Convergence of Blockchain and Edge Computing for Secure and Scalable IIoT Critical Infrastructures in Industry 4.0

Yulei Wu, *Senior Member, IEEE*, Hong-Ning Dai, *Senior Member, IEEE*, Hao Wang, *Member, IEEE*

***Abstract*—Critical infrastructure systems are vital to underpin the functioning of a society and economy. Due to ever-increasing number of Internet-connected Internet-of-Things (IoTs) / Industrial IoT (IIoT), and high volume of data generated and collected, security and scalability are becoming burning concerns for critical infrastructures in industry 4.0. The blockchain technology is essentially a distributed and secure ledger that records all the transactions into a hierarchically expanding chain of blocks. Edge computing brings the cloud capabilities closer to the computation tasks. The convergence of blockchain and edge computing paradigms can overcome the existing security and scalability issues. In this paper, we first introduce the IoT/IIoT critical infrastructure in industry 4.0, and then we briefly present the blockchain and edge computing paradigms. After that, we show how the convergence of these two paradigms can enable secure and scalable critical infrastructures. Then, we provide a survey on state-of-the-art for security and privacy, and scalability of IoT/IIoT critical infrastructures. A list of potential research challenges and open issues in this area is also provided, which can be used as useful resources to guide future research.**

***Index Terms*—Blockchain, Edge Computing, Critical Infrastructure, Industry 4.0, Internet of Things.**

I. Introduction

Critical infrastructure systems have been used to underpin the functioning of a society and economy. They range from traditionally-defined physical assets to a more broad definition of modern assets in the sectors of electricity, gas, water supply, agriculture, public health, transportation, security services, telecommunication, etc [1], [2]. This transition is largely due to the ever-increasing usage of Internet-of-Things (IoTs) and their significant support for critical infrastructure systems in the era of industry 4.0 [3], [4], [5], [6]. The international data corporation (IDC) has forecast that there will be an estimate of 41.6 billion connected IoT devices, generating 79.4 zettabytes (ZB) in 2025[1]. IoTs have become indispensable parts of critical infrastructures in industry 4.0, creating intelligent services such as smart grid and offering a range of advantages for cost savings and efficiencies [7], [8].

The industrial control system (ICS) is the heart of a critical infrastructure [9], [10]. It is mainly responsible for supervisory control and data collection (SCADA), monitoring the processes and control flows of system information in industry. The wide adoption of Internet-connected IoT devices has presented a variety of challenging issues to critical infrastructures. First, ICS was originally designed mainly for a proprietary and closed infrastructure without considering too much about security issues, as traditional critical infrastructures are sort of isolated and are not vulnerable to cyberattacks. With these infrastructures being connected to the Internet through IoTs, a wide range of cyberattacks, including distributed denial-of-service (DDoS), malware, breach attack, Brute force attack, Man-in-the-middle attack, SQL injection, and phishing, are threatening the operation of ICS to provision normal support for services [11], [12], [13], [14]. In addition, ICS is in a position for data acquisition in critical infrastructures. The compromised ICS by cyber attackers may create potential risks for the leakage of data privacy [15], [16]. Second, scalability is another challenge which ICS was not originally designed to solve. Given the remarkable increase in the number of IoT devices and the volume of data they are collecting and analysing, the traditional centralised manner for data collection and analysis is becoming the bottleneck of ICSs [17]. A decentralised way is inevitably needed to fulfill the emerging requirements of ICSs in support of advanced critical infrastructures in industry 4.0.

The emerging blockchain and edge computing paradigms are promising technologies that can tackle the above challenging issues, in terms of security and scalability considerations of critical infrastructures. The blockchain technology has emerged as a novel secure computing paradigm without the need of any centralised authority in a networked system [18], [19], [20], [21]. It is a distributed consensus scheme that allows transactions to be securely stored and verified. In terms of security and privacy, the blockchain is created and maintained securely through the use of asymmetric cryptography with crowd computing in a peer-to-peer manner. The zero-knowledge proof has been leveraged to increase privacy protection in the blockchain system [22]. Edge computing is a decentralised computing infrastructure that brings computing and storage capabilities closer to the location where it is needed [23], [24], [25]. In terms of privacy protection, data does not have to be transferred to the remote cloud for computation and storage. Blockchain can therefore inevitably compensate the security concerns and enhance the privacy

This work was partially supported by the Engineering and Physical Sciences Research Council of United Kingdom under Grant No. EP/R030863/1. *(Corresponding authors: Y. Wu and H.-N. Dai)*

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

H.-N. Dai is with Faculty of Information Technology, Macau University of Science and Technology, Macau. email: hndai@ieee.org

H. Wang is with Department of Computer Science, Norwegian University of Science and Technology, Gjøvik, Norway email: hawa@ntnu.no

[1] https://www.idc.com/getdoc.jsp?containerId=prUS45213219

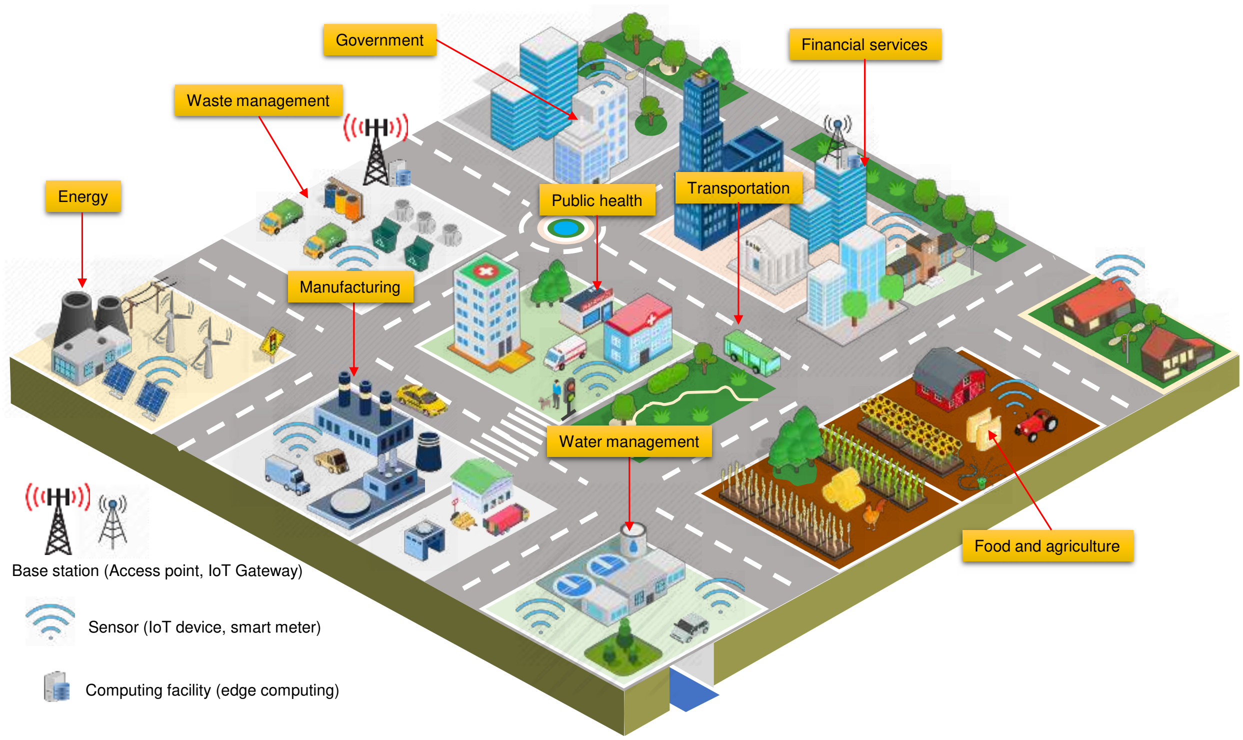


Fig. 1. Critical infrastructures with IoT.

TABLE I
A SUMMARY OF NATIONAL CRITICAL INFRASTRUCTURES IN DIFFERENT COUNTRIES.

Country	Number of Sectors	Critical Infrastructures	
		The Same Infrastructures	The Different Infrastructures
United Kingdom	13	Financial Services, Government Facilities, Communications, Energy, Health, Transportation Systems, and Water	Chemicals, Civil Nuclear, Defence, Emergency Services, Space, Food
United States of America	16		Chemicals, Dams, Information Technology, Commercial Facilities[2], Critical Manufacturing, Defence Industrial Base, Nuclear Reactors, Materials and Waste, Food
Canada	10		Information and Communication Technology, Food
Australia	8		Food
Singapore	9		Infocomm, Media

protection of edge computing. The convergence of these two technologies is vital to provide necessary computation and storage for IoTs, while guaranteeing the security and scalability of critical infrastructures in industry 4.0 [26].

Many research has been conducted to tackle security and privacy, and scalability issues of IoT based on blockchain and edge computing technologies. A systematic study of this area can take a further step to contribute to the research of IoT critical infrastructures in industry 4.0. With such a motivation, this paper introduces the critical infrastructure in industry 4.0 in Section II. Section III presents the technologies of blockchain and edge computing, followed by how they can be converged to provide necessary support for secure and scalable critical infrastructures as in Section IV. Sections V and VI review and discuss state-of-the-art for security and privacy, and scalability of IoT critical infrastructures, respectively. Section VII discusses potential challenges and open issues. Finally, Section VIII concludes this paper.

II. CRITICAL INFRASTRUCTURES IN INDUSTRY 4.0

Critical infrastructures refer to those vital assets, facilities, systems, sites, networks, information, people, processes, either physical or virtual, that are necessary to underpin the functioning of an economy and society[3], as shown in Fig. 1. It also includes those functions, sites and organisations that are not critical to the maintenance of essential services upon which daily life depends, but that needs to be protected due to potential risks to the public (e.g., civil nuclear sites). Different countries have their own definitions of national

[2] This includes a wide range of sites that draw large crowds of people for shopping, business, entertainment, or lodging.

[3] https://www.cpni.gov.uk/critical-national-infrastructure-0

critical infrastructures. Table I shows a summary of critical infrastructures in United Kingdom, United States of America, Canada, Australia, and Singapore.

Traditional critical infrastructures were quite isolated and were mainly vulnerable to physical attacks e.g., via an infected USB drive [27]. For example, the damage to the nuclear program of Iran by Stuxnet, a malicious computer worm, probably via an infected USB drive, has caused significant damage to industrial centrifuges used for enrichment of uranium[4]. Due to digital transformation of industry 4.0 driven by smart factories, big data and machine learning, critical infrastructures are equipped with a dramatic increasing number of IoT devices, or industrial IoT (IIoT) in the context of industry 4.0 [28], [29], creating the so-called *critical infrastructure with IoT* or *IoT critical infrastructure*.

Such a digital transformation of critical infrastructures is a double-edged sword. On the one hand, IoT critical infrastructures are in greater risks of being exposed of its internal structure, due to the connection to the Internet through massive IoT devices via open standard protocols [30], [31], [32], [33]. On the other hand, it provides more useful information that can be used for better maintenance of the system. For example, Airbus launched a digital manufacturing initiative called the "*Factory of the Future*"[5]. Due to the complex process of building a commercial airliner, many things that may go wrong during the manufacturing process and may further endanger passenger safety. To mitigate these potential risks, Airbus equipped sensors in its machines. Through the collected data, a set of useful actions (e.g., anomaly prediction, detection and localisation) are performed for proactive maintenance [34], [35]. Faults can be repaired by engineers before escalating to a more serious error that may stop service provision.

According to the nature of how IoT critical infrastructures work, a number of components of the infrastructure are vulnerable to cyberattacks, including the following aspects:

- *Industry devices.* There are a large number of already-deployed devices that are difficult to upgrade or patch, making critical infrastructures inflexible for efficient handling of potential faults and attacks. In contrast, the new IoT devices are connected to the Internet, and therefore, they are vulnerable to cyberattacks and can be easily compromised [6], [36].
- *Communication infrastructure.* IoT devices can now connect with other devices, including other IoT devices, computing and storage devices, through open medium such as cellular and Wi-Fi connections using open standard protocols [37]. The communication infrastructure itself is also vulnerable to cyberattacks and the communication may be eavesdropped [38].
- *Computing infrastructure.* Critical infrastructures were using centralised cloud computing, where all the data need to be transferred to the cloud data centre for processing. This creates the potential risk of privacy leakage [39], [40].

To cope with the above issues, the proposed solutions for critical infrastructures in industry 4.0 need to consider the following factors:

- *Security.* Appropriate security mechanisms need to be in place to safeguard the IoT devices, the computing infrastructure, the communication infrastructure, and various data running over these infrastructures.
- *Privacy.* Many control and maintenance decisions are learnt from data, e.g., fault prediction, detection and localisation are carried out based on many advanced data analytics methods [34], [41]. The data usage needs to be transparent, and sensitive data should not be transmitted outside its local network region.
- *Scalability.* Data analytics methods rely on data collection, storage and processing. The delay of these processes need to meet the stringent requirements of critical infrastructures and need to be scalable with the increase in the size of the infrastructure.

III. Blockchain and Edge Computing

The emerging blockchain and edge computing technologies have exhibited excellent features that can cope with the above issues mentioned in Section II. In this section, how the two technologies work and how they can handle these issues will be presented.

A. Blockchain

A blockchain is essentially a distributed and secure ledger that records all the transactions into a hierarchically expanding chain of blocks [42], [43], [44], [45], [46]. Each block in the blockchain is linked to its previous block through the hash value of the parent block, except for the first block, usually called the genesis block which does not have a parent block. New blocks can be committed to a blockchain only upon their successful completion of the competition enforced by a consensus algorithm [47], [48]. Each block consists of the following components (see Fig. 2):

- *Previous hash*, which is the hash of the parent block.
- *Timestamp*, recording the current time in seconds.
- *Nonce*, starting from 0 and increasing for every hash calculation.
- *Merkle Root*, which is the hash of all the hashes of all the transactions in the block.
- *Transactions (Tx)*, which is the transactions executed during a given period of time.

The blockchain technology possesses many features [42], [49], [50], [51] that are useful to tackle security, privacy and scalability issues of critical infrastructures in industry 4.0, including

- *Decentralisation.* A blockchain validates a new block in a decentralised way without any centralised third-party authority. In principle, every network user (node) can participate in this validation. This trustfulness validation process is essentially to complete a consensus procedure via competition amongst all the involved users, and this can be achieved by consensus algorithms, such as proof

[4] https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/642274/EPRS_BRI(2019)642274_EN.pdf

[5] http://e-lass.eu/media/2018/02/TTG-ZAL.pdf

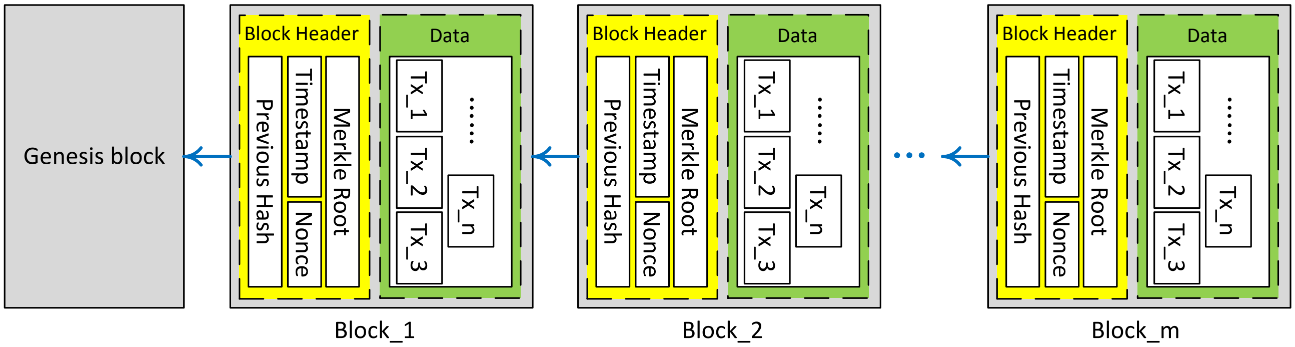


Fig. 2. An example blockchain structure.

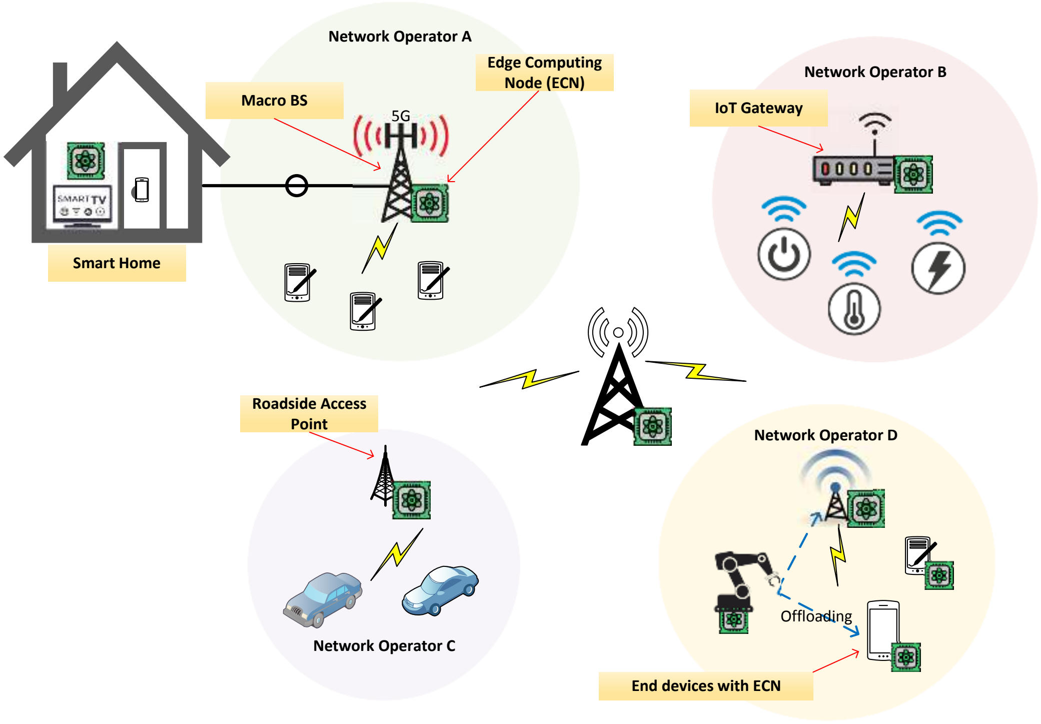


Fig. 3. Typical scenarios with edge computing.

of work (PoW) [52], proof of stake (PoS) [53], proof of burn (PoB) [53], Byzantine fault tolerance (BFT) [54], and practical BFT (PBFT) [55].

- *Immutability.* Each block in a blockchain has the hash of its previous (parent) block. Any changes to the parent block invalidates all the subsequent blocks. In addition, the Merkle root is the hash of all the hashes of all the transactions in the block. Any modification to any transactions in a block, after the block has been successfully committed into a blockchain, will result in a new Merkle root. The falsification to any transactions can therefore be easily detected.
- *Transparency.* Every user of a blockchain system can access and interact with the blockchain network.
- *Pseudonymity.* As blockchain addresses are allowed to be anonymous, users cannot access identification information of the users who have made those transactions. This preserves a certain level of user privacy [56].
- *Accountability/non-repudiation.* Blockchain systems have a digital signature scheme. Transaction initiator signs a message with her private key before issuing it out, and the recipient of this signed message uses the sender's public key to prove the validity of the message. The transaction initiator therefore cannot be denied its signed transaction.
- *Automation.* Blockchain systems allow smart contracts [57], [58], where approved contractual clauses are transformed into executable computer programs and are executed automatically when a certain condition is satisfied. The execution of each contract statement will be recorded as an immutable transaction in the blockchain.

B. Edge Computing

With the dramatic increase in the number of IoT/IIoT devices, centralised cloud computing is becoming more difficult to satisfy various quality-of-service (QoS) requirements of diversified industrial applications [59]. Edge computing has been introduced to bring the computation capability closer to a computation task, in order to reduce network latency and save bandwidth resources towards the remote cloud data centre [60], [61].

Edge computing nodes (ECNs) possess different functions and have different computation capacities according to their location distance with end users [62], as shown in Fig. 3. ECNs can be deployed at the macro base stations, providing main data computation and storage capacities. ECNs can also be deployed in a house in the smart home scenario, providing extra computing power for smart home IoT devices. They can also mounted at the roadside for the case of smart transportation, significantly reducing the response time for delay-sensitive applications such as autonomous driving. ECNs can also be deployed at IoT/IIoT gateways for industrial scenarios, providing data collection and aggregation functionalities. ECNs can even be deployed at the end devices, performing data pre-processing [63], [64].

IV. Convergence of Blockchain and Edge Computing for Secure and Scalable Critical Infrastructures

ECNs are operating by different third-party operators and are being deployed in a decentralised way, making it difficult to ensure the same level of security, transparency, and privacy preservation [65], [66]. The blockchain technology can essentially overcome the shortcomings of edge computing. In addition, edge computing can provide necessary local computing capabilities for computation tasks of blockchain systems, e.g., smart contract execution and consensus procedure. Therefore, the convergence of blockchain and edge computing paradigms can enable the following features that are crucial towards secure and scalable critical infrastructures in industry 4.0:

- *Security.* All transaction data in IoT/IIoT with edge computing are enforced automatically by smart contracts and added to a blockchain upon successfully committed to a block. Security mechanisms can be easily implemented by smart contracts.
- *Privacy.* Data can be collected and handled locally by edge computing. Data that is required to be transmitted outside where it originates, has a certain level of privacy protection by virtue of blockchain's pseudonymity mechanism.
- *Scalability.* Both blockchain and edge computing paradigms are decentralised schemes. In other words, they can be smoothly and readily converged without introducing additional scalability issues.

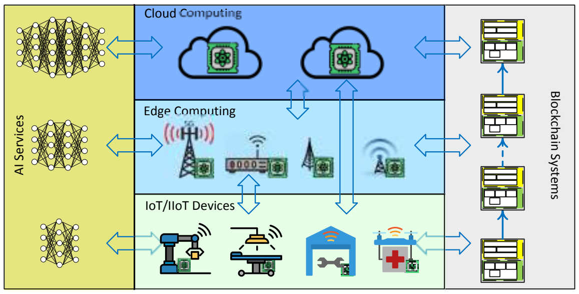


Fig. 4. A layered architecture for IoT/IIoT with the convergence of blockchain and edge computing.

Fig. 4 shows a layered architecture for IoT/IIoT in industry 4.0 with the convergence of blockchain and edge computing paradigms. The architecture consists of four layers: IoT/IIoT devices, edge computing, cloud computing and blockchain systems. *IIoT devices* are the smart devices in IoT/IIoT environment, such as robotic arms in smart factories, smart farm sensors in smart agriculture, and smart thermometer in smart home. They are responsible for data acquisition and pre-processing with light computation. *Edge computing* can be embedded within an IIoT device, deployed in a house, an office building, a micro base station, and even a macro base station; it provides necessary local computation and/or storage capabilities to satisfy stringent QoS requirements of many IIoT applications, such as ultra-low latency for autonomous vehicles and ultra-high reliability for remote surgery. In addition, edge computing allows local data to be processed locally, without being transferred to the remote cloud. In contrast, *cloud computing* has more computing power but it is located far away from computation tasks, and therefore the communication with cloud data centres can incur additional network latency and consume more network bandwidth. The *blockchain system* can ensure the security and transparency, and enhance privacy and scalability, of the above three layers in the critical infrastructure. *AI services* provide the ability for data processing at IoT/IIoT devices, edge computing and cloud computing layers.

Let us take an example to facilitate the understanding of the layered architecture shown in Fig. 4. A drone in the IoT/IIoT Devices layer is monitoring weather conditions and needs to transmit the pre-processed weather data to the weather station. Due to limited computing resources and energy-efficiency considerations at the drone, part of the collected data need to be offloaded to edge servers at the base station for processing, in the Edge Computing layer. All transactions are recorded by a blockchain, where the involved devices such as the drone and the base station are miners. If the local computing resources of miners are limited, miners can offload their computing works, such as achieving an agreement by consensus algorithms, to more powerful computing facilitates. For example, drones can offload the computing works to edge servers, and the computing works at an edge server can be offloaded to other edge servers or the Cloud Computing layer. The AI Services layer provides necessary AI models to make intelligent decisions, e.g., when is the best time for offloading.

In what follows, the state-of-the-art that consider the convergence of blockchain and edge computing, to ensure the security and scalability of critical infrastructures, will be investigated and discussed.

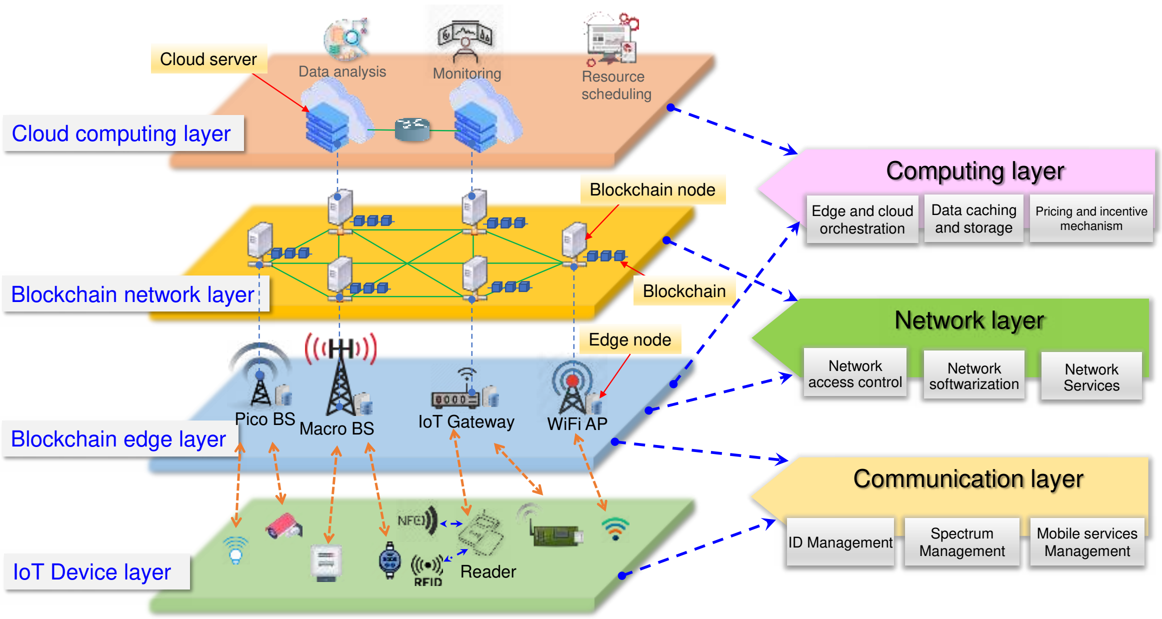


Fig. 5. Security and privacy solutions brought by the convergence of blockchain and edge computing.

V. Security and Privacy of IIoT Critical Infrastructures in Industry 4.0

The integration of blockchain with edge computing has the potential to secure IIoT critical infrastructures and also protect privacy-sensitive data in the infrastructure. Fig. 5 presents an overview for the state-of-the-art of security and privacy solutions brought by the convergence of blockchain and edge computing. In particular, the IoT device layer, blockchain edge layer and cloud computing layer correspond to the IoT/IIoT devices, edge computing and cloud computing, respectively, as presented in Section IV. It is worth mentioning that the blockchain network layer plays a crucial role in connecting ECNs and cloud servers in the same plane via an overlay network (i.e., the P2P network). We summarise the counter-measures to guarantee security and privacy in IIoT critical infrastructures in the communication, network and computing layers, which are illustrated as follows.

A. Communication layer

The integration of blockchain and edge computing can protect the security and privacy for IIoT in identification management and radio spectrum management.

1) Identification management: The proliferation of diverse IoT devices poses the challenges in identification (ID) management of IoT devices [67]. However, the incumbent ID management systems are not scalable with the explosion of heterogeneous IoT devices. Meanwhile, the centralised IoT ID management can inevitably lead to low efficient bureaucratic processes, huge administrative costs, vulnerability to malicious attacks and susceptibility to single-point-failure (SPF) and privacy breaches.

The advent of blockchain as well as edge computing technologies can potentially solve the above drawbacks of the centralised ID management systems. On the one hand, the decentralisation of blockchain systems can simplify the ID management process and lower the administration costs. Specifically, an IoT device can register, revoke and expire its ID in the decentralised blockchain-based ID management systems which can guarantee the trust without the necessity of a third party. Meanwhile, the privacy/security risks of the centralised systems can be eliminated or mitigated thanks to the temper-proof and non-repudiation characteristics of blockchains [68]. Moreover, the decentralisation brought by blockchain can also help to reduce the SPF risk in the centralised systems. In addition, blockchains can also ensure the anonymity of IoT devices since the generated addresses of IoT devices can only be used to interact with each other in the system.

On the other hand, edge computing can also disburden the centralised ID management systems by offloading tasks (e.g., registration, revoking and updating) to distributed ECNs. Integration with blockchain can further improve the transparency and security of ID management. All ID data stored in blockchain become traceable and immutable so as to improve the overall security of IIoT. There are several proposals on IoT ID management. For example, recent work [69] investigated the usage of blockchain for Lithium-ion (Li-ion) battery management. Moreover, Guo et al. [70] adopted an integration of blockchain and edge computing to achieve the trust of access control across diverse IoT systems.

2) Spectrum management: We have experienced the radio spectrum shortage due to the ever-growing demands on wireless bandwidth driven by massive IoT devices and diverse IoT applications [71], [72]. Blockchain also brings opportunities in radio spectrum management for IoT devices. Blockchain is essentially a distributed database (a.k.a. a distributed ledger), which can record the usage of radio spectrum and enforce the effective spectrum access mechanisms. For example, the work [73] investigated the adoption of blockchain as distributed spectrum database to achieve a fine-grained access control on radio spectrum, through which users may share radio spectrum through appropriate settings of licenses in blockchain.

Moreover, the built-in incentive and pricing mechanisms of blockchain can help to simplify the spectrum trading process. The work [74] discussed the possibilities of leveraging blockchain for radio spectrum auction. Smart contracts running on top of blockchain can also automate the spectrum auction and trading. Meanwhile, a blockchain-based spectrum sharing framework for 5G communications was proposed in [75]. In particular, a smart contract regularising the terms for spectrum sharing as well as the payments is given. The underlying blockchain can also protect the privacy of trading parties.

3) Mobile services management: In 5G and beyond 5G communication systems, the management of massive services subscribers is becoming a challenge due to the difficulty in coordinating the fragmented heterogeneous networks and the growing administrative cost for handling various mobile services. Blockchain technology can potentially address these emerging issues in mobile services management in 5G and beyond 5G networks.

As shown in Fig. 5, blockchain is essentially a middleware to connect distributed mobile networks together. Consequently, diverse communication networks can be integrated together to offer a seamless mobile service to users. Moreover, the built-in smart contracts on top of blockchain can also automate the service subscription, suspension, modification and termination, thereby reducing the administrative expenditure. The study [76] presented a blockchain-based roaming management system for cellular networks, providing users with an ubiquitous roaming service. Furthermore, the positioning accuracy is also a critical issue in mobile services, especially for vehicular networks. The study [77] proposed a blockchain-based framework on collaborative positioning. Particularly, blockchain can ensure the data provenance of positioning data.

B. Network layer

In the network layer, the incorporation of blockchain into edge computing can protect the security in aspects of network access control and network softwarisation. We next illustrate the research advances in these two aspects in detail.

1) Network access control: One of the major obstacles in IoT data sharing is the reciprocity absence across diverse IoT systems. The introduction of blockchain to the IoT ecosystem can not only improve the *interoperability* [42] but also provide fine-grained access control of various components in IoT systems. The work [78] presented a blockchain-based access control for IoT systems. In particular, a fine-grained access control based on attribute-based encryption (ABE) can ensure the permission attribute updating in time. As an example, the revoked users cannot access the on-chain data, which nevertheless can be visible to authorised users. Moreover, the work [79] presented a decentralised network management system for IoT on top of blockchain. Even though the performance improvement over the conventional IoT network management systems is not significant, the decentralisation feature of this system (mainly owing to distributed blockchain nodes) can improve the scalability of the entire system. In contrast to conventional network access control, blockchain-based network access control has the following advantages: 1) decentralization of network access control so as to improve the *interoperability* across the entire IoT system, 2) fine-grained access control can be achieved by the traceability of blockchain and ABE schemes.

The advances of blockchain-based smart contracts also foster the flexibility of network access control. In particular, the work [80] presented a smart contract-based access control scheme to achieve flexible network access control. In this scheme, there are three types of smart contracts for registration, judgement and multiple access control properties. An implemented prototype also demonstrated the effectiveness of the proposed framework. Moreover, Islam and Madria [81] proposed an attribute-based network access control scheme based on smart contracts running on top of Hyperledger Fabric, which is a permissioned blockchain. Experiments on an IoT testbed were conducted to further verify the effectiveness of the proposed scheme. In addition, in [82], the distributed trust in Internet-of-Vehicles (IoV) can be achieved through the consensus mechanism of blockchain.

2) Network softwarisation: In order to cater for the growing demands of diverse IoT applications, the *network softwarisation* has drawn extensive attention recently [83]. Typical network softwarisation technologies mainly include software-defined networks (SDN) [84], [85], network functions virtualisation (NFV) [86], [87] and network slicing [88], [89].

The advent of SDN can fulfill the flexible and scalable connections of massive IoTs while most of the existing SDN solutions that are centralised are susceptible to SPF or malicious attacks. The introduction of blockchain can decentralise SDN schemes thereby improving the reliability of SDN-based IoT systems. The recent study [90] presented a blockchain-based decentralised SDN solution, which can effectively solve the handover authentication problem. Moreover, the work of [91] also presented a blockchain-based SDN scheme for the IoV scenario, in which blockchain was adopted to achieve decentralisation and trustworthiness of multiple network entities and SDN was leveraged to guarantee the effectiveness of network management.

Meanwhile, the provision of NFV technologies can facilitate the diverse services for IoT applications while both security and trust among multiple virtualised network entities pose a challenge in popularising NFV to IoT communities. The convergence of blockchain with NFV can potentially overcome these challenges. The study presented in [92] investigated the integration of blockchain with NFV to secure NFV orchestration functions so as to achieve traceable and non-repudiated services. Moreover, the work [93] harnessed the auditability and incentive mechanism of blockchain to design a reverse auction scheme to solve the competition of virtual network functions (VNF) services providers.

Network slicing accompanying by SDN and NFV technologies can fulfill the diverse demands of various IoT applications via partitioning the entire physical network into multiple segregated network planes. The work [94] presented a blockchain-based broker mechanism for IoT devices in 5G networks, in which network resources can be securely leased to end users in a privacy-protected manner. Moreover, the study presented in [95] showed that the introduction of blockchain to network slicing can further improve the reliability of the content sharing in information-centric networks (ICN) [96].

3) Network services: The integration of network access control and network softwarisation mechanisms with blockchain can offer unified network services. On the one hand, blockchain and smart contracts can enable the flexible network access control. On the other hand, the combination of blockchain with network softwarisation technologies can also facilitate the network management. Consequently, the provision of secure and ubiquitous network services is envisioned for critical infrastructures.

There are several representative network services based on blockchain. In [97], a blockchain-based network storage service was presented. In particular, a blockchain-based data auditing scheme integrated with the bi-linear pairing cryptographic mechanism was devised to ensure the data integrity. Meanwhile, Aujla et al. [98] presented a framework of integrating SDN and blockchain to offer flexible network services. Particularly, blockchain-enabled SDN can mitigate the attacks such as malware and denial-of-service (DoS) attacks. Moreover, the study [99] investigated the integration of blockchain with ECNs to provide trusted edge services. Incentive schemes that are embedded with smart contracts can incentivise ECNs to contribute to edge services.

C. Computing layer

The integration of blockchain and edge computing can solve the following security issues in the computing layer. We discuss the research advances as follows.

1) Edge and cloud orchestration: IoT data has typically been uploaded to remote clouds for storage, analysis and interpretation [100]. However, cloud services have typically been owned by untrustworthy third parties, which may misuse IoT data or unintentionally disclose the privacy-sensitive data to others. Moreover, it may cause considerable end-to-end delay to upload IoT data to remote clouds. The advent of edge computing [101] can overcome the drawbacks of cloud computing through offloading computation and storage tasks to ECNs, which are close to users. Thus, edge computing can essentially complement with cloud computing to better serve IoT.

The effective edge and cloud orchestration is a necessity for IoT ecosystem while it also poses a number of security and privacy challenges especially in the trustless and heterogeneous computing environment [102]. There are a few studies to guarantee trust and security of edge and cloud orchestration enabled by blockchain. In particular, Xiong et al. [103] modeled the interactions among cloud servers, ECNs and blockchain miners as a multi-leader multi-follower game, which is essentially a computationally-complex problem while authors successfully solved the problem by an Alternating Direction Method of Multipliers (ADMM) approach. Meanwhile, the study of [104] investigated to disburden blockchain mining tasks from IoT devices to ECNs. In addition, Jiao et al. [105] presented an auction model to analyse the trading procedure between cloud/edge services vendors and blockchain miners. Moreover, the work [106] presented an overview on using blockchain for cloud services exchange in a cloud market. Furthermore, authors in [107] presented a cloud-edge orchestration framework to coordinate crowdsensing tasks in mobile IoT scenarios. In this framework, a cloud server playing a role as a controller can gather sensing data from ECNs, which outsource sensing tasks to mobile IoT devices to collect sensing data. An auction mechanism was proposed to incentivise participatory workers (i.e., IoT devices). Similarly, the work [108] presented a blockchain-based mobile crowdsensing system for IIoT. In contrast to conventional mobile crowdsensing systems, the decentralisation of blockchain can further enhance the reliability and security of the system.

2) Data caching and storage: The explosion of IoT data poses challenges in data management, especially in data storage and data analytics [118]. Cloud computing can offload storage and processing burdens at IoT devices while it also brings the challenges in data privacy and security protection. Edge computing can undertake storage and processing at ECNs in approximation to users, thereby improving context-awareness and protecting data privacy.

The in-depth integration of blockchain and edge/cloud can further preserve IoT data privacy and security. In particular, the work [109] presented a blockchain-based data management system for IoT, in which both edge and cloud computing facilities are integrated with blockchain to guarantee effective data sharing. Harnessing the non-repudiation and anti-tampering characteristics of blockchain, Xu et al. [110] proposed a blockchain-based data sharing system to support a diversity of edge applications. Experimental results further verified the effectiveness of the proposed scheme.

There are other studies on investigating the adoption of blockchain in other edge computing scenarios. In particular, the work [111] investigated to leverage blockchain to achieve the trust of multiple ECNs, which can temporarily store popular contents (a.k.a. caches) so as to improve user experience. Blockchain can also be used in the video streaming scenario. Liu et al. [112] presented a blockchain-based video streaming framework with edge computing. Meanwhile, a three-stage Stackelberg game was used to investigate the interaction among the users, base stations and video providers. Moreover, the work [113] exploited the merits of blockchain such as anti-tempering and decentralisation to achieve the fast repairing of data storage nodes in IIoT environment.

3) Pricing and incentive mechanisms in computing: The IIoT critical infrastructure consists of diverse computing facilities, such as IoT nodes, ECNs and cloud servers with different computing capabilities and storage capacities. It is crucial to motivate diverse computing nodes to participle in computing and storage tasks. In addition, many consensus algorithms of blockchain also require substantial computing contributions from some computing nodes (i.e., miners). Therefore, the pricing and incentive mechanisms become a challenge in the IIoT critical infrastructure.

Many recent studies aim at addressing this issue. Kang

TABLE II
SUMMARY OF SECURITY AND PRIVACY SOLUTIONS ENABLED BY BLOCKCHAIN AND EDGE COMPUTING

Perspectives	Issues	References
Communication layer	• Identification management • Spectrum management • Mobile services management	[67], [68], [69], [70] [73] [74] [75] [76] [77]
Network layer	• Network access control • Network softwarization • Network services	[78] [79] [80] [81] [82] [90] [91] [92] [93] [94] [95] [97] [98] [99]
Computing layer	• Edge and cloud orchestration • Data caching and storage • Pricing and incentive mechanisms	[102] [103] [104] [105] [106] [107] [108] [109] [110] [111] [112] [113] [114] [115] [116] [117]

et al. [114] proposed a two-stage strategy to mitigate the collusion of blockchain miners. In particular, a contract theory was introduced to incentivise miners to contribute to the block verification. Meanwhile, the study [115] investigated the incentive mechanisms in ECNs providing blockchain miners with computing services. Particularly, a two-stage Stackelberg game model was used to analyse the interactions between ECNs and miners. Moreover, the study [116] investigated a mechanism to promote the consensus propagation across the blockchain network. Furthermore, a credit-based approach was devised in [117] to achieve the computing resource trading between ECNs and blockchain-enabled IoT nodes.

D. Summary

The integration of blockchain and edge computing can address the security and privacy concerns in critical infrastructures of IIoT in communication, network and computing layers. Table II summarises the state-of-the-art solutions in different aspects.

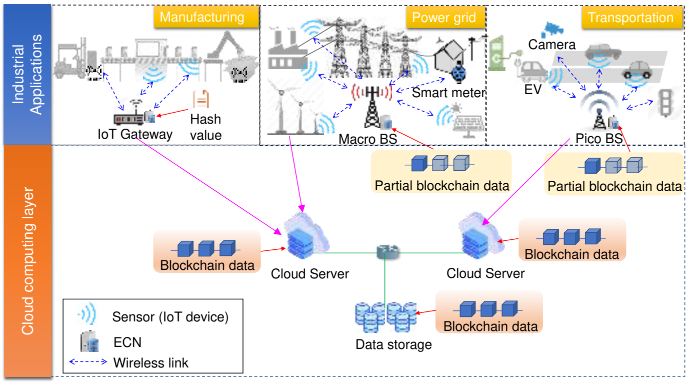


Fig. 6. An example to illustrate the working of the integration of blockchain and edge/cloud computing.

With respect to the practical realisation of the solutions, the integration of blockchain and edge/cloud computing facilities should be decomposed into diverse computing facilities, which are distributed across the entire IIoT critical infrastructure. Fig. 6 depicts an example of the integration of blockchain and edge/cloud computing facilities. In this scenario, cloud servers and data storage servers which have strong computing/storage capabilities may store the entire blockchain and also be responsible for the computationally-intensive tasks such as mining and executing machine learning/deep learning algorithms. However, ECNs and IoT devices may only store partial blockchains (e.g., hash values of the blockchain or a subset of blocks) due to the limited computing/storage capabilities. It is a critical issue to ensure the consistency of blockchain data across the entire network.

VI. SCALABILITY OF IIOT CRITICAL INFRASTRUCTURES IN INDUSTRY 4.0

In addition to security and privacy concerns of IIoT critical infrastructures, the scalability has limited the wide adoption of IIoT. The integration of edge computing and blockchain can improve the scalability of IIoT. First, edge computing can offer ubiquitous computing facilities to blockchain and IIoT nodes. Second, blockchain being a middleware across different IIoT systems can enhance the security and privacy of both ECNs and IIoT. In this section, we discuss the scalability of IIoT critical infrastructures mainly in two aspects: 1) the intrinsic scalability of IIoT and 2) the scalability of blockchain.

A. Scalability of IIoT

With the vision of ubiquitous connections everywhere and elastic access for everything, IIoT has the stringent requirement on the scalability in critical infrastructures [119]. However, as shown in Fig. 7, the scalability of IIoT is affected by heterogeneous IIoT devices, diverse IIoT networks, and massive IIoT data [120]. In particular, IIoT consists of various IoT devices such as RFID tags, sensors, controllers, and robot arms, which are connected through wired networks or wireless networks. The heterogeneity of IIoT devices exhibits in both hardware (e.g., ICs and sensors) and software (e.g., operating systems and firmware). In addition to heterogeneous IIoT devices, the networks connecting various IIoT devices also have different protocols across the entire protocol stack. For example, near-field communication (NFC), back-scatter communications, and Bluetooth have often been adopted for short-range communications, while WiFi, Low Power WAN and cellular communications (e.g., 4G and 5G) have been

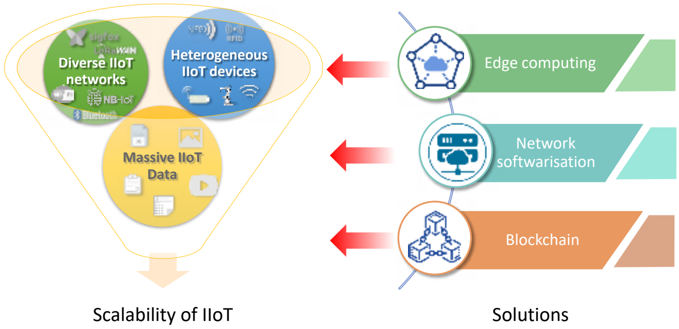


Fig. 7. Scalability of IIoT and solutions.

used to connect IoT devices over a longer distance [121], [122]. Moreover, a proliferation of massive structured and non-structured IIoT data also leads to the difficulties in data storage and analytics.

On the other hand, the heterogeneous IIoT critical infrastructures across different business sectors or government departments have led to difficulties in information sharing and reciprocal operations among different IIoT systems, consequently leading to the difficulty in reaching the scalability. Meanwhile, the insufficient resources of IIoT devices, as well as heterogeneity of IIoT devices and networks, are also the root causes of many security and reliability vulnerabilities [123]. Moreover, the massive volume of IIoT data has often been uploaded to remote clouds, which have nevertheless been possessed by trustless third parties, consequently leading to privacy leakage risks. Security, privacy and reliability vulnerabilities of existing IIoT critical infrastructures also increase the difficulty in achieving the scalability.

The fusion of edge computing, network softwarisation and blockchain technologies can offer solutions to the scalability of IIoT, as shown in Fig. 7. First, the recent advances in edge computing and network softwarisation can potentially address the scalability challenges of IIoT critical infrastructures. In particular, the work of [124] presented an edge computing-based attestation systems for IoT devices. An implemented prototype demonstrated the scalability of the entire system. Meanwhile, Togou et al. [125] presented a decentralised SDN to achieve the scalability of large-scale networks in contrast to the conventional centralised SDN solutions. The existing SDN solutions have bottlenecks at network controllers, which often have the limited computing capabilities. To address this issue, the work [126] proposed an integration of edge and cloud computing facilities to overcome the computing bottlenecks of SDN controllers. One of the most important scalability metrics is the latency. The recent work [127] presented a study of integrating SDN, NFV and network slicing to achieve the ultra-low latency in 5G networks. Moreover, both edge and cloud computing facilities have been deployed to the core network to improve the computing capabilities, thereby reducing the delay. Furthermore, the work [128] presented an optimisation scheme for network slicing recovery and reconfiguration, thereby improving the system reliability and scalability.

On the other hand, the introduction of blockchain technologies to edge computing and network softwarisation has become an inevitable trend to further improve the scalability of IIoT. In particular, Pan et al. [129] proposed a framework with integration of blockchain and ECNs to enhance IoT. The smart contracts running on top of blockchain can automate the regulation of IoT devices, consequently enhancing the reliability. Moreover, the work [130] presented a blockchain-based framework to improve the scalability with consideration of heterogeneous IoT devices. To address the transaction throughput bottleneck of blockchain systems, the authors also designed a new consensus scheme as well as a space-structured chain structure. The resource limitation of IoT devices also leads to the difficulty of the adoption of blockchain to IIoT scenarios. The work [131] proposed a solution to address this issue by localising blockchain peers, thereby improving the scalability.

B. Scalability of blockchain

The scalability of current blockchain technologies[6] is still far from meeting the demand of IIoT. One of the earlier analyses on the scalability of blockchain was conducted by Croman et. al. [132], which pointed out the large throughput gap between Bitcoin (7 transactions/second maximum) and the mainstream payment processor such as Visa credit card (2000 transactions/second on average). The authors proposed a decomposition of the Bitcoin system into 5 abstraction layers (planes): Network, Consensus, Storage, View, and Side. In each layer, the authors reviewed different approaches to improve the scalability. One limitation of this work was that it heavily focused on cryptocurrencies.

More recently in 2018, Dinh et. al. [133] presented a more comprehensive overview of different blockchain systems w.r.t. data processing and performance. The authors described another decomposition into 4 layers: Application, Consensus, Execution engine, and Data model. They performed extensive experiments, with their benchmarking framework BLOCKBENCH, to evaluate the throughput, latency, scalability, fault tolerance, and security metrics on three representative blockchain systems, namely Ethereum, Parity, and Hyperledger. Their evaluation showed that current blockchains' performance is "far below what a state-of-the-art database system can offer". One limitation of this work, despite its extensive coverage, paid insufficient attention to IoT applications. One reason can be in 2018, the IoT-oriented blockchains were less developed compared to general or crypto-currency blockchains.

Here we summarise in Table III the approaches that have been proposed in the community for the scalability of blockchains.

Very recently in 2020, Lao et. al. [146] presented a survey of IoT applications in blockchain systems. The survey did cover the direct acyclic graph (DAG) based distributed ledger technology (DLT), along with the fast growing IOTA

[6] Strictly speaking, some technologies reviewed here are currently preferred to be called distributed ledger technology, instead of blockchain. For example, the network topology of IOTA Tangle is not a chain structure, but a graph structure.

TABLE III
SUMMARY OF APPROACHES TO IMPROVING THE SCALABILITY OF BLOCKCHAINS

Aspects	Works	
Structure	DAG	Tangle [134], [135]
	Federated blockchains	[133], [136], [137], [138]
	Multiple chains	[139], [140], [141], [142], [143]
Consensus	Stellar [136], Ripple [137], CAPER [138]	
Database tech.	Sharding	[144]
	Transaction reordering	[145]

Tangle [134] implementation. However, this survey mainly focused on architecture, consensus, and traffic modeling, and thus, the coverage on the scalability is insufficient, and the authors did not review critically the weaknesses of IOTA Tangle.

DAG-based DLT has higher throughput and scalability compared to the original chain-structure-based blockchains [147]. It is due to the fact that DAG is unidirectional with no ring structure, which ensures high efficiency in searching and communication. A typical DAG implementation is the IOTA Tangle. IOTA Tangle recently grows fast especially in industries. IOTA, being a public permissionless distributed ledger, is designed for IoT applications to support high-frequency micro transactions. Considering those micro transactions are normally low value transactions, there are no explicit transaction fees in IOTA. When a new transaction arrives, it will select two previous transactions (called *tips*) to validate. This means IOTA, though having higher throughput, follows a PoW protocol. The tip selection algorithm (TSA), being the key component in the IOTA consensus, is an active research topic. IOTA Tangle proposed two TSA algorithms in their original white paper [134], the random selection algorithm and the random-walk-based Monte Carlo Markov Chain (MCMC) selection algorithm. But as recognised by themselves and follow-up improvements [135], IOTA Tangle is still vulnerable to the *parasite chain attack*, which could cause damage to the immutability and irreversibility of the ledger. In this aspect, IOTA Tangle still needs critical improvements to meet the high demands in security and fault tolerance from IIoT critical infrastructure applications.

As commented by [133], the main-stream consensus protocols based on PBFT [148] are still communication bound, thus they have hard limits in scalability. Stellar [136] and Ripple [137] can be called federated blockchain systems. Such blockchains divide the network into smaller groups called *federates* [133] or *quorums* [136], and each federate maintains local consensus. Local consensus can be propagated to the whole network, and the global consensus can be reached under certain conditions. The parallel executing federates improve throughput. CAPER [138] further elaborated and proposed 3 global consensus protocols. Interestingly, CAPER adopts the DAG structure for the distributed ledger.

One step further is to employ multiple chains with relevant cross-chain synchronisation protocols to ensure satisfactory global consensus. Atomic cross-chain swaps by Herlihy [139], modelled in a directed graph structure, enables the exchange of assets across multiple (unrelated) blockchains. Delegating the execution of some transactions from the main blockchain to a set of *sidechains* [140], or called *parachains* in Polkadot [141] is another well known approach. A recent work [142] on the multi-chain structure, in the context of industrial Internet, proposed a node-clustering strategy to reduce cross-chain interactions and improve throughput. The *delayed-replication* algorithm by Hellings and Sadoghi [143] aimed to improve the efficiency of processing read-only workloads.

The database community recently proposed several solid works in transitioning database technologies to blockchain systems with notable improvements on scalability. In SIGMOD 2019, Dang et. al. [144] presented a scalable blockchain based on sharding and achieved a throughput of over 3000 transactions/second. Sharma et. al. [145] successfully employed a well-known database technique, transaction reordering, and increased the throughput of successful transactions with a factor of 12x and decreased the average latency to almost half.

Research works integrating blockchain with wireless networks, IIoT, and cloud/edge computing started emerging very recently. Sun et. al. [149] presented a blockchain-enabled wireless IoT model and a search algorithm aiming to find the optimal deployment of full function nodes under a given node density and transaction throughput. Liu et. al. [150] also looked at the wireless IoT systems and proposed a new blockchain system that considers the heterogeneity, resource constraints, and dynamics (frequent join/leave due to on-off switching or mobility reasons) of IoT devices. Their prototype achieves a peak throughput of 3400+ transactions/second. Xiong et. al. [151] and Yao et. al. [152] studied resource management that allows IIoT devices to offload computational tasks to cloud/fog providers. Xiong et. al. [153] and Wu et. al. [154] proposed blockchain systems that offloads the miners' PoW computation tasks to the mobile edge computing (MEC) network.

From the above review on the scalability, we observe that the blockchain is developing towards multiple chains, modelled in graph structures, with hierarchical consensus protocols and more database techniques. We see the synergy between this trend and the development of edge/cloud computing, which has been envisioned in our proposed layered architecture for IoT/IIoT with convergence of blockchain and edge computing in Section IV.

VII. Potential Challenges and Open Issues

Although blockchain and edge computing technologies have been used to ensure secure and scalable IoT/IIoT critical infrastructures, there are still many on-going challenges and open issues that need to be considered in future research. In this section, we discuss a set of issues, in terms of architecture, secure infrastructure, and scalable infrastructure.

A. Architecture of IIoT critical infrastructures

1) Standard application programming interface for application developers: Edge computing is in a position to serve diversified applications, and each application has its own ecosystem that uses the platform that may be ecosystem-specific[7]. For example, the platforms and application programming interfaces (APIs) for transportation systems should be different from those required for government facilities. Each country has many critical infrastructures covering a range of sectors, e.g., financial services, energy, health, etc (see more details in Table I). A robust edge computing framework solution should be able to provide standard northbound APIs for application developers from different platforms and flexibly deploy necessary functionalities, along with the advanced networking technologies, e.g., SDN and NFV. It should also be able to accommodate various southbound transmission protocols between IoT/IIoT devices and the cloud. In addition, edge cloud may belong to different operators. An efficient east-west data transmission protocol may be needed for communication between different network operators. The design of these protocols should be coupled with the stringent requirements of diversified IoT/IIoT applications and security guarantee mechanisms (e.g., blockchain) in critical infrastructures.

2) Integrated networking, computing, storage and power resource allocation: Resource allocation is an important research topic in edge computing, which depends on many factors, including energy consumption, power allocation in energy renewable networks [155], [156], computing capabilities at the IoT/IIoT devices, the edge and the cloud, the key components of emerging network architectures, wireless communications, to name a few. Many studies only consider one or two of these factors. For example, most studies consider energy-computing trade-off for computation offloading solutions. It is challenging to have an integrated networking, computing, storage and power resource allocation scheme that is useful for a practical use case. For example, how to incorporate the in-network caching of ICN, which was designed to reduce the delay for content retrieval, into the resource allocation solutions of edge computing, is still an open issue.

3) Decentralised network management: The convergence of edge computing and blockchain is a decentralised network in nature. The traditional centralised or hierarchical network management would not work efficiently. In addition, the surge in data volume that will come from the massive IoT/IIoT devices enabled by 5G has made edge computing more difficult to manage. Furthermore, edge computing has been coupled with advanced networking technologies, e.g., SDN, NFV and network slicing, for efficient service deployment and network control. The complexity of edge computing due to these factors, coupled with the introduction of blockchain, has made the network management a hard task. Decentralised network management is definitely a trend, but how to design an efficient solution that considers the above factors and can be interworked/integrated with the management framework of emerging networking technologies, e.g., management and orchestration (MANO) in NFV, is still a challenging issue.

4) Network economy: The convergence of edge computing and blockchain plays an important role in enabling a wide range of use cases in critical infrastructures, e.g., industrial manufacturing and a variety of other sectors. The network economy models are crucial for the success of the ecosystem of these sectors. Existing solutions in this area seldom consider network economy models, and thus they are not sustainable and practical solutions. How to design a practical solution for the convergence of edge computing and blockchain, by considering network economy factors e.g. pricing mechanisms of real-world applications, is still an open issue. Game theory is a versatile tool that has been useful to make decisions related to network economy [25]. However, network environment is becoming much more dynamic than ever, we must bring in the tools (e.g., AI) that can capture the features of this ever-changing environment to help game theory do a better job.

B. Secure IIoT critical infrastructures

1) Security vulnerabilities of IIoT devices: The resource limitations of IIoT devices have often been the root causes of the security vulnerabilities. On the one hand, the limited computational capability and battery capacity lead to the difficulty of deploying computationally-complicated encryption algorithms at IIoT devices. Meanwhile, the failure of upgrading or patching IoT firmware also results in the IIoT devices being vulnerable to malicious attacks [157]. It is reported in [158] that blockchain-enabled smart contracts can automate the IoT firmware upgrading procedure through the contract clauses (i.e., instructions) built-in IoT devices since the date of production. Moreover, the recent work [159] also presented a blockchain-based solution via monitoring software status of IoT devices. Blockchain can store snapshots of IoT software status to monitor and detect any malicious activities (e.g., a backdoor firmware upgrading).

2) Security vulnerabilities of blockchain: Although blockchain has the advantages in security enhancement of the IoT ecosystem, the intrinsic security vulnerabilities of blockchain systems also prevent blockchain from being widely adopted in IIoT critical infrastructures. For example, it is reported in [160] that the failure of properly-configuring gas costs of Ethereum Virtual Machine (EVM) may lead to Ethereum suffering from DoS attacks. Moreover, blockchain-based domain name system (BDNS) can be abused by cyberattackers to conduct intrusion attacks [161] due to the anonymity of BDNS. The recent progress in big data analytics on blockchain data brings the opportunities to remedy the security vulnerabilities of blockchain. For example, the recent work [162] presented a framework to collect blockchain data and detect various attacks occurring on blockchain.

3) Integration of AI to secure IIoT critical infrastructures: Massive data has been generated from the entire IIoT critical infrastructures from the communication layer to the computing layer. Big data analytics (BDA) on IIoT critical infrastructures can classify abnormal behaviours, detect and recognise intrusions as well as malicious attacks [163]. Meanwhile, BDA on the operational data of IIoT critical infrastructures can also help to identify the performance bottlenecks and make proactive actions (like tuning performance metrics). Moreover, BDA on blockchain can be beneficial to pinpoint

[7] https://www.ericsson.com/491e83/assets/local/reports-papers/ericsson-technology-review/docs/2020/next-generation-cloud-edge-ecosystems.pdf

vulnerabilities of blockchain as analysed above. However, the heterogeneity and diversity of IIoT critical infrastructure data also pose the challenges in data analytics [164]. The recent advances in AI have brought opportunities to address the above issues.

First, the integration of AI with cloud computing can process massive IoT data and extract valuable information. Second, AI can empower ECNs and IoT devices with intelligence [165], [166]. Due to the resource limitation, IoT devices may possess the limited intelligence. The intelligence bestowed to ECNs by AI that is named as edge intelligence can serve an important complement to IoT devices [167]. For example, the work [168] proposed an amalgamation of blockchain with edge computing, in which a deep reinforcement learning (DRL) [169] was proposed to achieve the dynamic resource scheduling. Meanwhile, authors in [170] adopted a DRL method to allocate both computing resources and blockchain operations in an adaptive manner. Moreover, the work [171] presented a DRL method to optimize network slicing in 5G networks. Furthermore, deep learning approaches can help to identify these malicious attacks through analysing the activity reports and suggest relevant countermeasures. For example, the work [172] showed that deep learning can analyse the network traffic to identify the attacks.

4) Data privacy preservation: In addition to cloud servers, both IIoT devices and ECNs are vulnerable to privacy leakage risks. On the one hand, it is shown in a recent work [173] that user privacy during the spectrum auction can be breached. On the other hand, the privacy leakage risks exist when raw data collected from IIoT devices is sent to untrustworthy ECNs, which can be hijacked or misused by attackers. Consequently, data stored at ECNS can be stolen or misused.

Recent advances in differential privacy [174], homomorphic encryption [175] and federated learning [176], [177] bring the opportunities in offering privacy protection in IIoT critical infrastructures [178]. In particular, the work [174] presented a joint framework of blockchain, differential privacy and federated learning to protect data privacy in IIoT. Feng et al. [175] presented a privacy preservation method based on tucker decomposition on top of blockchain for IIoT. The authors in [176] proposed using federated learning to train machine learning models locally, which can be finally aggregated into a global model while the data privacy can be preserved.

Besides federated learning and cryptographic algorithms, the advent of recent machine learning and deep learning technologies can also potentially address the privacy concern. For example, Alkadi et al. [179] presented a blockchain-based framework with deep learning approaches to identify the intrusion attacks while preserving data privacy. Moreover, the work [180] introduced a privacy-aware deep learning method, which allows the collaboration of multiple nodes to train deep neural networks while preserving data privacy.

C. Scalable critical infrastructures

1) Scalability of IIoT: The scalability of IIoT is influenced by the heterogeneity of IIoT devices and the diversity of IIoT networks. Recent studies have demonstrated the effectiveness of the integration of SDN, NFV, network slicing and edge/cloud computing facilities to enhance the scalability of IIoT ecosystem. In addition, the introduction of blockchain to IIoT critical infrastructures can improve the interoperability (i.e., reciprocal operations) among different IIoT systems. Moreover, the massive data generated in IIoT can be used to identify the performance bottlenecks or abnormal activities so as to improve the scalability of IIoT [181]. In the future, the fusion of AI with the above technologies can further improve the scalability and elasticity of IIoT ecosystems.

2) Scalability of blockchain: The scalability of blockchain in itself is a big open problem, which prevents the adoption of this technology in many real-world application domains. There is still no tangible scalable solution for IoT applications. IOTA Tangle, being the largest and most successful one, is still far from satisfactory, with several critical vulnerabilities, including being not deterministic, relying on a central coordinator to avoid security attacks, and being susceptible to the parasite chain attack. The direction in coupling multiple chains, in graph structures, with hierarchical consensus protocols seems promising, but obviously calls for large amount of research efforts.

3) Coordination across disciplines: The momentum and interest shown in scalability from different communities (e.g., database, network, and high performance computing), while contributing good knowledge and insights in this important issue, expose the fragmented and un-coordinated nature of these efforts from different angles. The layered architecture with the convergence of blockchain, IIoT, and edge/cloud computing is a strong push towards coordinated research efforts, by linking the strengths from different communities, for scalable and secure solutions. This convergence opens up many research opportunities. A good coordination between the blockchain layer and cloud/edge computing and/or IIoT devices in the architecture (as shown in Fig. 4) has the potential of lifting the scalability of blockchain, and in general the critical infrastructure applications to a new level.

VIII. Conclusion

Critical infrastructures, also known as national critical infrastructures in the United Kingdom, are becoming vulnerable to cyberattacks due to wide adoption of Internet-connected IoT/IIoT devices in industry 4.0. Security and scalability are therefore becoming burning concerns for this "modern" critical infrastructures. In this paper, we introduced a layered architecture for IoT/IIoT critical infrastructures with the convergence of blockchain and edge computing. The state-of-the-art of security and privacy solutions, and scalability solutions, for IoT/IIoT infrastructures were reviewed and discussed. Despite numerous efforts have done, there are still many on-going challenges and open issues that need to be considered to ensure the success of critical infrastructures in era of industry 4.0. We then provided a range of potential research challenges and open issues at the end of this paper to guide the future research in this area.

References

[1] T. Wang, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and J. Cao, "Big data reduction for a smart city's critical infrastructural

health monitoring," *IEEE Communications Magazine*, vol. 56, no. 3, pp. 128–133, 2018.

[2] M. Chen, Y. Jiang, N. Guizani, J. Zhou, G. Tao, J. Yin, and K. Hwang, "Living with i-fabric: Smart living powered by intelligent fabric and deep analytics," *IEEE Network*, pp. 1–8, 2020.

[3] A. Petropulu, K. I. Diamantaras, Z. Han, D. Niyato, and S. Zonouz, "Contactless monitoring of critical infrastructure [from the guest editors]," *IEEE Signal Processing Magazine*, vol. 36, no. 2, pp. 19–21, 2019.

[4] L. Russell, R. Goubran, F. Kwamena, and F. Knoefel, "Agile iot for critical infrastructure resilience: Cross-modal sensing as part of a situational awareness approach," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4454–4465, 2018.

[5] J. M. Mcginthy and A. J. Michaels, "Secure industrial internet of things critical infrastructure node design," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8021–8037, 2019.

[6] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.

[7] Y. Wu, H. Huang, C.-X. Wang, and Y. Pan, *5G-enabled internet of things*. CRC Press, 2019.

[8] Y. Wu, F. Hu, G. Min, and A. Zomaya, *Big Data and Computational Intelligence in Networking*. CRC Press, 2017.

[9] R. Beerens, S. C. N. Thissen, W. C. M. Pancras, T. M. P. Gommans, N. van de Wouw, and W. P. M. H. Heemels, "Control allocation for an industrial high-precision transportation and positioning system," *IEEE Transactions on Control Systems Technology*, pp. 1–8, 2019.

[10] X. Jiang, Z. Pang, M. Luvisotto, R. Candell, D. Dzung, and C. Fischione, "Delay optimization for industrial wireless control systems based on channel characterization," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2020.

[11] F. Pan, Z. Pang, M. Luvisotto, M. Xiao, and H. Wen, "Physical-layer security for industrial wireless control systems: Basics and future directions," *IEEE Industrial Electronics Magazine*, vol. 12, no. 4, pp. 18–27, 2018.

[12] R. Paes, D. C. Mazur, B. K. Venne, and J. Ostrzenski, "A guide to securing industrial control networks: Integrating it and ot systems," *IEEE Industry Applications Magazine*, vol. 26, no. 2, pp. 47–53, 2020.

[13] C. Shen, C. Liu, H. Tan, Z. Wang, D. Xu, and X. Su, "Hybrid-augmented device fingerprinting for intrusion detection in industrial control system networks," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 26–31, 2018.

[14] Y. Qin, Q. Zhang, C. Zhou, and N. Xiong, "A risk-based dynamic decision-making approach for cybersecurity protection in industrial control systems," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pp. 1–8, 2018.

[15] M. Hassan, A. Gumaei, S. Huda, and A. Almogren, "Increasing the trustworthiness in the industrial iot networks through a reliable cyberattack detection model," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2020.

[16] M. Li, D. Hu, C. Lal, M. Conti, and Z. Zhang, "Blockchain-enabled secure energy trading with verifiable fairness in industrial internet of things," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2020.

[17] Y. Zhang, Z. Zheng, H. . Dai, and D. Svetinovic, "Guest editorial: Special section on "blockchain for industrial internet of things" in ieee transactions on industrial informatics," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3514–3515, 2019.

[18] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 18–21, 2018.

[19] M. Zhaofeng, W. Lingyun, W. Xiaochang, W. Zhen, and Z. Weizhe, "Blockchain-enabled decentralized trust management and secure usage control of iot big data," *IEEE Internet of Things Journal*, pp. 1–1, 2019.

[20] B. Yin, Y. Wu, T. Hu, J. Dong, and Z. Jiang, "An efficient collaboration and incentive mechanism for internet of vehicles (iov) with secured information exchange based on blockchains," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1582–1593, 2020.

[21] Y. Wu, H.-N. Dai, H. Wang, and K.-K. R. Choo, "Blockchain-based privacy preservation for 5g-enabled drone communications," *IEEE Network*, 2020.

[22] D. Gabay, K. Akkaya, and M. Cebe, "Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs," *IEEE Transactions on Vehicular Technology*, pp. 1–1, 2020.

[23] S. Deng, H. Zhao, W. Fang, J. Yin, S. Dustdar, and A. Y. Zomaya, "Edge intelligence: The confluence of edge computing and artificial intelligence," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[24] L. U. Khan, I. Yaqoob, N. H. Tran, S. M. A. Kazmi, T. N. Dang, and C. S. Hong, "Edge computing enabled smart cities: A comprehensive survey," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[25] J. Zhang, Y. Wu, G. Min, F. Hao, and L. Cui, "Balancing energy consumption and reputation gain of uav scheduling in edge computing," *IEEE Transactions on Cognitive Communications and Networking*, pp. 1–1, doi: 10.1109/TCCN.2020.3004592, 2020.

[26] H. Liu, P. Zhang, G. Pu, T. Yang, S. Maharjan, and Y. Zhang, "Blockchain empowered cooperative authentication with data traceability in vehicular edge computing," *IEEE Transactions on Vehicular Technology*, pp. 1–1, 2020.

[27] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973 – 993, 2014, special Issue on Dependable and Secure Computing. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0022000014000178

[28] D. Georgakopoulos, P. P. Jayaraman, M. Fazia, M. Villari, and R. Ranjan, "Internet of things and edge cloud computing roadmap for manufacturing," *IEEE Cloud Computing*, vol. 3, no. 4, pp. 66–73, 2016.

[29] H. Yang, A. Alphones, W. Zhong, C. Chen, and X. Xie, "Learning-based energy-efficient resource management by heterogeneous rf/vlc for ultra-reliable low-latency industrial iot networks," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2019.

[30] D. Ma, G. Lan, M. Hassan, W. Hu, and S. K. Das, "Sensing, computing, and communications for energy harvesting iots: A survey," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2019.

[31] C. K. Wu, K. F. Tsang, Y. Liu, H. Zhu, H. Wang, and Y. Wei, "Critical internet of things: An interworking solution to improve service reliability," *IEEE Communications Magazine*, vol. 58, no. 1, pp. 74–79, 2020.

[32] J. R. Foerster, X. Costa-Perez, and R. V. Prasad, "Communications for iot: Connectivity and networking," *IEEE Internet of Things Magazine*, vol. 3, no. 1, pp. 6–7, 2020.

[33] C. Luo, J. Ji, Q. Wang, X. Chen, and P. Li, "Channel state information prediction for 5G wireless communications: A deep learning approach," *IEEE Trans. Netw. Sci. and Eng.*, vol. PP, no. 99, pp. 1–1, Jun. 2018.

[34] Y. Zuo, Y. Wu, G. Min, C. Huang, and K. Pei, "An intelligent anomaly detection scheme for micro-services architectures with temporal and spatial data analysis," *IEEE Transactions on Cognitive Communications and Networking*, pp. 1–1, 2020.

[35] C. Huang, Y. Wu, Y. Zuo, K. Pei, and G. Min, "Towards experienced anomaly detector through reinforcement learning," in *AAAI Conference on Artificial Intelligence*, 2018. [Online]. Available: https://www.aaai.org/ocs/index.php/AAAI/AAAI18/paper/view/16048

[36] G. Falco, C. Caldera, and H. Shrobe, "Iiot cybersecurity risk modeling for scada systems," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4486–4495, 2018.

[37] Z. Zhou, J. Gong, Y. He, and Y. Zhang, "Software defined machine-to-machine communication for smart energy management," *IEEE Communications Magazine*, vol. 55, no. 10, pp. 52–60, 2017.

[38] Y. Yang, Y. Chen, W. Wang, and G. Yang, "Securing channel state information in multiuser mimo with limited feedback," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2020.

[39] S. R. Pokhrel, Y. Qu, and L. Gao, "Qos-aware personalized privacy with multipath tcp for industrial iot: Analysis and design," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[40] T. Hoang, A. A. Yavuz, and J. Guajardo Merchan, "A secure searchable encryption framework for privacy-critical cloud storage services," *IEEE Transactions on Services Computing*, pp. 1–1, 2019.

[41] C. Huang, G. Min, Y. Wu, Y. Ying, K. Pei, and Z. Xiang, "Time series anomaly detection for trustworthy services in cloud computing systems," *IEEE Transactions on Big Data*, pp. 1–1, 2017.

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

[43] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Communications Surveys Tutorials*, vol. 21, no. 3, pp. 2794–2830, 2019.

[44] 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 of Things Journal*, vol. 6, no. 5, pp. 8114–8154, 2019.

[45] K.-K. R. Choo, Z. Yan, and W. Meng, "Editorial: Blockchain in industrial iot applications: Security and privacy advances, challenges, and opportunities," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4119–4121, 2020.

[46] L. Cheng, J. Liu, G. Xu, Z. Zhang, H. Wang, H. Dai, Y. Wu, and W. Wang, "Sctsc: A semicentralized traffic signal control mode with attribute-based blockchain in iovs," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, pp. 1373–1385, 2019.

[47] H. Pourbabak, Q. H. Alsafasfeh, and W. Su, "A distributed consensus-based algorithm for optimal power flow in dc distribution grids," *IEEE Transactions on Power Systems*, pp. 1–1, 2020.

[48] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2020.

[49] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Comput. Surv.*, vol. 52, no. 3, Jul. 2019. [Online]. Available: https://doi.org/10.1145/3316481

[50] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu, "A survey on the scalability of blockchain systems," *IEEE Network*, vol. 33, no. 5, pp. 166–173, 2019.

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

[52] G. Ramezan and C. S. Leung, "An analysis of proof-of-work based blockchains under an adaptive double-spend attack," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2020.

[53] S. N. G. Gourisetti, M. Mylrea, and H. Patangia, "Evaluation and demonstration of blockchain applicability framework," *IEEE Transactions on Engineering Management*, pp. 1–15, 2019.

[54] T. Distler, C. Cachin, and R. Kapitza, "Resource-efficient byzantine fault tolerance," *IEEE Transactions on Computers*, vol. 65, no. 9, pp. 2807–2819, 2016.

[55] S. Gao, T. Yu, J. Zhu, and W. Cai, "T-pbft: An eigentrust-based practical byzantine fault tolerance consensus algorithm," *China Communications*, vol. 16, no. 12, pp. 111–123, 2019.

[56] T. Liu, J. Ge, Y. Wu, B. Dai, L. Li, Z. Yao, J. Wen, and H. Shi, "A new bitcoin address association method using a two-level learner model," in *Algorithms and Architectures for Parallel Processing*, S. Wen, A. Zomaya, and L. T. Yang, Eds. Cham: Springer International Publishing, 2020, pp. 349–364.

[57] W. Zou, D. Lo, P. S. Kochhar, X. D. Le, X. Xia, Y. Feng, Z. Chen, and B. Xu, "Smart contract development: Challenges and opportunities," *IEEE Transactions on Software Engineering*, pp. 1–1, 2019.

[58] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, "Blockchain and machine learning for communications and networking systems," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2020.

[59] O. Osanaiye, S. Chen, Z. Yan, R. Lu, K. R. Choo, and M. Dlodlo, "From cloud to fog computing: A review and a conceptual live vm migration framework," *IEEE Access*, vol. 5, pp. 8284–8300, 2017.

[60] Z. Zhao, G. Min, W. Gao, Y. Wu, H. Duan, and Q. Ni, "Deploying edge computing nodes for large-scale iot: A diversity aware approach," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3606–3614, 2018.

[61] L. Cui, D. Su, Y. Zhou, L. Zhang, Y. Wu, and S. Chen, "Edge learning for surveillance video uploading sharing in public transport systems," *IEEE Transactions on Intelligent Transportation Systems*, doi: 10.1109/TITS.2020.3008420, 2020.

[62] M. Chen, Y. Miao, H. Gharavi, L. Hu, and I. Humar, "Intelligent traffic adaptive resource allocation for edge computing-based 5g networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 2, pp. 499–508, 2020.

[63] S. Guo, Y. Dai, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing stackelberg game and double auction based task offlfloading for mobile blockchain," *IEEE Transactions on Vehicular Technology*, pp. 1–1, 2020.

[64] B. Yin, H. Yin, Y. Wu, and Z. Jiang, "Fdc: A secure federated deep learning mechanism for data collaborations in the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6348–6359, 2020.

[65] Y. Cheng, J. Zhang, L. Yang, C. Zhu, and H. Zhu, "Distributed green offloading and power optimization in virtualized small cell networks with mobile edge computing," *IEEE Transactions on Green Communications and Networking*, vol. 4, no. 1, pp. 69–82, 2020.

[66] D. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, "A survey on secure data analytics in edge computing," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4946–4967, 2019.

[67] B. Hamdaoui, M. Alkalbani, T. Znati, and A. Rayes, "Unleashing the Power of Participatory IoT with Blockchains for Increased Safety and Situation Awareness of Smart Cities," *IEEE Network*, vol. 34, no. 2, pp. 202–209, 2020.

[68] W. Viriyasitavat, L. D. Xu, Z. Bi, and D. Hoonsopon, "Blockchain technology for applications in internet of things—mapping from system design perspective," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8155–8168, 2019.

[69] T. Kim, J. Ochoa, T. Faika, A. Mantooth, J. Di, Q. Li, and Y. Lee, "An overview of cyber-physical security of battery management systems and adoption of blockchain technology," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, pp. 1–1, 2020.

[70] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: A distributed and trusted authentication system," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1972–1983, 2020.

[71] G. Min, Y. Wu, and A. Y. Al-Dubai, "Performance modelling and analysis of cognitive mesh networks," *IEEE Transactions on Communications*, vol. 60, no. 6, pp. 1474–1478, 2012.

[72] Y. Wu, G. Min, and A. Y. Al-Dubai, "A new analytical model for multi-hop cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 5, pp. 1643–1648, 2012.

[73] M. B. H. Weiss, K. Werbach, D. C. Sicker, and C. E. C. Bastidas, "On the application of blockchains to spectrum management," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 2, pp. 193–205, 2019.

[74] Y.-C. Liang, *Blockchain for Dynamic Spectrum Management*. Singapore: Springer Singapore, 2020, pp. 121–146.

[75] Z. Zhou, X. Chen, Y. Zhang, and S. Mumtaz, "Blockchain-empowered secure spectrum sharing for 5g heterogeneous networks," *IEEE Network*, vol. 34, no. 1, pp. 24–31, 2020.

[76] A. Refaey, K. Hammad, S. Magierowski, and E. Hossain, "A Blockchain Policy and Charging Control Framework for Roaming in Cellular Networks," *IEEE Network*, vol. 34, no. 3, pp. 170–177, 2020.

[77] 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 Transactions on Intelligent Transportation Systems*, pp. 1–15, 2020.

[78] G. Yu, X. Zha, X. Wang, W. Ni, K. Yu, P. Yu, J. A. Zhang, R. P. Liu, and Y. J. Guo, "Enabling attribute revocation for fine-grained access control in blockchain-iot systems," *IEEE Transactions on Engineering Management*, pp. 1–18, 2020.

[79] O. Novo, "Scalable Access Management in IoT Using Blockchain: A Performance Evaluation," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4694–4701, 2019.

[80] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594–1605, 2019.

[81] M. A. Islam and S. Madria, "A Permissioned Blockchain Based Access Control System for IOT," in *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 469–476.

[82] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2019.

[83] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," *Computer Networks*, vol. 167, p. 106984, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128619304773

[84] W. Miao, G. Min, Y. Wu, H. Wang, and J. Hu, "Performance modelling and analysis of software-defined networking under bursty multimedia traffic," *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 12, no. 5s, Sep. 2016. [Online]. Available: https://doi.org/10.1145/2983637

[85] G. Wang, Y. Zhao, J. Huang, and Y. Wu, "An effective approach to controller placement in software defined wide area networks," *IEEE Transactions on Network and Service Management*, vol. 15, no. 1, pp. 344–355, 2018.

[86] X. Cheng, Y. Wu, G. Min, and A. Y. Zomaya, "Network function virtualization in dynamic networks: A stochastic perspective," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 10, pp. 2218–2232, 2018.

[87] W. Miao, G. Min, Y. Wu, H. Huang, Z. Zhao, H. Wang, and C. Luo, "Stochastic performance analysis of network function virtualization in future internet," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 3, pp. 613–626, 2019.

[88] X. Cheng, Y. Wu, G. Min, A. Y. Zomaya, and X. Fang, "Safeguard network slicing in 5g: A learning augmented optimization approach," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 7, pp. 1600–1613, 2020.

[89] H. Wang, Y. Wu, G. Min, J. Xu, and P. Tang, "Data-driven dynamic resource scheduling for network slicing: A deep reinforcement learning approach," *Information Sciences*, vol. 498, pp. 106 – 116, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025519303986

[90] C. Wang, Y. Zhang, X. Chen, K. Liang, and Z. Wang, "Sdn-based handover authentication scheme for mobile edge computing in cyber-physical systems," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8692–8701, 2019.

[91] J. Gao, K. O. O. Agyekum, E. B. Sifah, K. N. Acheampong, Q. Xia, X. Du, M. Guizani, and H. Xia, "A Blockchain-SDN enabled Internet of Vehicles Environment for Fog Computing and 5G Networks," *IEEE Internet of Things Journal*, pp. 1–1, 2019.

[92] G. A. F. Rebello, I. D. Alvarenga, I. J. Sanz, and O. C. M. B. Duarte, "BSec-NFVO: A Blockchain-Based Security for Network Function Virtualization Orchestration," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, May 2019, pp. 1–6.

[93] M. F. Franco, E. J. Scheid, L. Z. Granville, and B. Stiller, "BRAIN: blockchain-based reverse auction for infrastructure supply in virtual network functions-as-a-service," in *2019 IFIP Networking Conference (IFIP Networking)*, 2019, pp. 1–9.

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

[95] V. Ortega, F. Bouchmal, and J. F. Monserrat, "Trusted 5G Vehicular Networks: Blockchains and Content-Centric Networking," *IEEE Vehicular Technology Magazine*, vol. 13, no. 2, pp. 121–127, June 2018.

[96] J. Ge, S. Wang, Y. Wu, H. Tang, and Y. E, "Performance improvement for source mobility in named data networking based on global–local fib updates," *Peer-to-Peer Networking and Applications*, vol. 9, no. 4, pp. 670–680, Jul 2016. [Online]. Available: https://doi.org/10.1007/s12083-015-0353-z

[97] Y. Xu, C. Zhang, G. Wang, Z. Qin, and Q. Zeng, "A Blockchain-enabled Deduplicatable Data Auditing Mechanism for Network Storage Services," *IEEE Transactions on Emerging Topics in Computing*, pp. 1–1, 2020.

[98] G. S. Aujla, M. Singh, A. Bose, N. Kumar, G. Han, and R. Buyya, "BlockSDN: Blockchain-as-a-Service for Software Defined Networking in Smart City Applications," *IEEE Network*, vol. 34, no. 2, pp. 83–91, 2020.

[99] B. Wu, K. Xu, Q. Li, S. Ren, Z. Liu, and Z. Zhang, "Toward Blockchain-Powered Trusted Collaborative Services for Edge-Centric Networks," *IEEE Network*, vol. 34, no. 2, pp. 30–36, 2020.

[100] H. Ko, J. Lee, and S. Pack, "Spatial and Temporal Computation Offloading Decision Algorithm in Edge Cloud-Enabled Heterogeneous Networks," *IEEE Access*, vol. 6, pp. 18 920–18 932, 2018.

[101] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On multi-access edge computing: A survey of the emerging 5g network edge cloud architecture and orchestration," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1657–1681, 2017.

[102] 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 Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019.

[103] 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 Transactions on Services Computing*, vol. 13, no. 2, pp. 356–367, 2020.

[104] W. Chen, Z. Zhang, Z. Hong, C. Chen, J. Wu, S. Maharjan, Z. Zheng, and Y. Zhang, "Cooperative and distributed computation offloading for blockchain-empowered industrial internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8433–8446, 2019.

[105] Y. Jiao, P. Wang, D. Niyato, and K. Suankaewmanee, "Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 9, pp. 1975–1989, 2019.

[106] S. Xie, Z. Zheng, W. Chen, J. Wu, H.-N. Dai, and M. Imran, "Blockchain for cloud exchange: A survey," *Computers & Electrical Engineering*, vol. 81, p. 106526, 2020.

[107] Q. Xu, Z. Su, M. Dai, and S. Yu, "APIS: Privacy-Preserving Incentive for Sensing Task Allocation in Cloud and Edge-Cooperation Mobile Internet of Things with SDN," *IEEE Internet of Things Journal*, pp. 1–1, 2019.

[108] J. Huang, L. Kong, H. Dai, W. Ding, L. Cheng, G. Chen, X. Jin, and P. Zeng, "Blockchain based mobile crowd sensing in industrial systems," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2020.

[109] 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 Network*, vol. 34, no. 1, pp. 166–173, 2020.

[110] C. Xu, K. Wang, P. Li, S. Guo, J. Luo, B. Ye, and M. Guo, "Making big data open in edges: A resource-efficient blockchain-based approach," *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 4, pp. 870–882, 2019.

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

[112] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, "Decentralized resource allocation for video transcoding and delivery in blockchain-based system with mobile edge computing," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11 169–11 185, 2019.

[113] W. Liang, Y. Fan, K. Li, D. Zhang, and J. Gaudiot, "Secure data storage and recovery in industrial blockchain network environments," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2020.

[114] 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 Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2906–2920, 2019.

[115] Z. Chang, W. Guo, X. Guo, Z. Zhou, and T. Ristaniemi, "Incentive Mechanism for Edge Computing-based Blockchain," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2020.

[116] J. Kang, Z. Xiong, D. Niyato, P. Wang, D. Ye, and D. I. Kim, "Incentivizing Consensus Propagation in Proof-of-Stake Based Consortium Blockchain Networks," *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 157–160, 2019.

[117] Z. Li, Z. Yang, S. Xie, W. Chen, and K. Liu, "Credit-Based Payments for Fast Computing Resource Trading in Edge-Assisted Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6606–6617, 2019.

[118] H.-N. Dai, R. C.-W. Wong, H. Wang, Z. Zheng, and A. V. Vasilakos, "Big data analytics for large-scale wireless networks: Challenges and opportunities," *ACM Computing Surveys (CSUR)*, vol. 52, no. 5, pp. 1–36, 2019.

[119] Y. Liu, H.-N. Dai, Q. Wang, M. K. Shukla, and M. Imran, "Unmanned aerial vehicle for internet of everything: Opportunities and challenges," *Computer Communications*, vol. 155, pp. 66 – 83, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366419318754

[120] M. Raza, N. Aslam, H. Le-Minh, S. Hussain, Y. Cao, and N. M. Khan, "A critical analysis of research potential, challenges, and future directives in industrial wireless sensor networks," *IEEE Communications Surveys Tutorials*, vol. 20, no. 1, pp. 39–95, 2018.

[121] R. Rondón, A. Mahmood, S. Grimaldi, and M. Gidlund, "Understanding the performance of bluetooth mesh: Reliability, delay, and scalability analysis," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2089–2101, 2020.

[122] J. Haxhibeqiri, I. Moerman, and J. Hoebeke, "Low Overhead Scheduling of LoRa Transmissions for Improved Scalability," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3097–3109, 2019.

[123] H. Xie, Z. Yan, Z. Yao, and M. Atiquzzaman, "Data collection for security measurement in wireless sensor networks: A survey," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2205–2224, 2019.

[124] M. M. Rabbani, J. Vliegen, J. Winderickx, M. Conti, and N. Mentens, "SHeLA: Scalable Heterogeneous Layered Attestation," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10 240–10 250, 2019.

[125] M. A. Togou, D. A. Chekired, L. Khoukhi, and G. Muntean, "A hierarchical distributed control plane for path computation scalability in large scale software-defined networks," *IEEE Transactions on Network and Service Management*, vol. 16, no. 3, pp. 1019–1031, 2019.

[126] F. P. Lin and Z. Tsai, "Hierarchical Edge-Cloud SDN Controller System With Optimal Adaptive Resource Allocation for Load-Balancing," *IEEE Systems Journal*, vol. 14, no. 1, pp. 265–276, 2020.

[127] D. A. Chekired, M. A. Togou, L. Khoukhi, and A. Ksentini, "5G-Slicing-Enabled Scalable SDN Core Network: Toward an Ultra-Low Latency of Autonomous Driving Service," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 8, pp. 1769–1782, 2019.

[128] R. Wen, G. Feng, J. Tang, T. Q. S. Quek, G. Wang, W. Tan, and S. Qin, "On robustness of network slicing for next-generation mobile networks," *IEEE Transactions on Communications*, vol. 67, no. 1, pp. 430–444, 2019.

[129] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, and Y. Zhao, "EdgeChain: An Edge-IoT Framework and Prototype Based on Blockchain and

Smart Contracts," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4719–4732, June 2019.

[130] Y. Liu, K. Wang, K. Qian, M. Du, and S. Guo, "Tornado: Enabling blockchain in heterogeneous internet of things through a space-structured approach," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1273–1286, 2020.

[131] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A Scalable Blockchain Framework for Secure Transactions in IoT," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4650–4659, 2019.

[132] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer *et al.*, "On scaling decentralized blockchains," in *International conference on financial cryptography and data security*. Springer, 2016, pp. 106–125.

[133] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366–1385, 2018.

[134] S. Popov, "The tangle, IOTA whitepaper," IOTA, Tech. Rep.[Online]. Available: https://iota. org/IOTA_Whitepaper.pdf, Tech. Rep., 2018.

[135] A. Cullen, P. Ferraro, C. King, and R. Shorten, "On the resilience of dag-based distributed ledgers in iot applications," *IEEE Internet of Things Journal*, 2020.

[136] Á. García-Pérez and M. A. Schett, "Deconstructing stellar consensus," in *23rd International Conference on Principles of Distributed Systems (OPODIS 2019)*, 2020.

[137] F. Armknecht, G. O. Karame, A. Mandal, F. Youssef, and E. Zenner, "Ripple: Overview and outlook," in *International Conference on Trust and Trustworthy Computing*. Springer, 2015, pp. 163–180.

[138] M. J. Amiri, D. Agrawal, and A. E. Abbadi, "Caper: a cross-application permissioned blockchain," *Proceedings of the VLDB Endowment*, vol. 12, no. 11, pp. 1385–1398, 2019.

[139] M. Herlihy, "Atomic cross-chain swaps," in *Proceedings of the 2018 ACM symposium on principles of distributed computing (PODC 2018)*, 2018, pp. 245–254.

[140] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, "Enabling blockchain innovations with pegged sidechains," *URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains*, vol. 72, 2014.

[141] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," [Online]. Available: https://www.win.tue.nl/∼mholende/seminar/references/ethereum_polkadot.pdf, Tech. Rep., 2016.

[142] S. Li, H. Xiao, H. Wang, T. Wang, J. Qiao, and S. Liu, "Blockchain dividing based on node community clustering in intelligent manufacturing cps," in *2019 IEEE International Conference on Blockchain (Blockchain 2019)*. IEEE, 2019, pp. 124–131.

[143] J. Hellings and M. Sadoghi, "Coordination-free byzantine replication with minimal communication costs," in *23rd International Conference on Database Theory (ICDT 2020)*, 2020.

[144] H. Dang, T. T. A. Dinh, D. Loghin, E.-C. Chang, Q. Lin, and B. C. Ooi, "Towards scaling blockchain systems via sharding," in *Proceedings of the 2019 International Conference on Management of Data*, 2019, pp. 123–140.

[145] A. Sharma, F. M. Schuhknecht, D. Agrawal, and J. Dittrich, "Blurring the lines between blockchains and database systems: the case of hyperledger fabric," in *Proceedings of the 2019 International Conference on Management of Data*, 2019, pp. 105–122.

[146] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of iot applications in blockchain systems: Architecture, consensus, and traffic modeling," *ACM Computing Surveys (CSUR)*, vol. 53, no. 1, pp. 1–32, 2020.

[147] F. M. Benčić and I. P. Žarko, "Distributed ledger technology: Blockchain compared to directed acyclic graph," in *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2018, pp. 1569–1570.

[148] M. Castro, B. Liskov *et al.*, "Practical byzantine fault tolerance," in *OSDI*, vol. 99, no. 1999, 1999, pp. 173–186.

[149] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, and M. A. Imran, "Blockchain-enabled wireless internet of things: Performance analysis and optimal communication node deployment," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5791–5802, 2019.

[150] Y. Liu, K. Wang, K. Qian, M. Du, and S. Guo, "Tornado: Enabling blockchain in heterogeneous internet of things through a space-structured approach," *IEEE Internet of Things Journal*, 2019.

[151] 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 of Things Journal*, vol. 6, no. 3, pp. 4585–4600, 2018.

[152] H. Yao, T. Mai, J. Wang, Z. Ji, C. Jiang, and Y. Qian, "Resource trading in blockchain-based industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3602–3609, 2019.

[153] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 33–39, 2018.

[154] L. Wu, L. Li, X. Li, Y. Yu, L. Zhang, M. Pan, and Z. Han, "Resource allocation in blockchain system based on mobile edge computing networks," in *2019 11th International Conference on Wireless Communications and Signal Processing (WCSP)*. IEEE, 2019, pp. 1–6.

[155] C. Luo, S. Guo, S. Guo, L. T. Yang, G. Min, and X. Xie, "Green communication in energy renewable wireless mesh networks: Routing, rate control, and power allocation," *IEEE Trans. Paral. and Distr. Syst.*, vol. 25, no. 12, pp. 3211–3220, Dec. 2014.

[156] C. Luo, G. Min, F. R. Yu, Y. Zhang, L. T. Yang, and V. C. M. Leung, "Joint relay scheduling, channel access, and power allocation for green cognitive radio communications," *IEEE J. Sel. Areas in Comm.*, vol. 33, no. 5, pp. 922–932, May 2015.

[157] G. Xu, W. Wang, L. Jiao, X. Li, K. Liang, X. Zheng, W. Lian, H. Xian, and H. Gao, "SoProtector: Safeguard Privacy for Native SO Files in Evolving Mobile IoT Applications," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2539–2552, 2020.

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

[159] S. He, W. Ren, T. Zhu, and K. R. Choo, "BoSMoS: A Blockchain-Based Status Monitoring System for Defending Against Unauthorized Software Updating in Industrial Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 948–959, Feb. 2020.

[160] T. Chen, X. Li, Y. Wang, J. Chen, Z. Li, X. Luo, M. H. Au, and X. Zhang, "An adaptive gas cost mechanism for ethereum to defend against under-priced dos attacks," in *International Conference on Information Security Practice and Experience*. Springer, 2017, pp. 3–24.

[161] Z. Huang, J. Huang, and T. Zang, "Leopard: Understanding the Threat of Blockchain Domain Name Based Malware," in *Passive and Active Measurement*, A. Sperotto, A. Dainotti, and B. Stiller, Eds. Cham: Springer International Publishing, 2020, pp. 55–70.

[162] T. Chen *et al.*, "SODA: A Generic Online Detection Framework for Smart Contracts," in *The Network and Distributed System Security Symposium (NDSS)*, 2020, pp. 1–17.

[163] M. Chen, Y. Cao, R. Wang, Y. Li, D. Wu, and Z. Liu, "Deepfocus: Deep encoding brainwaves and emotions with multi-scenario behavior analytics for human attention enhancement," *IEEE Network*, vol. 33, no. 6, pp. 70–77, 2019.

[164] X. Wang, L. T. Yang, Y. Wang, L. Ren, and M. J. Deen, "Adtt: A highly-efficient distributed tensor-train decomposition method for iiot big data," *IEEE Transactions on Industrial Informatics*, pp. 1–1, DOI: 10.1109/TII.2020.2967768, 2020.

[165] R. Wang, M. Chen, N. Guizani, Y. Li, H. Gharavi, and K. Hwang, "Deepnetqoe: Self-adaptive qoe optimization framework of deep networks," *IEEE Network*, 2020.

[166] J. Kang, Z. Xiong, D. Niyato, S. Xie, and J. Zhang, "Incentive Mechanism for Reliable Federated Learning: A Joint Optimization Approach to Combining Reputation and Contract Theory," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10 700–10 714, 2019.

[167] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo, and J. Zhang, "Edge Intelligence: Paving the Last Mile of Artificial Intelligence With Edge Computing," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1738–1762, 2019.

[168] K. Zhang, Y. Zhu, S. Maharjan, and Y. Zhang, "Edge Intelligence and Blockchain Empowered 5G Beyond for the Industrial Internet of Things," *IEEE Network*, vol. 33, no. 5, pp. 12–19, 2019.

[169] Z. Yan, J. Ge, Y. Wu, L. Li, and T. Li, "Automatic virtual network embedding: A deep reinforcement learning approach with graph convolutional networks," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1040–1057, 2020.

[170] J. Luo, Q. Chen, F. R. Yu, and L. Tang, "Blockchain-enabled software-defined industrial internet of things with deep reinforcement learning," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[171] Z. Xiong, Y. Zhang, D. Niyato, R. Deng, P. Wang, and L. Wang, "Deep Reinforcement Learning for Mobile 5G and Beyond: Fundamentals, Applications, and Challenges," *IEEE Vehicular Technology Magazine*, vol. 14, no. 2, pp. 44–52, 2019.

[172] Y. Chen, Y. Zhang, S. Maharjan, M. Alam, and T. Wu, "Deep Learning for Secure Mobile Edge Computing in Cyber-Physical Transportation Systems," *IEEE Network*, vol. 33, no. 4, pp. 36–41, 2019.

[173] Y. Chen, Z. Ma, Q. Wang, J. Huang, X. Tian, and Q. Zhang, "Privacy-preserving spectrum auction design: Challenges, solutions, and research directions," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 142–150, 2019.

[174] P. C. Mahawaga Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, and M. Atiquzzaman, "A trustworthy privacy preserving framework for machine learning in industrial iot systems," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2020.

[175] J. Feng, L. T. Yang, R. Zhang, and B. S. Gavuna, "Privacy Preserving Tucker Train Decomposition over Blockchain-Based Encrypted Industrial IoT Data," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2020.

[176] Y. Zhan, P. Li, Z. Qu, D. Zeng, and S. Guo, "A Learning-based Incentive Mechanism for Federated Learning," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

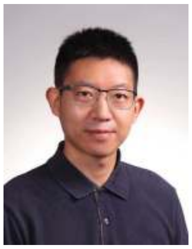
[177] J. Kang, Z. Xiong, D. Niyato, Y. Zou, Y. Zhang, and M. Guizani, "Reliable federated learning for mobile networks," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 72–80, 2020.

[178] M. Chen and Y. Hao, "Label-less learning for emotion cognition," *IEEE Transactions on Neural Networks and Learning Systems*, pp. 1–11, 2019.

[179] O. Alkadi, N. Moustafa, B. Turnbull, and K. R. Choo, "A Deep Blockchain Framework-enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[180] X. Liu, H. Li, G. Xu, S. Liu, Z. Liu, and R. Lu, "PADL: Privacy-aware and Asynchronous Deep Learning for IoT Applications," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[181] F. Estrada-Solano, O. M. Caicedo, and N. L. S. Da Fonseca, "NELLY: Flow Detection Using Incremental Learning at the Server Side of SDN-Based Data Centers," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1362–1372, 2020.



Yulei Wu [Senior Member, IEEE] is a Senior Lecturer with the Department of Computer Science, College of Engineering, Mathematics and Physical Sciences, University of Exeter, United Kingdom. He received the B.Sc. degree (First Class Honours) in Computer Science and the Ph.D. degree in Computing and Mathematics from the University of Bradford, United Kingdom, in 2006 and 2010, respectively. His expertise is on intelligent networking, and his main research interests include computer networks, networked systems, software defined networks and systems, network management, and network security and privacy. His research has been supported by Engineering and Physical Sciences Research Council of United Kingdom, National Natural Science Foundation of China, University's Innovation Platform and industry. He is an Editor of IEEE Transactions on Network and Service Management, IEEE Transactions on Network Science and Engineering, Computer Networks (Elsevier) and IEEE ACCESS. He is a Fellow of the HEA (Higher Education Academy).

Hong-Ning Dai [Senior Member, IEEE] is currently with Faculty of Information Technology at Macau University of Science and Technology as an associate professor. He obtained the Ph.D. degree in Computer Science and Engineering from Department of Computer Science and Engineering at the Chinese University of Hong Kong. His current research interests include Internet of Things, blockchain, and big data analytics. He has served as editors for Ad Hoc Networks (Elsevier), Connection Science (Taylor & Francis), and IEEE Access, guest editors for IEEE Transactions on Industrial Informatics, IEEE Transactions on Emerging Topics in Computing, and IEEE Open Journal of the Computer Society.

Hao Wang [Member, IEEE] is an Associate Professor in the Department of Computer Science in Norwegian University of Science and Technology, Norway. He has a Ph.D. degree (2006) and a B.Eng. degree (2000), both in computer science and engineering, from South China University of Technology, China. His research interests include big data analytics, industrial internet of things, high performance computing, and safety-critical systems. He served as a TPC co-chair for IEEE DataCom 2015, IEEE CIT 2017, ES 2017, and IEEE CPSCom 2020, and a senior TPC member for CIKM 2019. He is the Chair for Sub-TC on Healthcare of IEEE Industrial Electronics Society Technical Committee on Industrial Informatics.