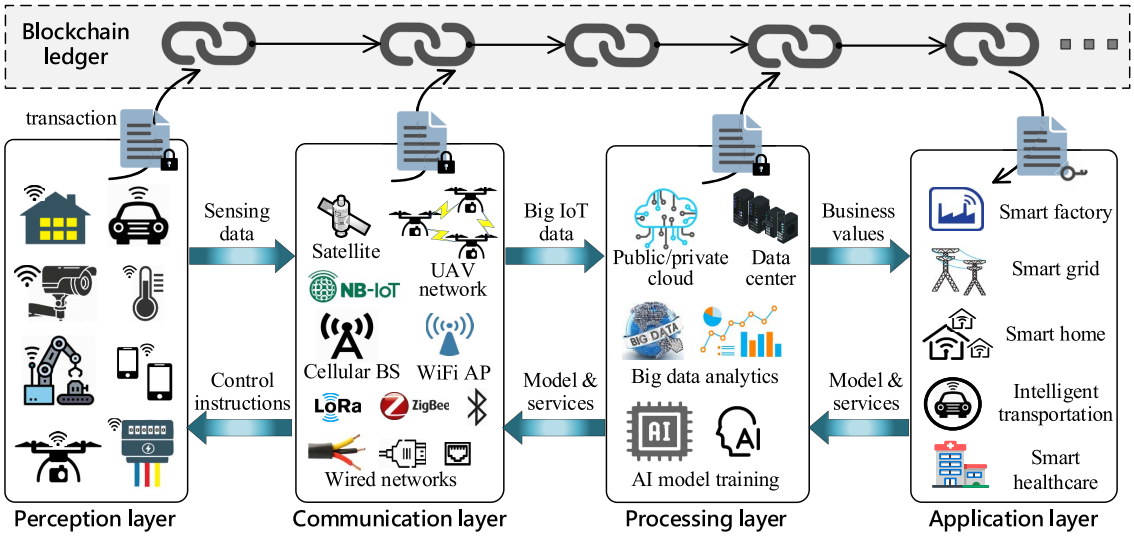


Fig. 3. Overview of blockchain-empowered SAG-IoT systems.

From the perspective of the life-cycle of data services, an SAG-IoT system consists of the perception layer, the communication layer, the cloud computing layer, and the application layer [30]. As shown in Fig. 3, the *perception layer* comprises various devices (e.g., sensors, radio frequency identification (RFID) tags, UAVs, and smart meters) which can gather and process environmental information and then take actions on the environment to bridge the cyber and physical worlds [31]. The *communication layer* is responsible for connecting a variety of wireless/wired devices via satellite communications, UAV networks, Wi-Fi APs, cellular base stations (BSs), etc., to form heterogeneous IoT networks. The network protocols, e.g., ZigBee, Bluetooth low energy (BLE), Wi-Fi, near field communication (NFC), LoRa, Sigfox, and narrowband-IoT (NB-IoT) [32] can be adopted to establish wireless connections depending on the specific scenarios and requirements. The *processing layer* performs feature extraction and knowledge abstraction from a wealth of collected data. It enables model training, smart prediction, and business value realization to support diverse intelligent IoT applications, such as smart factory, smart grid, smart home, smart healthcare, and intelligent transportation in the *application layer*.

Different from the conventional networks, SAG-IoT exhibits unique characteristics in the following aspects.

1) *Heterogeneity:* The heterogeneity of SAG-IoT includes heterogeneous devices (e.g., built on different hardware platforms), heterogeneous networking modes (e.g., satellite network, aerial network, and cellular network), heterogeneous communication protocols, and heterogeneous IoT data types (e.g., structured and unstructured) [30]. Moreover, as SAG-IoT integrates three distinct network segments (i.e., space, air, and ground), it can be seen as a complex multi-segment HetNet [3]. This entails the poor interoperability of SAG-IoT systems from both hardware and software perspectives for security provisioning and the exchange, analysis, and management of data generated by numerous devices [33].
2) *Resource Constraint and Unbalance:* SAG-IoT devices (such as sensors, smart meters, and mini-UAVs) typically suffer from constrained resources including storage space, computing resource, communication capacity, and battery lifetime. As typical security countermeasures (e.g., antivirus software, authentication, and firewalls) require considerable computing power for resource-constrained IoT devices [23], this also gives rise to the security and privacy vulnerability of IoT devices in face of various attacks. Although the on-board computing capacities of IoT devices keep increasing, the

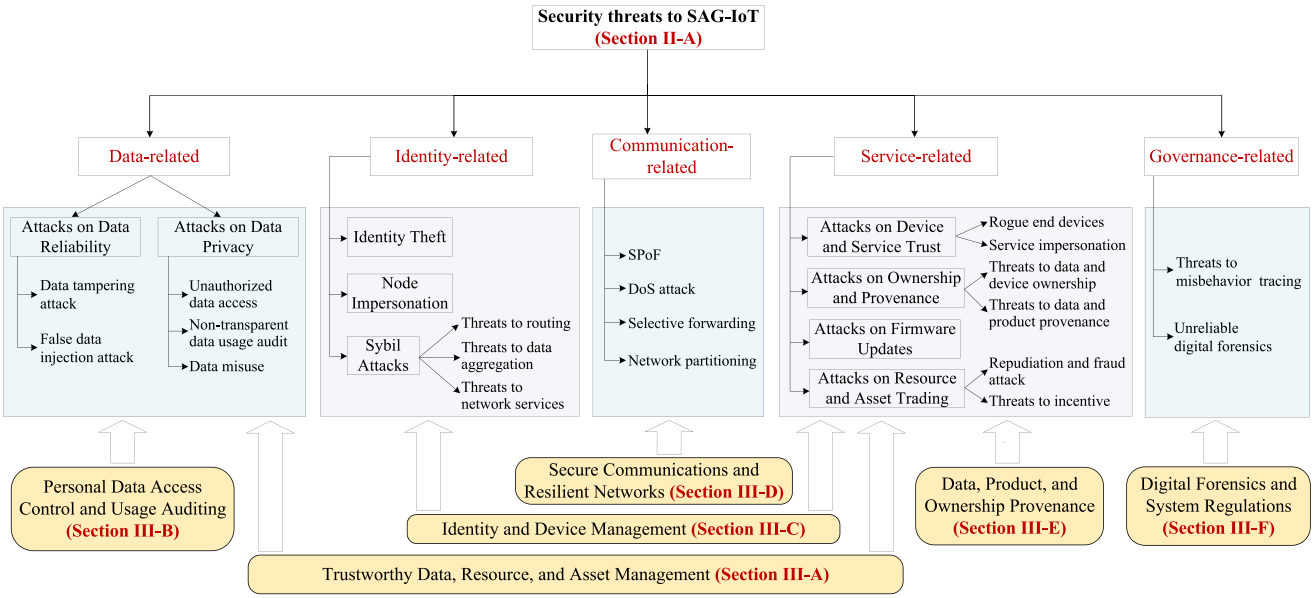


Fig. 4. Security threats towards the SAG-IoT system.

compute-intensive tasks and security provisioning missions may consume a considerable amount of their battery and overextend the response time. Besides, the unbalance resource distribution in SAG-IoT can also cause low resource utilization.

3) *Time-Variability:* In SAG-IoT, the high mobility of satellites, UAVs, and end devices (e.g., vehicles) entails the time-varying dynamic network topology, while the unstable wireless links can lead to intermittent and unpredictable network connectivity. The disconnected network partitions may coexist within an SAG-IoT network and these fragmentations may be time-varying [34].
4) *Self-Organization:* Through self-configuration, self-diagnostication, self-healing, and self-optimization, the devices in SAG-IoT can be self-organized to form MANETs (e.g., VANET and FANET) to enable a series of network functions (e.g., emergency communication, UAV swarm navigation, and radio network (RAN) optimization) in a flexible and on-demand manner.

With the exponential growth of connected devices and IoT data, the intrinsic characteristics of SAG-IoT make security and privacy protection become challenging. Specifically, since IoT devices are usually deployed to perform autonomous data collection, exchange, and processing with minimal human interventions, attackers may intrude and control these devices via physical and cyber interfaces [35]. Meanwhile, data generated by mobile/static sensors can be stored, forwarded, and distributed by different intermediaries, which raises the risks of being tampered with, replaced, forged, and misused [36]. Furthermore, the unreliable and open-accessed wireless channels and insecure softwares can bring extra vulnerabilities to SAG-IoT networks [37]. Typical threats to SAG-IoT networks are summarized from the bottom layer to the top in the life-cycle of IoT services [35], which are classified into the following types: data-related, identity-related, communication-related, service-related, and governance-related, as shown in Fig. 4.

1) Data-Related Threats: The IoT data generated by end devices may suffer from data-related threats in terms of data reliability [22] and data privacy [7] during the procedure of data sensing, transmitting, and processing.

① *Attacks on Data Reliability:* The reliability of sensory data in SAG-IoT applications may be compromised by the following attacks during data transmission.

- *Data Tampering Attack:* During the multi-hop and cross-layer data transmissions in SAG-IoT networks, attackers may alter, falsify, replace, and remove the original sensory data to mislead the normal activities of other entities [38]. Meanwhile, the attackers can also infiltrate the SAG-IoT network, modify the generated source data or the transmitted service data, and then falsify the corresponding log files to cover their traces.
- *False Data Injection Attack:* Adversaries can also inject false data (e.g., forged messages, fake statuses, viruses, and malwares) to misdirect and interfere with the system [39]. Once the false or forged information is accepted, wrong instructions or erroneous services may be returned from the SAG-IoT platform which results in unpredictable losses.

② *Attacks on Data Privacy:* During the sharing and processing process of SAG-IoT big data, the data confidentiality may be violated by the following attacks.

- *Unauthorized Data Access:* The shared sensory data in SAG-IoT often contains sensitive information, and should only be accessible for authorized entities (e.g., designated service providers or insurance agents). Once the data is shared, it is out of the control of the owner and can be illegally accessed by unauthorized parties, causing a high risk of data misuse [6], [40].
- *Non-Transparent Data Usage Audit:* Apart from the restriction on who can access the data with what policy,

the shared data may also be utilized for unintended purposes by authorized entities (e.g., privacy mining on the shared information) [41]. However, conventional cryptographic approaches and role-based access control (RBAC) mechanisms can neither meet performance bottlenecks nor attain fine-grained access control in SAG-IoT context [42].

- *Data Misuse:* The data collected from various devices in SAG-IoT generally contains private and sensitive user information. These data can be leaked intentionally by adversaries or unintentionally by service providers during the transmission and sharing process to facilitate personalized marketing and even illegal activities [12].

2) Identity-Related Threats: Identity management plays a critical role for massive connected devices in SAG-IoT. The following identity-related attacks are encountered.

① *Identity Theft:* A hacker can hack into an SAG-IoT network (e.g., home Wi-Fi network) via a connected end device and then gain access to other devices (e.g., fitness watches and smartphones). Once personal information is stolen by hackers via network intrusions or in-depth data mining, fake identities can be created [43]. With the fake or stolen identities, attackers can impersonate legitimate nodes and inject disrupted and malicious data, known as insider attack [44].

② *Node Impersonation Attack:* An adversary can launch the impersonation attack by masquerading the identity of another legitimate party in the communication protocols or services of SAG-IoT systems. For instance, by exploiting the Bluetooth authentication bug, the Bluetooth impersonation attacks [45] allow adversaries to insert rogue devices into established Bluetooth pairings and impersonate trusted endpoints. Consequently, the sensitive data of victim IoT devices may be captured or leaked.

③ *Sybil Attacks:* In Sybil attacks, an adversary can manipulate fake identities or fabricate multiple pseudonymous identities to gain disproportionately large influence in the network and compromise system effectiveness [46]. More specifically, the adversary can either create multiple real identities associated with a single physical device or generate many virtual identities to interact with his/her real identities, which can result in many threats as follows:

- *Threats to Routing:* An attacker can generate multiple Sybil identities and guide contradicting routing paths that pass through himself/herself to confuse the geographic routing protocols in SAG-IoT [7].
- *Threats to Data Aggregation:* Sybil attackers can generate multiple biased reports to manipulate the collective results in crowdsensing applications (e.g., noise pollution and air quality monitoring) which employ distributed IoT devices to collect data from cyber-physical systems [47].
- *Threats to Network Services:* Sybil attackers can manipulate a series of faked identities to interfere and even abort the normal operations of network services (e.g., voting-based service and reputation service) [20], leading to system paralysis.

3) Communication-Related Threats: Various attacks including SPoF, denial of service (DoS) attacks, selective forwarding, and network partitioning threaten SAG-IoT systems by exploiting the vulnerabilities of network architectures and communication protocols [48], [49].

- *SPoF:* For convenient device management and reduced operation cost, traditional IoT networks are usually built on the cloud-based architecture [26]. On one hand, in face of unpredictable natural disasters (e.g., earthquakes and lightning strikes), it can cause a SPoF. On the other hand, as the IoT data are handled and stored using the centralized cloud infrastructures, the internal personnel of the centralized platform may mine user's sensitive information, and forge, replace, or delete these data in pursuit of monetary profits, known as insider job attack [50].
- *DoS Attack:* An attack can launch the DoS attack to make the network functionality unavailable by overwhelming the centralized server with giant traffic in a short time [25]. Accordingly, authorized SAG-IoT devices may fail to access the requested service in time, and the SAG-IoT network can no longer function as planned. For instance, in a smart home, if the IoT gateway is manipulated by adversaries, each end device in the house connected to the gateway may be the victim and become a member of IoT botnets [8] such as Mirai to launch DoS attacks.
- *Selective Forwarding:* In large-scale SAG-IoT networks, information usually requires multiple hops to reach its destination [5]. To subvert the routing protocol in SAG-IoT, a malicious node can carry out the selective forwarding attack (or called gray hole attack) by intentionally dropping certain packets and forwarding the others [7]. This type of attack is a variant of black hole attacks; in the black hole attack, the adversary node rejects forwarding all incoming packets.
- *Network Partitioning:* In the SAG-IoT network composed of mobile "things" such as satellites, UAVs, and vehicles in different network layers, the connected SAG-IoT network may be divided into multiple subnetworks, where "things" in different subnetworks cannot communicate with each other [36]. For example, nodes A and B are in the same subnetwork, while nodes C and D are located in another. If the switching device between two subnetworks goes down, a network partition occurs. Due to the unavailability of information exchange, existing self-organizing collaborative systems (e.g., VANETs and FANETs) built atop the SAG-IoT will suffer deteriorated service performance [47].

4) Service-Related Threats: During the delivery of network services in SAG-IoT systems, various attacks can threaten the trust and security in device provenance, firmware update, and resource trading.

① *Attacks on Device and Service Trust:* The SAG-IoT networks are vulnerable to insider rogue IoT devices and impersonated IoT services.

- *Rogue End Devices:* Rogue and counterfeit IoT devices [51] may disseminate dishonest, meaningless, and low-quality information to interfere with normal operations of SAG-IoT systems, which can be hardly detected by conventional authentication mechanisms [52].

- *Service Impersonation Attack:* An adversary can launch the service impersonation attack by assuming or posing as the identity of a legitimate service to illegally access resources of that victimized service. By impersonating a legitimate service, the adversary can maliciously use the victimized service's privileges. As the trust is imparted to service credentials once they pass the authentication [53], it is tricky under conventional security mechanisms.

② *Attacks on Ownership and Provenance:* In the life-cycle of IoT services, it is hard to trace the ownership and provenance of data, device, and product [42].

- *Threats to Data and Device Ownership:* Once the owner shares his/her personal data or devices to others, he/she may lose physical control of the shared assets and fail to directly monitor the usage of data and devices in time [40], [54].
- *Threats to Data and Product Provenance:* During the whole life-cycle of IoT services such as sourcing, producing, warehousing, distribution, and sales, adversaries may tamper with the original data or inject false information in any phase [55], as well as replacing the products in any process [56] (e.g., raw materials in manufacturing).

③ *Attacks on Firmware Updates:* To prevent newly discovered bugs or security vulnerabilities in SAG-IoT, the latest firmware patch is required to be downloaded and installed on the end devices for security updates. Due to their limited communication and storage capacities, it is difficult to deliver security firmware updates timely for all the SAG-IoT devices from vendors [23]. Besides, if an SAG-IoT device is hacked due to the failure of firmware updates, the victimized end device can be a springboard to other connected devices in an SAG-IoT network to facilitate subsequent network invasions [8].

④ *Attacks on Resource and Asset Trading:* In SAG-IoT networks, device owners need to frequently trade their available resources (e.g., computing, storage, and energy) or idle assets (e.g., car and park sharing). It is challenging to ensure trustworthy interactions among various distrustful IoT device owners [57], [58].

- *Repudiation and Fraud Attack:* An adversary can repudiate the corresponding transactions of resources and assets and refuse to pay [59]. Besides, a fraudster can sell fake data or products and generate fraudulent payment details to cheat others during resource and asset trading.
- *Threats to Incentive:* IoT devices are assumed to be rational and selfish in the network, and they aim at pursuing the maximum self-interest [60]. The uncooperative behaviors of IoT devices can deteriorate the efficiency of resource allocation, security policy management, and network self-governance.

5) Governance-Related Threats: The efficiency of supervision and governance in SAG-IoT systems may be deteriorated by the following threats in terms of misbehavior tracing and digital forensics.

- *Threats to Misbehavior Tracing:* In large-scale SAG-IoT networks, an adversary may hide the trails of his/her misbehaviors by dynamically changing the anonymous identities to remain undetected. In addition, conventional centralized mechanisms rely on the TTPs for misbehavior association, identification and tracking, and lack of transparency and auditability [61], [62].
- *Unreliable Digital Forensics:* Digital forensics can facilitate the virtual reconstruction of facts in face of cyber crimes and disputes by identifying, extracting, and analyzing valuable evidences [63]. However, the privacy rights of suspects and witnesses may be violated for the success of forensics investigation [64]. Currently, cloud-based architecture is widely adopted in SAG-IoT forensics applications. The auditable evidence identification and extraction for transparent supervision are also challenging in cloud-based SAG-IoT forensics [65].

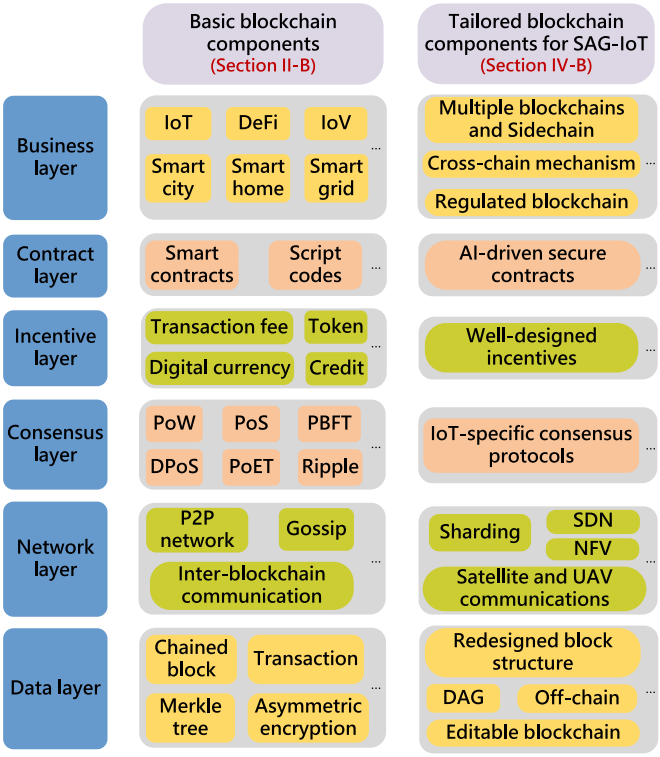


Fig. 5. A general blockchain architecture and the optimizations of blockchain technology in its integration with SAG-IoT.

B. Blockchain Technology

As a promising technique, blockchain holds great potential to address the aforementioned security threats to safeguard SAG-IoT services, which will be detailed in Section III. In the following, we will first review the fundamentals of blockchain technology in terms of architecture, characteristics, types, consensus protocols, smart contracts, and roles of entities.

1) Architecture of Blockchain: As depicted in Fig. 5, a basic blockchain architecture usually includes six layers, namely, data layer, network layer, consensus layer, incentive layer, contract layer, and business layer [20], [23], [24]. The *data layer* locates at the bottom of the blockchain architecture and encapsulates an ordered list of data blocks. Each block contains multiple time-stamped transactions and a hash of the previous block to link its prior block, resulting in a "chained" block

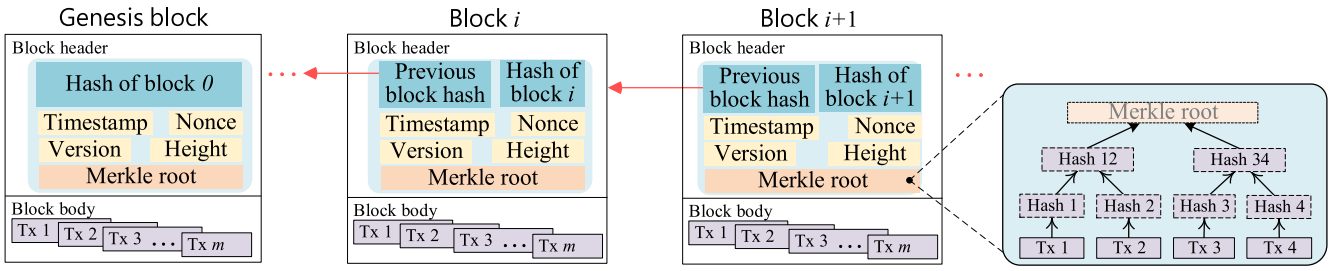


Fig. 6. A typical block structure.

structure [9]. In a typical blockchain structure, as shown in Fig. 6, each block is composed of two parts, namely, the block header and the block body. A list of transactions are ordered by their timestamps and recorded in the block body, where the hash values of transactions are commonly compressed into a Merkle tree (a kind of hash binary tree) for efficient transaction verification in terms of rapidly checking the existence and integrity of transactions. The block header, also known as the metadata of block, mainly includes the version number to track protocol updates, the previous block hash, the block size, the timestamp, the Merkle root (i.e., the root of a Merkle tree), and the block height.

The *network layer* is to disseminate, forward, and verify the transactions across the network. Generally, the peer-to-peer (P2P) network is used to model the topology of the blockchain network, where peer nodes are equally privileged. Once a transaction is issued, it is propagated or gossiped to all neighboring peers. Upon receiving the transactions, each node validates them based on predefined specifications and forwards them to other nodes if verification passes. The invalid transactions will be discarded. Thereby, in the blockchain network, only valid transactions are stored by each node in its memory pool. The *consensus layer* is to ensure the consistency of blockchain ledgers agreed by all participating entities without any central authorities via the consensus protocols. The detailed description is elaborated in Section II-B4. By integrating the economic incentives into the blockchain, the *incentive layer* works as a benign impetus to stimulate the nodes to contribute their efforts to validate block data and reach consensus. Specifically, during the new block generation and consensus procedure, the corresponding nodes can be rewarded with economic gains (e.g., digital currencies and tokens) based on their contributions. The *contract layer* brings programmability into blockchain and enables more complex and automated transactions via smart contracts and various scripts. The detailed description is elaborated in Section II-B5. The *business layer*, which locates at the top of the blockchain architecture, offers a variety of business services and applications for blockchain ecosystems such as decentralized finance (DeFi), IoT, and smart city.

2) Characteristics: The special data structure, intrinsic economic incentives, together with exquisite cryptography and distributed consensus, provide the following prominent features of blockchain systems.

- *Decentralization:* In the blockchain network, the transactions of digital assets can be done in a secure and decentralized fashion, without the jurisdiction and authentication offered by the central agency (e.g., TTP). Therefore, the service cost can be reduced, and the performance bottlenecks as well as SPoF risks can be mitigated.
- *Immutability:* Due to the special hash-chained data structures of blockchain, any modification on one of the blocks invalidates all the consequent blocks. Furthermore, each committed transaction needs to be validated and confirmed by other nodes, thereby the data recorded in blockchain is nearly immutable.
- *Traceability:* The blockchain inherently offers traceability with the trusted information (e.g., immutable audit trails) via collecting, sharing, and transmitting the authentic data during the whole life-cycle of IoT services, e.g., sourcing, producing, warehousing, distribution, and sales.
- *Transparency:* The data of ledgers (i.e., committed transactions and global states) can be accessed and publicly verifiable by any participating entity in the blockchain network, which brings transparency to end-users.
- *Pseudo-anonymity:* In permissionless blockchain networks, each node can be identified by a publicly anonymous address (e.g., the public key) while keeping its real-world identity hidden. Nevertheless, the naive public blockchains can only acquire pseudonymity, instead of the full anonymity [66] such as the linkability of previously used blockchain addresses.

3) Types of Blockchain: Typically, blockchain systems can be classified into three types, namely, public blockchain, consortium blockchain, and private blockchain [23], [26]. Public blockchains are termed permissionless and can be publicly accessed by any node over the Internet, while consortium or private blockchains are permissioned ones and are restricted to a certain group of registered entities in the network [21]. A detailed comparison of these three blockchain types is shown in Table V.

- *Public blockchain:* The public blockchain is fully decentralized, where all its members can publicly access blockchain data and engage in validating new blocks. The identity of each node in public blockchains may remain anonymous. As a processing fee is attached to every transaction to be added to the blockchain, it can incentivize nodes to jointly maintain the blockchain data and statuses, thereby strengthening the security of public blockchain in defending against data tampering.

TABLE V
COMPARISON OF PUBLIC, PRIVATE, AND CONSORTIUM BLOCKCHAINS

	Public blockchain	Private blockchain	Consortium blockchain
Permission	Permissionless	Permissioned	Permissioned
Identity	Pseudo-anonymity	Approved parties	Approved parties
Decentralization	Fully decentralized	Centralized	Partially decentralized
Immutability	Immutable	Partially immutable	Partially immutable
Transparency	Transparent	Opaque	Partially transparent
Scalability	Poor	Superior	Good

- *Consortium blockchain:* In contrast to public blockchains, in consortium blockchains or called federated blockchains, the write access to blockchain is restricted to multiple organizations, where the identity registration and entity enrollment process is needed for all involved parties. Consortium blockchains, in essence, do not depend on tokens or coins as there exist no transaction fees for each transaction. The consortium blockchain is usually leveraged as a distributed and auditable database where the data exchanges between consortium members can be immutably traced [26].
- *Private blockchain:* In private blockchains, the read and write accesses of blockchain are controlled by an organization and only a group of approved individuals can participate. Similar to consortium blockchains, the identity of users is required before joining the private blockchain network and there are no transaction fees for transactions. The private blockchain is suited to perform a synchronized distributed database that tracks data exchanges between different departments or individuals in a single enterprise. As only delegated nodes can publish blocks in the network, private blockchains are not essentially as immutable as public blockchains, thereby the organization can roll back the blockchain to any past point or status.

4) Consensus Protocols: In the blockchain, it is essential to ensure the ledgers agreed by all participating entities are identical and consistent since there are no central authorities. How to reach consensus among various distrustful parties is a typical Byzantine generals problem [21]. The consensus protocol is the core function of blockchain-based SAG-IoT systems to determine its performance in terms of block time, security, scalability, and consistency. A consensus protocol in the blockchain should contain the following key components.

- *Block proposal:* Producing blocks attached with proofs. The producer of a block can be selected via mining competition, stake-based election, round-robin manner, etc.
- *Block propagation:* Disseminating generated blocks across the network through protocols like Gossip [67] and Graphene.[1]
- *Block audit:* Validating block proposals. Each consensus node independently verifies the correctness of the received block proposal. For instance, checking the nonce, signature, and Merkle root within the received block.
- *Synchronization:* Reaching agreement on the acceptance of audited blocks. In the longest-chain rule, the longest branch of blockchain is adopted as the legitimate one. In GHOST (greedy heaviest-observed sub-tree) rule [68], it weighs all branches and miners can select the better one to follow.
- *Incentives:* Promoting honest participation and distributing digital coins or virtual tokens (e.g., block rewards, transaction fees, and reputation credits).

Existing common approaches to reach consensus in blockchain are mainly divided into the following types.

- *Proof of work (PoW):* PoW produces problems which are hard to solve but easy to be verified by using hash functions [69]. In PoW, miners (i.e., consensus nodes) compete to solve a cryptographic puzzle via hash operations. The miner who first addresses a hash puzzle becomes the block manager and gains the right to "write" the next block data to the blockchain.
- *Proof of X (PoX) series:* In PoX, the probability of a node to earn the accounting right is related to its possession of a certain resource. Here, the resource should be valuable and is hard to monopolize, and its possession can be quickly verified. Proof of stake (PoS) is a popular alternative, in which peers need to prove the ownership of the number of coins during block generation. A variant of PoS is the delegated PoS (DPoS), where delegates are elected by voting to allow fast transaction confirmation. Other PoX approaches include proof of authority (PoA) [70], proof of elapsed time (PoET) [71], proof of burn (PoB),[2] proof of importance (PoI),[3] Proof of space (PoSpace) [72], etc.
- *Byzantine fault tolerance (BFT) series:* Practical BFT (PBFT) is a typical voting-based BFT mechanism, which yields the communication overhead of $O(n^2)$ among n peers [73]. Federated Byzantine agreement (FBA) [74] is another form of BFT algorithms, where each participant decides whom to trust and builds its own quorum slice for reaching consensus. Notable cryptocurrencies using FBA include Ripple and Stellar [74]. Other variants include delegated BFT (dBFT) [75], specular BFT (SBFT) [76], HoneyBadgerBFT [77], etc.

More details of consensus protocols in blockchain systems can refer to the survey [21]. The comparison of existing representative consensus mechanisms is summarized in Table VI. In general, PoW-based consensus mechanisms are simple to implement and secure under a majority honest assumption. Nevertheless, the required computing-intensive block mining tasks of PoW mechanisms prohibit their potentials for

[1]http://forensics.cs.umass.edu/graphene/graphene-short.pdf

[2]https://getmonero.org

[3]https://docs.nem.io/ja/gen-info/what-is-poi

TABLE VI
COMPARISON OF TYPICAL CONSENSUS MECHANISMS

Name	Throughput	Scalability	Finality	Tolerated Power of Adversary	Pros	Cons	Vulnerability	Implementations
PoW	Low	Low	Probabilistic	$< 51\%$ computing power	Fair voting, Free to join	Energy waste	Selfish mining [78]	Bitcoin, Ethereum
PoS	Low	Low	Probabilistic	$< 51\%$ stake	Energy efficient	Matthew effect	Long range attack [19], Nothing-at-stake [19]	Ethereum, Peercoin
DPoS	Medium	Medium	Probabilistic	$< 51\%$ faulty validators	Democratic, Fast consensus validation	Matthew effect, Risk of centralization	DDoS attack	BitShares, EOS
PoA [70]	Medium	Medium	Probabilistic	$< 50\%$ identity stake	Energy efficient	Trust requirement, Risk of centralization	SPoF attack	Decred
PoET [71]	Medium	Low	Probabilistic	$< \Theta(\frac{\log \log n}{\log n})$ faulty nodes [71]	Energy efficient	Reliance on Intel, Hardware requirement	Trust on Intel	Sawtooth
PoB	Medium	Low	Probabilistic	$< 51\%$ coins	Long-term incentive	Low throughput	Denial-of-spending [79]	XCP
PoI	Medium	Low	Probabilistic	$< 51\%$ stake	Less chance of hoarding	Trust requirement	SPoF attack	NEM
PoSpace [72]	Medium	Low	Probabilistic	$< 51\%$ storage space	Energy efficient	Low throughput	Waste disk space	IPFS
PBFT [73]	High	Medium	Deterministic	$< 1/3$ faulty nodes	Energy efficient, Fast block finality	High communication overhead	33% attack	Hyperledger
dBFT [75]	High	Medium	Deterministic	$< 1/3$ Byzantine voting power	High throughput	Need tokens	Collusion attack, Risk of centralization	NEO
Ripple	High	High	Deterministic	$< 21\%$ faulty nodes	Fast block finality	Trust requirement	SPoF attack	Ripple
Stellar [74]	High	High	Deterministic	$< 1/3$ faulty quorum slices	Low latency, Flexible trust	Need enough quorum slices	Network fragmentation attack	Stellar
Tangle [80]	High	High	Probabilistic	$< 1/3$ computing power	High throughput, Non-mining	Communication overhead	Sybil attack, Shadow chain attack	IOTA

resource-constrained IoT devices. Compared with PoW, PoX-based consensus mechanisms are able to alleviate the energy consumption in block mining significantly and thereby offer a chance for IoT devices to participate in blockchain maintenance. However, the block time and the confirmation speed of transactions are still limited to satisfy the quality of service (QoS) requirements in SAG-IoT. Besides, a trade-off among security, decentralization, network accessibility, and efficiency needs to be achieved in developing PoX consensus protocols. BFT-based consensus mechanisms are widely adopted in permissioned blockchains and can offer a high block generation rate for SAG-IoT systems. However, they also bring constraints on the number of participating entities in the network [81], thereby posing severe concerns regarding the network scalability. Besides, nodes in most BFT-based blockchain systems cannot dynamically join or exit. Apart from the consensus mechanisms, the throughput and scalability of blockchain-based SAG-IoT applications also depend on the specific running environment and network configurations (e.g., block size, network bandwidth, and communication speed).

5) Smart Contract: A smart contract refers to a set of digital commitments among anonymous parties that can be automatically enforced in a prescribed fashion [82]. Smart contracts are resided on blockchain and implemented on top of the blockchain. The execution of each smart contract is recorded as transactions [23]. The functions of smart contracts can be defined beyond the range of cryptocurrencies and extended to general digital assets (e.g., the digital key of a car) and the business logic of services. All blockchain platforms have built-in mechanisms for deploying smart contracts from simple stack-based scripting systems like Bitcoin to Turing-complete systems like Ethereum and Hyperledger [83]. The whole procedure of the smart contract contains the following four steps. ① *Creation:* After multiple involved parties (e.g., stakeholders, software engineers, and lawyers) reach an agreement on the contractual clauses, the smart contract is created which is written in executable computer codes and assigned with appropriate access permission and contract enforcement [84]. ② *Deployment:* Any changes need the creation of a new contract. Once the smart contract is deployed after mutual validation, it is accessible to all the consensus nodes on the blockchain, while the digital wallets of involved entities are locked and frozen [82]. ③ *Execution:* Once the contractual conditions reach, the corresponding functions will be automatically executed in a deterministic manner. The execution of smart contracts is recorded as verifiable transactions and stored on the blockchain. ④ *Completion:* All committed transactions and updated states (e.g., balances of all involved parties) are recorded in the blockchain thereafter, and then the smart contract completes. More details of smart contracts can refer to the surveys [22], [26].

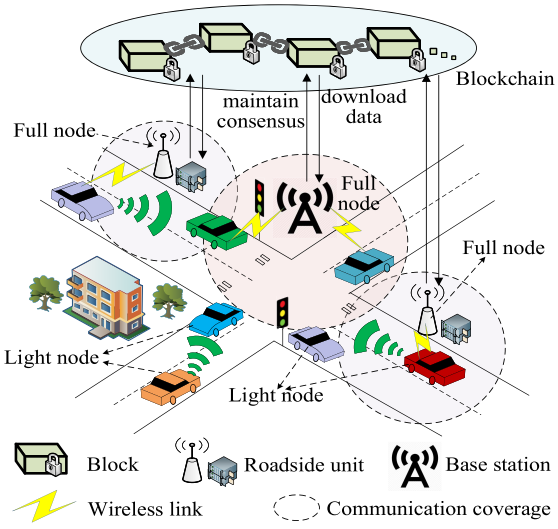


Fig. 7. An example of the implementation of blockchain system in IoV.

6) Role of Entities: Fig. 7 shows an example of the blockchain-IoT system in a typical Internet of Vehicles (IoV)

scenario, where nodes in the blockchain network can serve as different kinds of roles according to their resource capacities. In general, there exist two kinds of nodes in blockchain-IoT systems [38], [85], [86], i.e., *full nodes* and *light nodes*. Full nodes (e.g., BSs and roadside units (RSUs)) store a copy of the full blockchain and can participate in the block creation, transaction verification, and ledger management [36]. It requires massive storage and a certain level of computation power to become a full node [85]. Part of full nodes can be the consensus nodes (or called miners in the PoW-based blockchain), which maintain the consensus process and data correctness of blockchain [60]. As shown in Fig. 7, the IoT devices (e.g., vehicles) can run as light nodes which only store the block metadata and do not require high hardware specifications [86]. Light nodes can generate transactions but cannot join in the consensus process (e.g., mine blocks) [38], and they can obtain the blockchain data from full nodes. Simplified payment verification (SPV) [87] and wallet [88] technologies are supported for light nodes.

III. Blockchain Solutions for SAG-IoT Security

SAG-IoT networks are data-centric and SAG-IoT applications are data-driven, where massive data are generated by numerous end devices and processed to power diverse applications. As illustrated in Fig. 3, the blockchain is promised to enrich the SAG-IoT paradigm by providing a trusted shared ledger and decentralized computing capacities for secure perception, networking, communication, monetization, and data analysis, where the recorded cryptographic information (e.g., hash value and signature) of device information, sensory data, processed data, and digital asset transactions can be traceable, reliable, immutable, and undeniable [25]. As illustrated in Fig. 4, blockchain technologies are anticipated to play a major role in managing and securing SAG-IoT services from the following aspects to defend against the security threats in the aspects of data, identity, communication, service, and governance, as defined in Section II-A.

A. Trustworthy Data, Resource, and Asset Management

Trust is one of the key features brought by blockchain [20]. On one hand, the trust of delivered data can be guaranteed since all participants have a copy of the global blockchain and can verify the correctness through hash validation-comparison functions and block synchronization rules (e.g., longest-chain and GHOST). On the other hand, in blockchain-empowered SAG-IoT systems, the special hash-linked blocks and tree-structured transactions in each block provide tamper-resistance of recorded SAG-IoT data in blockchain ledgers. Therefore, the blockchain technology can build cross-border trust among distrustful entities during the entire processes of data sensing, sharing, processing, storage, and destruction. Besides, the trust-free SAG-IoT services and applications instantiated by smart contracts (e.g., resource and asset trading) can be constructed atop the blockchain in an automatic fashion.

1) For SAGINs: Generally, blockchain-based large-scale applications may suffer from an intolerable delay in sequential transaction verification and incur massive storage spaces in storing the whole blockchain data in each node. Meanwhile, each segment (i.e., space, air, and ground subnetworks) in SAGINs has diverse QoS requirements. To mitigate this issue, Sun *et al.* [10] propose a multiple blockchain architecture in SAGINs for secure and efficient resource management in different network segments, where every segment of SAGIN maintains a specially designed blockchain (namely, ground chain, air chain, and space chain) and the relay chain method is employed for necessary cross-segment collaboration. The system architecture is shown in Fig. 8. Specifically, to alleviate the computation burden in satellite subnetworks, BFT consensus protocol is employed in the space chain, where capable satellites act as full nodes that store a complete copy of the space chain. To compensate the limited capacity, high mobility, and unstable links in air subnetworks, the BFT consensus protocol is also exploited in the air chain, where part of ground stations and capable aircrafts serve as full nodes to maintain blockchain security and offer blockchain access services in their coverage. To accommodate the high throughput requirements in ground subnetworks, the DPoS consensus protocol is leveraged in the ground chain. In general, BFT consensus protocols are computation-efficient but yield high communication overhead, while DPoS consensus protocols enjoy high throughput but involve higher amount of computation. As such, the efficiency and scalability of large-scale SAGINs can be improved by running multiple parallel blockchains.

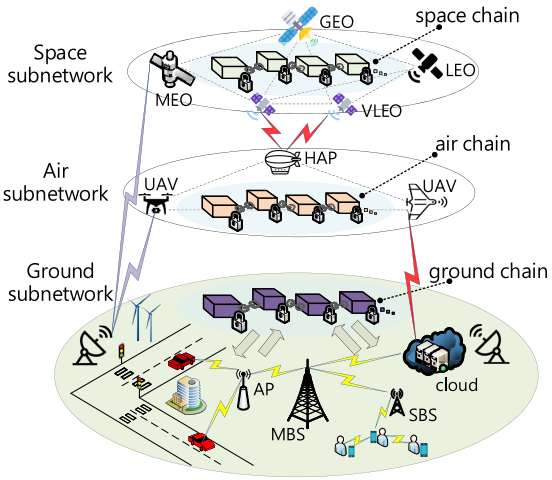


Fig. 8. The multiple blockchain architecture in SAGINs in [10].

For efficient inter-segment resource allocation in the multiple blockchain architecture, a reverse auction game is also designed in [10] between the relay chain (i.e., resource manager) and users (i.e., resource requesters) in SAGINs, where users (i.e., bidders) submit the bidding information including resource request and reserve price to the relay chain (i.e., the auctioneer). Then, the relay chain selects the winners and their payments to optimize the system efficiency. In such a manner, nodes' participation and cooperation can be encouraged across different segments with minimum cost. However, the proposed architecture in [10] brings cross-chain security issues as the entire system security relies on the parallel chain with the lowest security.

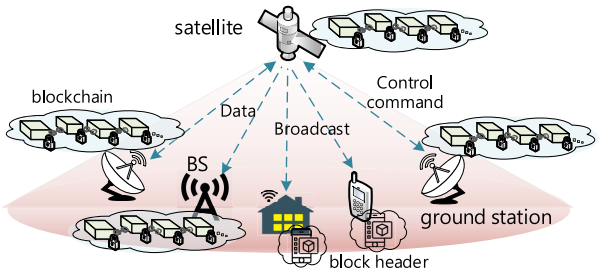


Fig. 9. A typical example of blockchain implementation in satellite-terrestrial networks.

2) For Space-Ground Integrated Networks: Satellite-terrestrial networks enable wide coverage and seamless network access for ground devices and users, which have been widely used in navigation, positioning, and emergency assistance. Data reliability and fairness are two critical issues that hinder the improvement of user QoE in satellite-terrestrial networks. To ensure the trusted transmission of massive data in satellite-terrestrial systems, as shown in Fig. 9, Fu *et al.* [89] investigate a blockchain-based framework to ensure both data security and throughput fairness. In their framework, there exist three main entities: LEO satellites, ground stations, and ground data-gathering devices. The LEO satellites periodically collect traffic information from ground stations. In their implementation of the blockchain system, traffic data is first accumulated as a data block, then each ground station continually computes the hash value of the data block and a random nonce, and finally the specific block is delivered to LEO satellites and added to the blockchain after mutual verification. For joint caching, computing, and communication (3C) resource management, a Nash bargaining game-based optimization model is also developed by authors to ensure fairness and data security in the system, as the Nash bargaining game can enforce a unique fair Pareto optimal solution. And the Pareto optimal solution including 3C power allocation and serving period of satellites is derived by using dual decomposition methods.

However, the proposed framework in [89] has a drawback of the efficiency of the blockchain system, especially for large-scale satellite-terrestrial applications with massive number of devices. To partially circumvent this drawback, Wei *et al.* [90] propose to coordinate the node behaviors in different network segments. In particular, the authors design a blockchain platform in satellite-terrestrial IoT networks with reduced block propagation latency and enhanced communication efficiency. In their approach, one satellite node and three kinds of nodes (i.e., supernodes, ordinary nodes, and gateways) are considered. The supernode can only receive data from the satellite while ordinary nodes can neither send nor receive data with the satellite. As satellite communications are more expensive than ground ones, only the gateways can communicate with the satellite. Simulation results in [90] demonstrate that, under 20% supernodes and 9 Mbit block size, the throughput measured by transaction per second (TPS) in the proposed scheme is about 2.4 times higher than that in the baseline scheme.

Different from [90], Carter *et al.* [91] propose to integrate fog-cloud computing techniques into space information networks to improve system efficiency. Two typical scenarios, i.e., data encryption and key management are investigated by the authors, as well as potential risks, in the practical deployments. Another critical issue in satellite networks is the trusted and reliable positional data for space object location and collision avoidance. To resolve the relevant data integrity and security issues, based on the Ethereum blockchain, Molesky *et al.* [92] study the trusted data sharing via on-orbit satellite communications to facilitate the exchange of positions and velocities in space. Two modes of operation are considered in their work: full-history and sliding window. The Earth observation and communication centers (EOCCs) operate at the former mode and store the entire history of blockchain, while part of satellites can run in the latter mode by only storing the latest 48 hours of the blockchain data due to resource constraints. As such, by tracking the recorded position, momentum data, and other space debris of satellites in the blockchain ledgers, the collisions can be detected and prevented in advance by EOCCs.

3) For Space-Air Integrated Networks: As UAVs and LEOs are susceptible to external hijacking attacks, Pokhrel [93] present a secure blockchain-enabled architecture among a constellation of LEO satellites and a swarm of UAVs for trustworthy data management and cooperative resource allocation. Under this architecture, owing to the satellite handovers, potential channel impairments, and time-varying wireless network parameters, miners in the blockchain may fail to propagate data in time or be compromised, which may result in undesirable forking events. The authors further develop a novel method for efficient prediction of regular forking occurrence and the quantification of forking impacts. Furthermore, by considering the mobility of LEOs and UAVs, an energy consumption minimization algorithm, as well as a double Q-learning-based resource sharing mechanism is developed for miners in the blockchain. Simulation results show that the proposed scheme enjoys higher overall utility and faster convergence rate than conventional approaches.

4) For Air-Ground Integrated Networks: In air-ground integrated networks (AGINs), the aircrafts such as UAVs can be employed to perform various tasks such as crowd surveillance, traffic monitoring, and disaster rescue. As illustrated in Fig. 10, the main functions that UAVs can play in AGINs are listed as below [94].

- *Aerial data collector:* UAVs equipped with a wealth of advanced sensors can be dispatched for immediate information collection. For example, a swarm of UAVs can collaboratively create 3D maps of disaster sites to assist rescue efforts. Moreover, UAVs can act as data hubs in the sky to collect and aggregate the data generated from ground IoT devices in their flight cruises [95].
- *Mobile relay:* UAVs can serve as the aerial mobile relays for data transmission when the direct communication link between the ground data transmitter and ground data receiver is unavailable [96].
- *Aerial BS:* A UAV that connects to the satellites can serve as an aerial BS to provide on-demand emergency

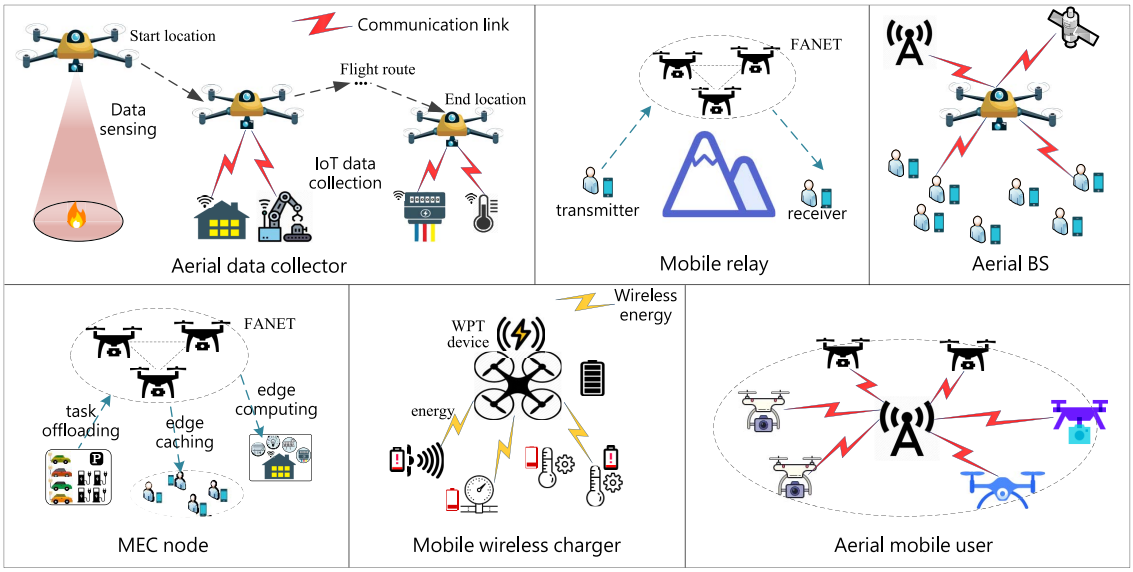


Fig. 10. Typical use cases of UAVs in air-ground integrated networks.

communication services for users or devices in its coverage in environmental harsh areas such as disasters. Moreover, in hotspot areas, cellular-connected UAVs can be deployed as temporary aerial BSs can improve the network capacity to accommodate the surge of data traffic [57].

- *Mobile edge computing (MEC) node:* A swarm of UAVs can be employed as the aerial MEC platform to assist data computing, task offloading, and edge caching for ground users and IoT devices [97].
- *Mobile wireless charger:* UAVs equipped with wireless power transfer (WPT) devices can be employed to charge a group of outdoor battery-powered IoT devices along their flight routes [98].
- *Aerial mobile user:* UAVs can also act as mobile users in the air to receive data services (e.g., computing, communication, and caching) from cellular networks, ground MEC nodes, and cloud servers [99].

In UAV-aided IoT applications, due to the open-access networking, IoT devices may be vulnerable to external invasions. Islam and Shin [96] investigate a permissioned blockchain-based approach for secure data acquisition and delivery in UAV-aided IoT, where the integrity and security of sensed and delivered information can be ensured by the hash-chained structure of blockchain. In their work, the UAVs act as communication relays to transmit the gathered IoT data to the MEC servers which maintain the blockchain. The security analysis proves the data tampering resistance of the proposed scheme. However, their work does not support the multi-UAV scenario and the mobility analysis of UAVs is absent. Meanwhile, in practical deployment, the limited battery energy of UAVs can cause a constrained lifetime of network access.

As an effort to address this issue, Xu *et al.* [95] propose a multi-UAV-aided secure and energy-efficient data collection framework for ground IoT devices based on blockchain technology. In their framework, via regular cruises, UAVs perform the data collection at the edge of the network and offer network access for IoT devices. Meanwhile, the distributed ledgers in blockchain are maintained by the UAV swarm to resist external invaders. Furthermore, the authors utilize the virtual currency to reward the honest UAVs and present an adaptive linear prediction mechanism to alleviate the energy consumption in wireless transmissions by sending prediction models instead of the raw data. In the simulation, the root mean square error (RMSE) of all collected values is employed to evaluate the data accuracy, and the energy efficiency is measured by the average energy consumption of UAV in data sensing, flying, data transmission, and PoW mining. Simulation results show that the proposed framework results in higher data accuracy and energy efficiency in data collection, compared to conventional algorithms. However, in [95], the used PoW algorithm for blockchain management can be resource-hungry for battery-limited UAVs while the optimal rewarding mechanism under dynamic scenarios is absent.

To address the challenge in [95] under general blockchain-as-a-service (BaaS), Asheralieva Niyato [97] present a BaaS platform which is compatible to current dominated consensus protocols in AGIN. In this BaaS platform, the peer nodes in the blockchain collect data from IoT devices, and the blockchain tasks are executed in the cloud server. The UAVs act as the aerial BSs to assist the terrestrial BSs to forward the task data to the cloud server. In [97], the resource management problem for BSs is modeled as a stochastic Stackelberg game among BSs and peers under incomplete information. Moreover, a hierarchical learning-based algorithm is devised, which consists of the Bayesian deep learning for peers and the deep Q-learning for BSs. Simulation results show that the higher number of peers, the longer convergence time, the higher average payoff of the peer, and the smaller average payoff of the BS in the highly dynamic AGIN.

Different from [97], Xu *et al.* [99] propose to combine edge computing for efficient PoW mining task offloading for UAVs. In their framework, UAVs can receive convenient edge computing resources from ground edge computing

servers (ECSs) for data processing and blockchain maintenance. Moreover, the authors develop an efficient resource trading mechanism for UAVs and ground ECSs by integrating the game-based algorithm into the blockchain framework, where the Stackelberg game is employed to obtain players' optimal resource pricing and demand strategies and the entire trading process is recorded in blockchain ledgers with security and privacy guarantees. Simulation results in [99] show the convergence of each player's strategy and the existence of Stackelberg equilibrium in the proposed game approach.

Apart from the aforementioned works in securing data or computing resource sharing in AGINs, Qiu *et al.* [57] and Jiang *et al.* [98] employ blockchain technologies to safeguard spectrum trading and WPT process between UAVs and ground devices. Specifically, the authors in [57] design a novel spectrum blockchain scheme to secure spectrum allocation between the aerial and terrestrial IoT networks, where drones can rent spectrum resources from the primary mobile network operator via Stackelberg game-based pricing approaches. By running consensus protocols independently in various consensus nodes, invalid transactions (e.g., double-spending) can be detected to prevent fraud. Moreover, to enhance the security of UAV-assisted WPT under untrusted wireless environments, the authors in [98] present a hybrid blockchain framework consisting of a directed acyclic graph (DAG) and a consortium blockchain to efficiently charge low-battery aerial/ground IoT devices. In their work, the DAG is deployed in the aerial network to verify the large number of energy micro-transactions and the ground main chain utilizes the consortium blockchain to confirm the timeout of micro-transactions. However, due to the high mobility of UAVs, part of UAVs may be offline in generating and receiving the micro-transactions, causing the security issues of blockchain in synchronization of the entail blockchain network.

5) For Ground IoT Networks: In the blockchain, data are organized into a growing list of hash-chained blocks which have been time-stamped and verified by a majority of consensus nodes via consensus operations. Empowered by the blockchain technology, the security of IoT-related data can be protected in the form of transactions and is featured with traceability, transparency, non-tampering, and non-repudiation.

To facilitate trusted data sharing among neighboring vehicles on road, Chen *et al.* [100] develop a permissioned blockchain system in the IoV. In the proposed blockchain system, local aggregators such as RSUs perform as edge computing nodes and execute transaction audits, PoW mining, and ledger maintenance in the blockchain; meanwhile, moving vehicles are no-mining nodes and are classified into data sellers and data buyers in the data trading market. As selfish vehicles may bid untruthfully (e.g., bid a higher price larger than its data cost) in the market, the authors also develop a truthful double auction model to encourage vehicles' truthful participation, maximize social welfare (i.e., the overall payoff of all seller vehicles and buyer vehicles), and improve data trading efficiency. Findings from the simulations show that the proposed scheme can quickly search the optimal auction solutions (i.e., with low running time) and acquire the maximum social welfare.

However, in [100], the proposed scheme directly utilizes the PoW consensus algorithm for block mining, which may suffer long block time (i.e., block generation interval), especially for vehicles with high mobility. To mitigate the above issue, Wang *et al.* [38] propose reputation-based PoW consensus mechanisms for autonomous vehicular networks, where the difficulty target of PoW mining can be dynamically adjusted based on the reputation of RSUs. Via tamper-resistant ledgers, the security of information sensing, dissemination, and storage of vehicles can be ensured. Furthermore, two reputation algorithms are separately devised atop the blockchain system for RSUs and moving vehicles to motivate their legitimate behaviors. The reputation of RSUs is evaluated based on their behaviors recorded in the blockchain, while the reputation of vehicles is evaluated based on the overall quality of their completed tasks. In the simulation, the secure delivery ratio (i.e., ratio of successfully delivered secure and true data to the total delivered data in the system) is employed to measure the content dependability. Simulation results show that the proposed scheme outperforms the conventional cryptographic scheme in attaining improved content dependability.

Different from [38], Li *et al.* [101] propose to employ the BFT-DPoS consensus protocol to improve the consensus efficiency of blockchain system. In their proposed scheme, blockchain is leveraged as a tamper-resistant ledger to share GPS positioning error evolutions between common vehicles and sensor-rich vehicles in a cooperative manner, aiming to reduce GPS positioning error on road. Compared with the naive DPoS protocol, in the BFT-DPoS consensus protocol, after a validator proposes a new block, other validators run the BFT-based voting process to reach consensus instead of building their own blocks simultaneously. Furthermore, in [101], edge servers run the BFT-DPoS consensus protocol for blockchain management, and deep neural network (DNN)-based prediction algorithms are proposed to predict vehicles' positioning errors. Simulation results show that the block time in their scheme can be reduced to 0.5s and the block confirmation speed can increase significantly.

Different from the above works in [38], [100], [101], Liu *et al.* [102] exploit blockchain technologies to secure industrial IoT. Specifically, by leveraging blockchain, the authors in [102] propose a secure data sharing mechanism in the industrial IoT environment to prevent potential device and communication failures during data exchange among industrial IoT devices. The Ethereum platform is utilized to guarantee data reliability for industrial IoT devices by publicly sharing a tamper-proof ledger among them. Besides, to ensure high-quality data collection and geographic fairness of industrial IoT devices with limited energy and sensing capacities, deep reinforcement learning (DRL) techniques are incorporated in blockchain-based crowdsourcing systems to suppress their selfishness. However, their proposed blockchain-IoT systems heavily depend on network infrastructures for resource-intensive blockchain storage and consensus maintenance tasks, and they may not be applicable in infrastructure-free scenarios.

Meanwhile, blockchain can build trust among various distrustful entities in SAG-IoT during network resource management regarding spectrum [103]–[105], computing [84], [106],

caching [107], [108], and energy [60], [109]–[111]. In static spectrum allocation approaches, as the allocated spectrum of license holders, i.e., primary users (PUs), are not continuously and fully utilized, causing a waste of the scarce spectrum resource. The introduction of secondary users (SUs) to reuse the idle spectrum by monitoring the spectrum resource has been widely regarded as a solution to the spectrum scarcity problem [103], [112]. However, the high administrative expenses and the trust and security concerns impede the efficient deployment of such spectrum sharing schemes. As pointed by the federal communications commission (FCC), blockchain holds great potentials to cut administrative expenses of dynamic spectrum monitoring for improved spectrum efficiency. For example, Zhu *et al.* [104] propose a blockchain-based auction framework to address intelligent spectrum sensing and secure sharing in mobile networks. In their framework, a group of BSs run the PBFT consensus protocol to jointly maintain the consortium blockchain which stores the spectrum auction results (i.e., winners and payments). In the proposed auction mechanism, PUs act as bidders which compete to purchase the required spectrum from the BSs, while each SU selects the most preferred PU for association to maximize its utility. Simulation results demonstrate that the proposed auction is able to increase the utility of SUs (i.e., the benefits minuses the cost in spectrum trading) by 141.5% and increase the throughput (in Mbps) by 189.3%.

Different from [104], Xue *et al.* [105] propose a new consensus mechanism for performance improvement in blockchain-based spectrum trading with quick confirm time and concise code implementation. Particularly, by adaptively dividing the whole network into several intersecting parts based on the spectrum ownership, the system scalability can be improved and the message complexity can be lowered. Moreover, by exploiting the temporary anonymous transaction methods, the spectrum holder can be anonymized during its usage, while the identity verifiability is guaranteed to ensure the legality of transactions. By using the Omnetpp simulation, the results show that the spectrum utilization can reach about 78% with 93.8s transaction confirmation delay when the transaction success rate approaches 1.

In [84], [106], the authors utilize the blockchain to secure computing resource management in IoT context. Notably, the computation offloading framework without tamper-proof audit can result in security risks such as spoofing attacks and free-riding behaviors. To address this issue, Huang *et al.* [84] build a decentralized vehicular fog computing (VFC) framework in IoV to eliminate free-riding and fraud attacks in the distrustful environment. In their framework, parked vehicles perform as VFC nodes (as a supplement of fog computing) and can cooperatively trade their idle computation resources with moving vehicles with computation desires. The task requests, node activities in offloading, task evaluation, and rewards are recorded in the immutable and traceable blockchain for public audit.

Different form [84], Xiong *et al.* [106] combine the edge-cloud computing for enhanced consensus efficiency in blockchain-enabled IoT, as shown in Fig. 11. Specifically, to accommodate PoW-based permissionless blockchains in the

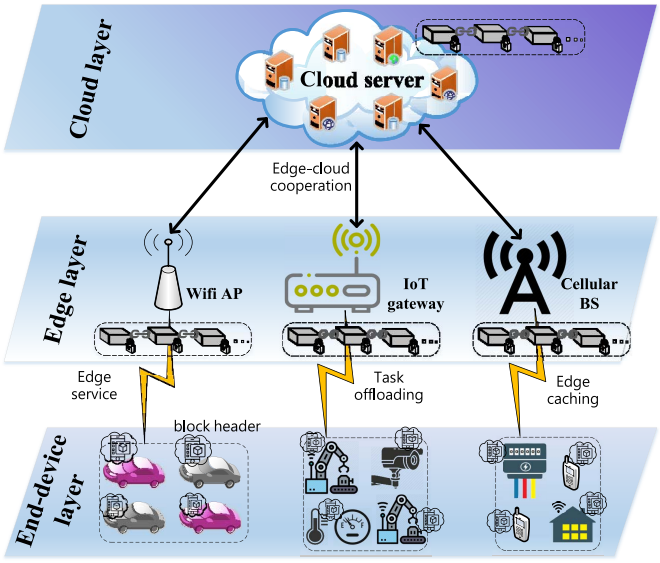


Fig. 11. A typical example of blockchain implementation in ground IoT context under edge-cloud environment.

IoT context, an efficient computation offloading framework is proposed in [106] by utilizing edge and cloud resources to offload computation-intensive PoW tasks from resource-limited IoT devices. A two-stage Stackelberg game model is devised in [106] for efficient and dynamic resource allocation. In the proposed game, the edge/cloud server (leader) first announces its unit price of shared computing resource in the first stage. Then, the miners (followers) determine their amount of computing resource to purchase in the second stage based on the announced resource price. The backward induction method is employed to solve the game by searching the SE under both uniform pricing and discriminatory pricing scenarios. Simulation results show that the pricing mechanism can significantly affect resource utilization and user profits.

In IoT, edge caching services can greatly reduce the data delivery latency and improve the QoS especially for delay-sensitive applications (e.g., online games and video watching), by providing contents from nearby edge devices with fewer hops. However, the reliability of delivered content data and the incentive of selfish edge devices are two challenges. To address these challenges, Liu *et al.* [107] present a secure content caching scheme in edge computing networks, where the blockchain maintained by edge devices offers the tamper-proof credentials for caching resource trading activities. Besides, to motivate edge devices' participation, a caching order matching algorithm is devised to schedule the caching resource exchange between data providers and edge devices. Simulation results show that the proposed scheme can improve the matching efficiency and decrease the data transmission cost of edge caching.

Unlike [107], Xu *et al.* [108] propose a blockchain optimization approach in mobile social networks to delete expired caching transactions on ledgers to alleviate the heavy blockchain burden. In their work, a blockchain-based edge caching mechanism is implemented to prevent malicious edge

nodes from returning incorrect results and malicious mobile users who deliberately refuse to pay. As all transaction details are immutably recorded in the blockchain, each party cannot repudiate them or refuse to pay. Meanwhile, for improved fairness in allocation, a max-min fairness algorithm is devised in [108] to fairly assign caching resources to social users, where the unused resources from users with low demands are evenly distributed to users with large demands to ensure fairness. Simulation results show the low delivery latency in the proposed approach, compared with the fixed and random caching approaches.

Apart from the network resource management, blockchain can also be utilized for secure distributed energy trading. Nowadays, the proliferation of electric vehicles (EVs) and renewable energy have attracted worldwide attention to building future green cities with energy sustainability. To address the data security and user incentives in large-scale energy delivery, Wang *et al.* [60] propose an innovative blockchain-enabled vehicular energy network (VEN) which utilizes EVs as energy carriers to transport energy from clean energy sources to other areas. In their work, a discriminatory pricing-based incentive mechanism is devised to motivate EVs to collaboratively transmit clean energy to areas with different energy loads while optimizing their payoffs. Meanwhile, in [60], both the data transactions and energy payments are recorded in the blockchain to offer reliable incentives and eliminate double-spending and refuse-to-pay behaviors in VENs. Simulation results show the fast convergence and improvement of EV utility (i.e., user satisfaction minuses the cost in energy delivery) of the proposed scheme.

In addition to the VEN paradigm, vehicle-to-grid (V2G) and EV-to-EV are two promising energy trading paradigms for EVs to benefit smart grids, e.g., peak load shifting. To secure energy trading in V2G, Zhou *et al.* [109] leverage the consortium blockchain to build a secure energy trading scheme with moderate cost, where edge nodes (i.e., local energy aggregators) perform block mining and store the full ledgers while EVs act as non-mining nodes which only store the block header. To reduce the degree of demand-supply mismatch in V2G, the authors also devise a contract theoretical approach, where each LEAG designs the optimal contracts for various types of EVs (i.e., discharging preferences) to maximize its payoff under the constraints of incentive compatibility (IC) and individual rationality (IR). The IC constraints ensure that each EV prefers to opt for the contract designed for its types instead of others, while the IR constraints enforce the non-negative payoff of EVs if it participates.

For the EV-to-EV energy trading, Hassan *et al.* [110] develop a secure V2V renewable energy auction scheme for smart homes by utilizing blockchain and differential privacy (DP) technologies, where the blockchain provides a trusted ledger for authorized buyers/sellers and DP offers rigorous privacy protection in the energy auction. As such, the historical activities of resource usage, sharing, and trading, as well as the corresponding financial settlements, can be safely recorded in the blockchain without any trusted intermediary and privacy leakage. The simulation results show that the proposed scheme attains an improved revenue for EVs and overall network benefit than the Vickrey-Clarke-Groves (VCG) auction mechanism.

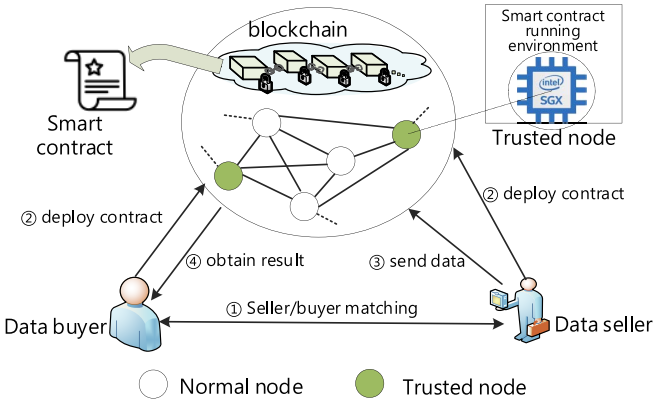


Fig. 12. Blockchain-enabled data trading system (SDTE) under data processing-as-a-service mode [58]. In SDTE, data owners only sell the access of the data for analysis instead of their raw private data. The data buyer deploys the detailed data analysis contract on the blockchain to process the seller's raw data and acquire data processing results. The data analysis contracts are executed by a group of trusted nodes implemented by the Intel SGX.

With the boom of EVs, the range anxiety of EV users become a new concern, especially for remote and underpopulated areas. Motivated by the concept of sharing economy, the authors in [111] present a novel blockchain-enabled private charging pile (PCP) sharing approach to mitigate EV users' range anxiety by using shared PCPs to charge a group of EVs. As PCP owners and EV users are commonly strangers, the blockchain platform is to deliver trust-free sharing services for EVs and PCPs. Moreover, the preference of EVs (e.g., distances and social relations) are considered in [111] for generating efficient and stable matching pairs for EVs and PCPs by utilizing the well-established deferred acceptance rules. However, in the above-mentioned works, the joint scheduling of system resources (including spectrum, computing, caching, and energy) based on blockchain for IoT devices with distinct characteristics (e.g., social, location, and privacy) in an automatic and intelligent fashion remains a research challenge.

The programmable smart contracts further enable the automated data, resource, and asset trading with complex logic in a variety of SAG-IoT applications. For example, participants can automatically trade their resources such as data, battery energy, caching space, and computing capacity, under the predefined contractual prices and triggering conditions [84], [108]. Besides, by leveraging smart contracts in Ethereum virtual machines (EVMs), Dai *et al.* [58] present a novel blockchain-enabled data trading ecosystem under data processing-as-a-service mode, as illustrated in Fig. 12. In their system, data owners only share the extracted knowledge from their private data for privacy preservation. The trusted nodes with secure SGX provisions are introduced for executing the data analysis smart contracts within SGX-protected EVMs. In addition, network operators can be benefited by designing smart contracts with collaborative participants to enable automatic and convenient resource management. Nonetheless, in the above system built on smart contracts, potential code vulnerabilities (e.g., transaction congestion attack, random

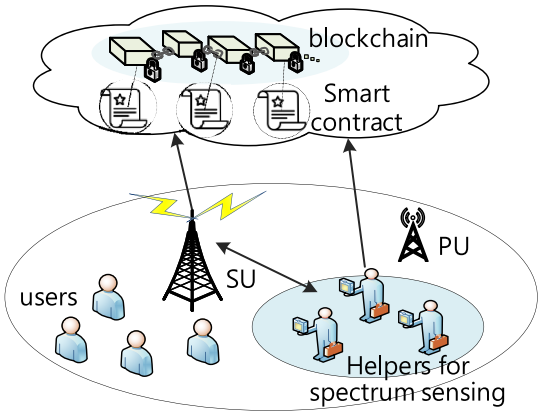


Fig. 13. Smart contract-enabled spectrum sensing framework (Spass) [113]. In Spass, the SU can lease the PU's licensed band opportunistically with tolerable interference to serve its users. To avoid the high deployment cost in massive sensors for spectrum sensing, the crowdsourced spectrum sensing is employed, where a group of helpers offer distributed sensing services. The spectrum sensing service and payment are processed via the smart contracts atop the blockchain.

number attack, and reentrancy attack) may also arise in smart contracts during their deployment in SAG-IoT.

As an effort to resolve the efficiency and security issues in smart contracts, Bayhan *et al.* [113] combine K-means clustering methods to identify independent malicious users in smart contract-enabled spectrum sensing, as illustrated in Fig. 13. In their framework, the spectrum monitoring is outsourced to a group of helpers to save the prohibitive cost in deploying spectrum sensors, and the smart contract system enables automated helper selection, service payment to honest helpers, and free-riding or faulty helper identification. Moreover, by using both lossless and lossy compression of spectrum sensing reports, the amount of data to be stored in smart contracts can be reduced for alleviated system overhead. By implementing a prototype using Ethereum, the experimental results validate the feasibility and cost-saving of the proposed approach.

6) Blockchain-Based SAG-IoT Data, Resource, and Asset Management Solutions in Industry: In industry, various startups are exploring blockchain technology in this field. For example, IoT Chain [114] offers a decentralized approach based on the public blockchain to build trust among IoT devices. It aims to build a decentralized lightweight operating system (OS) which supports trustworthy information/value exchange towards secured IoT.

IOTW [115] is a blockchain-enabled IoT big data unifying platform, which aims to make data accessing from various IoT devices simple and efficient. In IOTW, the proof of assignment protocol is adopted for consensus, where part of IoT devices are preselected in every consensus interval to directly execute some simple cryptographic missions, known as "micro-mining". Moreover, transaction ledgers are stored in the trusted ledger servers. As such, compared with PoW, only limited competition exists in solving the cryptographic task, and the storage for the whole ledger on IoT devices is eliminated.

Power Ledger [116] is a blockchain-based system which enables P2P clean energy trading for community residents by recording electricity consumption and generation activities on ledgers. In Power Ledger, residents can sell their surplus energy, and the electricity pricing and electricity distribution are completed through smart contracts.

Lessons Learned: In this subsection, we have discussed blockchain-enabled academic and industrial solutions for trustworthy data, resource, and asset management under five network paradigms in SAG-IoT. Tables VII and VIII compare the recent blockchain-based solutions in this field from several perspectives. The key lessons learned from this subsection are as follows.

- In conventional approaches such as cloud-based schemes, it is hard to establish trusted interactions among distrustful entities in SAG-IoT. In blockchain-based approaches, by offering consistent, tamper-resistant, and non-repudiable ledgers that record transactions, events, and registry of assets across decentralized networks via consensus operations, the cross-border trust among distrustful SAG-IoT users/devices can be established without reliance on any trusted intermediary.
- By deploying smart contracts atop the blockchain, the distributed resources management policies (e.g., scheduling models), participants' data and resource sharing strategies (e.g., game and learning models), and asset trading across multiple segments in SAG-IoT can be enabled in an automatic manner, as well as the corresponding financial settlements.
- Blockchain-based large-scale applications usually incur intolerable latency due to sequential transaction verification and consensus reaching. Meanwhile, blockchain-based security services usually require huge storage spaces and considerable computing capacity for a single node. Due to the high mobility of satellites, UAVs, and part of ground IoT devices (such as vehicles) and the resource constraints of devices in SAG-IoT, the blockchain platform for SAG-IoT applications needs to be redesigned according to the specific scenarios and QoS requirements in different segments.
- By deploying the blockchain platform, the risks of SPoF and corrupt services arising from TTPs can be mitigated and the operational fee in SAG-IoT services (e.g., sharing economy) can be eliminated.
- Blockchain can also bring reliable incentives to promote the collaboration of selfish entities in SAG-IoT. For example, their resource-sharing activities and contributions (as evidence for rewarding) can be permanently recorded on the decentralized ledgers. Another example is the utilization of smart contracts to implement resource scheduling and pricing algorithms.

B. Personal Data Access Control and Usage Auditing

1) Problems With Traditional SAG-IoT Data Management Solutions: With the pervasive smart devices in our surroundings, it is possible to deliver contextualized and personalized intelligent services for end-users. Nevertheless, these services require the frequent collection of our personal data to create personal profiles, which inevitably leads to high risks of

TABLE VII
SUMMARY OF BLOCKCHAIN SOLUTIONS FOR TRUSTWORTHY DATA, RESOURCE, AND ASSET MANAGEMENT IN SAG-IOT APPLICATIONS (PART I)

	Layers	Security Threats	Threat Type	Ref.	Purposes	Technology Used in/with Blockchain	Data in Blockchain
Trustworthy Data, Resource, and Asset Management	SAGIN	Efficiency issue in blockchain	①	[10]	Secure and efficient resource management in different layers of SAGIN	Relay chain Reverse auction	Resource transactions
	Space-Ground Integrated	Untrusted traffic data transmission	①	[89]	High throughput and security in traffic data transmission from ground stations to LEOs	Bargaining game	Ground traffic data
	Space-Ground Integrated	Uncoordinated data delivery	①	[90]	Reduced block propagation delay of blockchain services in satellite-terrestrial IoT	N/A	Transactions
	Space-Ground Integrated	Compromised fog nodes	④	[91]	Secure integration of fog computing with space-ground IoT	Cloud-fog computing	Transactions
	Space-Ground Integrated	Untrusted data sharing among satellites	①	[92]	Trusted data (e.g., positions and velocities) sharing among satellites in space	Ethereum	Transactions
	Space-Air Integrated	Hijacking, Compromised miners	④	[93]	Trustworthy data and resource management for LEO satellites and UAVs	Federated double Q-learning	Resource transactions
	Air-Ground Integrated	Invasions, Limited battery of UAV	①	[95]	Secure and energy-efficient data collection for ground IoT devices	Adaptive linear prediction	Resource transactions
	Air-Ground Integrated	Tampering of sensory data	①	[96]	Secure data acquisition for UAV-assisted IoT	Bloom filter	Data transactions
	Air-Ground Integrated	Billing and resource management issues	④	[97]	Energy-efficient resource management in blockchain services in air-ground IoT	Stochastic game, Hierarchical learning	Resource transactions
	Air-Ground Integrated	Untrusted energy trading environment	④	[99]	Secure WPT services for UAV-aided IoT	Hybrid blockchain	Energy micro-transactions
	Air-Ground Integrated	Fraud, Malicious TTPs	④	[57]	Secure spectrum trading for cellular-connected drone networks	Reputation, Stackelberg game	Spectrum transactions
	Air-Ground Integrated	Trust issues	④	[98]	Secure and distributed UAV-aided WPT in untrusted IoT environment	Contract game	Energy transactions
	Ground	Data tampering, Bidding leakage	①	[100]	Secure and truthful data trading in IoV	Edge computing, Double auction	Data transactions
	Ground	False and low-accuracy shared GPS data	①	[101]	Secure GPS positioning error evolution sharing for vehicles	Edge computing	Data transactions
	Ground	Eclipse attack, Transaction forgery	④	[102]	Secure and high-quality shared data among mobile terminals	DRL	Data transactions
	Ground	Service trust	④	[104]	Intelligent spectrum sensing and secure spectrum sharing	Stable matching	Spectrum transactions
	Ground	Double-spending, DDoS	④	[105]	Improved consensus performance in blockchain-based spectrum trading	Temporary anonymous transaction	Spectrum transactions
	Ground	Lack trust, SPoF	①	[38]	Secure and trustworthy data delivery in autonomous driving	Reputation-based incentives	Data transactions
	Ground	Lack incentive, Privacy leakage	④	[117]	Secure and efficient spectrum sharing in 5G HetNets	Contract game, Matching game	Spectrum transactions
	Ground	Refuse to pay Fraudulent energy service	④	[59]	Secure and efficient charging for EVs in a charging station	Contract game	Energy transactions
	Ground	False-reporting, Free-riding	④	[84]	Transparent and traceable computation offloading with parked vehicles	Smart contract, Vehicular fog computing	Task transactions
	Ground	Selfish agents	④	[106]	Secure computation offloading to cloud/fog servers in PoW tasks	Stackelberg game	Task transactions
	Ground	Content reliability	①	[107]	Secure edge caching for digital contents in wireless networks	Matching	Caching transactions
	Ground	Refuse to pay, Untrusted edge nodes	④	[108]	Trustworthy edge caching for mobile users	PoW, Smart contract	Caching transactions
	Ground	Transaction tampering, Lack incentives	④	[60]	Secure and incentive EV-aided clean energy distribution network	Dynamic pricing	Energy transactions
	Ground	Transaction tampering, Lack incentives	④	[109]	Secure and efficient V2G energy trading with moderate cost	Contract game	Energy transactions
	Ground	Untruthful bidding, Information leakage	④	[110]	Secure and privacy-preserving microgrid energy auction	Auction, Differential privacy	Energy transactions
	Ground	Untrusted environment, Information leakage	④	[111]	Secure private charging pile sharing for EVs	Matching, Coalition game	Energy transactions
	Ground	Repudiation and fraud, Information leakage	④	[58]	Decentralized P2P data trading for knowledge sharing	Smart contract, SGX-protected EVM	Data transactions
	Ground	Free-riding, Efficiency of smart contract	④	[113]	Automated spectrum sensing, malicious helper identification, and payment	Smart contract, Clustering	Spectrum transactions

① means data-related threats; ④ means service-related threats.

Continued on next page

privacy leakage and privacy misuse. With the enforcement of General Data Protection Regulation (GDPR) legislations,[4] the world has paid increasing attention to the breaches of data privacy with strict data legislations which aim to bring full control back to data owners. To be GDPR-compliant, traditional centralized approaches of personal data management, such as OAuth 2.0,[5] allow users to share their private data via a single sign-on operation to specify the usage policies for different entities. OAuth 2.0 is a widely adopted authorization framework in IoT applications, which utilizes access tokens to grant or revoke access privileges of IoT users [26]. However, these measures are based on the client-server architecture and can only offer limited transparency and truthfulness, as well as simple options to either "accept all" or "opt-out".

In particular, from the user's perspective, it fully depends on the truthfulness of the centralized authentication and authorization server (AAS) for (i) the authentication and authorization of entities, and (ii) data access control and data ownership provenance. Besides, users' private data managed by the AAS may be handed over to other third parties without the data owner's consent. From the AAS's perspective, it is challenging to declare that it has been legally and continuously processing all private data as required. As a result, existing centralized solutions can pose severe privacy concerns due to the lack of transparency and accountability in private data management.

2) Blockchain-Based SAG-IoT Data Management Solutions in Research: The blockchain offers a decentralized solution

[4]https://gdpr-info.eu/

[5]https://tools.ietf.org/id/draft-ietf-oauth-v2-31.html

TABLE VIII
SUMMARY OF BLOCKCHAIN SOLUTIONS FOR TRUSTWORTHY DATA, RESOURCE, AND ASSET MANAGEMENT IN SAG-IOT APPLICATIONS (PART II)

Continued from previous page

	Ref.	Blockchain Type	Consensus Protocol	Advantages	Disadvantages	Smart Contract	Implementation Platform
Trustworthy Data, Resource, and Asset Management	[10]	Hybrid	Hybrid	Reduced implementation cost to meet QoS requirement in each layer of SAGIN	Cross-chain security issues in management of parallel chains	✓	Ethereum
	[89]	N/A	N/A	Improved fairness and data reliability of satellite-terrestrial systems	Inefficiency of the large-scale blockchain implementation	×	N/A
	[90]	N/A	N/A	Reduced propagation time and improved data synchronization speed in satellite-terrestrial system	Lack dynamic network scheduling and prone to DoS attacks	×	N/A
	[91]	N/A	N/A	Improved system efficiency by integrating with fog-cloud computing	Propagation delay issues in low-latency application	×	N/A
	[92]	Private	PoW	Trusted data sharing for satellites	Limited number of nodes and prone to DDoS attacks	×	Ethereum
	[93]	N/A	PoW	Efficient energy estimation for LEO satellites and UAVs in consensus process	Realistic network testing for deployment	×	N/A
	[95]	Public	PoW	Secure data collection and payment in UAV-aided IoT	Resource-hungry for UAVs and lack optimal rewarding mechanism	×	N/A
	[96]	Consortium	PoW	Efficient data acquisition from IoT devices with UAV-MEC integration	Lack mobility analysis of UAVs and work for single UAV scenario	×	Ethereum
	[97]	N/A	Hybrid	Obtain optimal strategies of peers and BSs in resource management in BaaS	Security issues of compromised MEC nodes	×	N/A
	[99]	Public	PoW	Maximize ECSs' utility while optimizing UAVs' resources demands	Accurate players' parameters acquisition in practical deployment	×	N/A
	[57]	Consortium	PBFT	Maximize profits of UAVs and the MNO under different pricing schemes	Lack energy constraint and trajectory planning of UAVs	×	N/A
	[98]	Consortium	DAG	Improved efficiency in verification of large amount of energy micro-transactions	Security of blockchain synchronization due to UAVs' high mobility	×	N/A
	[100]	Consortium	PoW	Encourage vehicles' truthful participation and maximize social welfare	Long block time in PoW for vehicles with high mobility	×	N/A
	[101]	Consortium	BFT-DPoS	Improved efficiency in positioning error correction and security of data sharing	Eliminate random errors by considering multipath effects in urban cities	✓	N/A
	[102]	Consortium	PoW	Defend against eclipse attack, majority attack, and terminal device failure	Depend on network infrastructures for blockchain maintenance	✓	Ethereum
	[104]	Consortium	PBFT	Improved efficiency and security of spectrum auction	High communication load and computing overhead in blockchain	✓	N/A
	[105]	Consortium	PoW	Improved efficiency and security of spectrum auction	Incompatible with public blockchains	×	Omnetpp
	[38]	Consortium	Modified PBFT	Improved security of data delivery in autonomous driving	Lack joint security provisioning and network optimization	×	N/A
	[117]	Consortium	PoW	Transparent spectrum sharing and efficient spectrum allocation	Need prior knowledge of PU types	×	N/A
	[59]	Consortium	Modified PBFT	Improved energy efficient for EVs in charging pot under RE constraint	Need prior knowledge of EV types	✓	N/A
	[84]	Consortium	PoW	Defend against false-reporting, free-riding, and spoofing attacks for vehicles	Lack privacy sensitivity and social ties of vehicle users	✓	EVM
	[106]	Consortium	PoW	Improved consensus efficiency by integrating with fog-cloud computing	Not support the oligopoly market with multiple CFPs	×	Ethereum
	[107]	Public	PoW	Improved content reliability and caching resource utilization	Inefficiency of the large-scale blockchain implementation	✓	N/A
	[108]	Public	PoW	Trustworthy and high-quality edge caching in mobile social networks	No cooperations of edge nodes to increase their profits and users' QoE	✓	N/A
	[60]	Consortium	Modified PoW	Improved participation level of EVs for energy delivery in VEN	Not support for energy source tracing in VEN	×	N/A
	[109]	Consortium	PoW	Optimal task offloading strategies for EVs under information asymmetry	Need prior knowledge of EV types	×	N/A
	[110]	Consortium	PoW	Protection of bid privacy in blockchain-based VCG auction process	Lack prototype development	×	N/A
	[111]	Consortium	Modified PoW	Eliminate of SPoF and privacy leakage in centralized PCP sharing market	Lack prototype development	×	N/A
	[58]	Public	N/A	Protection of raw data and analysis result in data trading market	Not support source data tracking in data sharing	✓	EVM
	[113]	Public	N/A	Automated helper selection, malicious helper identification, and payment	Lack defense of malicious helpers who change strategies to escape detection	✓	Ethereum

to build trust between service providers and data owners for personal data sharing and management [12], [118], [119]. In the blockchain, the public key is usually employed to create pseudo-identities for users. In [40], the *compound identity* (*c-ID*), as an extension of traditional public/private key-pairs, is introduced to represent the shared identity for two or more entities involved in a common digital asset (e.g., private datasets). As shown in Fig. 14, in the proposed compound identity mechanism, the c-ID consists of the signing key-pairs for both data owners and guests, as well as a symmetric key for data encryption and decryption. As such, some entities are owners of the identity, and the rest are guests who only have restricted access to the asset, thereby the access of personal data can be protected from all other entities.

However, the detailed authorization models and access control protocols are not given in [40]. For practical implementation of blockchain-based access control system, Ouaddah *et al.* [120] present a fair and transparent access control mechanism named FairAccess in IoT context to prevent the loss of control of the IoT data after sharing with service providers (SPs) for personalized services. By introducing new types of access transactions for granting, delegating, obtaining, and revoking access rights using blockchain, every entity can transparently audit the access statuses recorded in the blockchain. Besides, in the proposed authorization model, access tokens are issued as the access right that a particular SP can access the particular data, where the maintenance and validation of access tokens are controlled by

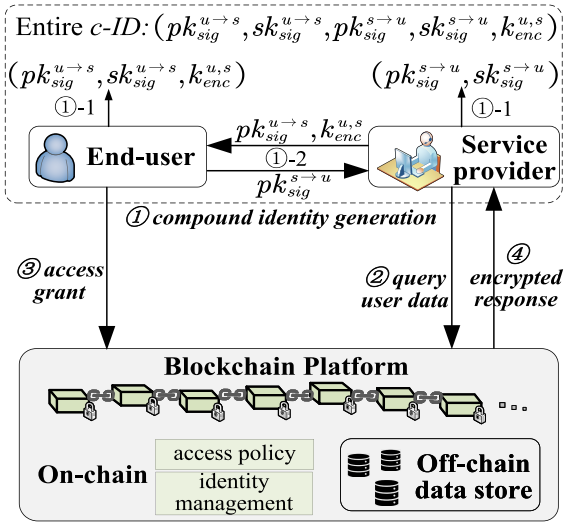


Fig. 14. High-level system architecture of the blockchain platform for private data access in [40]. ① c-ID generation process (①-1. The end user generates its signing key-pair $pk_{sig}^{u\to s}$, $sk_{sig}^{u\to s}$ and a symmetric key $k_{enc}^{u,s}$ for data encryption/decryption; meanwhile, the service provider (SP) generates its signing key-pair $pk_{sig}^{s\to u}$, $sk_{sig}^{s\to u}$. ①-2. The end user shares $pk_{sig}^{u\to s}$, $k_{enc}^{u,s}$ with SP, and SP shares $pk_{sig}^{s\to u}$ with user. Then, the entire c-ID is created, which is externally observed by a 2-tuple $c-ID_{u,s}^{public} = \{pk_{sig}^{u\to s}, pk_{sig}^{s\to u}\}$.) ② The SP sends the data query to the blockchain. ③ The user sends its permissions to grant or deny the access request, which are recorded as access policies in the blockchain. ④ The blockchain platform returns the encrypted response to SP according to the recorded latest user access policies.

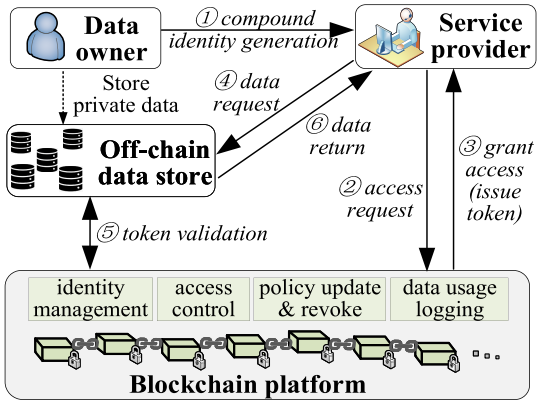


Fig. 15. High-level system architecture of blockchain-based GDPR-compliant data management platform in [42]. ① c-ID generation process (similar to [40]). ② The service provider (SP) sends the query of user's data to the blockchain. ③ The blockchain issues the access token to grant the data access request according to user's latest access policies. ④ The SP sends data request and the access token to the off-chain data store (DS). ⑤ DS validates the token by using the blockchain data. ⑥ DS returns the encrypted data to SP.

the decentralized blockchain network. In token-based access control mechanisms enabled by blockchain, smart devices can easily validate the validity of the tokens while further improving the end-to-end security by getting rid of outsourcing these functionalities to TTPs. An implementation using a Raspberry PI device equipped with a camera module and Bitcoin blockchain is conducted in [120] for baby monitoring to validate its feasibility.

However, the prototype built on Bitcoin in [120] can suffer from low throughput and scalability (e.g., about 10 min confirmation delay, only support about 1 MB block size, and Turing-incomplete scripting language). To further improve the system scalability, Qi *et al.* [121] develop a blockchain-based compressed and private data sharing framework named Cpds via efficient on-chain and off-chain collaboration and hybrid access control. A tree-based data compression mechanism is developed for off-chain data storage to improve storage efficiency and I/O efficiency by compressing product data before submission and packing all records of each product into a single transaction. Besides, an attribute-based encryption (ABE) model is adopted for IoT users while identity-based encryption (IBE) models are applied for TTPs to alleviate key distribution and authority definition overheads, where access policies are specified in encryptions and data users' access authorities are assigned via key distribution.

Apart from the access control (e.g., who can access what data under which condition) of private data in the above works [40], [120], [121], the blockchain can offer an innovative approach for usage auditing (e.g., the time and purpose for data processing) of personal information. For example, in [41], by utilizing the publicly auditable ledgers and hierarchical IBE schemes, the usage activities of users' private data can be safely logged to achieve transparency and traceability. For users, the tamper-proof evidence of their granted data access can be recorded in the blockchain platform before processing their private information. Besides, the hierarchical IBE scheme guarantees that each data owner can create his/her identity-based key-pair for the encryption of the data that he/she is willing to share with a TTP.

However, the verifiable compliance of GDPR regulations in data access control and usage auditing in the above works [40], [41], [120], [121] is not sufficiently studied. To be GDPR-compliant in auditing data usage activities, as shown in Fig. 15, Truong *et al.* [42] develop a blockchain-based data management scheme to publicly and transparently audit whether a service provider continuously adheres to the GDPR legislations. In [42], two types of blockchain ledgers (i.e., $3A_{ledger}$ for authentication, authorisation and access control, and log_{ledger} for validating access tokens and data usage logging) are introduced to record the access authorization statuses and usage logging statuses during private data sharing.

Faber *et al.* [122] further consider the identity management of users and data monetization in developing a GDPR-compliant data sharing platform based on blockchain, where the identity information of users can be proved and recorded in the blockchain and the monetization of private data can be realized by existing game theoretical models.

In the above works [41], [42], [122], the smart contracts are further employed to automate the access policy making, validating, and usage auditing process for IoT users and service providers. Particularly, with the help of programmable smart contracts, data owners can define fine-granular access control policies to specify their preferences on data usage other than simple policies predefined by AASs. As such, the implemented blockchain platform turns into an automated access control manager to allow users to fully control their data access and

TABLE IX
SUMMARY OF BLOCKCHAIN SOLUTIONS FOR PERSONAL DATA ACCESS CONTROL AND USAGE AUDITING IN SAG-IOT APPLICATIONS (PART I)

	Layers	Security Threats	Threat Type	Ref.	Purposes	Technology Used in/with Blockchain	Data in Blockchain
Personal Data Access Control and Usage Auditing	Ground	Unauthorized access, Private data misuse	①	[40] [120]	Secure personal data access control	Off-chain storage	Access control policies
	Ground	Lack unified data access control cross factories	①	[121]	Unified and compressed product data sharing in industrial IoT	Hybrid access control, Off-chain compression	Access control policies
	Ground	Privacy leakage in private data collection	①	[41]	Secure personal data usage audit	Public blockchain, Smart contract	Access control policies, Data usage logs
	Ground	Unauthorized access, Private data misuse	①	[42] [122]	GDPR-compliant private data sharing with fine-grained access control	Off-chain storage, Smart contract	Access control policies, Data usage logs
	Ground	Collusion attack, Manipulation attack	①	[123]	Secure and verifiable data sharing in vehicular social networks	CP-ABE	Access control policies
	Ground	Manipulation attack, Fraud, Data misuse	①	[124]	Verifiable and traceable medical information sharing	Two-layer blockchain architecture	Hash of medical record

① means data-related threats.

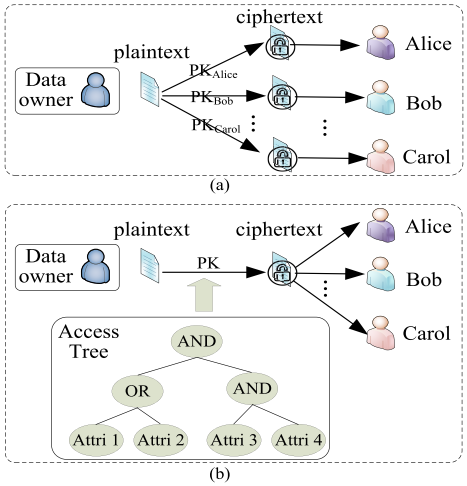


Fig. 16. Illustration of the workflow of data sharing based on (a) traditional PKI cryptography and (b) ABE cryptography.

usage permissions in terms of to whom they will share the data, for what purpose, under what conditions, and at what price.

Other optimized blockchain approaches for secure personal data sharing are proposed in various SAG-IoT applications such as IoV and medical IoT. For example, in IoV, Fan *et al.* [123] propose a verifiable one-to-many information sharing mechanism in ciphertext-policy ABE (CP-ABE) cryptography for collaborative vehicles on road based on the blockchain. Fig. 16 illustrates the workflow of public key infrastructure (PKI)-based and ABE-based data sharing, respectively. In conventional CP-ABE schemes, access policies are recorded and granted by the could server, which lacks transparency and auditability due to centralization. The target of their mechanism is to resolve the privacy violation in conventional CP-ABE schemes for vehicles where the honest-but-curious cloud is the only entity that can grant access to vehicular users. In particular, the blockchain is employed to immutably store the access control policies to realize self-certification for users and non-repudiation for the cloud, where the access policy tree is formulated by linear secret sharing schemes (LSSS). Moreover, to protect users' sensitive information involved in access policies, the authors design a cryptographic policy hiding mechanism and prove its security via security analysis.

Besides, in medical IoT, Du *et al.* [124] design a blockchain-based decentralized medical data sharing framework to facilitate scientific research and disease diagnosis among various distrustful medical institutions. The shared information can be securely stored, exchanged, and publicly audited by using the decentralized ledgers, while a supervised anonymous data sharing method is presented for processing anonymous information. In the proposed anonymous sharing method, to preserve the data privacy in blockchain, the transactions (which include sensitive medical records) can only be audited by regulatory agencies and accessible by related institutions. Moreover, to achieve the high TPS and consensus speed in the blockchain system, a novel two-layer blockchain architecture is developed, where the blockchain network is split into two layers: high-level consensus group (HCG) and low-level consensus group (LCG). Nodes in LCG are responsible for verifying, processing, and packaging transactions into a mini-block and transmitting it to the HCG. Then, nodes in HCG validate and package the received mini-blocks from the LCG and build a large block. Experimental results show that, when the number of consensus nodes in LCG increases, TPS increases linearly while the confirmation delay does not grow significantly.

3) Blockchain-Based SAG-IoT Data Management Solutions in Industry: The startup Datum [125] leverages the blockchain technology to construct a decentralized data storage and monetization platform for IoT (e.g., smart homes and wearables) based on NoSQL databases. Datum exploits the programmable smart contracts in Ethereum for secure and anonymous storage and employs the distributed storage system such as InterPlanetary File System (IPFS) [126] to ensure high performance in data handling.

Lessons Learned: In this subsection, we have discussed blockchain-enabled solutions for personal data access control and usage auditing in SAG-IoT. Tables IX and X compare the recent blockchain-based solutions in this field from several perspectives. The key lessons learned from this subsection are as follows.

- From the SP's perspective, conventional centralized private data management schemes such as OAuth 2.0 depend on the truthfulness of the SP (e.g., cloud and fog servers) for data storage and processing, thereby only offering limited transparency and accountability. From the user's perspective, potential security risks and data misuse

TABLE X
SUMMARY OF BLOCKCHAIN SOLUTIONS FOR PERSONAL DATA ACCESS CONTROL AND USAGE AUDITING IN SAG-IOT APPLICATIONS (PART II)

	Ref.	Blockchain Type	Consensus Protocol	Advantages	Disadvantages	Smart Contract	Implementation Platform
Personal Data Access Control and Usage Auditing	[40]	Public	N/A	Trust-free access control for users' private data	Trusted computing issues for private data in blockchain	×	N/A
	[120]	Public	PoW	Fair and transparent access control for IoT devices	Low throughput and scalability	×	Bitcoin
	[121]	Consortium	PoW	Reduced system overhead via tree-based data compression and off-chain storage	Lack data usage auditing	×	Fabric
	[41]	Public	N/A	Transparent and controlled IoT data access and processing	Lack verifiable compliance of GDPR regulations	✓	N/A
	[42]	Consortium	Kafka	GDPR-compliant data sharing with fine-grained access control	Lack data monetization	✓	Fabric
	[122]	N/A	N/A	GDPR-compliant data sharing with data monetization	Secure issues in data transfer from SPs to off-chain data stores	✓	N/A
	[123]	Consortium	PBFT	Self-certification and non-repudiation in CP-ABE for vehicular data sharing	High latency in reaching consensus	×	N/A
	[124]	Consortium	Modified PBFT	Privacy-preserving medical data sharing in IoT	Trusted and privacy-preserving processing of medical data	✓	Fabric

issues may occur without user awareness. Thereby, users' sensitive information can be exposed, and the functionalities of deployed services can be affected. Blockchain can offer a transparent and verifiable ledger for personal data management including data access control and usage auditing. As such, the single point of trust can be avoided, and both access policies and usage logs can be immutably recorded for public audit.

- According to works [42], [120], in blockchain-based data management approaches, the issuance and management of access tokens (as a "proof-of-permission") on blockchain ledgers can facilitate the verifiable and anonymous access control for SAG-IoT users/devices.
- By deploying smart contracts on Turing-complete blockchains, the automated access policy design, update, and revocation, as well as usage logging, can be enabled. Moreover, data owners can define fine-granular policies for data access and usage via smart contracts to specify their preferences on different data.
- By integrating with cryptographic schemes for restricted data access and sharing such as CP-ABE and key-policy ABE (KP-ABE), the blockchain platform can turn into a decentralized access control manager to enable automated and transparent entity authentication, authorization, and access control.
- In blockchain-based data management approaches, the raw personal data is generally stored off-chain to relieve the storage burden of blockchain. As the on-chain data is publicly accessible in permissionless blockchains or restricted to specific entities in permissioned blockchains, designing privacy-preserving on/off-chain models becomes essential to determine what data operations are revealed to the public or individuals. Moreover, efficient on/off-chain computation/storage models are required, where data operations are conducted off-chain and verified on-chain with privacy protection functions.
- Existing works on personal data access control and usage auditing mainly focus on the ground IoT context, while few works concentrate on the aerial networks and space networks.

C. Identity and Device Management

Identity management is fundamental for SAG-IoT applications. In SAG-IoT, each end device is featured with multiple attributes (e.g., manufacturer, type, and serial number), and devices typically have various relationships with real persons (e.g., sold by, used by, owned by, upgraded by, and repaired by) as well as with other devices (e.g., temporal and spatial correlations) [127]. The identity management of SAG-IoT devices with multiple attributes and relationships is a challenging issue. For example, the ownership of an IoT device may be changed or revoked, if the device is resold or compromised [128]. Besides, the access policies of a certain device can be time-varying for different users. Typically, according to [129], the identifiers in the IoT standard can be classified into the following three types:

- *Object identifier* uniquely identifies a physical or virtual object. For example, barcodes and RFID tags can be used as object identifiers.
- *Communication identifier* uniquely identifies a node with communication capacity in a network, which is generally represented by an IP address.
- *Application identifier* uniquely identifies the services and logical entities involved in IoT applications, such as the uniform resource locator (URL) and uniform resource identifier (URI).

Although a large number of solutions have been proposed for the management of "identities of things", there is no unified identification scheme for IoT to manage and recognize device identities across different solutions and platforms [129]. Besides, in traditional approaches, the identity and corresponding keys of a user, as an authorization for network access, are created and managed by the centralized network operator, where users may lose control of their personally identifiable information (PII). The blockchain can facilitate identity management for IoT devices including entity registration and certificate issuance, by immutably storing and tracing their identities, attributes, and relationships across all participating entities via the distributed ledgers [130]. For example, Xu *et al.* [131] develop a decentralized identity management mechanism based on blockchain to enable users to fully control their identifying information by creating self-sovereign

identities (SSIs) and public/private key-pairs. The SSIs and public keys are recorded in the blockchain and the illegal ones can be publicly detected by using the chameleon hash. Simulation results show that the proposed mechanism attains a smaller storage overhead, compared with the certificate revocation lists (CRL)-based mechanism.

Moreover, in conventional IBE schemes, it relies on the security parameters of other domains for cross-domain authentication. To secure D2D communications of industrial IoT devices during their collaboration on the same task involving various administrative IoT domains, Shen *et al.* [132] propose a decentralized cross-domain device authentication scheme based on permissioned blockchain. In their framework, the domain-specific trusted data sharing can be enabled by using decentralized ledgers across various IoT domains. To further protect users' privacy, an identity management mechanism is designed to remedy the drawback of identity-based cryptography in terms of identity revocation when the private key is compromised or lost. Simulation results validate the feasibility of the proposed scheme in terms of computation overhead, communication overhead, and write/query latency (i.e., the time duration from invoking the write/query chaincode to successfully returning the messages).

Generally, the communication and routing protocols in different network segments in SAG-IoT such as MQTT (Message Queuing Telemetry Transport), RPL (IPv6 Routing Protocol for Low-power and lossy networks), and 6LoWPAN (IPv6 over Low-power Wireless Personal Area Network) protocols [5] are not secure by design. Accordingly, such protocols need to be wrapped by other security protocols, such as DTLS (Datagram Transport Layer Security) for secure communication and IPSec (Internet Protocol Security) for secure routing [7]. A plausible solution is assigning a unique global unique identifier (GUID) for each node in communications. With blockchain, the complicated key management and distribution in protocols like DTLS and IPSec can be eliminated, as every IoT device has its GUID, e.g., public/private key pairs for identification, once connected to the blockchain network. Specifically, for permissionless blockchains such as Bitcoin and Ethereum, participants are identified by their public addresses. Meanwhile, for permissioned blockchains such as Hyperledger Fabric [83], identity management is fundamental for node enrollment and authorization to access the blockchain network. For example, all participating entities need to register themselves at the certificate authority (CA) with their true identities (e.g., the unique vehicle identification number of vehicles) in permissioned blockchain systems.

1) For Space-Ground Integrated Networks: Unauthorized access and impersonation attack are two typical threats in space-ground integrated networks (SGINs). Anonymous authentication is regarded as an essential approach to address these two attacks. However, existing anonymous authentication schemes in SGINs either do not support cross-domain authentication or require heavy computation overhead for users especially under dynamic scenarios. By exploiting blockchain technology, Liu *et al.* [133] design a decentralized cross-domain anonymous authentication scheme with high computational efficiency to prevent unauthorized access and impersonation attack in SGINs. As shown in Fig. 17, their proposed scheme consists of six kinds of entities, i.e., ground stations, NOCCs, satellites, end-users, an opening authority, and a blockchain network. Users can receive services from various satellite operators via anonymous authentication operated by corresponding NOCCs. The ground station serves as the satellite gateway between NOCC and satellites, which offers a ground interface for satellites. The opening authority is a TTP which deals with disputes between satellite operators and end-users by revealing the real identities of misbehaving entities. The proposed scheme also supports fast handover in switching to different satellite networks operated by different companies. Meanwhile, to defend against insider attackers in service-oriented applications, a fair billing protocol is designed by authors based on the smart contract atop the blockchain platform.

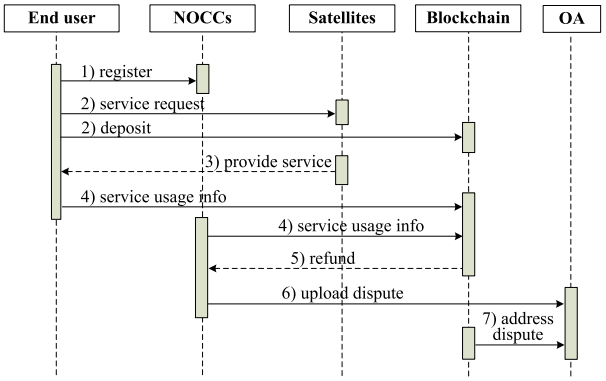


Fig. 17. Workflow of blockchain-based service authentication in SGINs in [133]. An end-user first registers with all NOCCs and receives a partial credential from each of them. Then, the user can aggregate them into a complete credential. After finishing the deposit at the blockchain, the user can request network services from a NOCC via its domestic satellite. Users can enjoy network services after the verification and upload the usage information such as the volume of the consumed traffic to the blockchain. A billing algorithm deployed by smart contracts calculates the service cost and refunds money to involved entities automatically. Once the misbehavior of the user is found, the NOCC sends a report request to the opening authority (OA) which will reveal the misbehaving user's identity.

2) For Space-Air Integrated Networks: In space-air integrated networks, the global navigation satellite system (GNSS) can offer precise navigation for multiple UAVs in a UAV swarm to operate cooperatively, and attackers can forge a malicious signal which has stronger power than that of the true GNSS signal, as shown in Fig. 18. To defend against GNSS spoofing attacks, Han *et al.* [134] propose a permissioned blockchain-based approach to detect malicious GNSS signals in FANET. In their approach, the authentication process in blockchain ensures the legality of UAVs' identities while any misbehaving entities in sharing spoofed information can be immutably traced. Moreover, using cooperation position methods, the UAV can obtain its current locations timely in the case that a GNSS spoofing is detected. However, the proposed approach only works if the ratio of UAVs under GNSS spoofing attacks is lower than one-third in a UAV swarm.

3) For Air-Ground Integrated Networks: Due to the time-varying network topology and unreliable wireless channels

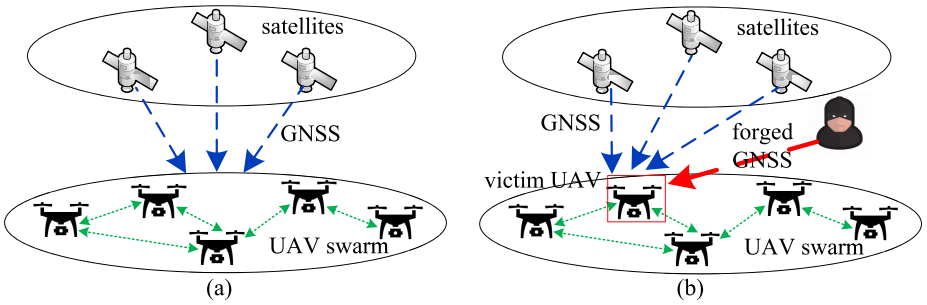


Fig. 18. Illustration of GNSS spoofing attack for UAVs in [134]: (a) normal GNSS operation; (b) GNSS spoofing attack. The detailed workflow of GNSS spoofing attack contains the following steps. ① The adversary tracks the target UAV's GNSS signals and calibrates a forged one with power stronger than that of the legal GNSS signal. ② As legal GNSS signals are suppressed by the forged one, the victim UAV receives the forged GNSS signals and acquires wrong navigation information.

in FANETs, it may be frequent for UAVs to miss certain group key messages. To address this issue, Li *et al.* [135] present a mutual-healing mechanism for group key distribution and recovery based on blockchain. In their mechanism, the distributed group keys and the list of UAVs' membership certificates are stored in the private blockchain which is maintained by the ground station. Experimental results show that the proposed mechanism supports mutual authentication and resists reply attacks.

However, UAV can still suffer high communication overhead in [135] especially for large-scale UAV applications. To alleviate the communication overhead of UAVs in traditional key management based on ground BSs, Tan *et al.* [136] present a distributed key management scheme for UAV swarms to automatically and securely update the key pairs, distribute cluster keys, and revoke malicious UAVs, in providing IoT services for ground devices. The authors also modify the transaction structure in the block and the miner election procedure to implement a more lightweight blockchain with reduced consensus duration. Experimental results show that the proposed scheme can resist impersonation attacks, reply attacks, and internal attacks, and attain low time delay in miner election. However, their scheme is based on the assumption that head UAVs are honest to follow the protocols.

In large-scale IoV, there exist multiple security domains maintained by different CAs, thereby the cross-domain identity authentication becomes an essential issue for high-speed vehicles. To resolve this problem, based on the blockchain, Zhao *et al.* [137] develop a lightweight and cross-border identity authentication scheme for ground vehicles to securely manage the transmitted data while satisfying low latency requirements in IoV. As shown in Fig. 19, the low-altitude UAVs are employed to be the security managers of security domains and are responsible for maintaining the blockchain. In their scheme, the security managers upload and maintain the vehicle's identity information in the blockchain, and transactions are used to package identifiable information from the source node to the destination node. Besides, the verification and backup of block data are conducted based on the distributed Kafka algorithm instead of the consensus process, to achieve high throughput and low latency. Simulation results show that the average authentication delay in the proposed scheme is 8.6ms for vehicles, which is significantly

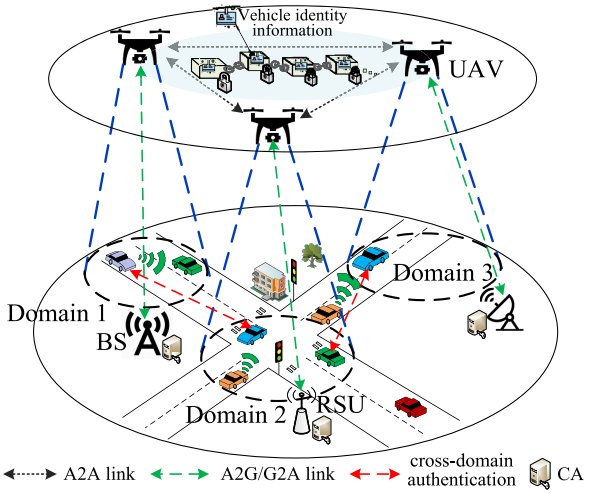


Fig. 19. Architecture of blockchain-based cross-domain identity authentication in UAV-assisted IoV in [137]. In [137], each UAV serves as the security manager of a security domain and is responsible for maintaining the blockchain which stores the vehicle's identity information in a distributed and tamper-resistant manner.

reduced compared with conventional Bitcoin and Ethereum blockchains.

4) For Ground IoT Networks: Blockchain technologies are also promised to build digital identity services for smart city applications [138] and a unified and distributed platform in the digital city operating system [139] for the identification of devices and individuals. In vehicular cloud computing (VCC) environment, conventional identity access management (IAM) approaches are service provider (SP)-centered, which is hard to support flexible access control for vehicular users such as cross-cloud access without re-authentication. In federated identity management, by exchanging users' authorization and authentication credentials (e.g., PII) across different cloud SPs with the assistance of TTPs, the cross-cloud access control can be enabled by only providing the unique PII for once. However, it relies on a trusted intermediary and needs the protection of PII to prevent unauthorized access and abuse. Fig. 20 shows a typical identity-as-a-service (IDaaS) model.

By utilizing the PII of on-board vehicular devices in VCC, Yao *et al.* [138] develop a privacy-enhanced and

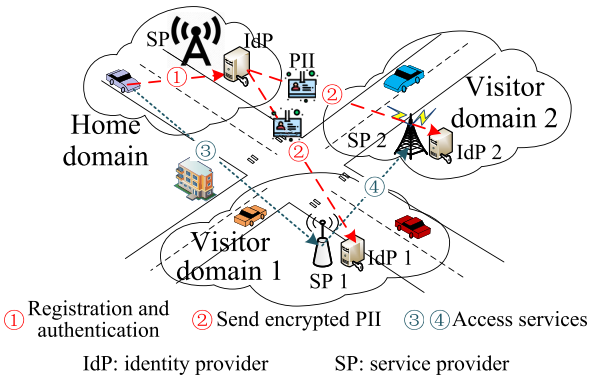


Fig. 20. Illustration of the general IDaaS model in VCC with multiple clouds [138]. ① A vehicle user registers at the home IdP of its home domain. ② The home IdP sends the encrypted PII of the user to other visitor domains. ③&④ The vehicle then can access multiple cloud services in visitor domains on demand with the federated identities.

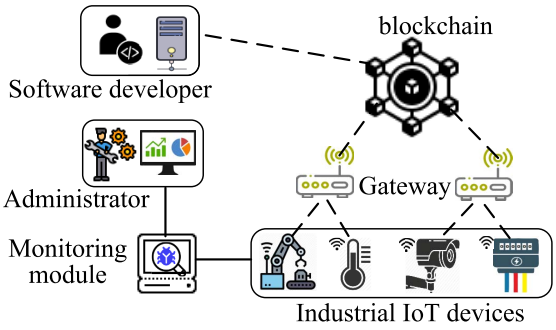


Fig. 21. Architecture of blockchain-based IoT software status monitoring system [140]. The public blockchain is employed as a trusted and distributed database to store software technical status snapshots produced by software developers. The gateway connects to the blockchain network and delivers blockchain data and services to resource-constrained IoT devices. The monitoring module monitors the software status and delivers it to the administrator.

lightweight IDaaS architecture based on CP-ABE and permissioned blockchain to promote efficient access control. In the proposed architecture, registered vehicles can access multiple cloud services in an on-demand and privacy-preserving manner. By only storing the addressing information of ciphertexts instead of the raw ciphertexts in the blockchain, the storage and transmission overheads of privacy policies of users and ciphertexts of PII in traditional CP-ABE based IDaaS models are reduced. The security analysis validates the security features of their proposed architecture including confidentiality, forward secrecy, and privacy protection of PII.

Apart from the vehicular environment, Asamoah *et al.* [139] study the unified digital identity solution for digital city operating system in smart cities. Concretely, a secure identity monitoring mechanism based on blockchain is developed in [139] for automatic identity generation and illegal activities reporting, aimed to facilitate digital identification and identity control of devices and users. In their mechanism, the hashes of device firmware and configurations are recorded in the ledgers to prevent unauthorized manipulation, while the access policies of devices are determined according to their attributes in the registration process. Here, the signatures of the device owner are regarded as attributes of the device and are included in the transactions in blockchain for verification. An implementation is deployed on a private Ethereum blockchain platform to evaluate the latency of ID generation, signing on attributes, signature verification, etc.

In SAG-IoT, malicious codes, bugs, and viruses can compromise IoT end devices if they are exposed to outside or updated unauthentically. As IoT devices typically have limited resources, it is challenging to implement strong security provisions for them. By integrating SAG-IoT with blockchain techniques such as smart contracts, the firmware and software of IoT devices can be automatically updated to remedy vulnerable breaches, thereby enhancing the security of SAG-IoT systems. For example, as shown in Fig. 21, He *et al.* [140] develop a secure IoT software status monitoring system based on blockchain by taking snapshots of statuses of the monitored software, where the blockchain platform is employed to immutably store the snapshots of software status to facilitate the detection of unauthorized software statuses. With the increasing number of IoT devices, another challenging issue for SAG-IoT security is to efficiently deliver security updates (e.g., patches) offered by vendors to all devices. To effectively motivate users' collaboration in the delivery of security updates, Leiba *et al.* [141] present a blockchain-based framework by making commitments to compensate collaborative users with digital currency in delivering security updates to other devices. The commitments are publicly verifiable and realized by using smart contracts, while the unforgeable proof of their distribution of security updates is generated by zero-knowledge contingent payment and recorded in the immutable ledgers. However, both the throughput and scalability need to be improved to accommodate the large-scale IoT applications.

In SAG-IoT, the rogue and compromised SAG-IoT devices can undermine the service trust and become potential insider threats. To defend against rogue and compromised devices in SAG-IoT systems, blockchain-based trust and reputation approaches can be effective practices through decentralized feedback aggregation, credibility evaluation, and trustworthiness computing [60]. One of the main challenges is user privacy preservation in developing efficient trust and reputation models in the transparent and public verifiable blockchain. To protect users from being tracked or retaliated after posting feedbacks, Liu *et al.* [142] develop an anonymous reputation mechanism for the preservation of user identities and confidentiality of ratings. The tamper-proof PoS-based blockchain with off-chain rating token creation is implemented to ensure transparent feedback aggregation in reputation computing, while the randomizable signature with the ZKP method is adopted to enable only aggregated feedback statistics available for the public. A prototype built on Ethereum validates the superiority of the proposed mechanism in terms of computation cost (i.e., time for cryptographic operations).

5) Blockchain-Based SAG-IoT Identity and Device Management Solutions in Industry: Many startups have been launched for secure identity and device management in SAG-IoT by using blockchain technology. For example,

TABLE XI
SUMMARY OF BLOCKCHAIN SOLUTIONS FOR IDENTITY AND DEVICE MANAGEMENT IN SAG-IOT APPLICATIONS (PART I)

	Layers	Security Threats	Threat Type	Ref.	Purposes	Technology Used in/with Blockchain	Data in Blockchain
Identity and Device Management	Space-Ground Integrated	Unauthorized access, Impersonation attack	②	[133]	Cross-domain anonymous authentication in space-ground integrated networks	Smart contract	Billing transactions
	Space-Air Integrated	GNSS spoofing attack	②	[134]	Efficient detection of malicious GNSS signals in FANET	Hybrid blockchain	Identities of UAVs, Spoofed GNSS
	Air-Ground Integrated	Active eavesdropper	②	[135]	Mutual-healing group key distribution and recovery for UAVs	Mutual-healing cryptography	Group keys, Membership certificates
	Air-Ground Integrated	Passive eavesdropper, Internal attackers	②	[136]	Distributed cluster key management with low overhead for UAVs	Modified transaction structure	Transactions
	Air-Ground Integrated	Data security, Node authentication	②	[137]	Lightweight cross-border identity authentication for vehicles and satellites	Hashchain	Transactions
	Ground	Lack trusted identities	②	[130]	Survey blockchain-based solutions for identity and access management	Distributed ledger technology (DLT)	Transactions
	Ground	Identity and key theft	②	[131]	Enable users to control their personal identifying information	Chameleon hash	Identities and keys
	Ground	Lack trusted third party in cross-domain IoT	②	[132]	Cross-domain IoT device authentication in collaborative manufacture	Off-chain, IBE	Security parameters of each IoT domain
	Ground	Identity privacy leakage	②	[138]	Secure and efficient IDaaS in vehicular networks	CP-ABE	Ciphertext link addresses
	Ground	Privacy leakage	②	[139]	Secure digital identities of residents	Zero-coin	Transactions
	Ground	Malicious code, Malicious software update	④	[140]	Secure software status monitoring for IoT devices	Status monitor	Snapshot of software status
	Ground	Selfish IoT devices	④	[141]	Secure security update delivery services from vendors to IoT devices	Proof-of-distribution, Smart contract	Payment transactions
	Ground	Identity privacy leakage	④	[142]	Privacy-preserving blockchain-based reputation system	ZKP	Feedback transactions
	Ground	Malicious device firmware	④	[147]	Efficient integrity verification of light IoT device firmware	DLT	Firmware information

② means identity-related threats; ④ means service-related threats.

SmartAxiom [143] develops an embedded IoT security software by integrating blockchain with edge computing to protect data integrity, device identification, and authentication. Experimental results show that SmartAxiom is about 20% faster in running database software by moving authentication services from cloud servers to the edge of the network.

UniquID [144] offers a decentralized IAM architecture for SAG-IoT device management with high robustness. Besides, ShoCard wallet [145] is a permissioned blockchain-based IDaaS platform for secure identity verification and information sharing, where SAG-IoT users can fully control their PII in local devices data and share them with granted users.

Xage Security [146] provides a decentralized industrial control platform for trusted interactions among devices in industrial IoT. In Xage Security, the registered certificate, the fingerprint, and/or the serial number of industrial IoT devices are employed to validate identity authenticity and device ownership, thereby supporting zero-touch device provisioning.

Lessons Learned: In this subsection, we have discussed blockchain-enabled solutions for identity and device management in SAG-IoT. A comparative summary of recent blockchain-based solutions in this field is shown in Tables XI and XII. The following key lessons are learned from this subsection.

- Due to the complex and time-varying pseudonyms, attributes, and relationships of SAG-IoT devices, identity and device management in SAG-IoT are challenging. Traditional approaches for identity management, authentication, and authorization are managed by the centralized network operator, causing that users lose control of their PII. Besides, there lack unified IDaaS models in SAG-IoT for managing identities of devices and users across different administrative domains and service platforms.
- Blockchain offers a decentralized identity management solution for entity registration, key distribution, revocation, etc., in SAG-IoT, via the distributed and immutable ledgers which store the encrypted PII, attributes, and relationships for all parties. Moreover, by replacing the central "data broker" with a group of distributed entities who run the same consensus protocol to reach consensus, the security risks of PII misuse and SPoF can be eliminated.
- In blockchain-based identity management systems, it should offer sustainable benefits (e.g., ease of use, transparency, security enhancement, and economic profits) for both end-users and service providers. Moreover, blockchain-based approaches can further facilitate the "trusted and regulated" identities for digital city operating systems by adding law-compliant regulatory authorities [130].
- As the identity-related information stored in permissionless blockchains is publicly accessible, the prevention of privacy leakage should be taken into account in designing such blockchain-based approaches by leveraging access control policies and advanced cryptography tools such as ZKP (details are shown in Section IV-B9).

D. Secure Communications and Resilient Networks

By getting rid of the centralized network architecture, the distributed ledgers and consensus operations used in the decentralized blockchain systems can offer better robustness to prevent SPoF and distributed DoS (DDoS) attacks [28]. In permissionless blockchains, the one-CPU-one-vote strategy in PoW protocol and the proof of possession of valuable resources in PoW-variant protocols can efficiently mitigate the risks of Sybil attacks in the consensus process due to

TABLE XII
SUMMARY OF BLOCKCHAIN SOLUTIONS FOR IDENTITY AND DEVICE MANAGEMENT IN SAG-IOT APPLICATIONS (PART II)

	Ref.	Blockchain Type	Consensus Protocol	Advantages	Disadvantages	Smart Contract	Implementation Platform
Identity and Device Management	[133]	Public or consortium	N/A	Low authentication delay, fast handover, and fair billing	Lack real-world test of blockchain system	✓	Ethereum
	[134]	Consortium	N/A	GNSS spoofing prevention for UAVs	Rely on the one-third honest assumption	×	Ethereum
	[135]	Private	Raft	Efficient group key recovery for UAVs	High communication overhead in large-scale applications	×	Fabric
	[136]	Consortium	Modified PoW	Efficient key distribution, update, and revocation for UAVs	Rely on the honesty of head UAVs	×	N/A
	[137]	Consortium	Kafka	Low authentication delay for vehicles	Need actual tested results	×	N/A
	[130]	N/A	N/A	Secure identity management from industrial and ecosystem perspectives	Only focus on ground IoT	✓	N/A
	[131]	Consortium	PBFT	Secure generation of SSIs and deletion of illegal users' information	Low scalability for large-scale applications	×	N/A
	[132]	Consortium	N/A	Secure cross-domain authentication and key agreement in IoT	Lack consensus algorithm selection	×	N/A
	[138]	Permissioned	PBFT	Lightweight and privacy-preserving IDaaS in VCC	High latency in encrypting and delivering vehicle's PII	×	N/A
	[139]	Private	N/A	Secure identification of city residents	Low scalability	×	Ethereum
	[140]	Public	N/A	Intrusion prevention and low exception response latency	Lack consensus algorithm selection	×	BigchainDB
	[141]	Public	N/A	Sustainable security updates delivery for IoT software	Lack scalability improvements in large-scale applications	✓	Ethereum
	[142]	Public	PoS	Anonymous and transparent retailer reputation computation	Lack efficient committee partition methods	✓	Parity Ethereum
	[147]	Private	N/A	Secure IoT device firmware update and integrity verification	Lack consensus algorithm selection	×	N/A

the high cost of adversaries to fabricate or control multiple legitimate and fake identities. To resist Sybil attacks on reputation services in evaluating the trustworthiness of agents, a DAG-structured blockchain system named TrustChain [148] is presented with high scalability and openness, where transactions are reorganized into blocks and gossiped across the network. A Sybil-resistant mechanism named NetFlow is also developed to calculate the trustworthiness of agents via network theory and contribution accounting, where prior transactions are employed to compute the subjective work graphs for agents who have a partial view of the network. Experimental results show that TrustChain can resist free-riders and Sybils without any trusted intermediary.

Moreover, in permissioned blockchains, the entity enrollment process for network and resource access directly prevents the Sybil attacks due to the overwhelming cost of controlling multiple Sybil identities. Besides, the time-stamped transactions in blockchain can be naturally resistant to reply attacks. Blockchain technology can remove the risks of SPoF attacks and be beneficial for efficient and resilient SAG-IoT networking through distributed computing, storage, caching, and communication resource allocation.

1) For Space-Ground Integrated Networks: In satellite communications, the long-distance transmission can cause long transmission delay, the communication interferences can cause high error rates, the high mobility of satellites and complex space environment can cause link disruption, and hackers can conduct various cyber attacks against satellite communications to disrupt satellite services. As an effort to resolve the above challenges, Feng and Xu [149] investigate a blockchain-enhanced satellite communication system with a high level of security and adaption to intermittently connected space environments, by exploiting the delay-tolerant characteristics in space networks. Specifically, the authors integrate delay-tolerant network (DTN) structures with the blockchain network for mutual supervision and secure data communication. Moreover, two smart contracts are designed for critical satellite data management and network degradation handling, i.e., the satellite user profile contract for access control of satellite information and the satellite group profile contract for audit log sharing.

Different from [149], Zhang and Liu [150] combine satellite broadcasting techniques with the blockchain architecture to address the low throughput and high overhead in blockchain-based satellite communications. Particularly, the authors reap the advantage of satellite broadcasting as the communication channels of the blockchain system for information propagation and consensus missions, aimed to improve the throughput of large-scale blockchain-based space-ground applications. As shown in the simulated satellite broadcasting link with 20 Gbps bandwidth, it yields about a 6% packet drop rate and 6 million TPS with 300 bytes transaction size.

2) For Air-Ground Integrated Networks: In modern UAV networks, a current research trend is ultra-reliability (in terms of availability, connectivity, and survivability). By incorporating neural networks into blockchain-based UAV networks, Sharma *et al.* [151] develop the neural-blockchain to provide ultra-reliable communications for UAV swarms under the edge computing paradigm by transferring conventional hierarchical layout into a flat one (via blockchain). In the developed neural model, the UAVs are deployed to support on-demand data retrieval and reduce failure rates, while relevant factors including flyby time, connectivity probability, and energy consumption are taken into account. Findings from the simulation show that the proposed scheme reaches 99% connectivity probability, 60.34% energy saving, and over 90% survivability.

Different from [151], Abichandani *et al.* [152] carry out extensive experimental validations on an Ethereum blockchain-based architecture for securing communications and data transmissions among multiple small UAVs, where three DJI M100 quadrotors are involved in the experiment to share sensed images in the flight. In their architecture, each UAV equipped with GPU, Wi-Fi antenna, and so on acts as the miner in the blockchain. Also, the smart contracts written by Solidity are deployed to ensure that only the intended recipients can receive the specific image captured by UAVs. Findings from the experiment demonstrate that the PoA consensus protocol offers lower image transfer time compared with PoW, and the proposed blockchain-enabled UAV communication system is proved to resist communication disruptions.

Unlike [152], Gai *et al.* [153] propose to combine the ABE cryptography with blockchain systems. In their work, the ABE cryptography is leveraged to support multi-party authentication and trusted group communications in UAV networks. The blockchain platform is employed to record communication activities among UAVs while the smart contract serves as the attribute manager. Two threats: facility-related attack (i.e., the controller/station can be compromised) and communication-related attack (i.e., part of UAV devices are compromised) are considered in their work. Security analysis proves the defense against facility- and communication-related attacks, and the simulation results validate its feasibility in terms of time cost and Gas cost in transaction and smart contract execution.

Apart from the cryptography tools, the SDN can implement a programmable and agile network by centralizing data routing on the control plane, thereby alleviating the complexity of the data plane and improving the network flexibility. Fig. 22 shows an example of SDN-based blockchain-IoT architecture. By reaping the advantages of blockchain and SDN technologies, Hu *et al.* [155] propose a scheme named SUV to quickly construct agile and resilient UAV networks based on the practical environment and service requirements. In their scheme, the blockchain is utilized to build a logically centralized but physically distributed control plane in software-defined UAV networks to facilitate configuration management and routing computing.

In addition, the integration of blockchain with IoT can facilitate resilient and flexible emergency networks during or after the events of man-made or natural disasters. For example, in [36], drones are utilized to perform immediate rescue missions due to their fast deployment and flexible mobilities, while a lightweight blockchain is deployed over drone swarms to secure the delivery of rescue commands, road damage, and maps of affected areas to ground relief networks. Moreover, a credit-based DPoS consensus algorithm is developed in [36] to efficiently reach consensus between UAVs and vehicles under disasters. Simulation results show the proposed approach in [36] can motivate nodes' participation and coordination while improving the secure witness node ratio (i.e., the ratio of legitimate consensus nodes to the total number of elected witnesses in the consensus committee).

3) For Ground IoT Networks: With the rapid growth of IoV, the conventional cloud-based IoV approach faces huge challenges in secure distributed storage for massive data, intelligent network management, and data security; meanwhile, the central server can be a bottleneck of the entire system. To address this issue, Gai *et al.* [156] consolidate the promising edge computing technology into blockchain-based IoT networking to improve the scalability of the blockchain-IoT system. To supplement the cloud computing architecture, edge computing nodes are deployed in their system to offload the heavy blockchain tasks (e.g., running consensus protocol, and ledger management) from resource-limited IoT devices. Besides, DP techniques are implemented in data aggregation on edge machines to prevent privacy leakage from data mining attacks on the blocks. Evaluations conducted on the Ethereum platform validate the performance of the proposed approach in terms of privacy protection and energy-saving.

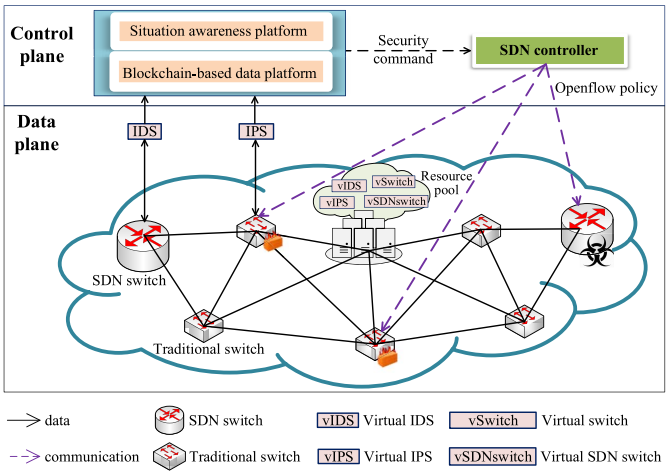


Fig. 22. An example of SDN-based blockchain-IoT architecture. Here, network statistics (e.g., logs) of SDN devices (e.g., SDN switch and traditional switch) can be periodically collected from the data plane by security devices (e.g., intrusion detection system (IDS) and intrusion protection system (IPS)) via a standardized interface such as OpenFlow [4], and then analysed in the situation awareness platform in control plane to detect any network anomalies. Moreover, through network function virtualization (NFV) [154], virtualized network resources (e.g., virtual firewall, virtual IDS, and virtual IPS) can form resource pools and dynamically allocated in accordance with real-time users' demands. Once any anomaly is detected, security commands will be delivered to instruct the controller how to reprogram the data plane for alleviating it.

Different from [156], Jiang *et al.* [157] concentrate on an optimized blockchain-based architecture for vehicular networking, where multiple sub-blockchain networks are considered for the distributed storage of IoV data. In their architecture, vehicle data is classified into five types and is stored into different sub-blockchains according to IoV applications, i.e., vehicle driving data, vehicle sensory data, user private data (e.g., in-car recordings), e-commerce and transaction data (e.g., car washing and charging), and vehicle insurance data. An outward transmission model is also established with theoretical and numerical analysis to prove the feasibility of the proposed architecture.

Apart from the resilient emergency networking in [36], it is significant to coordinate the collaboration among various parties (e.g., volunteers) in their relief efforts to offer

TABLE XIII
SUMMARY OF BLOCKCHAIN SOLUTIONS FOR SECURE COMMUNICATIONS AND RESILIENT NETWORKS IN SAG-IOT APPLICATIONS (PART I)

	Layers	Security Threats	Threat Type	Ref.	Purposes	Technology Used in/with Blockchain	Data in Blockchain
Secure Communications and Resilient Networks	Space-Ground Integrated	Flooding issue, Unauthorized access	③	[149]	Secure satellite communication system under intermittently connected space environments	Smart contract	Transactions
	Space-Ground Integrated	Low throughput of blockchain	③	[150]	Improve blockchain throughput in large-scale applications using satellite communications	Satellite broadcasting	Transactions
	Air-Ground Integrated	Unreliable communication	③	[151]	On-demand drone-caching under ultrareliable communication	Neural-blockchain	Caching transactions
	Air-Ground Integrated	Insecure UAV communication	③	[152]	Secure communications and data transmissions among multiple small UAVs	IPFS, Smart contract	Captured images
	Air-Ground Integrated	Untrusted UAV communications	③	[153]	Trusted group communications for UAVs with multi-party authentication	ABE	Communication activities
	Air-Ground Integrated	SPoF, Lack flexibility	③	[155]	Quickly build agile and resilient UAV networks based on service requirements	SDN	Configurations, Routing tables
	Air-Ground Integrated	Misbehavior tampering, Untrusted environments	③	[36]	Build resilient emergency network and secure wireless transmissions	Credit-based DPoS, Reinforcement learning	Data transactions, Misbehaviors
	Ground	Sybil attack, Free-riding	③	[148]	Sybil-resistant blockchain mechanism in reputation evaluation of agents	DAG blockchain	Financial transactions
	Ground	Insider attack, Identity theft	③	[156]	Privacy-preserving edge-based IoT system for task allocation	Smart contract, Differential privacy	Task transactions
	Ground	SPoF	③	[157]	Secure and intelligent vehicle networking for data distribution	DLT	Vehicle-related data
	Ground	Uncoordinated rescue	③	[158]	Speed up availability of needed services and materials among volunteers	Token, Regulation	Financial transactions

③ means communication-related threats.

rapid and efficient emergency response across different geographic disaster sites. In this field, blockchain can bring coordination and collaboration among all involved parties by providing an immutable and trusted ledger, as well as potential tokenization solutions to incentivize volunteers' efforts. For example, a federated blockchain model is introduced by Badarudin *et al.* [158] to enhance the availability and transparency of materials and services required for first responders and community volunteers to carry out the search, rescue, and recovery missions under disasters. In their approach, monetary tokens are rewarded as compensations for rescuers, and the usage activities of tokens are publicly verified by all parties. Besides, the disaster response agencies (e.g., fire rescue, police, and military authorities) form the regulator group to audit and monitor illegal activities such as money laundering.

Lessons Learned: In this subsection, we have discussed blockchain-enabled solutions for secure communications and resilient networks in SAG-IoT. A comparison of recent blockchain-based solutions in this field is presented in Tables XIII and XIV. The following key lessons are learned from this subsection.

- In SAG-IoT, the fast-changing topology and potential link disruptions caused by nodes' high mobility and multi-segment HetNet environment raise huge challenges to build resilient networks. Blockchain can provide high robustness and fault tolerance for devices in the complex SAG-IoT applications (e.g., emergency services) to facilitate secure communications and establish resilient networks. Moreover, the blockchain-based solutions are fully distributed to adapt to the fast-changing SAG-IoT, thereby eliminating the SPoF risks caused by the centralized network architecture.
- The deployment of smart contracts can be beneficial for cooperative networking and resource allocation (in terms of computing, storage, caching, and communication) for resource-constrained SAG-IoT devices, where the trading transactions can be immutably recorded in the blockchain ledgers for public audit.
- To facilitate agile and intelligent routing and networking in the fast-growing SAG-IoT landscape, emerging techniques such as network slicing, NFV, and SDN can be further integrated with future blockchain-empowered SAG-IoT systems (details are shown in Section V-A and Section V-B).

E. Data, Product, and Ownership Provenance

1) Problems With Traditional SAG-IoT Provenance Solutions: Provenance refers to the metadata of evidence data that tracks the originality of the data, product, and corresponding operations in the life-cycle of SAG-IoT services. The metadata contains the involved parties, input records, and the processes or activities on the data and product. Providing provenance ensures data accountability, product traceability, access violation, and forensic capabilities for network administrators. Traditional data provenance solutions in the cloud-based SAG-IoT are mainly based on user logging and data auditing conducted on the centralized authority. For example, a data provenance tool named PASS [159] collects and processes the data related to the operations conducted at the system level. The S2Logger [160] offers data tracking services in cloud environments using end-to-end resource monitoring at the file level. However, current data provenance solutions come with three issues, i.e., high complexity, SPoF risk, and privacy violation.

- Firstly, tracking data, product, and resource usage can be complex, since (i) the data can be replicated in various areas for high availability; (ii) the resources may be migrated to other machines for load balancing; and (iii) the life-cycle of a product generally involves various processes including manufacturing, distribution, and selling. Moreover, the deployment of security techniques, e.g., encryption, IDS, IPS, and signatures adds additional system complexity.
- Secondly, in current approaches, a central TTP is required to store the logging and monitoring information

TABLE XIV
SUMMARY OF BLOCKCHAIN SOLUTIONS FOR SECURE COMMUNICATIONS AND RESILIENT NETWORKS IN SAG-IOT APPLICATIONS (PART II)

	Ref.	Blockchain Type	Consensus Protocol	Advantages	Disadvantages	Smart Contract	Implementation Platform
Secure Communications and Resilient Networks	[149]	N/A	N/A	Secure delay-tolerant satellite communication networks	Lack consensus algorithm selection	✓	Ethereum
	[150]	Public	N/A	Reduced communication delay by integrating with satellite broadcasting	Suitable for domestic/continental applications	×	N/A
	[151]	Public	N/A	Low energy consumption and high failure rate of UAV networks	Lack consensus algorithm selection	×	N/A
	[152]	Public	PoA & PoW	Communication disruption resistance using real-world tests	Lack blockchain optimizations	✓	Ethereum
	[153]	Consortium	PBFT	Secure ABE authentication in group communications for UAVs	Lack proactive incident response and forensic investigation	✓	Ethereum
	[155]	Consortium	PBFT	Eliminate the fragility and SPoF of SDN-based IoT	Lack multi-dimensional resource management in UAV networks	✓	N/A
	[36]	Consortium	Modified DPoS	Lightweight blockchain implementation for UAVs in disasters	Lack real-time misbehavior detection in blockchain	×	N/A
	[148]	Public	DAG	High scalability and Sybil-resistance	Lack large-scale deployment and testing	×	A prototype
	[156]	Public	N/A	Low energy consumption and privacy preservation in industrial IoT	Lack large-scale deployment and testing	✓	Ethereum
	[157]	Public	PoW	Theoretical transmission modeling of vehicle blockchain data	Lack analysis of traffic and channel reliability in IoV	✓	Bitcoin
	[158]	Consortium	Proof of vote	Coordinated material management in disaster rescue	Lack ownership provenance and misbehavior tracing	✓	Ethereum

for provenance services, which is a potential SPoF. Moreover, under existing centralized approaches, it is difficult to ensure that the provenance information has not been tampered, falsified, or altered.

- Thirdly, the provenance requires the exposure of ownership and originality of data, products, and resources, which may violate user privacy in such a tracking process. Thereby, in current researches, enforcing data provenance without privacy violation is a challenging issue to be resolved.

2) Blockchain-Based SAG-IoT Provenance Solutions in Research: Blockchain offers a potential solution for data provenance services by storing the evidence of the originality of the data, product, and operations into transactions in the ledgers. The publicly shared ledger among untrusted IoT entities can guarantee that all historical transactions are reliable, transparent, and auditable [22]. For example, in the food supply, all raw materials produced by different farmers are associated with RFID tags that upload the information about the raw materials to the tailored blockchain platform [54]. Then, customers can trace the provenance of their purchased food and trust the provenance information due to the immutability of blockchain. In [54], an RFID tag offers a unique identity of the raw material and a 900-MHz sensor is equipped for real-time quality monitoring; meanwhile, the blockchain helps establish a tamper-resistant distributed database of food packages. A prototype of an RFID-integrated sensor is deployed for performance evaluation in terms of communication cost and fake transaction detection ratio.

However, in [54], the RFID tags for ownership management can be easily cloned and their genuineness cannot be guaranteed. To resolve this issue, Toyoda *et al.* [55] propose a blockchain-based platform based on Ethereum for efficient product ownership management and anti-counterfeits in the supply chain. Each participant can publicly audit the unique "proof of possession of products", which is recorded in the blockchain as cryptographic evidences. The authors also devise a full-fledged protocol to enforce all parties involved in the supply chain to prove and transfer their ownerships of products attached with RFID tags. Besides, as the blockchain records a sequence of time-stamped transactions and each recorded transaction is impossible to be withdrawn, altered, or deleted, the ownership of digital assets can be securely identified without repudiation. As such, the ownership of digital assets (e.g., copyrighted music and car) can be recorded in the blockchain via a unique certificate before sharing them, and the usage activities of digital assets can be recorded in subsequent transactions.

However, the proposed platform in [55] lacks prototype design and real-world implementation. The following two works [56], [162] design a real-world prototype for permissionless blockchain and permissioned blockchain, respectively. To enable efficient provenance of electronic parts during the process of manufacturing, distribution, and selling, Cui *et al.* [56] build a blockchain system atop Hyperledger Fabric, where a confirmation-based ownership transfer mechanism with two-phase transaction is developed to ensure ownership traceability. In [162], the physical producing process of a new product out of existing components can be projected onto the Ethereum blockchain ledgers by creating corresponding product tokens. Accordingly, the input and manufactured goods can be traced during the complex manufacturing process.

However, the aforementioned works [54]–[56], [162] ignore the quality traceability in food/product provenance and suffer low scalability. To further promote food provenance and quality traceability while preventing food mislabeling, as shown in Fig. 23, Malik *et al.* [161] establish a permissioned blockchain ecosystem named ProductChain among various food supply entities in the entire process of food supply chain, where the final product can be linked to raw ingredients involved in the supply chain via the transaction vocabulary. Users' read/write privileges (i.e., access rights) of on-chain information are managed by the proposed tiered architecture, while the blockchain sharding is applied to improve system scalability. By using non-fungible digital tokens, every batch of manufactured

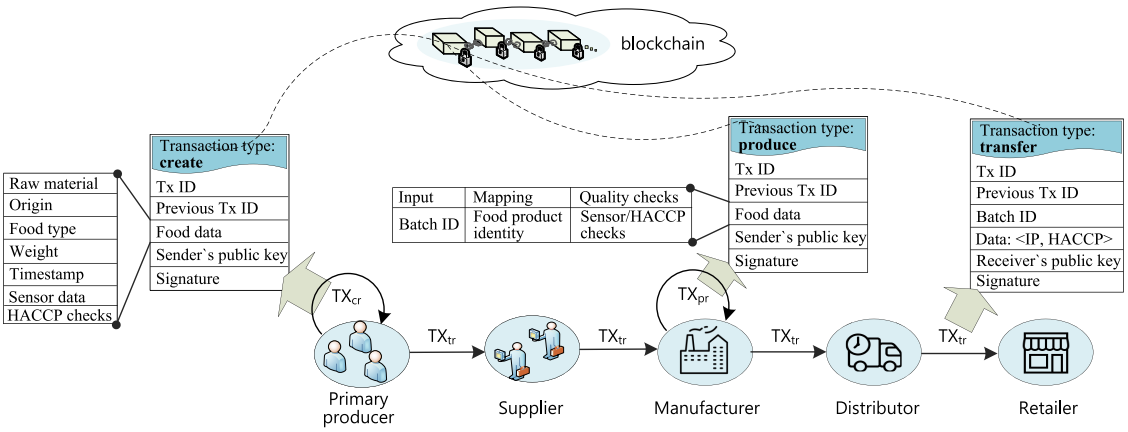


Fig. 23. Structure of the entire transaction flow in the blockchain-enabled food supply chain (i.e., ProductChain [161]). In ProductChain, three types of transactions are involved (i.e., create, transfer and produce) among primary producers, suppliers, manufacturers, logistical distributors, and retailers. The primary producer issues a *create* transaction TX_{cr} after producing a raw material and then sends a *transfer* transaction TX_{tr} to the supplier. TX_{tr} describes the ownership transfer between entities in the supply chain and has the same structure with TX_{cr}. The manufacturer generates a *produce* transaction TX_{pr} which binds the batch ID to the final product identity. Each bundle of raw material is assigned with a unique batch ID. TX_{pr} describes the mapping relation of batches of multiple raw materials with the final product.

products and their components needed in manufacturing can be digitalized and tokenized.

In the blockchain, once the transactions (e.g., payment operation, transfer of a digital asset, and the usage record of copyrighted music) are completed and committed, the cryptographic evidence will reside on the blockchain with auditable and immutable trails [84]. By leveraging these salient features, the authors in [111] and [163] present blockchain-based solutions for charging pile sharing and ride sharing in sharing economy, respectively. To facilitate the energy charging of EVs in cities without sufficient charging infrastructures, Wang *et al.* [111] propose a permissioned blockchain-based private charging pile sharing framework. A matching-coalition game is also exploited to formulate their cooperations and cooperations in energy interactions, where users are identified by their public keys to facilitate punish countermeasures to misbehaving entities. To defend against SpoF, DDoS, and Sybil attacks in ride-sharing services, Baza *et al.* [163] construct a decentralized ride-sharing platform based on permissionless blockchain, where a time-locked deposit algorithm is devised in smart contract systems by utilizing zero-knowledge proof (ZKP) to prevent multiple malicious ride requests or offers without any commitment.

In both works [111], [163], reputation models are adopted based on the aggregated rating or historical behaviors to evaluate the trustworthiness of users in the blockchain system. As the transactions are ordered by their timestamps and are compressed into a tree structure, the historical activities on specific content, product, or IoT device in the sharing economy can be traceable. Besides, compared with the centralized architecture, the operation fee can be greatly saved under the decentralized architecture. However, the recorded provenance information in the blockchain is publicly available, such that privacy issues may be triggered. To preserve the user privacy in ownership provenance in the shared economy, Wang *et al.* [164] develop a blockchain-enabled private parking spot sharing scheme with decentralized privacy protection functions for users during the identity and message authentication process. Besides, in [164], a variant of Monero is adopted to enhance user privacy in the blockchain using confidential anonymous payment and anonymous credentials.

Still, the cooperation among heterogeneous IoT devices is absent in most of the existing works in tracking the provenance of data, products, and ownership. To facilitate the collaboration (e.g., joint research project developing on a shared cloud repository) among IoT users in cloud storage platforms, Ritzdorf *et al.* [165] introduce the concept of *shared ownership* where a file is jointly owned by *n* users and the access request of each file should receive consents from a predefined threshold of *t* owners. A blockchain-based instantiation is also investigated, where the blockchain is adopted to achieve consensus on access control decisions among untrusted collaborators.

3) Blockchain-Based SAG-IoT Provenance Solutions in Industry: In industry, blockchain has been widely used to provide traceable and transparent logistics and supply chain information for users. For example, WaltonChain [166] is a decentralized supply chain management platform which integrates RFID technology with IoT for efficient product tracking and provenance in the life-cycle of IoT services. BlockVerify [167] targets anti-counterfeiting in various applications (e.g., medicine, luxury goods, and electronics industry) by recording the transfer of ownership based on blockchain technology.

Lessons Learned: In this subsection, we have discussed blockchain-enabled solutions for data, product, and ownership provenance in SAG-IoT. Tables XV and XVI compare the recent blockchain-based solutions in this field from several perspectives. In the following, the key lessons learned from this subsection are discussed.

- Provenance is essential to recognize the originality, timing, and validity of data and product, as well as tracking the data ownerships and recording the changes. Conventional provenance technologies are

TABLE XV
SUMMARY OF BLOCKCHAIN SOLUTIONS FOR DATA, PRODUCT, AND OWNERSHIP PROVENANCE IN SAG-IOT APPLICATIONS (PART I)

	Layers	Security Threats	Threat Type	Ref.	Purposes	Technology Used in/with Blockchain	Data in Blockchain
Data, Product, and Ownership Provenance	Ground	Fake identity, Provenance tampering	④	[54]	Transparent food supply chain with real time quality monitoring	Proof of object	Food package information
	Ground	Fraud, Counterfeits of RFID tags	④	[55]	Secure product and ownership management in supply chain	Smart contract, ZKP	Payment transactions
	Ground	Unauthorized access, Illegal device transfer	④	[56]	Traceable electronic components provenance in supply chain	Hyperledger Fabric	Transfer of device
	Ground	Provenance tampering	④	[162]	Traceable supply chain in manufacturing processes	EVM	Product token
	Ground	Food mislabeling, Information leakage	④	[161]	Transparent food provenance with confidential trade flows	Sharding	Food-related information
	Ground	Location cheating, Eavesdropping	④	[163]	Protect rider/driver privacy and ensure fair payment	ZKP, Time-locked deposit	Payment transactions
	Ground	Information leakage, Identity theft	④	[164]	Privacy-preserving private parking spot sharing without trusted agent	ZKP, Anonymous payment	Payment transactions
	Ground	Unauthorized access, Collusion attack	④	[165]	Distributed enforcement of shared ownership in cloud	Smart contract	File access rights

④ means service-related threats.

TABLE XVI
SUMMARY OF BLOCKCHAIN SOLUTIONS FOR DATA, PRODUCT, AND OWNERSHIP PROVENANCE IN SAG-IOT APPLICATIONS (PART II)

	Ref.	Blockchain Type	Consensus Protocol	Advantages	Disadvantages	Smart Contract	Implementation Platform
Data, Product, and Ownership Provenance	[54]	Public	Proof of object	Tamper-proof food package evidence storage	Threats of cloning RFID tags and hardware security	×	N/A
	[55]	Public	PoW	Efficient product ownership management with anti-counterfeits	Lack prototype design and real-world implementation	×	Ethereum
	[56]	Consortium	Raft	Protect the supply chain from counterfeit IoT devices	Lack exploration of physically unclonable functions (PUF) in product provenance	✓	Fabric
	[162]	Public	N/A	Transparent supply chain with comprehensible production information	Lack of payments and market incentives	✓	Ethereum
	[161]	Consortium	BFT	Improved auditability for food quality	Low scalability of blockchain-based system	×	A prototype
	[163]	Public	N/A	Fair and private pay-as-you-drive in ride sharing	High computation cost	✓	Ethereum
	[164]	Consortium	N/A	Anonymous authentication and payment in parking spot sharing	Lack real-world system implementation	×	N/A
	[165]	Public	N/A	Distributed enforcement of shared ownership among cloud storage providers	Lack thorough performance testing	✓	Ethereum

mostly centralized, complex, and can suffer SPoF risks and privacy violations for sensitive information.

- In blockchain-based supply chain provenance, blockchain can offer trusted and shared ledgers that record the evidence of data/product originality and the corresponding events (e.g., ownership change) in the system to facilitate transparent provenance services.
- The sophisticated cryptography technologies (e.g., ABE-based access control) in the blockchain system can help users' privacy protection in data/product provenance services. The complexity of computation in [163] and communication in [165] demonstrate that it requires more research efforts for designing lightweight cryptography and the proper utilization of smart contracts on blockchain-based provenance systems.

F. Digital Forensics and System Regulations

In digital forensics, it is crucial to guarantee that law enforcement agencies can accurately integrate diverse sources of data to trace nodes' misbehaviors and reconstruct the facts without violating the privacy rights of related suspects. The decentralized blockchain can well match the provenance and integrity requirements of digital forensics and misbehavior tracing in evidence collection across jurisdictional borders. The details of evidence identification, extraction, storage, analysis, and misbehavior records are transparently and immutably recorded in the blockchain, while the provenance and traceability of evidence items can also be guaranteed.

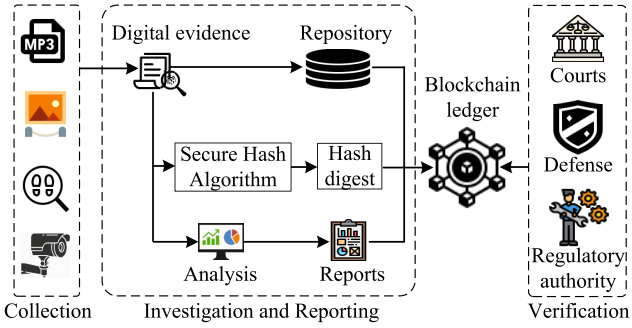


Fig. 24. Structure of the blockchain-based IoT forensics management for chain of custody (CoC) in [61]. Three phases are involved in the digital forensics process, i.e., evidence collection, investigation and reporting, and verification. In the first phase, nodes collect all the relevant multi-source heterogeneous evidence information. In the second phase, the critical information (e.g., forensics reports and hash digests) is stored in the on-chain ledger while other non-critical information (e.g., raw evidence items and analysis results) is stored in the off-chain repository. In the third phase, the court and regulatory authority can verify the forensics reports by synchronizing the latest blockchain ledgers.

For example, by employing blockchain technologies and considering social effects, a decentralized IoT forensics

investigation framework is developed by Li *et al.* [61] to offer full data provenance and privacy-preserving evidence item examination between evidential entitles and examiners, as shown in Fig. 24. The digital transactional evidence together with their provenance information is compressed into a Merkel tree structure and recorded into hash-chained blocks to facilitate evidence identification, verification, and acquisition. The evidence items are encrypted, identified by the digital fingerprints, and are only accessible for authorized entities. The proposed blockchain serves as a browser to search and view the recorded evidence where specific restrictions are specified based on the access policies.

However, the work in [61] has a drawback that both efficient collection of high-quality digital evidence and the forensics during the entire life-cycle of IoT services are not considered. To partially address this drawback, Le *et al.* [65] investigate a blockchain-enabled IoT forensics architecture to store all events during the entire life cycle of digital evidence while ensuring collaborative and high-quality evidence collection. In their framework, the blockchain serves as the digital chain of custody (CoC) across several distrustful IoT devices to form the overall flow of events by linking all evidences with guaranteed transparency, non-repudiation, and traceability. Meanwhile, the smart contracts enable automatic and collaborative digital evidence reporting and recording into a CoC for IoT devices. A practical one-time signature-based cryptographic approach is also designed to preserve devices' identity. However, the implementation on IoT testbeds is still needed in this approach to validate its reliability.

Different from [65], Pourvahab and Ekbatanifard [168] combine SDN with the CoC architecture to prevent evidence deletion or alteration while ensuring data integrity in SDN-IoT networks. In their approach, an SDN-enabled CoC architecture for IoT is established, where three traffic types of flow table rules are considered, i.e., file transfer protocol (FTP), voice over Internet protocol (VoIP), and hypertext transfer protocol (HTTP). In their approach, the neuro multi-fuzzy algorithm is employed to classify malicious packets for attacker detection, and the logs of events as well as the collected evidence are stored on the blockchain for analysis by the forensic team. By using simulations, the feasibility of the proposed approach is validated in terms of the response time (i.e., the time to receive the response from IoT devices for requested services), throughput (defined as the successfully transmitted packets between devices in a given time), and processing time (defined as the packet handling time from the gateway to SDN control plane). Still, the reliability of CoC in the evidence acquisition process could be further improved by deploying smart contract scripts.

Unlike the above work in [168], smart contracts are deployed by Lu *et al.* [169] to perform automated price auditing in ride-hailing services (e.g., Didi and Uber) to mitigate price discrimination and ensure accountability. In ride-hailing services, malicious service providers (SPs) may acquire illegal profits by price discrimination (or called "personalized pricing"), by manipulating the price for costumers unfairly according to their profiling information such as race and gender. Moreover, as prices can fluctuate according to various traveling factors, e.g., traffic conditions, destinations, and timing, it is hard to detect whether SPs manipulatively change prices based on users' characteristics. Generally, the unfairly discriminated price causes individuals to lose trust in online SPs in a long run. To resolve this issue, the authors in [169] propose a decentralized and automated price auditing scheme named Spas by defining and executing self-enforcing contracts (i.e., Price Policy Contracts (PPC) and Price Auditing Contracts (PAC)). Specifically, the PPC can be deployed by SPs to publish their current price policies; then, the PAC can be invoked to compute the actual price by using corresponding price policies. A prototype of Spas is instantiated on Hyperledger Fabric to test its performance in terms of blockchain throughput and latency of different operations.

Apart from the price auditing in ride-hailing, blockchain can also facilitate post-accident forensics in IoV among drivers, insurance companies, maintenance SPs, and manufacturers. By collecting vehicle-related data from neighboring cooperative vehicles, Cebe *et al.* [62] introduce a permissioned blockchain-based framework for post-accident forensics in autonomous driving to reveal the faulty party. As all necessary evidences gathered from all related parties (e.g., drivers, vehicle manufacturers, and law enforcement agencies) are recorded on ledgers, efficient vehicular forensics solutions for an accident can be generated without relying on a trusted agent. Besides, blockchain technologies can promote the cooperation of participants in evidence collection and identification by offering reliable incentives and contribution recording. However, the above two works lack efficient punishment or incentive mechanisms to suppress adversarial actors (i.e., insider attackers), and they can only be applicable in the IoV context.

Apart from the ground IoT networks, blockchain can also be beneficial for efficient system regulations in the space networks and air networks in SAG-IoT.

1) For Space-Ground Integrated Networks: In satellite-assisted IoV, location-based services (LBS) can provide convenient e-commerce, mobile positioning, etc., for vehicular users. However, due to the open communication environment and complex network structure, protecting vehicles' privacy while maintaining high communication efficiency is a challenging issue. As an effort to address this problem, Li *et al.* [170] propose a blockchain-enabled privacy-preserving model for efficient and reliable LBS in satellite-assisted IoV, where a K-anonymous algorithm is developed for location privacy protection, and a trust evaluation algorithm is developed for detection of vehicles' misbehaviors in anonymous region construction. In the proposed blockchain system, RSUs serve as the APs of ground IoV and are responsible for trust management and blockchain maintenance. However, the detailed implementation of DAG-based consensus is missing.

2) For Air Networks: In air networks, air traffic management and flying policy enforcement are essential for UAVs to avoid collision and ensure public safety. In [171], Rahman *et al.*. investigate a typical UAV-based delivery scenario and exploit a private blockchain-based system to ensure air traffic management and policy compliance of UAVs' flights. In their system, the flight paths of UAVs at different times are pre-allocated, and the flying policies are implemented and enforced by the smart contracts to (i) avoid

TABLE XVII
SUMMARY OF BLOCKCHAIN SOLUTIONS FOR DIGITAL FORENSICS AND SYSTEM REGULATIONS IN SAG-IOT APPLICATIONS (PART I)

	Layers	Security Threats	Threat Type	Ref.	Purposes	Technology Used in/with Blockchain	Data in Blockchain
Digital Forensics and System Regulations	Space-Ground Integrated	Privacy leakage	⑤	[170]	Reliable location-based services with misbehavior detection in satellite-assisted IoV	DAG, Trust evaluation	Misbehaviors, Trust scores
	Space-Ground Integrated	Untrusted inter-satellite communication	⑤	[174]	Trusted data routing and reduced data relay latency in a constellation of small satellites	Reputation mechanism	Behavior records
	Air	Lack trust, DDoS	⑤	[175]	Secure air traffic management among multiple operators	Cryptography	Transactions
	Air	Lack regulations	⑤	[171]	Ensure policy compliance of UAVs' flights and restrict UAVs' access to unauthorized areas	Smart contract	Flight policies
	Air	Compromised UAVs	⑤	[172]	Real-time detection of UAVs' abnormal behaviors	Trust mechanism	Trust scores
	Ground	Evidence provenance, Privacy leakage	⑤	[61]	Trustworthy and privacy-preserving digital forensics in social IoT	N/A	Evidence identification
	Ground	Opaque forensics	⑤	[65]	Transparent IoT forensics during the entire life-cycle of digital evidence	BFT, Smart contract	Forensic data
	Ground	Evidence deletion, Evidence alteration	⑤	[168]	Secure and distributed forensic in SDN	PoW, Fuzzy logic	Evidence data
	Ground	Unfair price	⑤	[169]	Fair payment in ride-hailing services	Smart contract	Price policy
	Ground	Single point of trust, Privacy leakage	⑤	[62]	Trustworthy forensic process of traffic accidents in autonomous driving	Fuzzy logic	Forensic data

⑤ means governance-related threats.

TABLE XVIII
SUMMARY OF BLOCKCHAIN SOLUTIONS FOR DIGITAL FORENSICS AND SYSTEM REGULATIONS IN SAG-IOT APPLICATIONS (PART II)

	Ref.	Blockchain Type	Consensus Protocol	Advantages	Disadvantages	Smart Contract	Implementation Platform
Digital Forensics and System Regulations	[170]	Consortium	Conflux	Privacy-preserving and efficient LBS for vehicular users	Lack detailed implementation of DAG-based consensus	×	Fabric
	[174]	Consortium	N/A	Resilient reputation-based routing in satellite relay networks	Lack analysis of network dynamics	×	Fabric
	[175]	Public	Modified PoW	Efficient flight plan for UAVs with communication security	High transmission latency and computation cost	×	N/A
	[171]	Private	N/A	Moderate scalability for policy-compliant UAV flights	Lack real-world implementation and test	✓	Ethereum
	[172]	Consortium	N/A	Distributed detection of UAVs' abnormal activities	Lack real implementation and test	×	N/A
	[170]	Public	PoW	Traceable IoT forensic investigation for evidential entitles and examiners	Vulnerable to 51% majority attack	✓	N/A
	[65]	Permissioned	BFT	Trusted and cooperative IoT forensic evidence collection	Lack reliability test on an IoT testbed	✓	N/A
	[168]	Public	PoW	Efficient forensic in IoT with multiple SDN controllers	Lack evidence acquisition using smart contracts	×	Bitcoin
	[169]	Consortium	Kafka	Automated price auditing to resist price discrimination in ride-hailing	Hard to acquire accurate location data due to privacy issues	✓	Fabric
	[62]	Consortium	PBFT	Post-accident forensics with low storage and computing overheads	Lack efficient punishment or incentives	×	N/A

collisions during flights and (ii) restrict UAVs' access to unauthorized areas for citizens' privacy protection. Meanwhile, UAVs' misbehaviors are immutably recorded in the blockchain ledgers, thereby non-compliant UAVs can be identified to punish the corresponding SP of UAV.

However, the detailed misbehaving UAV detection and identification process are missing in [171]. To efficiently detect the compromised UAVs in the dynamic network, Keshavarz *et al.* [172] design a decentralized trust management mechanism by tracking and storing UAVs' misbehavior records and trust scores in the tamper-resistant blockchain ledgers. The behaviors of UAVs in task performing are regularly monitored by a group of collaborative observers, and the trustworthiness of each observer is evaluated based on its neighbors' recommendations. Simulation results demonstrate that the proposed mechanism attains a high detection accuracy of malicious UAV agents and compromised observers.

3) Blockchain-Based SAG-IoT Regulation Solutions in Industry: The startup AirUTM [173] is a scalable air traffic management platform built on the public blockchain, which aims to offer remote ID management, trusted aerial data sharing, and transparent monetization by deploying smart contracts.

Lessons Learned: In this subsection, we have discussed blockchain-enabled solutions for digital forensics and system regulations in SAG-IoT. A comparison of current blockchain-enabled solutions in this field is summarized in Tables XVII and XVIII. The key lessons learned from this subsection are discussed below.

- In traditional forensics approaches, the authorities have to manually collect all the evidence items from various involved parties and store them in a central repository for analysis. This investigation procedure is not only time- and labor-consuming but also error-prone. Moreover, this process lacks transparency and accountability to declare policy compliance for the public.
- The blockchain technology can facilitate digital forensics services in SAG-IoT by providing a transparent and immutable ledger to record related evidences and regulation policies among distrustful parties. Besides, by defining and enforcing smart contracts atop the blockchain system, automated evidence collection, analysis, and

policy compliance verification can be enabled in a fully distributed fashion.
- In blockchain-based forensics and regulation services, the system throughput and scalability are at a relatively low level, compared with conventional centralized approaches. Moreover, the privacy concerns and intrinsic vulnerabilities issues related to various blockchain platforms need more research efforts (details are shown in Section IV-A).

IV. Blockchain Challenges and Tailored Blockchain Approaches For SAG-IoT

Despite the salient features of blockchain technology, it still has a series of challenging issues that limit the practicality of blockchain for securing SAG-IoT applications discussed in the previous section. In this section, we first elaborate on the challenges in the integration of blockchain and SAG-IoT, and then investigate existing/potential tailored blockchain solutions for SAG-IoT security.

A. Blockchain Challenges

The integration of blockchain technology with SAG-IoT is non-trivial. Blockchain is originally designed for P2P homogeneous networks with powerful computers, which is far from the SAG-IoT reality. The inherent characteristics of SAG-IoT systems along with the limitations of blockchain technology pose a series of fundamental challenges when incorporating blockchain into SAG-IoT networks. To harness the potentials of blockchain to resolve the SAG-IoT security, the following challenges need to be considered.

1) Resource Limitation: The blockchain can be resource-hungry (e.g., computation, storage, communication, and energy), and is unaffordable for lightweight SAG-IoT devices. For example, the sizes of the whole Bitcoin and Ethereum blockchain are nearly 150 GB and 400 GB, respectively [127]. With all blocks in its storage, a full node is able to query and verify transactions [86], which causes heavy loads of storage and computation for SAG-IoT devices. Besides, lightweight SAG-IoT devices are unable to run computation-intensive PoW-based blockchains. For example, Raspberry Pi3, as a powerful IoT device, only supports roughly 100 hash/s [176], which is far lower than the required 10^{19} hash/s in the case of Bitcoin. Although SAG-IoT devices can opt to run as light nodes to ease storage and computation burdens, they still need to store the headers of blocks. In Bitcoin and Ethereum, all headers are nearly 38 MB and 2 GB, respectively. Besides, to generate new transactions, SAG-IoT devices need historical block data (e.g., transaction tree and balance). Consequently, SAG-IoT devices should either trust themselves by suffering the storage load (i.e., become full nodes) or perform as light nodes and trust remote servers, which also imposes extra communication overhead between end devices and remote servers.

In the blockchain, nodes need frequent data exchanges and transmissions. Compared with wired connections, due to the effect of fading, shadowing, and interference, the wireless links used to connect SAG-IoT devices may be intermittent and unreliable. Moreover, the capacity of wireless technologies in SAG-IoT networks is far lower than the requirement of blockchain. For example, ZigBee (IEEE 802.15.4), Bluetooth (IEEE 802.15.1), and Wi-Fi (802.11 a/b/g) can provide data rate of 250 kbps, 720 kbps, and 54 Mbps, respectively [177]. The NB-IoT can offer about a 100 kbps signal rate. In addition, the blockchain operations (e.g., consensus management, signature operations, and frequent data transmissions) may consume a huge amount of constrained battery energy of end devices. Consequently, the time needed for basic data sensing and processing operations of SAG-IoT devices can be dramatically prolonged, resulting in a degradation of system performance.

2) Throughput and Scalability: A huge amount of data is expected to be generated and consumed in the ubiquitous SAG-IoT networks. For example, the data volume generated by a driverless car on real-time road testing is about 8 TB per hour [178], and the vehicular traces of 700 cars in a day is 4.03 GB [179]. However, existing blockchain implementations have limitations in both throughout and scalability, e.g., 1 MB per block every 10 min in Bitcoin, which may be a bottleneck for SAG-IoT, especially for delay-sensitive applications such as traffic and air quality monitoring. The system throughput means the number of computations that can be supported in the system (e.g., number of processed transactions) in a unit time period [180]. As each block needs to be duplicated m times in a blockchain network with m full nodes, the duplication of big data in SAG-IoT can impose a huge communication overhead. Moreover, it is expensive to store data on the blockchain in practical SAG-IoT applications, e.g., the cost per GB data storage in Ethereum is nearly $\$\ 2\times10^5$ [181]. In essence, blockchain is not designed to store huge amounts of data like those produced in SAG-IoT. Furthermore, with the proliferation of heterogeneous end devices and the interoperability of security protocols at different layers co-existed in SAG-IoT [5], the scalability represents a great barrier to the integration of SAG-IoT and blockchain.

The throughput and scalability of current PoW-based blockchains are significantly affected by the block size and block time [182]. For example, the current block time of Bitcoin is about 10 minutes while the block size is limited to 1 MB. To meet the growing demand for transactions, one plausible solution is to increase the upper limit of block size and shorten the block time. As such, more transactions or blocks can be "written" to the blockchain at the same time. However, this could also give rise to the increased probability of block orphan and blockchain forking [182], thereby threatening the security of blockchain systems. Research work on the Bitcoin network in 2012 shows that for larger blocks (more than 20 KB), the block propagation time increases linearly with the block size. Another research [183] on the Bitcoin network in 2014 and 2015 uses the metric "x% effective throughput", which is defined as the percentage of nodes that receive a block, to evaluate the block propagation delay. Their finding shows that given the average block time of 10 minutes, to attain 50% effective throughput, the block size cannot exceed 38 MB; and to reach 90% effective throughput, the block size cannot exceed 4 MB [183]. Besides, given the block size of

80 KB, to acquire 90% effective throughput, the block time should be more than 12 seconds [183].

3) Blockchain Vulnerabilities and Interoperability: In spite of offering robust methods to secure SAG-IoT networks, the public blockchain network is also vulnerable, e.g., the 51% vulnerability of PoW consensus mechanisms and the susceptibleness to network fragmentation. Moreover, if the user's private key is stolen by adversaries, his/her blockchain account may under risk of being tampered with, and it is hard to trace the adversary's misbehaviors and recover the modified account information. The security breaches of blockchain systems can be classified as follows.

- *Attacks on data layer:* In current "chained" blockchain structures, a hard/soft fork of blockchain may occur unintentionally due to incompatibilities of client software upgrades or protocol malfunctions and intentionally conducted by malicious entities, thereby compromising the safety and inconsistency of blockchain.
- *Attacks on network layer:* Attacks targeted at the blockchain network mainly include the domain name system (DNS) attack [184], border gateway protocol (BGP) hijacking attack [185], and Eclipse attack [18]. In DNS attacks, a new user can be compromised during peer discovery via cache poisoning and stale records. In BGP hijacking attacks, Internet routing tables maintained via BGP can be corrupted by adversaries to illegally control a group of blockchain nodes. In Eclipse attacks, an honest node can be isolated by its neighboring malicious entities via IP addresses to compromise its incoming and outgoing traffic.
- *Attacks on consensus layer:* Attackers can exploit the vulnerabilities of consensus protocols to violate blockchain consistency and safety. The threats of typical consensus protocols as summarized in Table VI.
- *Attacks on incentive layer:* During the consensus process, multiple orphaned blocks and stale blocks may occur, which are valid and verified blocks but rejected by the blockchain network due to the time lag [184], thereby damping the enthusiasm of legitimate participants. Besides, selfish miners can launch the selfish mining attacks [78] to seek more economic profits by deliberately keeping their mined blocks private to reach a longer chain than the current one.
- *Attacks on contract layer:* The vulnerabilities of smart contracts such as reentrancy attack [186], short address attack [186], criminal smart contracts, and mishandled exceptions can be exploited by adversaries to threaten the security of applications built atop them.
- *Attacks on application layer:* The applications and services built on blockchain also bring various attack surfaces such as key exposure and theft, software client vulnerabilities, and in-browser cryptojacking [184] into blockchain systems.

Apart from the security vulnerabilities in blockchain systems, the interoperability concern related to different SAG-IoT applications built on heterogeneous blockchains [187] (in terms of using different transaction formats, consensus protocols, block structures, hash algorithms, and signature schemes) is an open research issue. For example, the security during the exchange of digital currencies among IoT applications developed on Bitcoin, Ethereum, and Hyperledger Fabric platforms should be handled carefully.

4) Decentralization-Scalability-Security Trilemma: According to the well-known blockchain trilemma [16], [21], [188] derived from the observations of existing blockchain systems, there exist no blockchain system that can simultaneously acquire: 1) decentralization (of geographic diversity, computation power, and storage resources), 2) scalability (of transaction throughput with network size), and 3) security (against adversarial attacks in consensus process). Specifically,

- *Decentralization:* Refers to the blockchain system's decentralization profile, which is generally related to the fraction of consensus nodes participating in building, verifying, and storing blocks, and the geographic diversity.
- *Scalability:* Generally refers to the capacity of the blockchain system to remain secure and efficient with higher transaction throughput and larger network size.
- *Security:* Refers to the property of consensus security (i.e., safety and liveness) in blockchain network with the presence of Byzantine nodes. Informally, the *safety* property stipulates that something "bad" will not happen during system execution, and the *liveness* property expresses that something "good" eventually happens during system execution.

In public blockchains using PoW protocols, it relies on the long block intervals and best-effort mining to maintain the consensus security, at the cost of low throughput. A shorter block interval gives rise to higher throughput but also yields a higher risk of the 51% attack. Moreover, the mandatory multi-block confirmation and probabilistic consensus finality lead to high decentralization (e.g., permissionless access), and scalability in network size. In permissioned blockchains using classical BFT protocols, the high communication complexity leads to a small number of consensus nodes (e.g., low decentralization) that can be supported. Meanwhile, the lower fault-tolerance threshold (i.e., sacrificing security) causes fewer consensus rounds or fewer exchanged messages per round, thereby alleviating communication overhead and improving transaction throughput. A system designer should carefully design the blockchain system for SAG-IoT applications to attain a tradeoff among decentralization, scalability, and security based on practical scenarios and needs.

5) Privacy Issues in Public Blockchains: Blockchain in public networks such as Bitcoin and Ethereum can suffer from confidentiality and privacy concerns, such as the linkability of transaction addresses, the number of transferred coins, and the business logic of smart contracts. As transactions are publicly accessed and verified by all entities in the blockchain network, privacy issues of IoT users may arise. Although multiple virtual identities (i.e., pseudonyms) in blockchain are generated to hide the true identity of a user, the one-to-many mapping between the user and his/her used pseudonyms can still be established by exploiting transaction graphs, and consequently, the user's true identity can

be deduced [66], [189], [190]. Besides, in existing smart contract platforms built on public blockchains, the data (in terms of the state information stored within the contract, underlying codes of contracts, and all inputs to and outputs from the contract) involved in smart contracts require to be replicated over all nodes to verify the correctness of contract execution. As such, current smart contract systems lack data confidentiality and privacy protection.

6) Legal Issues: The integrated blockchain-as-a-service (BaaS) for SAG-IoT applications is also influenced by regulations and laws regarding personal privacy and information handling, such as European Union (EU)'s GDPR. The exploitation of the blockchain should obey existing regulations and adapt to new laws and standards to help construct secure IoT systems. However, the decentralized and trust-free blockchain intrinsically gets rid of the centralized authority or trusted intermediary. Furthermore, due to the anonymity and cryptcity of transactions and behavior patterns, blockchain-based platforms may turn into the seedbed of crimes if without sufficient regulations [191]. The regulations will deeply affect the future of blockchain-empowered SAG-IoT systems.

B. State-of-the-Art Solutions

Currently, there have been a mass of works in both academia and industry aimed to efficiently integrate the blockchain into SAG-IoT scenarios. As shown in Fig. 5, the state-of-the-art blockchain optimization approaches for efficient integration with SAG-IoT are summarized as below, which are listed from the bottom layer to the top layer of the blockchain architecture.

1) Redesigned Data Structure: To scale up the throughput of the Bitcoin network, Bitcoin-NG (Next Generation) [180] is proposed, where the block generation process is decoupled into two phases: leader election and transaction serialization. Besides, two kinds of blocks, i.e., key block and micro block, are respectively corresponded to the two phases. The key block records the winner of the PoW race and contains a solution to the PoW puzzle. The transactions are included in the subsequent micro blocks of the key block and each micro block contains a pointer linking to the previous block. Here, the subsequent micro blocks are created by the current key block miner in a non-mining manner. As the micro block does not contain the PoW solution, its generation rate is deterministic and can be much higher than that of the key block. Experimental results validate the feasibility of Bitcoin-NG in terms of consensus delay (i.e., the time taken to reach consensus), fairness (i.e., the ratio of mining power not owned by the largest miner multiples the ratio of transitions not coming from the largest miner), and mining power utilization (i.e., the ratio between the mining power which secures the network and the total mining power).

Another solution to improving system capacity and scalability is to leverage the discarded blocks which are excluded from the main chain due to forks [192]. It can be done by adjusting the data structure in the blockchain. The Tangle [80] developed by the IOTA project is one of the typical consensus protocols which employs the DAG structure to organize blocks, instead of the traditional chained structure. DAG is a finite directed graph without cycles connecting the edges, where transactions are denoted as vertices and each edge stands for approvals in Tangle. Any participant who intends to generate a new transaction must approve (i.e., verify) two previous transactions in the Tangle network. Tangle allows conflicting transactions in different branches of the DAG to eventually merge as the heaviest branch [80], which overcomes the ongoing throughput limit of the blockchain. Besides, in IOTA, a full node can only store the full data (i.e., all transactions) produced after a snapshot to save its storage space. Meanwhile, the permanodes [80] are introduced which permanently store the complete transaction history (i.e., all transactions ever made). As shown in [192], the DAG-based blockchain can attain about 90% block utilization (i.e., the ratio of valid blocks). DAG-based blockchain has been widely adopted in various IoT scenarios, such as industrial IoT [85], wireless energy trading [98], and vehicular networks [170]. Other projects exploiting the DAG-based "blockless" structure include IoT Chain [114], Byteball,[6] and Nano.[7] However, the DAG-based approach is still in its infancy without thorough tests to its limits and hence may be prone to attacks especially with fewer users.

2) Off-Chain Mechanisms: The cost of data storage may be prohibitive for data-centric SAG-IoT systems. For example, the cost per Bitcoin transaction is about $1.3, and per transaction in Ethereum is about $0.15. Off-chain mechanisms offer a possible option to reduce the storage and computation overhead by moving data and computation from the blockchain to another datastore or third party while keeping a pointer to index to the blockchain [14]. Compared with on-chain approaches, only specific data elements (e.g., hash of a piece of data) are stored on the blockchain in off-chain mechanisms, thereby the blockchain "footprint" can be considerably reduced. A cloud storage (e.g., AWS, Dropbox, and Azure), a traditional DBMS (e.g., Oracle, MySQL, and MongoDB) or a distributed storage system (e.g., Storj and IPFS [126]) can be employed for off-chain data storage, depending on the specific scenarios. Besides, the latest global state of the ledger can be extracted from the blockchain by using a snapshot, which can be duplicated and stored in an off-chain data store (e.g., LevelDB or CouchDB used in Hyperledger Fabric [83]) for supporting advanced query and better performance. An off-chain key-value store such as distributed hash table (DHT) is implemented in Symphony [193] to efficiently provide a mapping between storage locations and the hashes of pieces of data in a wide area network. The main challenge is to ensure the fundamental properties of blockchain in the combination of off-chain storage.

To support high-frequent micro-payment scenarios, the lightning networks [194] are investigated, where the transaction sequences on each channel are kept "off-chain". In lightning networks, value transfers between two end nodes on an established channel are kept locally, instead of broadcasting to the whole network. Thereby, the frequency of validation and synchronization of global blocks can be reduced to a large extent.

[6]https://github.com/byteball
[7]https://nano.org/

3) Editable Blockchain: Currently, numerous data are generated by the explosively growing IoT devices, while only a limited part is valuable for extracting knowledge and deriving useful insights. Furthermore, in some latency-sensitive SAG-IoT applications such as weather prediction and traffic monitoring, only the latest data that meet the stringent data freshness requirements is useful. Therefore, part of data can be deleted from the blockchain ledgers to alleviate the storage burden in SAG-IoT systems, which raises the demand for editable blockchain techniques such as snapshot, block pruning [17] and block summarization [195] without breaking the reliability of on-chained data. As such, the older transactions can be deleted or compressed into a snapshot to mitigate the growing storage overhead of blockchain. As the "editability" may somewhat contrast to the intrinsic "immutability" of blockchain, the deletion and modification of part of blocks in editable blockchain should ensure reliable records and secure conditions for any edit operations [195].

4) Sharding: Sharding means breaking up the entire blockchain network into multiple segments (i.e., shards), where each shard processes a unique set of transactions in parallel [15]. With sharding, the throughput of blockchain increases linearly with the number of SAG-IoT devices in the system. Besides, participants are assigned to different shards for transaction verification, instead of processing all transactions in the entire network, thereby the burden of running blockchain on SAG-IoT devices can be mitigated. In addition, the SAG-IoT data is typically featured with a strong locality (i.e., only useful in local regions), which gives an opportunity for sharding blockchain in SAG-IoT networks. For example, the global chain is to record important but less frequent global events over large-scale SAG-IoT systems, while the frequent local events are recorded in other shards in regional networks. The sharding technology is widely implemented by many blockchain projects such as Ethereum, NEAR, Polkadot, and Zilliqa. However, the main challenges of blockchain sharding relate to the security of segmented blockchain and cross-shard communication for inter-shard transactions [188]. Within a single shard, it is easier for attackers to take over it, known as 1% attack. To mitigate this attack, a random sampling method named OmniLedger is studied in [188] by randomly assigning nodes to different shards. Besides, nodes' strategic behaviors in shard-based blockchains are analyzed by Manshaei *et al.* [196] for optimal reward sharing and consensus management via a game-theoretical approach.

5) IoT-Specific Consensus Mechanisms: A suitable consensus protocol for SAG-IoT scenarios requires attaining a balance among resource consumption, security, decentralization, and system performance [21]. In particular, the IoT-specific consensus mechanisms should be both energy-efficient and lightweight. To implement blockchain into resource-limited SAG-IoT devices with high energy efficiency, a feasible alternative is exploiting social features [197] (e.g., social relationships, location-based relationships, movement pattern similarity, social trust, and reputation) of SAG-IoT devices and their collaboration in consensus management in blockchain networks. Extensive researches [60], [198], [199] have demonstrated the effectiveness of incorporating social trust and reputation into consensus management in terms of promotion of honest behaviors, energy saving, and security of consensus results. In [38], [60], the social reputation values are incorporated into PoW consensus mechanisms to adjust the PoW difficulty for mining nodes. As only trusted consensus nodes with high reputation can join in the consensus process, the security of blockchain management can be enhanced. Besides, the energy consumption of honest consensus nodes in PoW can be reduced while that of malicious entities is increased, thereby increasing the cost of attacks and motivating honest behaviors. In [198], the reputation values are employed in the leader election in the DPoS consensus mechanism to improve the consensus security (against miner voting collusion and block verification collusion) in a blockchain network comprised of vehicles. In addition, the contract game is exploited to design the optimal contract menus for standby miners to motivate their participation in transaction relaying and block verification.

By exploiting the collaboration among SAG-IoT devices with spatial and temporal correlations, it raises the potentials to design content-oriented consensus algorithms to improve the correctness of sensory data via cross-validation from the historical data and the neighbors of device [200]. In LightChain [86], a green and resource-efficient consensus protocol is developed by promoting the cooperation of consensus nodes in PoW to improve nodes' mining participation and ensure a stable block generation rate. In their work, the mining efficiency is measured by the hash quality, which is defined as the ratio between hash power paid for successfully proposing new blocks and the total hash power of miners. Simulation results in [86] show the improved mining efficiency in LightChain. Mondal *et al.* [54] develop a novel proof of object consensus mechanism in the supply chain scenario based on the fact that users indeed own the physical object in the supply chain, which is similar to the cryptocurrency domain. As such, a user who owns a physical object can claim his/her possession by attaching cryptographical proof, and other participants can audit the authenticity of the claim.

Besides, the hybrid consensus mechanisms can offer potential solutions for better performance in SAG-IoT. In IoT Chain [114], both PBFT and DAG are harnessed towards a light operating system on the basis of blockchain, where the main chain adopts PBFT and the side chains employ DAG. In WaltonChain [166], a parent-child chain structure is adopted by incorporating PoW, PoS, and proof of labor (PoL), where PoW and PoS work for the parent chain and PoL works for the data exchange between parent and child chains. In [124], Du *et al.*. design a novel mixed BFT consensus algorithm for secure medical data sharing by splitting consensus nodes into two groups and adopting a two-layer transaction process to reduce fork probability and guarantee high consensus speed. To summarize, IoT-specific consensus mechanisms will play a critical role in the inclusion of blockchain as a part of SAG-IoT infrastructures. The specifically designed consensus algorithms for various applications with distinct requirements will significantly benefit the future SAG-IoT landscape. Beyond the capacity and scalability enhancement, both the rigorous theoretical analysis and the thorough test of their security

and performance are required before the wide real-world adoption.

6) Incentives: A well-designed incentive mechanism is a benign impetus for both SAG-IoT and blockchain networks [85]. By charging transaction fees and rewarding for mining or proving a block, the cost of attacks (e.g., DoS attack and forged message) can increase, thereby discouraging the misbehaviors while promoting benign behavioral patterns in blockchain [38]. Beyond digital currencies, network tokens (e.g., reputation and honesty credits) [85] can compensate users' cost in blockchain operations and also be a stimulus for a variety of SAG-IoT applications. In RepChain [201], the reputation of consensus nodes is exploited as an incentive to suppress the selfishness of nodes with limited bandwidth, computation, and energy resources. The reputation value is evaluated based on node behaviors in transaction and block verification and the feedbacks from other consensus nodes. In RepuCoin [202], the social reputation, as a measurement of a miner's power, is investigated to reduce computation cost and improve the security of PoW mining process, where the progression of reputation is modeled as a sigmoid function in a parameterizable manner. Besides, in [85], by incorporating credits into consensus management, both the security and transaction efficiency in DAG-structured blockchains for industrial IoT can be enhanced, where two abnormal behaviors, namely, lazy tips and double-spending, are taken into consideration in the credit evaluation.

Game theory is an efficient tool to formulate the optimal strategies of players in distributed and dynamic network environments. Various game models are investigated under the blockchain framework to optimize nodes' behavior patterns, including stimulating nodes' participation, cooperation, and honest behaviors. For example, Zhou *et al.* [117] develop a two-tier game-theoretical model for secure and efficient allocation of spectrum resource in blockchain-based 5G HetNets with the coexistence of human-to-human (H2H) and machine-to-machine (M2M) communications, where a contract game is employed in the first tier to incentivize H2H users to share their underutilized spectrum and a many-to-many matching game is used to allocate spectrum between H2H users and M2M devices. Moreover, Xiong *et al.* [203] formulate the optimization problem of computation offloading between cloud/fog servers and miners as a two-stage Stackelberg game, where the cloud/fog servers act as game leaders to decide the pricing strategies in the first stage while the miners perform as followers to determine the amount of purchased computation resource in the second stage. The alternating direction method of multipliers (ADMM) approach is adopted to analyze the Stackelberg equilibrium due to the complexity of the formulated game. Furthermore, in [204], Liu *et al.*. utilize the evolutionary game to model the mining pool selection dynamics of individual miners, where both the hash rate in PoW and the block propagation latency are considered in the mining race. In addition, Kang *et al.* [205] obtain the maximized energy trading efficiency and social welfare for EVs in blockchain by designing the optimal energy pricing and traded energy amount strategies based on the double auction mechanism.

Generally, existing game-theoretical approaches assume that the parameters of the network model and user model are readily available. For example, the cost parameters of players in the Stackelberg game, matching game, and auction game are public. Even in the information asymmetry scenarios, such as in the contract theory, the contract designer is assumed to know the distribution of user types in advance. In the practical environment, it is hard to accurately estimate all the parameters of the time-varying network and the private parameters of users. A learning-based scheme can overcome this challenge by getting rid of reliance on the knowledge of accurate network and user parameters [206]. For example, Wang *et al.* [207] develop a two-tier Q-learning mechanism to motivate user's participation and high-quality data sharing via trials in blockchain-based disaster relief networks consisting of collaborative UAVs and rescue vehicles. Besides, Liu *et al.* [102] harness DRL techniques to maximize the quantity of collected data and ensure the data quality of mobile terminals via trajectory optimization in the blockchain-based industrial IoT environment.

7) Multiple Blockchains and Sidechain: To cope with the performance bottleneck of single blockchain architecture, a plausible approach is exploiting the multiple blockchain architectures. In multiple blockchain architecture [187], different blockchains can cooperatively store different types of transactions to support various SAG-IoT applications. For example, in vehicular networks, by recording safety-related transactions and entertainment-related transactions into two different blockchains, their distinct service requirements (such as latency) can be better satisfied. Via network slicing and access control, vehicles can participate in different blockchain platforms to obtain interested services while the network load can be eased. The main problem exists in supporting efficient data transfer across multiple blockchain systems while guaranteeing the atomicity of transactions and maintaining the security of the blockchain ecosystem.

The high mobility of some SAG-IoT devices (e.g., vehicles and drones) can cause potential network partitions, where each partition operates a separate blockchain and the data of these devices may be embedded in different blockchains. Due to the immutable nature of blockchain, a challenging issue is to migrate and integrate the involved blocks back to the home blockchain when the network connection recovers while maintaining the consistent records of these devices. The sidechain technology offers a solution to allow that data and digital assets from the main chain (i.e., home blockchain) can be linked to/from the sidechains [15], [208]. Sidechains refer to separate blockchains that run in parallel, operate independently of the main chain, and are attached to the home blockchain via a bidirectional peg [208]. The sidechain can empower existing blockchains with improved throughput, flexibility, and liquidity, and it is adopted in many popular projects like Liquid, Rootstock, Loom, and Plasma. However, a series of problems in sidechains remain to be resolved including the implantation of sidechains into the main chain in a secure and efficient manner.

8) Cross-Chain Mechanisms: In current blockchain ecosystem, the SAG-IoT services built on various blockchain

platforms are isolated, raising increasing demands for trusted assert transfer and data exchange among various blockchains. Cross-chain mechanisms aim to enable interoperability for heterogeneous blockchains by using techniques such as the notary scheme [209], hash-locking [210], and relay chain/sidechain [211]. In notary scheme [209], it relies on one or a group of witnesses which serve as the trusted intermediary to listen cross-chain events and verify cross-chain messages. However, notary schemes rely on the honesty of witnesses and may lead to the risk of centralization or SPoF. In hash-locking [210], the tokens or assets are locked by the hash lock and time lock to ensure credibility, which can be transferred to the receiver in the destination blockchain only if the receiver produces a commitment before the deadline. In relay chain [211], the block information of the source blockchain is replicated in the relay chain to allow the destination blockchain to validate the correctness of transactions on the source blockchain. In sidechain [15], the two-way peg connectivity is exploited to move information or assets from its home chain to the sidechain. However, current cross-chain researches mainly concentrate on cross-chain communication, asset transfer, and data exchange. More research efforts are required to investigate the authenticity, inter-chain write mutual exclusion, and real-time cross-chain regulation during data/value exchange between blockchains.

9) Privacy-Preserving Blockchain: Current works mainly focus on the advanced cryptographic mechanisms such as ZKP [142], secure multi-party computation (SMC) [212], confidential transaction [213], and ABE [121] to build privacy-preserving blockchains. However, these advanced cryptographic mechanisms have overwhelming overhead and are too heavy for resource-limited SAG-IoT devices. Computation-efficient and energy-efficient cryptographic solutions for both user and data protection are imperative in the SAG-IoT context. Another plausible option is exploiting TEE such as Intel SGX [214] as a complementary of blockchain systems by providing verifiable and confidential computation on sensitive data through software remote attestation. For example, the computation over private data can be executed in off-chain TEEs and separated from the consensus process to resolve the lack of confidentiality and poor performance of smart contracts [58]. Nonetheless, the remaining problem is to prevent potential pitfalls and new attack vectors along with the implementation of TEE such as rewinding attacks and side-channel attacks [215]–[217].

10) Regulated Blockchain: With a decentralized blockchain platform, it makes regulatory and legal decisions simpler during collecting, sharing, tracing, and storing private and sensitive SAG-IoT data. For example, the distributed blockchain ledgers can serve as legal evidence for accessing or collecting data due to the traceability and tamper-resistance. Huang *et al.* [191] develop a blockchain system for efficient drug traceability and regulation. To offer immutable audit trails for all data flows in the supply chain, Cydon [218] provides a distributed ledger with digital data sharing regulation within and across various entities. LegalXchain [219] exploits blockchain to build the underlying infrastructure of regulation, law, and government affairs by obeying the legal rules. To regulate normal behaviors, avoid disputes and prohibit criminal acts for blockchain-based SAG-IoT applications, new laws, standards and regulations together with the government are required to be seamlessly involved to strengthen regulations [220]. Furthermore, regulations, laws, and standards can be programmed into the blockchain platform in the form of smart contracts, making them automatically enforced. The regulations are keys to the inclusion of blockchain and SAG-IoT as part of government infrastructures. To avoid being the seedbed of criminals for unlawful purposes, research efforts should further be made to ensure the legitimacy of transactions and correctness of smart contracts in blockchain platforms towards building the most secured and trusted blockchain-IoT systems.

C. Summary and Insights

As seen in Section IV-A, although blockchain technologies have great potential in building a secure SAG-IoT, it still has limitations in terms of resource limitation, scalability, security vulnerabilities, cross-chain interoperability, privacy issues, and legal issues. Indeed, blockchain itself is a nascent technique and has ample room for further development, especially in the SAG-IoT domain. The discussed blockchain challenges and state-of-the-art solutions for SAG-IoT applications are summarized in Table XIX. Besides, a comparative summary of existing representative blockchain projects for SAG-IoT applications is shown in Table XX. In the following, the insights of the state-of-the-art research works are discussed.

According to the decentralization-scalability-security trilemma, a tradeoff among these three contradictory targets needs to be carefully considered in the practical deployment of blockchain-empowered SAG-IoT applications. Moreover, the unique characteristics of SAG-IoT should be fully considered. For example, in an SAG-IoT network with sparse connections, better-connected entities can gain unfair advantages in disseminating new blocks faster than weakly connected entities, which potentially impairs consensus security. As such, an attacker may require less than 50% of mining capacity to launch a double-spending attack under the longest-chain rule. Another example is that, under a certain security premise, in a small and well-connected SAG-IoT network with enforceable time-out mechanisms, a higher transaction throughput can be acquired, compared with to the large-scale and less-connected network [21].

Public blockchains offer immutability, accountability, and pseudo-anonymity as all transactions are visible to all participants of the blockchain network. Private or consortium blockchains retain privacy within one or multiple organization(s), and both of them are not sufficiently decentralized. The type of blockchain for implementation of SAG-IoT services should be pre-considered depending on practical needs.

In consensus improvement, feasible alternatives including social features (e.g., social trust, reputation, locations, and movement pattern similarity), node cooperation (with spatial and temporal correlations), as well as the hybrid consensus in layered blockchain architecture, can be exploited to design energy-efficient and lightweight consensus mechanisms

TABLE XIX
A SUMMARY OF BLOCKCHAIN CHALLENGES AND STATE-OF-THE-ART SOLUTIONS FOR SAG-IOT APPLICATIONS

Blockchain Challenge	Description	Existing Solution	Key Idea
Resource limitation	Resource-constrained SAG-IoT devices lack sufficient computation, communication, and storage resources for transaction exchange and blockchain maintenance	Redesigned data structure	Scale up blockchain throughput by redesigning transaction&block structure and leverage discarded blocks by using DAG structure.
		Off-chain mechanism	Move data, computations, and payments to off-chain repositories, third parties, and channels.
		IoT-specific consensus mechanism	Exploit social features, node collaboration, and hybrid consensus to design new consensus protocols for specific scenarios.
Capacity	Decentralized consensus sacrifices transaction throughput for security guarantees	Sharding	Split blockchain network into multiple shards and each shard processes inter-shard transactions in parallel.
		Incentives	Well-designed incentives are a benign impetus for efficient node cooperation in transaction relay, resource sharing, etc.
Scalability	Exchanging, validating, and/or storing network-wide transactions cause huge communication, computing, and storage overhead for large-scale SAG-IoT applications	Multiple blockchains	Different blockchains store different transactions cooperatively.
		Sidechain	Use sidechains attached to the main chain via a bidirectional peg.
		Editable blockchain	Alleviate blockchain storage burden by pruning and summarizing blockchain data without violating data reliability.
Security vulnerability	Intrinsic/external security threats resulted from data, network, consensus, incentive, contract, and business layers in blockchain-empowered SAG-IoT systems	AI-driven secure blockchain	Exploit machine learning methods for predicting and identifying security threats and vulnerabilities in blockchain system.
Interoperability	Cross-chain data/value exchange among heterogeneous blockchains using different transaction formats, consensus protocols, block structures, hash algorithms, and signature schemes in blockchain-based SAG-IoT ecosystem	Cross-chain mechanism	Enable trusted cross-chain data/value exchange among heterogeneous blockchains via hash-locking, relay chain, etc.
Privacy issue	Data and computations of smart contracts on public blockchains are transparent for public audit	Privacy-preserving blockchain	Protect user privacy on blockchain ledgers and smart contracts via advanced cryptographic mechanisms and trust computing.
Legal issue	The decentralized public blockchain with anonymous addresses and covert transaction patterns intrinsically gets rid of the centralized authorities for regulations	Regulated blockchain	Ensure the legitimacy of transactions and avoid the unlawful behaviors in blockchain platforms.

TABLE XX
A SUMMARY OF EXISTING REPRESENTATIVE BLOCKCHAIN PROJECTS FOR SAG-IOT APPLICATIONS

Name	Type	Solution	Throughput	Scalability	Featured application
Ethereum[8]	Permissionless	PoS + GHOST + Sharding	13 seconds/block	10^5	Cryptocurrency, Smart contract
Hyperledger Fabric [83]	Permissioned	PBFT	3500 tps	10^3	Blockchain platform, Smart contract
IOTA [80]	Permissionless	PoW + Tangle	$>$ 800 tps	10^3	General IoT
Quorum[9]	Permissioned	RAFT	150 tps	N/A	Blockchain platform, Smart contract
IoT Chain [114]	Permissionless	PBFT + DAG	10^3 tps	10^3	General IoT
IoTeX [221]	Permissionless	Roll-DPoS + Sidechain	$>$ 2000 tps	N/A	Shared economy, Smart home
Xage Security [146]	Permissioned	FBA	N/A	10^6	Identity access management in industrial IoT
SmartAxiom	Permissionless	Multi-chain	N/A	N/A	IoT device identification and authentication
IOTW [115]	Permissionless	Proof of Assignment	3000 tps	N/A	IoT data management
Atonomi [199]	Permissioned	PoS+ Reputation + Token	N/A	N/A	IoT security
Datum [125]	Permissionless	Off-chain	N/A	N/A	Decentralized data storage and monetization
WaltonChain [166]	Permissionless	PoW + PoS + PoL	N/A	N/A	Supply chain
Power Ledger [116]	Hybrid	PoS + Token	N/A	N/A	Renewable energy
LegalXchain [219]	Permissioned	BFT + Sidechain	10^4 tps	$> 10^4$	Justice and regulation
Cosmos	Permissionless	Tendermint + Relay chain	N/A	N/A	Cross-chain infrastructure for data/value transfer

tailored to SAG-IoT environment. The orchestration of cloud and edge resources in SAG-IoT for consensus improvement and blockchain maintenance is also essential, which is shown in Section V-B.

In incentive mechanisms, both digital currencies and network tokens (e.g., reputation and honesty credits) can be employed as a stimulus for node operations in blockchain-enabled SAG-IoT applications. Game theory and reinforcement learning are two essential tools to build distributed incentive mechanisms in the SAG-IoT environment. Besides, reinforcement learning-based mechanisms can work more efficiently under highly dynamic network environments without the accurate knowledge of network parameters and user parameters.

For AI-driven secure blockchains, machine learning and deep learning methods can efficiently help the prediction and identification of cybersecurity threats and vulnerabilities in blockchain systems to build the more secure and trusted SAG-IoT, which is shown in Section V-D.

[8]https://github.com/ethereum/wiki/wiki/White-Paper
[9]https://github.com/ConsenSys/quorum

V. FUTURE RESEARCH DIRECTIONS

Apart from the blockchain technology, SAG-IoT itself expects to integrate with other emerging technologies, such as network slicing, SDN, edge/cloud computing and AI, to become an essential part of future smart city infrastructures. With a bright future ahead, the road towards their full harmonization is fraught with challenges. Although blockchain has brought numerous potentials to enrich SAG-IoT security, significant research efforts are required to cope with the following concerns.

A. Orchestration With Network Slicing

To satisfy the stringent QoS requirements of various SAG-IoT services, dynamic and flexible network slicing is needed for SAG-IoT. Network slicing technology [222] can support distinct SAG-IoT services and applications on a dedicated network by sharing the same physical infrastructures through network softwarization. As one of the main enablers of network slicing, network function virtualization (NFV) [154] can create different network functions (e.g., load balancing, serving gateway, and traffic monitoring) in an on-demand manner by decoupling network functions from infrastructures.

In B5G-enabled SAG-IoT, apart from the provisioned isolation guarantee of network slicing, one of the major challenges is the automatic creation, leasing, and coordination of slices for diverse SAG-IoT applications. A common approach is the adoption of network slice broker [223] to facilitate participants to request and lease slice resources from infrastructure providers (e.g., cloud operators). Blockchain technology can bring about numerous potentials for trusted slice and infrastructure sharing among mobile network operators (MNOs), fraud prevention and dynamic MNO switching for users, toward an open, transparent and fair ecosystem in SAG-IoT. For example, the blockchain can facilitate trusted slice brokering and on-demand slice management for MNOs and users by providing secure and traceable slice ledgers to automatically record the slice leasing and sharing behaviors. Besides, the slice negotiation and cooperation procedure can be accelerated via smart contract-based automatic agreements for improved network efficiency. Future researches are also required for blockchain-based network slicing in SAG-IoT applications from business, law, and policy perspectives.

B. Orchestration With SDN

As the number of SAG-IoT devices is in billions, how to efficiently control and manage them in a large-scale distributed SAG-IoT network becomes a complex task. SDN is an enabling technology in B5G-empowered SAG-IoT. In SDN, network intelligence is centralized into one network component (i.e., SDN controller) via the separation of control plane (i.e., routing process of packets) and data plane (i.e., forwarding process of packets) [224]. As such, it enables fast and simplified network configurations in the deployment of new protocols for SAG-IoT networks regardless of the underlying techniques. Besides, the logically centralized SDN controllers can offer much-improved flexibility and programmability by using standardized interfaces such as OpenFlow in network management to efficiently manage millions of SAG-IoT devices [4]. However, the centralization of network intelligence in SDN-based architecture has its drawbacks when it comes to security, such as SPoF. In addition, the recorded network statistics and Openflow policies for system configuration in SDN may be modified, replaced or deleted, thereby deteriorating the data reliability. Blockchain is rendered as a critical security factor to build a securer SDN-based SAG-IoT [225]. For example, blockchain technology can be utilized to secure flow rule table updating of Openflow switches in SDN-based large-scale SAG-IoT, where Openflow switches can publicly verify the version and correctness of flow rule tables while synchronizing the up-to-date flow rule tables with no administrators [225]. Besides, in the distributed control plane setting with multiple SDN controllers, blockchain can be exploited to attain the consensus of global view among multiple SDN controllers in a distributed fashion [224]. The open issues in the integration of blockchain with SDN-based SAG-IoT are scalability, energy efficiency, interoperability, and regulation. For example, with the increasing size of the blockchain, the heavy storage and computation tasks involved in the blockchain may consume considerable resources for SDN switches, which may become a network bottleneck.

C. Orchestration With Edge-Cloud Computing

Due to the heterogeneity of network devices and the diverse resource requirements of various SAG-IoT applications, it is necessary to orchestrate both cloud and edge resources for efficient SAG-IoT services. Compared with cloud computing, edge computing [106] can significantly reduce service latency, alleviate backbone burden, and improve user's quality-of-experience (QoE) by migrating part of cloud resources (e.g., communication, computation, and storage) proximally at the edge servers which are typically installed at Wi-Fi APs, IoT gateways, macro BSs, and small BSs. However, edge servers are usually provisioned with inferior capability, while cloud servers can offer unlimited storage space and computing resources via the abstraction of infrastructures [24]. Furthermore, edge servers are heterogeneous in terms of networking resource, storage space, and computing capability. Consequently, edge servers alone cannot accommodate the communication, computation, and storage demands for the provision of services for the ever-increasing SAG-IoT devices. The orchestration of edge computing and cloud computing can facilitate flexible and on-demand resource allocation in heterogeneous SAG-IoT networks. Blockchain can promote the orchestration of massive edge-cloud resources through decentralized key distribution, cross-domain authentication, reliable task assignment, and secure computation offloading. For example, the agreements and provisions for resource and infrastructure sharing between edge-cloud servers and end-users in B5G can be negotiated on-the-fly by using smart contracts [226], while the resource usage can be traceable in the blockchain ledger for regulators [227]. Besides, the orchestration with edge-cloud computing can benefit blockchain-IoT systems by offering efficient edge/cloud caching, computing, and communication for resource-constrained SAG-IoT devices during the life-cycle of data services. However, due to the fast-changing network topology and the existence of heterogeneous blockchains [187] in diverse SAG-IoT applications, the efficient deployment of blockchain-as-a-infrastructure (BaaI) with high interoperability in the future SAG-IoT deserves to focus on.

D. Orchestration With AI

Driven by the unprecedented SAG-IoT big data and the demand for smarter devices, AI technologies (e.g., machine learning (ML), deep learning, and reinforcement learning) can bring intelligence to billions of sensors and end devices and power a variety of smart city applications. By learning and extracting knowledge from the massive SAG-IoT data, the disruptive AI paradigm can bring numerous benefits to blockchain-empowered SAG-IoT systems including energy-efficient consensus management, fraudulent transaction detection, misbehavior suspecting, dynamic smart contract audit, auto-coding smart contracts, and automated governance. For example, AI-governed blockchain can enable intelligent smart contract audit to prevent code vulnerabilities in advance

and thus secure the applications and functionalities built on top of blockchain [228]. AI could also perform the adaptation and optimization of blockchain parameters (e.g., block size, block time, and type of consensus mechanisms) for improved robustness and scalability of blockchain systems. On the other hand, blockchain technology can also be beneficial to AI, especially edge AI. The edge AI [229], empowered by the large amount of SAG-IoT data generated at the edge of the network, can bring AI capacity from the cloud to the edge and proximally process the collected SAG-IoT data from end devices. Under federated edge AI, the training data are kept locally and only the local learning model (e.g., gradients) is shared by each edge server; then the central curator aggregates a global model and distributes it to all involved edges. Blockchain can facilitate the distributed and collaborative model training process (e.g., federated ML) in the edge AI paradigm via trust-free data and knowledge sharing among multiple distrustful edge nodes [229]. For example, blockchain can settle the trust issues in contribution verification and offer reliable incentives to participants to promote a healthy and sustainable ecosystem. Moreover, by employing the blockchain, the central curator for model synthesization can be removed in the federated learning process for edge nodes to prevent SPoF and potential learning failure due to its malfunction [230]. However, as the local learning models trained by sensitive SAG-IoT data are transparently recorded in the blockchain to ensure authenticity, smart adversaries can conduct attacks, e.g., differential attacks, inference attacks and model inversion attacks, to infer the used private training data from the shared gradients, which may result in unintended data privacy leakages [231]. Besides, AI-specific consensus protocols, as a concept of *proof of useful work* in blockchain, which recycle the wasted mining power in PoW blockchains to useful works such as image segmentation and training deep learning models, should be designed to efficiently support SAG-IoT applications.

VI. Conclusion

In this article, we have presented a comprehensive survey of the blockchain solutions for SAG-IoT security. Specifically, we have introduced the security and privacy threats in SAG-IoT. Then, the opportunities and recent advances for building the blockchain solutions to address the security and privacy issues are examined for safeguarding SAG-IoT services. Afterwards, we have discussed the critical challenges in restricting the practicality of current blockchain-based security services and reviewed the state-of-the-art solutions in designing tailored blockchains for SAG-IoT. This survey is anticipated to shed light on blockchain-IoT integration, and encourage more research efforts on the blockchain-based solutions for improving the security and privacy of SAG-IoT applications.

References

[1] M. Arnott, E. Buckland, M. Ranken, and P. Ranken. *IoT Global Forecast and Analysis, 2015–2025.* (2017). Gartner, Stamford, CT, USA. Accessed: Jan. 10, 2020. [Online]. Available: https://machinaresearch.com/news/press-release-global-internet-of-things-market-to-grow-to-27-billion-devices-generating-usd3-trillion-revenue-in-2025/

[2] N. Cheng *et al.*, "A comprehensive simulation platform for space-air-ground integrated network," *IEEE Wireless Commun.*, vol. 27, no. 1, pp. 178–185, Feb. 2020.

[3] J. Liu, Y. Shi, Z. M. Fadlullah, and N. Kato, "Space-air-ground integrated network: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2714–2741, 4th Quart., 2018.

[4] N. Zhang, S. Zhang, P. Yang, O. Alhussein, W. Zhuang, and X. S. Shen, "Software defined space-air-ground integrated vehicular networks: Challenges and solutions," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 101–109, Jul. 2017.

[5] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.

[6] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the Internet of Things," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1636–1675, 2nd Quart., 2019.

[7] I. Butun, P. Osterberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 616–644, 1st Quart., 2020.

[8] E. Bertino and N. Islam, "Botnets and Internet of Things security," *Computer*, vol. 50, no. 2, pp. 76–79, Feb. 2017.

[9] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Integration of blockchain and cloud of things: Architecture, applications and challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2521–2549, 4th Quart., 2020.

[10] W. Sun, L. Wang, P. Wang, and Y. Zhang, "Collaborative blockchain for space-air-ground integrated networks," *IEEE Wireless Commun.*, vol. 27, no. 6, pp. 82–89, Dec. 2020.

[11] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 858–880, 1st Quart., 2019.

[12] X. S. Shen *et al.*, "Data management for future wireless networks: Architecture, privacy preservation, and regulation," *IEEE Netw.*, vol. 35, no. 1, pp. 8–15, Jan./Feb. 2021.

[13] *Blockchain Will Strengthen the Future of IoT*. (2019). IDC, Needham, MA, USA. Accessed: Feb 10, 2020. [Online]. Available: https://www.leanix.net/en/blog/blockchain-will-strengthen-the-future-of-iot

[14] W. Chen, Y. Chen, X. Chen, and Z. Zheng, "Toward secure data sharing for the IoV: A quality-driven incentive mechanism with on-chain and off-chain guarantees," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1625–1640, Mar. 2020.

[15] A. Garoffolo, D. Kaidalov, and R. Oliynykov, "Zendoo: A zk-SNARK verifiable cross-chain transfer protocol enabling decoupled and decentralized sidechains," in *Proc. IEEE 40th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2020, pp. 1257–1262.

[16] S. Li, M. Yu, C.-S. Yang, A. S. Avestimehr, S. Kannan, and P. Viswanath, "PolyShard: Coded sharding achieves linearly scaling efficiency and security simultaneously," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 249–261, 2020.

[17] E. Palm, O. Schelen, and U. Bodin, "Selective blockchain transaction pruning and state derivability," in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, 2018, pp. 31–40.

[18] Q. Tan, Y. Gao, J. Shi, X. Wang, B. Fang, and Z. Tian, "Toward a comprehensive insight into the eclipse attacks of tor hidden services," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1584–1593, Apr. 2019.

[19] E. Deirmentzoglou, G. Papakyriakopoulos, and C. Patsakis, "A survey on long-range attacks for proof of stake protocols," *IEEE Access*, vol. 7, pp. 28 712–28 725, 2019.

[20] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A comprehensive survey of blockchain: From theory to IoT applications and beyond," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8114–8154, Oct. 2019.

[21] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1432–1465, 2nd Quart., 2020.

[22] A. Reyna, C. Martin, J. Chen, E. Soler, and M. Diaz, "On blockchain and its integration with IoT challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.

[23] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.

[24] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1508–1532, 2nd Quart., 2019.

[25] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.

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

[27] T. Hong, W. Zhao, R. Liu, and M. Kadoch, "Space-air-ground IoT network and related key technologies," *IEEE Wireless Commun.*, vol. 27, no. 2, pp. 96–104, Apr. 2020.

[28] V. Hassija *et al.*, "Fast, reliable, and secure drone communication: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2802–2832, 4th Quart., 2021, doi: 10.1109/COMST.2021.3097916.

[29] Y. Wang, Z. Su, N. Zhang, and D. Fang, "Disaster relief wireless networks: Challenges and solutions," *IEEE Wireless Commun.*, vol. 28, no. 5, pp. 148–155, Oct. 2021.

[30] T. Qiu, N. Chen, K. Li, M. Atiquzzaman, and W. Zhao, "How can heterogeneous Internet of Things build our future: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2011–2027, 3rd Quart., 2018.

[31] L. Chettri and R. Bera, "A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 16–32, Jan. 2020.

[32] J. Xu, J. Yao, L. Wang, Z. Ming, K. Wu, and L. Chen, "Narrowband Internet of Things: Evolutions, technologies, and open issues," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1449–1462, Jun. 2018.

[33] S. L. Keoh, S. S. Kumar, and H. Tschofenig, "Securing the Internet of Things: A standardization perspective," *IEEE Internet Things J.*, vol. 1, no. 3, pp. 265–275, Jun. 2014.

[34] X. Zha *et al.*, "The impact of link duration on the integrity of distributed mobile networks," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2240–2255, Sep. 2018.

[35] I. Andrea, C. Chrysostomou, and G. C. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, 2015, pp. 180–187.

[36] Z. Su, Y. Wang, Q. Xu, and N. Zhang, "LVBS: Lightweight vehicular blockchain for secure data sharing in disaster rescue," *IEEE Trans. Depend. Secure Comput.*, early access, Mar. 13, 2020, doi: 10.1109/TDSC.2020.2980255.

[37] M. Abomhara and G. M. K. Ien, "Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks," *J. Cyber Secur. Mobility*, vol. 4, no. 1, pp. 65–88, 2015.

[38] Y. Wang, Z. Su, K. Zhang, and A. Benslimane, "Challenges and solutions in autonomous driving: A blockchain approach," *IEEE Netw.*, vol. 34, no. 4, pp. 218–226, Jul./Aug. 2020.

[39] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[40] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops*, 2015, pp. 180–184.

[41] N. Kaaniche and M. Laurent, "A blockchain-based data usage auditing architecture with enhanced privacy and availability," in *Proc. IEEE 16th Int. Symp. Netw. Comput. Appl. (NCA)*, 2017, pp. 403–407.

[42] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, "GDPR-compliant personal data management: A blockchain-based solution," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1746–1761, 2019.

[43] N. Zhang, W. Yu, X. Fu, and S. K. Das, "Maintaining defender's reputation in anomaly detection against insider attacks," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 40, no. 3, pp. 597–611, Jun. 2010.

[44] L. Liu, O. De Vel, Q.-L. Han, J. Zhang, and Y. Xiang, "Detecting and preventing cyber insider threats: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1397–1417, 2nd Quart., 2018.

[45] D. Antonioli, N. Tippenhauer, and K. Rasmussen, "BIAS: Bluetooth impersonation attacks," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2020, pp. 549–562.

[46] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 372–383, Oct. 2014.

[47] F. Montori, L. Bedogni, and L. Bononi, "A collaborative Internet of Things architecture for smart cities and environmental monitoring," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 592–605, Apr. 2018.

[48] N. Zhang, R. Wu, S. Yuan, C. Yuan, and D. Chen, "RAV: Relay aided vectorized secure transmission in physical layer security for Internet of Things under active attacks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8496–8506, Oct. 2019.

[49] N. Zhang *et al.*, "Physical-layer authentication for Internet of Things via WFRFT-based Gaussian tag embedding," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 9001–9010, Sep. 2020.

[50] Univ. New South Wales, School Elect. Eng. Telecommun., Sydney, NSW, Australia. *Inside Job-Security and Privacy Threats for Smart-Home IoT Devices*. (2016). Accessed: June 12, 2019. [Online]. Available: https://accan.org.au/grants/completed-grants/1442-inside-job

[51] Q. Xu, Z. Su, and R. Lu, "Game theory and reinforcement learning based secure edge caching in mobile social networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3415–3429, 2020.

[52] X. Liu, M. Zhao, S. Li, F. Zhang, and W. Trappe, "A security framework for the Internet of Things in the future Internet architecture," *Future Internet* , vol. 9, no. 3, p. 27, 2017.

[53] R. Gamble and S. AlQahtani, "Mitigating service impersonation attacks in clouds," in *Proc. Future Technol. Conf. (FTC)*, 2016, pp. 998–1007.

[54] S. Mondal, K. P. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, and P. Chahal, "Blockchain inspired RFID-based information architecture for food supply chain," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5803–5813, Jun. 2019.

[55] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain," *IEEE Access*, vol. 5, pp. 17465–17477, 2017.

[56] P. Cui, J. Dixon, U. Guin, and D. Dimase, "A blockchain-based framework for supply chain provenance," *IEEE Access*, vol. 7, pp. 157113–157125, 2019.

[57] J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator's perspective," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 451–466, Jan. 2020.

[58] W. Dai, C. Dai, K.-K. R. Choo, C. Cui, D. Zou, and H. Jin, "SDTE: A secure blockchain-based data trading ecosystem," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 725–737, 2019.

[59] Z. Su, Y. Wang, Q. Xu, M. Fei, Y. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4601–4613, Jun. 2019.

[60] Y. Wang, Z. Su, and N. Zhang, "BSIS: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3620–3631, Jun. 2019.

[61] S. Li, T. Qin, and G. Min, "Blockchain-based digital forensics investigation framework in the Internet of Things and social systems," *IEEE Trans. Comput. Social Syst.*, vol. 6, no. 6, pp. 1433–1441, Dec. 2019.

[62] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4Forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 50–57, Oct. 2018.

[63] J. Ricci, I. Baggili, and F. Breitinger, "Blockchain-based distributed cloud storage digital forensics: Where's the beef?" *IEEE Security Privacy*, vol. 17, no. 1, pp. 34–42, Jan./Feb. 2019.

[64] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1191–1221, 2nd Quart., 2020.

[65] D.-P. Le, H. Meng, L. Su, S. L. Yeo, and V. L. L. Thing, "BIFF: A blockchain-based IoT forensics framework with identity privacy," in *Proc. TENCON IEEE Region 10 Conf.*, 2018, pp. 2372–2377.

[66] D. Ron and A. Shamir, "Quantitative analysis of the full Bitcoin transaction graph," in *Financial Cryptography and Data Security*. Berlin, Germany: Springer, 2013, pp. 6–24.

[67] A. Nugraha Tama, H. Kusuma Wardana, and S. Nugroho, "Gossip algorithm implementation for network protocol," in *Proc. Int. Seminar Appl. Technol. Inf. Commun.*, 2018, pp. 299–303.

[68] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in Bitcoin," in *Financial Cryptography and Data Security*. Berlin, Germany: Springer, 2015, pp. 507–527.

[69] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*, (2009). [Online]. Available: https://bitcoin.org/bitcoin.pdf

[70] S. De Angelis, L. Aniello, F. Lombardi, A. Margheri, and V. Sassone, "PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain," in *Proc. Italian Conf. Cyber Secur.*, 2018, p. 11.

[71] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (PoET)," in *Stabilization, Safety, and Security of Distributed Systems*. Berlin, Germany: Springer 2017, pp. 282–297.

[72] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proof of Space," *IACR Cryptol. ePrint Arch.*, vol. 2013, p. 796, 2013.

[73] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *Proc. 3rd Symp. Oper. Syst. Design Implement. (OSDI)*, 1999, pp. 173–186.

[74] D. Mazières, *The Stellar Consensus Protocol: A Federated Model for Internet-Level Consensus,* Stanford CS140/CS251, Stellar Develop. Found., vol. 32, 2015.

[75] *The dBFT Algorithm*. [Online]. Available: https://docs.neo.org/docs/en-us/basic/consensus/consensus_algorithm.html (Accessed: Oct. 2021).

[76] R. Kotla, L. Alvisi, M. Dahlin, A. Clement, and E. Wong, "Zyzzyva: Speculative byzantine fault tolerance," *ACM Trans. Comput. Syst.*, vol. 27, no. 4, 2010, Art. no. 7.

[77] A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song, "The honey badger of BFT protocols," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2016, pp. 31–42.

[78] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in Bitcoin," 2016, *arxiv:abs/1507.06183*.

[79] T. Ruffing, S. A. Thyagarajan, V. Ronge, and D. Schroder, "(short paper) burning Zerocoins for fun and for profit–A cryptographic denial-of-spending attack on the Zerocoin protocol," in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, 2018, pp. 116–119.

[80] *Meet the Tangle*. [Online]. Available: https://www.iota.org/research/meet-the-tangle (Accessed: Oct. 2021).

[81] L. Luu, V. Narayanan, K. Baweja, C. Zheng, S. Gilbert, and P. Saxena, "SCP: A computationally-scalable byzantine consensus protocol for blockchains," *IACR Cryptol. ePrint Arch.*, vol. 2015, p. 1168, 2015.

[82] Q. Wang, R. Y. K. Lau, and X. Mao, "Blockchain-enabled smart contracts for enhancing distributor-to-consumer transactions," *IEEE Consum. Electron. Mag.*, vol. 8, no. 6, pp. 22–28, Nov. 2019.

[83] E. Androulaki *et al.*, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. EuroSys*, 2018, p. 30.

[84] X. Huang, D. Ye, R. Yu, and L. Shu, "Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design," *IEEE/CAA J. Automatica Sinica*, vol. 7, no. 2, pp. 426–441, Mar. 2020.

[85] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3680–3689, Jun. 2019.

[86] Y. Liu, K. Wang, Y. Lin, and W. Xu, "LightChain: A lightweight blockchain system for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3571–3581, Jun. 2019.

[87] P. P. Ray, N. Kumar, and D. Dash, "BLWN: Blockchain-based lightweight simplified payment verification in IoT-assisted e-Healthcare," *IEEE Syst. J.*, vol. 15, no. 1, pp. 134–145, Mar. 2021.

[88] W. Dai, J. Deng, Q. Wang, C. Cui, D. Zou, and H. Jin, "SBLWT: A secure blockchain lightweight wallet based on Trustzone," *IEEE Access*, vol. 6, pp. 40638–40648, 2018.

[89] S. Fu, J. Gao, and L. Zhao, "Integrated resource management for terrestrial-satellite systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 3256–3266, Mar. 2020.

[90] H. Wei, W. Feng, C. Zhang, Y. Chen, Y. Fang, and N. Ge, "Creating efficient blockchains for the Internet of Things by coordinated satellite-terrestrial networks," *IEEE Wireless Commun.*, vol. 27, no. 3, pp. 104–110, Jun. 2020.

[91] J. M. Carter, H. S. Narman, O. Cosgun, and J. Liu, "Trade-off model of fog-cloud computing for space information networks," in *Proc. IEEE Cloud Summit*, 2020, pp. 91–96.

[92] M. J. Molesky, E. A. Cameron, J. Jones, M. Esposito, L. Cohen, and C. Beauregard, "Blockchain network for space object location gathering," in *Proc. IEEE 9th Annu. Inf. Technol. Electron. Mobile Commun. Conf. (IEMCON)*, 2018, pp. 1226–1232.

[93] S. R. Pokhrel, "Blockchain brings trust to collaborative drones and LEO satellites: An intelligent decentralized learning in the space," *IEEE Sensors J.*, vol. 21, no. 22, pp. 25331–25339, Nov. 2021, doi: 10.1109/JSEN.2021.3060185.

[94] B. Li, Z. Fei, and Y. Zhang, "UAV communications for 5G and beyond: Recent advances and future trends," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2241–2263, Apr. 2019.

[95] X. Xu, H. Zhao, H. Yao, and S. Wang, "A blockchain-enabled energy-efficient data collection system for UAV-assisted IoT," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2431–2443, Feb. 2021.

[96] A. Islam and S. Y. Shin, "BUAV: A blockchain based secure UAV-assisted data acquisition scheme in Internet of Things," *J. Commun. Netw.*, vol. 21, no. 5, pp. 491–502, Oct. 2019.

[97] A. Asheralieva and D. Niyato, "Distributed dynamic resource management and pricing in the IoT systems with blockchain-as-a-service and UAV-enabled mobile edge computing," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1974–1993, Mar. 2020.

[98] L. Jiang, B. Chen, S. Xie, S. Maharjan, and Y. Zhang, "Incentivizing resource cooperation for blockchain empowered wireless power transfer in UAV networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15828–15841, Dec. 2020.

[99] H. Xu, W. Huang, Y. Zhou, D. Yang, M. Li, and Z. Han, "Edge computing resource allocation for unmanned aerial vehicle assisted mobile network with blockchain applications," *IEEE Trans. Wireless Commun.*, vol. 20, no. 5, pp. 3107–3121, May 2021.

[100] C. Chen, J. Wu, H. Lin, W. Chen, and Z. Zheng, "A secure and efficient blockchain-based data trading approach for Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 9110–9121, Sep. 2019.

[101] C. Li, Y. Fu, F. R. Yu, T. H. Luan, and Y. Zhang, "Vehicle position correction: A vehicular blockchain networks-based GPS error sharing framework," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 2, pp. 898–912, Feb. 2021.

[102] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3516–3526, Jun. 2019.

[103] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access," *IEEE Veh. Technol. Mag.*, vol. 13, no. 1, pp. 32–39, Mar. 2018.

[104] R. Zhu, H. Liu, L. Liu, W. Hu, and B. Yuan, "A blockchain-based two-stage secure spectrum intelligent sensing and sharing auction mechanism," *IEEE Trans. Ind. Informat.*, early access, Aug. 12, 2021, doi: 10.1109/TII.2021.3104325.

[105] L. Xue, W. Yang, W. Chen, and L. Huang, "STBC: A novel blockchain-based spectrum trading solution," *IEEE Trans. Cogn. Commun. Netw.*, early access, Jun. 4, 2021, doi: 10.1109/TCCN.2021.3086490.

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

[107] J. Liu, S. Guo, Y. Shi, L. Feng, and C. Wang, "Decentralized caching framework toward edge network based on blockchain," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 9158–9174, Sep. 2020.

[108] Q. Xu, Z. Su, and Q. Yang, "Blockchain-based trustworthy edge caching scheme for mobile cyber-physical system," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 1098–1110, Feb. 2020.

[109] Z. Zhou, B. Wang, M. Dong, and K. Ota, "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 1, pp. 43–57, Jan. 2020.

[110] M. U. Hassan, M. H. Rehmani, and J. Chen, "DEAL: Differentially private auction for blockchain-based microgrids energy trading," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 263–275, Mar./Apr. 2020.

[111] Y. Wang *et al.*, "Blockchain-based secure and cooperative private charging pile sharing services for vehicular networks," *IEEE Trans. Vehicle Technol.*, early access, Dec. 1, 2021, doi: 10.1109/TVT.2021.3131744.

[112] N. C. Luong, X. Lu, D. T. Hoang, D. Niyato, and D. I. Kim, "Radio resource management in joint radar and communication: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 780–814, 2nd Quart., 2021.

[113] S. Bayhan, A. Zubow, P. Gawlowicz, and A. Wolisz, "Smart contracts for spectrum sensing as a service," *IEEE Trans. Cogn. Commun. Netw.*, vol. 5, no. 3, pp. 648–660, Sep. 2019.

[114] "ITC white paper," Kolkata, West Bengal. [Online]. Available: https://iotchain.io/whitepaper/ITCWHITEPAPER.pdf (Accessed: Oct. 2021).

[115] "IOTW," Kowloon, Hong Kong. [Online]. Available: https://iotw.io/ (Accessed: Oct. 2021).

[116] "Power ledger white paper," Perth, WA, Australia. (2019). [Online]. Available: https://www.powerledger.io/company/power-ledger-whitepaper (Accessed: Oct. 2021).

[117] Z. Zhou, X. Chen, Y. Zhang, and S. Mumtaz, "Blockchain-empowered secure spectrum sharing for 5G heterogeneous networks," *IEEE Netw.*, vol. 34, no. 1, pp. 24–31, Jan./Feb. 2020.

[118] Z. Xiong, Y. Zhang, N. C. Luong, D. Niyato, P. Wang, and N. Guizani, "The best of both worlds: A general architecture for data management in blockchain-enabled Internet -of-Things," *IEEE Netw.*, vol. 34, no. 1, pp. 166–173, Jan./Feb. 2020.

[119] Y. Wang *et al.*, "SPDS: A secure and auditable private data sharing scheme for smart grid based on blockchain," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7688–7699, Nov. 2021.

[120] A. Ouaddah, A. A. E. Kalam, and A. A. Ouahman, "FairAccess: A new blockchain-based access control framework for the Internet of Things," *Security Commun. Netw.*, vol. 9, no. 18, pp. 5943–5964, 2016.

[121] S. Qi, Y. Lu, Y. Zheng, Y. Li, and X. Chen, "Cpds: Enabling compressed and private data sharing for industrial Internet of Things over blockchain," *IEEE Trans. Ind. Informat.*, vol. 17, no. 4, pp. 2376–2387, Apr. 2021.

[122] B. Faber, G. C. Michelet, N. Weidmann, R. Mukkamala, and R. Vatrapu, "BPDIMS: A blockchain-based personal data and identity management system," in *Proc. 52nd Hawaii Int. Conf. Syst. Sci.*, 2019, pp. 6855–6864.

[123] K. Fan *et al.*, "A secure and verifiable data sharing scheme based on blockchain in vehicular social networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5826–5835, Jun. 2020.

[124] M. Du, Q. Chen, J. Chen, and X. Ma, "An optimized consortium blockchain for medical information sharing," *IEEE Trans. Eng. Manag.*, vol. 68, no. 6, pp. 1677–1689, Dec. 2021.

[125] Datum, Johns Creek, GA, USA. [Online]. Available: https://datum.org/assets/Datum-WhitePaper.pdf (Accessed: Oct. 2021).

[126] S. Ohashi, H. Watanabe, T. Ishida, S. Fujimura, A. Nakadaira, and J. Kishigami, "Token-based sharing control for IPFS," in *Proc. IEEE Int. Conf. Blockchain*, 2019, pp. 361–367.

[127] X. Wang *et al.*, "Survey on blockchain for Internet of Things," *Comput. Commun.*, vol. 136, pp. 10–29, Feb. 2019.

[128] I. Friese, J. Heuer, and N. Kong, "Challenges from the identities of things: Introduction of the identities of things discussion group within Kantara initiative," *Proc. IEEE World Forum Internet Things (WF-IoT)*, 2014, pp. 1–4.

[129] H. Aftab, K. Gilani, J. Lee, L. Nkenyereye, S. M. Jeong, and J. S. Song, "Analysis of identifiers in IoT platforms," *Digit. Commun. Netw.*, vol. 6, no. 3, pp. 333–340, 2020.

[130] M. Kuperberg, "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1008–1027, Nov. 2020.

[131] J. Xu, K. Xue, H. Tian, J. Hong, D. S. L. Wei, and P. Hong, "An identity management and authentication scheme based on redactable blockchain for mobile networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6688–6698, Jun. 2020.

[132] M. Shen *et al.*, "Blockchain-assisted secure device authentication for cross-domain industrial IoT," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 5, pp. 942–954, May 2020.

[133] X. Liu, A. Yang, C. Huang, Y. Li, T. Li, and M. Li, "Decentralized anonymous authentication with fair billing for space-ground integrated networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 8, pp. 7764–7777, Aug. 2021.

[134] R. Han, L. Bai, J. Liu, and P. Chen, "Blockchain-based GNSS spoofing detection for multiple UAV systems," *J. Commun. Inf. Netw.*, vol. 4, no. 2, pp. 81–88, Jun. 2019.

[135] X. Li, Y. Wang, P. Vijayakumar, D. He, N. Kumar, and J. Ma, "Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 11309–11322, Nov. 2019.

[136] Y. Tan, J. Liu, and N. Kato, "Blockchain-based key management for heterogeneous flying ad hoc network," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7629–7638, Nov. 2021.

[137] C. Zhao, M. Shi, M. Huang, and X. Du, "Authentication scheme based on hashchain for space-air-ground integrated network," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2019, pp. 1–6.

[138] Y. Yao, X. Chang, J. Mišić, and V. B. Mišić, "Lightweight and privacy-preserving ID-as-a-service provisioning in vehicular cloud computing," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 2185–2194, Feb. 2020.

[139] K. O. Asamoah *et al.*, "Zero-Chain: A blockchain-based identity for digital city operating system," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10336–10346, Oct. 2020.

[140] S. He, W. Ren, T. Zhu, and K.-K. R. Choo, "BoSMoS: A Blockchain-based status monitoring system for defending against unauthorized software updating in industrial Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 948–959, Feb. 2020.

[141] O. Leiba, Y. Yitzchak, R. Bitton, A. Nadler, and A. Shabtai, "Incentivized delivery network of IoT software updates based on trustless proof-of-distribution," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS PW)*, 2018, pp. 29–39.

[142] D. Liu, A. Alahmadi, J. Ni, X. Lin, and X. Shen, "Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3527–3537, Jun. 2019.

[143] SmartAxiom, Brea, CA, USA. [Online]. Available: https://www.smartaxiom.com/ (Accessed: Oct. 2021).

[144] A. Giaretta, S. Pepe, and N. Dragoni, "UniquID: A quest to reconcile identity access management and the Internet of Things," 2019, *arXiv: abs/1905.04021*.

[145] ShoCard, Palo Alto, CA, USA. [Online]. Available: https://www.shocard.com/en.html (Accessed: Oct. 2021).

[146] Xage Security, Palo Alto, CA, USA. [Online]. Available: https://xage.com/ (Accessed: Oct. 2021).

[147] S. Dhakal, F. Jaafar, and P. Zavarsky, "Private blockchain network for iot device firmware integrity verification and update," in *Proc. IEEE 19th Int. Symp. High Assurance Syst. Eng. (HASE)*, 2019, pp. 164–170.

[148] P. Otte, M. de Vos, and J. Pouwelse, "TrustChain: A sybil-resistant scalable blockchain," *Future Gener. Comput. Syst.*, vol. 107, pp. 770–780, Jun. 2020.

[149] M. Feng and H. Xu, "MSNET-Blockchain: A new framework for securing mobile satellite communication network," in *Proc. 16th Annu. IEEE Int. Conf. Sens. Commun. Netw. (SECON)*, 2019, pp. 1–9.

[150] Y.-H. Zhang and X. F. Liu, "Satellite broadcasting enabled blockchain protocol: A preliminary study," in *Proc. Inf. Commun. Technol. Conf. (ICTC)*, 2020, pp. 118–124.

[151] V. Sharma, I. You, D. N. K. Jayakody, D. G. Reina, and K.-K. R. Choo, "Neural-blockchain-based ultrareliable caching for edge-enabled UAV networks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 10, pp. 5723–5736, Oct. 2019.

[152] P. Abichandani, D. Lobo, S. Kabrawala, and W. McIntyre, "Secure communication for multiquadrotor networks using Ethereum blockchain," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1783–1796, Feb. 2021.

[153] K. Gai, Y. Wu, L. Zhu, K.-K. R. Choo, and B. Xiao, "Blockchain-enabled trustworthy group communications in UAV networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4118–4130, Jul. 2021.

[154] M. Pattaranantakul, R. He, Q. Song, Z. Zhang, and A. Meddahi, "NFV security survey: From use case driven threat analysis to state-of-the-art countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3330–3368, 4th Quart., 2018.

[155] N. Hu *et al.*, "Building agile and resilient UAV networks based on SDN and blockchain," *IEEE Netw.*, vol. 35, no. 1, pp. 57–63, Jan./Feb. 2021.

[156] K. Gai, Y. Wu, L. Zhu, Z. Zhang, and M. Qiu, "Differential privacy-based blockchain for industrial Internet-of-Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4156–4165, Jun. 2020.

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

[158] P. H. A. P. Badarudin, A. T. Wan, and S. Phon-Amnuaisuk, "A blockchain-based assistance digital model for first responders and emergency volunteers in disaster response and recovery," in *Proc. 8th Int. Conf. Inf. Commun. Technol. (ICoICT)*, 2020, pp. 1–5.

[159] K.-K. Muniswamy-Reddy, D. A. Holland, U. Braun, and M. Seltzer, "Provenance-aware storage systems," in *Proc. Annu. Conf. USENIX Annu. Tech. Conf.*, 2006, pp. 43–56.

[160] C. H. Suen, R. K. L. Ko, Y. S. Tan, P. Jagadpramana, and B. S. Lee, "S2logger: End-to-end data tracking mechanism for cloud data provenance," in *Proc. 12th IEEE Int. Conf. Trust Secur. Privacy Comput. Commun.*, 2013, pp. 594–602.

[161] S. Malik, S. S. Kanhere, and R. Jurdak, "ProductChain: Scalable blockchain framework to support provenance in supply chains," in *Proc. IEEE 17th Int. Symp. Netw. Comput. Appl. (NCA)*, 2018, pp. 1–10.

[162] M. Westerkamp, F. Victor, and A. Küpper, "Tracing manufacturing processes using blockchain-based token compositions," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 167–176, 2020.

[163] M. Baza, N. Lasla, M. M. E. A. Mahmoud, G. Srivastava, and M. Abdallah, "B-ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1214–1229, Apr.-Jun. 2021.

[164] L. Wang, X. Lin, E. Zima, and C. Ma, "Towards Airbnb-like privacy-enhanced private parking spot sharing based on blockchain," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 2411–2423, Mar. 2020.

[165] H. Ritzdorf, C. Soriente, G. O. Karame, S. Marinovic, D. Gruber, and S. Capkun, "Toward shared ownership in the cloud," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 12, pp. 3019–3034, Dec. 2018.

[166] "WaltonChain white paper v2.0 2018," Seoul, South Korea. [Online]. Available: https://www.waltonchain.org/pdf/5edf3d0304205.pdf (Accessed: Oct. 2021).

[167] "BlockVerify," London, U.K. [Online]. Available: https://www.cbinsights.com/company/block-verify (Accessed: Oct. 2021).

[168] M. Pourvahab and G. Ekbatanifard, "An efficient forensics architecture in software-defined networking-IoT using blockchain technology," *IEEE Access*, vol. 7, pp. 99573–99588, 2019.

[169] Y. Lu, Y. Qi, S. Qi, Y. Li, H. Song, and Y. Liu, "Say no to price discrimination: Decentralized and automated incentives for price auditing

in ride-hailing services," *IEEE Trans. Mobile Comput.*, early access, Jul. 9, 2020, doi: 10.1109/TMC.2020.3008315.

[170] B. Li, R. Liang, W. Zhou, H. Yin, H. Gao, and K. Cai, "LBS meets blockchain: An efficient method with security preserving trust in SAGIN," *IEEE Internet Things J.*, early access, Mar. 8, 2021, doi: 10.1109/JIOT.2021.3064357.

[171] M. S. Rahman, I. Khalil, and M. Atiquzzaman, "Blockchain-powered policy enforcement for ensuring flight compliance in drone-based service systems," *IEEE Netw.*, vol. 35, no. 1, pp. 116–123, Jan./Feb. 2021.

[172] M. Keshavarz, M. Gharib, F. Afghah, and J. D. Ashdown, "UASTrustChain: A decentralized blockchain- based trust monitoring framework for autonomous unmanned aerial systems," *IEEE Access*, vol. 8, pp. 226074–226088, 2020.

[173] AirUTM. [Online]. Available: https://airdonex.com/ (Accessed: Oct. 2021).

[174] L. Clark, Y.-C. Tung, M. Clark, and L. Zapanta, "A blockchain-based reputation system for small satellite relay networks," in *Proc. IEEE Aerosp. Conf.*, 2020, pp. 1–8.

[175] Y. Wu, X. Lu, and Z. Wu, "Blockchain-based trust model for air traffic management network," in *Proc. IEEE 6th Int. Conf. Comput. Commun. Syst. (ICCCS)*, 2021, pp. 92–98.

[176] "Can You Use a Raspberry Pi to Mine Cryptocurrency?," 2021. [Online]. Available: https://www.makeuseof.com/can-you-use-a-raspberry-pi-mine-cryptocurrency/ (Accessed: Oct. 2021).

[177] J.-S. Lee, Y.-W. Su, and C.-C. Shen, "A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi," *Proc. IECON 33rd Annu. Conf. IEEE Ind. Electron. Soc.*, 2007, pp. 46–51.

[178] A. Nanda, D. Puthal, J. J. P. C. Rodrigues, and S. A. Kozlov, "Internet of autonomous vehicles communications security: Overview, issues, and directions," *IEEE Wireless Commun.*, vol. 26, no. 4, pp. 60–65, Aug. 2019.

[179] M. M. Rathore, A. Ahmad, A. Paul, and S. Rho, "Urban planning and building smart cities based on the Internet of Things using big data analytics," *Comput. Netw.*, vol. 101, pp. 63–80, Jun. 2016.

[180] I. Eyal, A. E. Gencer, E. G. Sirer, and R. V. Renesse, "Bitcoin-NG: A scalable blockchain protocol," in *Proc. 13th USENIX Symp. Netw. Syst. Design Implement. (NSDI)*, Santa Clara, CA, USA, Mar. 2016, pp. 45–59.

[181] I.-H. Hou and P. R. Kumar, "Real-time communication over unreliable wireless links: A theory and its applications," *IEEE Wireless Commun.*, vol. 19, no. 1, pp. 48–59, Feb. 2012.

[182] K. Croman *et al.*, "On scaling decentralized blockchains," in *Financial Cryptography and Data Security*. Berlin, Germany: Springer, 2016, pp. 106–125.

[183] C. Decker and R. Wattenhofer, "Information propagation in the Bitcoin network," in *Proc. IEEE P2P*, 2013, pp. 1–10.

[184] M. Saad *et al.*, "Exploring the attack surface of blockchain: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1977–2008, 3rd Quart., 2020.

[185] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking Bitcoin: Routing attacks on cryptocurrencies," in *Proc. IEEE Symp. Secur. Privacy (SP)*, 2017, pp. 375–392.

[186] S. Sayeed, H. Marco-Gisbert, and T. Caira, "Smart contract: Attacks and protections," *IEEE Access*, vol. 8, pp. 24416–24427, 2020.

[187] L. Kan, Y. Wei, A. Hafiz Muhammad, W. Siyuan, L. C. Gao, and H. Kai, "A multiple blockchains architecture on inter-blockchain communication," in *Proc. IEEE Int. Conf. Softw. Quali. Rel. Secur. Companion (QRS-C)*, 2018, pp. 139–145.

[188] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "OmniLedger: A secure, scale-out, decentralized ledger via sharding," in *Proc. IEEE Symp. Secur. Privacy (SP)*, 2018, pp. 583–598.

[189] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in Bitcoin," in *Financial Cryptography and Data Security*. Berlin, Germany: Springer, 2013, pp. 34–51.

[190] M. C. K. Khalilov and A. Levi, "A survey on anonymity and privacy in Bitcoin-like digital cash systems," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2543–2585, 3rd Quart., 2018.

[191] Y. Huang, J. Wu, and C. Long, "Drugledger: A practical blockchain system for drug traceability and regulation," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber Phys. Soc. Comput. (CPSCom) IEEE Smart Data (SmartData)*, 2018, pp. 1137–1144.

[192] L. Cui, S. Yang, Z. Chen, Y. Pan, M. Xu, and K. Xu, "An efficient and compacted DAG-based blockchain protocol for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4134–4145, Jun. 2020.

[193] G. S. Manku, M. Bawa, and P. Raghavan, "Symphony: Distributed hashing in a small world," in *Proc. 4th USENIX Symp. Internet Technol. Syst.*, 2003, pp. 127–140.

[194] Y. Guo, J. Tong, and C. Feng, "A measurement study of Bitcoin lightning network," in *Proc. IEEE Int. Conf. Blockchain*, 2019, pp. 202–211.

[195] A. Palai, M. Vora, and A. Shah, "Empowering light nodes in blockchains with block summarization," in *Proc. 9th IFIP Int. Conf. New Technol. Mobility Secur. (NTMS)*, 2018, pp. 1–5.

[196] M. H. Manshaei, M. Jadliwala, A. Maiti, and M. Fooladgar, "A game-theoretic analysis of shard-based permissionless blockchains," *IEEE Access*, vol. 6, pp. 78100–78112, 2018.

[197] L. Atzori, A. Iera, and G. Morabito, "SIoT: Giving a social structure to the Internet of Things," *IEEE Commun. Lett.*, vol. 15, no. 11, pp. 1193–1195, Nov. 2011.

[198] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled Internet of vehicles: Optimizing consensus management using reputation and contract theory," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2906–2920, Mar. 2019.

[199] "Atonomi for trusted IoT," [Online]. Available: https://assets.website-files.com/5b95e56c7572f5c98b3993d9/5bea12e1bc354be65c577c0c_Atonomi-White-Paper-v0.9.4b.pdf (Accessed: Oct. 2021).

[200] M. C. Vuran, O. B. Akan, and I. F. Akyildiz, "Spatio-temporal correlation: theory and applications for wireless sensor networks," *Comput. Netw.*, vol. 45, pp. 245–259, Jun. 2004.

[201] C. Huang *et al.*, "RepChain: A reputation based secure, fast and high incentive blockchain system via sharding," 2019, *arXiv: abs/1901.05741*.

[202] J. Yu, D. Kozhaya, J. Decouchant, and P. Esteves-Verissimo, "RepuCoin: Your reputation is your power," *IEEE Trans. Comput.*, vol. 68, no. 8, pp. 1225–1237, Aug. 2019.

[203] Z. Xiong, J. Kang, D. Niyato, P. Wang, and H. V. Poor, "Cloud/edge computing service management in blockchain networks: Multi-leader multi-follower game-based admm for pricing," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 356–367, Mar./Apr. 2020.

[204] X. Liu, W. Wang, D. Niyato, N. Zhao, and P. Wang, "Evolutionary game for mining pool selection in blockchain networks," *IEEE Wireless Commun. Lett.*, vol. 7, no. 5, pp. 760–763, Oct. 2018.

[205] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[206] W. Chen, X. Qiu, T. Cai, H.-N. Dai, Z. Zheng, and Y. Zhang, "Deep reinforcement learning for Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1659–1692, 3rd Quart., 2021.

[207] Y. Wang, Z. Su, Q. Xu, R. Li, and T. H. Luan, "Lifesaving with RescueChain: Energy-efficient and partition-tolerant blockchain based secure information sharing for UAV-aided disaster rescue," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, 2021, pp. 1–10.

[208] A. Back *et al.* (2014). Enabling blockchain innovations with pegged sidechains. [Online]. Available: https://blockstream.com/sidechains.pdf

[209] A. Hopebailie and S. Thomas, "Interledger: Creating a standard for payments," in *Proc. Int. Conf. Companion World Wide Web*, 2016, pp. 281–282.

[210] L. Deng, H. Chen, Z. Jing, and L. J. Zhang, *Research on Cross-Chain Technology Based on Sidechain and Hash-Locking*. Cham, Switzerland: Springer, 2018, pp. 144–151.

[211] P. Frauenthaler, M. Sigwart, C. Spanring, and S. Schulte, "Testimonium: A cost-efficient blockchain relay," 2020, *arXiv:2002.12837*.

[212] A. Peter, E. Tews, and S. Katzenbeisser, "Efficiently outsourcing multiparty computation under multiple keys," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2046–2058, Dec. 2013.

[213] B. B´unz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short proofs for confidential transactions and more," in *Proc. IEEE Symp. Secur. Privacy (SP)*, 2017, pp. 315–334.

[214] F. Zhang *et al.*, "The ekiden platform for confidentiality-preserving, trustworthy, and performant smart contracts," *IEEE Security Privacy*, vol. 18, no. 3, pp. 17–27, May/Jun. 2020.

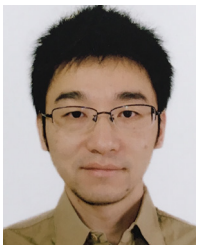
[215] W. Wang *et al.*, "Leaky cauldron on the dark land: Understanding memory side-channel hazards in SGX," in *Proc. 2017 ACM SIGSAC Conf. Comput. Commun. Secur.*, 2017, pp. 2421–2434.

[216] J. V. Bulck *et al.*, "Foreshadow: Extracting the keys to the intel SGX kingdom with transient out-of-order execution," in *Proc. 27th USENIX Secur. Symp.*, 2018, pp. 991–1008.

[217] N. Zhang, K. Sun, D. Shands, W. Lou, and Y. T. Hou, "TruSense: Information leakage from TrustZone," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, 2018, pp. 1097–1105.

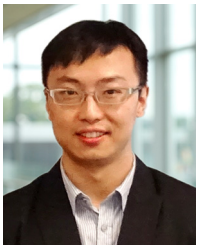
[218] G. Epiphaniou, P. Pillai, M. Bottarelli, H. Al-Khateeb, M. Hammoudeh, and C. Maple, "Electronic regulation of data sharing and processing using smart ledger technologies for supply-chain security," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1059–1073, Nov. 2020s.
[219] "LegalXchain technical white paper." [Online]. Available: https://www.legalxchain.com/en/technology (Accessed: Oct. 2021).
[220] Y. Li *et al.*, "Toward privacy and regulation in blockchain-based cryptocurrencies," *IEEE Netw.*, vol. 33, no. 5, pp. 111–117, Sep./Oct. 2019.
[221] "IoTex white paper." [Online]. Available: https://iotex.io/white-paper (Accessed: Oct. 2021).
[222] S. Wijethilaka and M. Liyanage, "Survey on network slicing for Internet of Things realization in 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 957–994, 2nd Quart., 2021.
[223] B. Nour, A. Ksentini, N. Herbaut, P. A. Frangoudis, and H. Moungla, "A blockchain-based network slice broker for 5G services," *IEEE Netw. Lett.*, vol. 1, no. 3, pp. 99–102, Sep. 2019.
[224] J. Luo, Q. Chen, F. R. Yu, and L. Tang, "Blockchain-enabled software-defined industrial Internet of Things with deep reinforcement learning," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5466–5480, Jun. 2020.
[225] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, Sep. 2017.
[226] J. Xie *et al.*, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2794–2830, 3rd Quart., 2019.
[227] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 33–39, Aug. 2018.
[228] J.-W. Liao, T.-T. Tsai, C.-K. He, and C.-W. Tien, "SoliAudit: Smart contract vulnerability assessment based on machine learning and fuzz testing," in *Proc. 6th Int. Conf. Internet Things Syst. Manag. Secur. (IOTSMS)*, 2019, pp. 458–465.
[229] D. C. Nguyen *et al.*, "Enabling AI in future wireless networks: A data life cycle perspective," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 553–595, 1st Quart., 2021.
[230] Y. Wang, Z. Su, N. Zhang, and A. Benslimane, "Learning in the air: Secure federated learning for UAV-assisted crowdsensing," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1055–1069, Apr.-Jun. 2021.
[231] W. Y. B. Lim *et al.*, "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 2031–2063, 3rd Quart., 2020.

Yuntao Wang is currently pursuing the Ph.D. degree with the School of Cyber Science and Engineering, Xi'an Jiaotong University, Xi'an, China. His research interests include security and privacy protection in wireless networks and vehicular networks.



Zhou Su (Senior Member, IEEE) research interests include wireless networking, mobile computing, and network security. He received the Best Paper Award of IEEE ICC2020, IEEE BigdataSE2019, and IEEE CyberSciTech2017. He served as the Track/Symosuim Chair for several international conferences including IEEE VTC, IEEE/CIC ICCC, and WCSP. He is an Associate Editor of IEEE INTERNET OF THINGS JOURNAL, IEEE OPEN JOURNAL OF COMPUTER SOCIETY, and IET *Communications*.

Jianbing Ni (Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Waterloo in 2018. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, Queen's University, Kingston, ON, Canada. His research interests are applied cryptography and network security, with current focus on edge computing, mobile crowdsensing, Internet of Things, and blockchain technology.



Ning Zhang (Senior Member, IEEE) received the Ph.D. degree from the University of Waterloo, Canada, in 2015. After that, he was a Postdoctoral Research Fellow with the University of Waterloo and University of Toronto, Canada. He is an Associate Professor with the University of Windsor, Canada. He received the Best Paper Awards from IEEE Globecom in 2014, the IEEE WCSP in 2015, and *Journal of Communications and Information Networks* in 2018, the IEEE ICC in 2019, the IEEE Technical Committee on Transmission Access and Optical Systems in 2019, and the IEEE ICCC in 2019. He also serves/served as a track chair for several international conferences and a co-chair for several international workshops. He serves as an Associate Editor of IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, IEEE ACCESS, and *IET Communications*, and *Vehicular Communications* (Elsevier); and a Guest Editor of several international journals, such as IEEE WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, and IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING.

Xuemin (Sherman) Shen (Fellow, IEEE) received the Ph.D. degree in electrical engineering from Rutgers University, New Brunswick, NJ, USA, in 1990. He is currently a University Professor with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research focuses on network resource management, wireless network security, the Internet of Things, 5G and beyond, and vehicular ad hoc, and sensor networks. He received the R.A. Fessenden Award from IEEE, Canada, in 2019; the Award of Merit from the Federation of Chinese Canadian Professionals, ON, Canada, in 2019; the Technical Recognition Award from the Wireless Communications Technical Committee in 2019; the James Evans Avant Garde Award from the IEEE Vehicular Technology Society in 2018; the Education Award in 2017 and the Joseph LoCicero Award in 2015 from the IEEE Communications Society; the AHSN Technical Committee in 2013; the Excellent Graduate Supervision Award from the University of Waterloo in 2006; and the Premier's Research Excellence Award (PREA) from the Province of Ontario, Canada, in 2003. He served as the Technical Program Committee Chair/Co-Chair for IEEE Globecom'16, IEEE Infocom'14, IEEE VTC'10 Fall, and IEEE Globecom'07, and the Chair for the IEEE Communications Society Technical Committee on Wireless Communications. He was the Vice President for the Technical and Educational Activities and Publications; a Member-at-Large on the Board of Governors; and the Chair of the Distinguished Lecturer Selection Committee. He is also the President Elect of the IEEE Communications Society. He served as the Editor-in-Chief for IEEE INTERNET OF THINGS JOURNAL, *IEEE Network*, and *IET Communications*. He was a member of the IEEE Fellow Selection Committee of the ComSoc. He is a Fellow of the Engineering Institute of Canada, the Canadian Academy of Engineering, the Royal Society of Canada, the Chinese Academy of Engineering Foreign Member, and a Distinguished Lecturer of the IEEE Vehicular Technology Society and Communications Society. He is also a Registered Professional Engineer in ON, Canada.