This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.3020092, IEEE Communications Surveys & Tutorials

Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges

Dinh C. Nguyen, *Student Member, IEEE,* Pubudu N. Pathirana, *Senior Member, IEEE,*
Ming Ding, *Senior Member, IEEE,* and Aruna Seneviratne, *Senior Member, IEEE*

***Abstract*—The blockchain technology is taking the world by storm. Blockchain with its decentralized, transparent and secure nature has emerged as a disruptive technology for the next generation of numerous industrial applications. One of them is Cloud of Things enabled by the combination of cloud computing and Internet of Things. In this context, blockchain provides innovative solutions to address challenges in Cloud of Things in terms of decentralization, data privacy and network security, while Cloud of Things offer elasticity and scalability functionalities to improve the efficiency of blockchain operations. Therefore, a novel paradigm of blockchain and Cloud of Things integration, called BCoT, has been widely regarded as a promising enabler for a wide range of application scenarios. In this paper, we present a state-of-the-art review on the BCoT integration to provide general readers with an overview of the BCoT in various aspects, including background knowledge, motivation, and integrated architecture. Particularly, we also provide an in-depth survey of BCoT applications in different use-case domains such as smart healthcare, smart city, smart transportation and smart industry. Then, we review the recent BCoT developments with the emerging blockchain and cloud platforms, services, and research projects. Finally, some important research challenges and future directions are highlighted to spur further research in this promising area.**

***Index Terms*—Blockchain, cloud computing, Internet of Things, Cloud of Things, security, industrial applications.**

I. Introduction

Recent years have witnessed the explosion of interest in blockchain, across a wide span of applications from cryptocurrencies to industries [1], [2]. The rapid development in the adoption of blockchain as a disruptive technology is paving the way for the next generation of financial and industrial service sectors. Indeed, new research activities on blockchain and its applications take place every day, impacting many aspects of our lives, such as finance [3], energy [4], and government services [5].

From a technical perspective, blockchain is a distributed ledger technology that was first used to serve as the public digital ledger of cryptocurrency Bitcoin [6] for economic transactions. The blockchain is basically a decentralized, immutable and public database. The concept of blockchain is based on a peer-to-peer network architecture in which transaction information is not controlled by any single centralized entity. Transactions stored in a chain of blocks are publicly accessible to all blockchain network members in a trustworthy manner. Blockchain uses consensus mechanisms and cryptography to validate the legitimacy of data transactions, which guarantees resistance of linked blocks against modifications and alterations [7]. In particular, the blockchain technology also boasts the desirable characteristics of decentralization, accountability, and security which improve service efficiency and save operational costs. Such exceptional properties promote the usage of applications built on blockchain in recent years. Thus, it makes now the right time to pay attention to this hot research topic.

On the other side, the revolution in the field of information and communication has created a wealth of opportunities for advanced technologies, especially Internet of Things (IoT) and Cloud computing. IoT has reshaped and transformed our lives with various new industrial, consumer, and commercial services and applications [8], [9]. Typically, IoT is a system of physical objects that can be monitored, controlled or interacted with by ubiquitous electronic devices to enable ubiquitous industrial services, e.g., smart cities, smart industries, etc. Due to the limited resources of IoT devices, they always delegate IoT application tasks to Cloud computing, which gives birth to the Cloud of Things (CoT) paradigm [10], [11]. The CoT provides a flexible, robust cloud computing environment for processing and managing IoT services, showing great potentials to improve the system performance and efficiency of service delivery [12]. However, the conventional CoT infrastructures tend to be ineffective due to the following challenges. First, the conventional CoT solutions have mainly relied on centralized communication models, e.g., central cloud, for IoT service operations which make it hard to scale when IoT networks become more widespread [13]. Moreover, most current CoT systems mandate trusting a third party, e.g., a cloud provider, for IoT data processing, which raises data privacy concerns. Final, the centralized network infrastructure results in higher communication latency and power consumption for IoT devices due to long data transmission, which hinders the large-scale deployments of CoT in practical scenarios [14].

In order to achieve a sustainable development of CoT, building a more decentralized ecosystem has been regarded as a future direction to replace centralized computing models used in current applications, as illustrated in Fig. 1. It is

*This work was supported in part by the CSIRO Data61, Australia.

Dinh C. Nguyen is with School of Engineering, Deakin University, Waurn Ponds, VIC 3216, Australia, and also with the CSIRO Data61, Docklands, Melbourne, Australia (e-mail: cdnguyen@deakin.edu.au).

Pubudu N. Pathirana is with School of Engineering, Deakin University, Waurn Ponds, VIC 3216, Australia (email: pubudu.pathirana@deakin.edu.au).

Ming Ding is with the CSIRO Data61, Australia (email: ming.ding@data61.csiro.au).

Aruna Seneviratne is with School of Electrical Engineering and Telecommunications, University of New South Wales (UNSW), NSW, Australia (email: a.seneviratne@unsw.edu.au).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.3020092, IEEE Communications Surveys & Tutorials

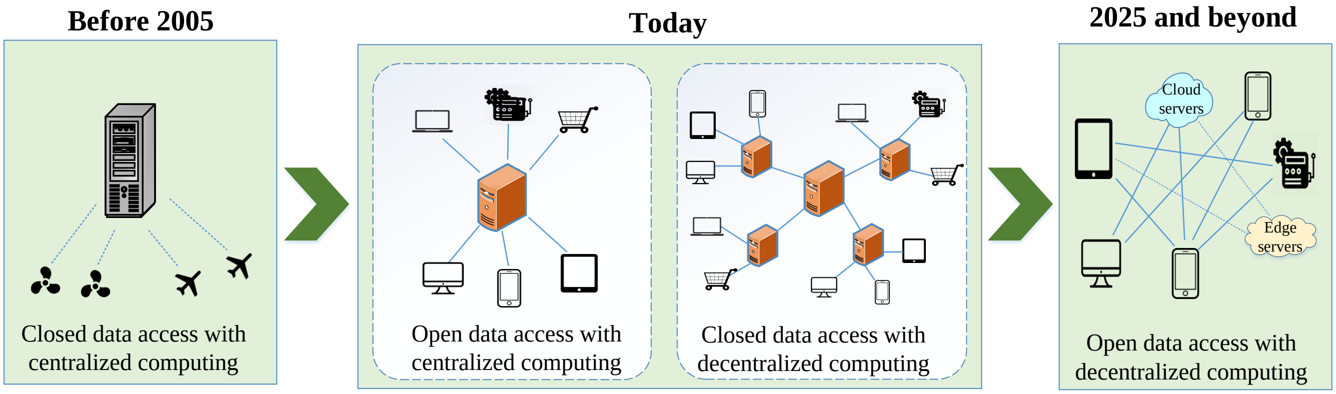
Before 2005
Today
2025 and beyond
Closed data access with centralized computing
Open data access with centralized computing
Closed data access with decentralized computing
Cloud servers
Edge servers
Open data access with decentralized computing

Fig. 1: Past, present and future Cloud of Things infrastructure.

strongly believed that blockchain will be a strong candidate to realize the full decentralization of future CoT networks. Particularly, the integration of blockchain and CoT leads to a novel paradigm called as *BCoT*. The combination of these emerging technologies brings great benefits to both worlds and thus gains sustainable interest in academics and industries. In fact, the blockchain and CoT have a number of complementary connections for practical applications. In the context of cloud computing, blockchain has been regarded as a service called Blockchain as a Service (BaaS). By providing a decentralized storage architecture using virtual storage nodes, blockchain can enable completely new cloud storage functions which are strongly resistant to data modifications. Instead of relying on traditional cloud data centres, blockchain interconnects computer nodes, including virtual machines on cloud and external computers, to build a fully decentralized storage system without requiring a central authority. Blockchain also functions as network management services which are closely related to smart contract-based applications. In such scenarios, blockchain acts as a communication layer among cloud servers, IoT devices, and end users. Specifically, the adoption of blockchain can provide many potential benefits for CoT systems as follows.

- Decentralization: Blockchain with its decentralized nature is a promising methodology to effectively solve the bottleneck and single-point failure issues by eliminating the requirement for a trusted third party in the CoT network [15]. Further, the peer-to-peer architecture of blockchain allows all network participants to verify IoT data correctness and ensure immutability with equal validation rights.
- Security and Privacy: The BCoT system can achieve a trustworthy access control by using blockchain-enabled smart contracts [16] which enable to authorize automatically all operations of cloud providers and IoT devices and prevent potential threats to cloud resources and enhance fine-grained control on IoT data [17]. Moreover, the blockchain enables users to track their transactions over the network so as to maintain device and data ownership for improving information privacy.
- Corporation: Blockchain enables a new cooperation ecosystem among multiple entities with unlimited data sharing capabilities without trusting each other. The removal of the third party helps establish open environments where any IoT users and cloud providers interested in the system can participate and collaborate to achieve the common goals within the BCoT ecosystem [18].

On the other hand, CoT can support blockchain platforms with the following key benefits:

- Scalable support for blockchain transactions: In large-scale blockchain applications, the number of transactions in blockchain networks can be enormous. Therefore, it is highly necessary to provide powerful data processing services to accelerate transaction execution in order to enable scalable blockchain services. In this context, the cloud can offer on-demand computing resources for blockchain operations thanks to its elasticity and scalability capability [19]. For example, public clouds can offer a large-scale network of resources for blockchain service operators in a federated cloud environment. Therefore, the combination of cloud computing and blockchain can achieve a high scalability of the integrated system.
- Fault tolerance: Cloud can help replicate blockchain data across a network of computing servers which are interconnected robustly by collaborative clouds [20]. This will minimize the single-failure risks due to the disruption of any cloud node and thus ensure uninterrupted services. Further, the inter-cloud ecosystem can enable the blockchain system to operate continuously in the event of a certain cloud server being under attack.

Reviewing the state of the art in the field, we find that BCoT attracts enormous interests of research communities as shown in Fig. 2. Cloud computing and IoT have gained popularity in the last five years with considerable research publications. Interestingly, blockchain is increasingly becoming a hot research area in recent years with a fast-growing research trend, showing a really promising topic for both academics and industries in the future. The sustainable development of CoT and blockchain will drive breakthrough innovations to empower intelligent services and applications.

A. *Related Works and Contributions of This Survey*

Many studies in CoT, blockchain and related issues have been investigated over the recent years in a wide range of technical aspects. Many efforts have been made to provide review articles on this research area in different scopes. The

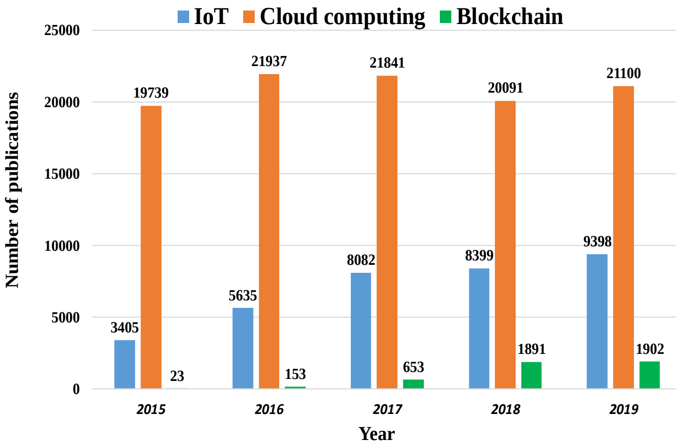

Fig. 2: Research trends about IoT, Cloud and blockchain (Source: Web of Science).

TABLE I: Surveys on blockchain and Cloud, IoT technologies.

Paper	Topic	Main contributions
[23]	Blockchain and IoT	A survey of blockchain protocols for IoT, research issues and challenges of IoT-blockchain integration.
[24]	Blockchain and IoT	A comprehensive survey of underlying blockchain concepts, architectures, applications for IoT.
[25]	Blockchain and IoT	A brief review on the usage of blockchain for IoT.
[26]	Blockchain and IoT	The investigation of the potential of blockchain for IoT applications.
[27]	Blockchain and IoT	Analysis on the technical aspects of blockchain and potentials of blockchain for IoT.
[28]	Blockchain and Cloud	A brief survey of blockchain in cloud computing and its security solutions for cloud-based applications.
[29]	Blockchain and Cloud	An introduction of blockchain for cloud platforms with associated challenges opportunities.
[30]	Blockchain and edge computing	A systematic survey of the combination of blockchain and edge computing
This paper	Blockchain and CoT	A comprehensive review on the integration of blockchain and CoT with a detailed discussion on concepts, architectures, BCoT applications and BCoT platforms along with challenges and future research directions.

survey papers [21], [22], [23] presented the review of recent efforts in the adoption of blockchain technology in various IoT scenarios and applications. The authors in [24] also discussed the integration of blockchain technology with IoT. The key focus of this work is on the investigation of the potential of blockchain for IoT applications, from smart manufacturing to the Internet of vehicles, unmanned aerial vehicles, and 5G networks. The survey in [25] paid attention to analysis on the technical aspects of blockchain, such as underlying concepts, networking and consensus strategies. Meanwhile, the authors in [26] discussed research issues, challenges and opportunities of combination between blockchain and cloud computing. The work [27] presented a survey on the use of the blockchain technology to provide security services and its technical properties to solve associated challenges in various application domains, including IoT and Cloud computing. More recently, the overview of the integrated model of blockchain and edge computing, an extended cloud computing concept, was discussed in the survey [28]. Table I summarizes the main topics and contributions of the literature surveys related to BCoT and our paper.

Although blockchain and CoT have been studied extensively in the literature works, there is no existing work to provide a comprehensive survey on the combination of these important research areas, to our best knowledge. In comparison to the above review works, in this paper, we provide an extensive survey on the integration of blockchain and CoT with a comprehensive discussion on many aspects, ranging from concept background, integrated architectures to application domains, service platforms and research challenges. The main goal of this survey is to provide readers with thorough knowledge of the blockchain and CoT integration which is collected from respective websites, technical reports, academic articles and newspapers. The main contributions of this survey are highlighted as follows.

1) We provide a state-of-the-art survey on the corporation of blockchain and CoT with a comprehensive discussion on different technical aspects, from BCoT background, integration motivations to the conceptual BCoT integrated architecture.
2) We present the updated review on the use of BCoT models in various application domains. We analyse the benefits of BCoT adoption and the important lessons learnt in each use case are then summarized. Moreover, the emerging BCoT platforms and services are also presented and discussed.
3) From the extensive review on BCoT integrations, we identify possible research challenges and open issues in the field. Some future research directions are also explored to extend the scope of BCoT in future services and applications.

B. Structure of The Survey

The structure of this survey is organized as Fig. 3. Section II describes the background knowledge of both blockchain and CoT and presents the motivations of the BCoT integration. The conceptual BCoT architecture is presented in Section III. We review the recent developments of BCoT in Section IV with extensive discussions on the roles of BCoT in a wide range of application domains. Moreover, the emerging BCoT platforms and services are also presented and discussed. Section V discusses possible research challenges and open issues in the BCoT integration, while future directions are outlined in Section VI. Finally, Section VII concludes the paper.

II. Blockchain, CoT, and Integration Motivation

In this section, we first introduce the background knowledge of blockchain and CoT. Then, we present the motivations of the integration of such two technologies.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.3020092, IEEE Communications Surveys & Tutorials

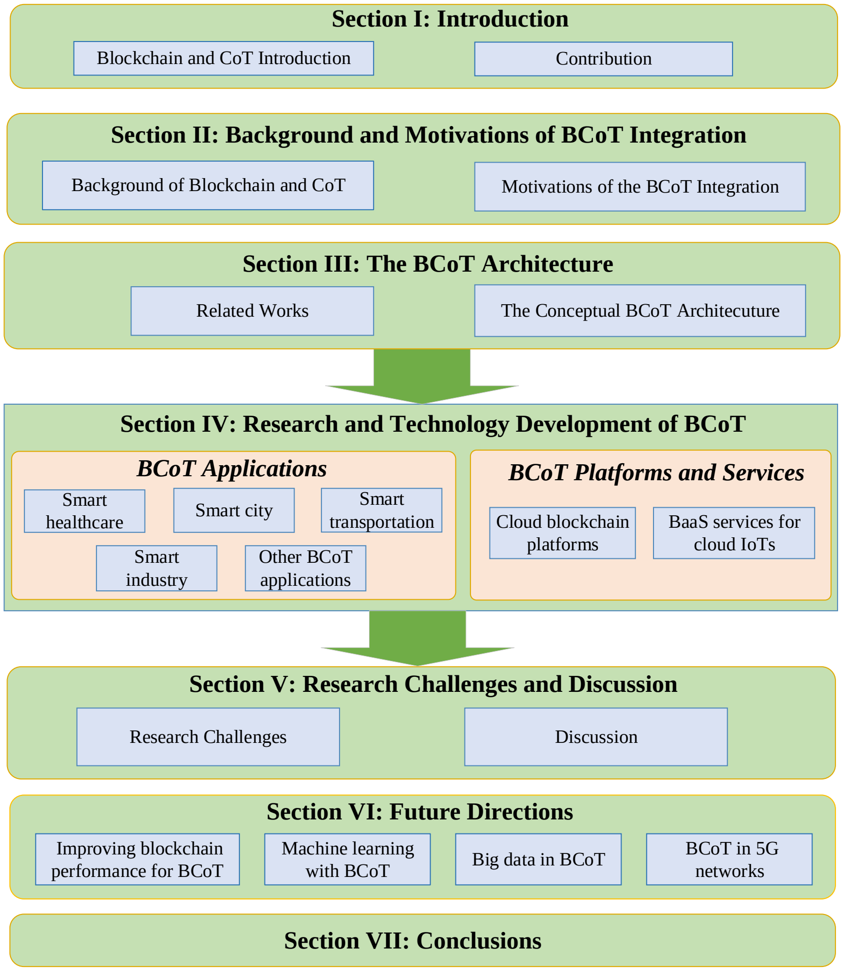
Section I: Introduction
Blockchain and CoT Introduction
Contribution
Section II: Background and Motivations of BCoT Integration
Background of Blockchain and CoT
Motivations of the BCoT Integration
Section III: The BCoT Architecture
Related Works
The Conceptual BCoT Architecuture
Section IV: Research and Technology Development of BCoT
BCoT Applications
Smart healthcare
Smart city
Smart transportation
Smart industry
Other BCoT applications
BCoT Platforms and Services
Cloud blockchain platforms
BaaS services for cloud IoTs
Section V: Research Challenges and Discussion
Research Challenges
Discussion
Section VI: Future Directions
Improving blockchain performance for BCoT
Machine learning with BCoT
Big data in BCoT
BCoT in 5G networks
Section VII: Conclusions

Fig. 3: Organization of the paper.

A. *Blockchain and Cloud of Things*

1) Blockchain: Blockchain is mostly known as the technology underlying the virtual cryptocurrency Bitcoin which was invented in 2008 by a person known as Satoshi Nakamoto [8]. In a nutshell, the blockchain is briefly explained as public, trusted and shared ledger based on a peer-to-peer network. This emerging technology has also recently become a hot topic for researchers and been argued to innovate blockchain-based applications beyond Bitcoin. The core idea of the blockchain network is decentralization which means blockchain is distributed over a network of nodes. Each node has the possibility of verifying the actions of other entities in the network, as well as the capability to create, authenticate and validate the new transaction to be recorded in the blockchain. This decentralized architecture ensures robust and secure operations on blockchain with the advantages of tamper resistance and no single-point failure vulnerabilities. Basically, blockchain can be classified into two main categories, including public (or permission-less) and private (or permissioned) blockchain. A public blockchain (e.g., Bitcoin platform) is an open network which means it is accessible for everyone to join and make transactions as well as participate in the consensus process. Meanwhile, private blockchain is an invitation-only network managed by a central entity and all participations in blockchain for submitting or writing transactions have to be permissioned by a validation mechanism. A general concept on how blockchain operates is presented in Fig. 4 and the most popular and promising blockchain platforms are summarized in Table II.

A blockchain network is built from some key components, including data block, distributed ledger, consensus, and smart contracts. To be clear, each block contains a number of transactions and is linked to its immediately-previous block through a hash label. In this way, all blocks in the chain can be traced back to the previous one, and no modification or alternation to block data is possible [39]. A distributed ledger is a type of database which is shared and replicated among the entities of a peer-to-peer network. Moreover, blockchain consensus is a process used to reach agreement on a single data block among multiple unreliable nodes, aiming to ensure security in a blockchain network. Final, smart contracts are programmable applications that run on a blockchain network according to predefined contractual conditions such as payment terms, liens, confidentiality, and even enforcement [40].

Blockchain can provide high-security properties for its applied scenarios, such as CoT. The most important feature is decentralization which means blockchain does not rely on a central point of control to manage transactions. This exceptional property brings promising benefits, including

TABLE II: Popular blockchain platforms.

Platforms	Consensus	Operation Modes	Smart contract support?	Programming language	Latest version	Open source?
Bitcoin	PoW	Public	Yes	Ivy, RSK, BitML	v0.18.0, May. 2019	Yes [29]
Ethereum	PoW, PoS	Public and permissioned	Yes	Solidity, Flint, SCILLA	v1.8.27, Apr. 2019	Yes [30]
Hyperledger	PBFT	Permissioned	Yes	Go, Node.js, Java	v2.0 Alpha, Apr. 2019	Yes [31]
IBM Blockchain	PoW, PoS	Permissioned	Yes	Go, Java	v2.0, Jun. 2019	Yes [32]
Multichain	PBFT	Permissioned	No	C++, Go, Java, Python, PHP	beta 2.0, Mar. 2016	Yes [33]
Hydrachain	PoW, PoS	Permissioned	Yes	Python	hydrachain 0.3.2, 2018	Yes [34]
Ripple	PoW	Permissioned	Yes	C++	v1.2.4, Apr. 2018	Yes [35]
R3 Corda	PoW, PoS	Permissioned	Yes	Kotlin, Java	V4.0, Feb. 2019	Yes [36]
BigChainDB	BFT	Public and permissioned	Yes	Java	v2.0.0b9, Nov. 2018	Yes [37]
Openchain	Partionned	Permissioned	Yes	C++, Java	v0.7.0, Nov. 2017	Yes [38]

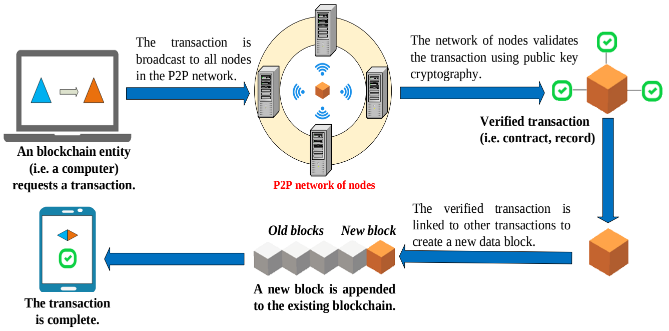
The transaction is broadcast to all nodes in the P2P network.
The network of nodes validates the transaction using public key cryptography.
An blockchain entity (i.e. a computer) requests a transaction.
P2P network of nodes
Verified transaction (i.e. contract, record)
The verified transaction is linked to other transactions to create a new data block.
Old blocks
New block
A new block is appended to the existing blockchain.
The transaction is complete.

Fig. 4: The concept of blockchain operation.

eliminating single point failure risks due to the disruption of central authority, saving operational costs and enhancing trustworthiness. Further, blockchain is able to keep transaction data immutable over time. The hashing process of a new block always contains metadata of the hash value of the previous block, which makes the chain strongly unalterable. In this way, it is impossible to modify, change or delete data of the block after it is validated and placed in the blockchain. Another important feature is transparency which stems from the fact that all information of transactions on blockchain is viewable to all network participants. In other words, the same copy of records of blockchain spreads across a large network for public verifiability. As a result, all blockchain users can fully access, verify and track transaction activities over the network with equal rights.

In addition to these security benefits, blockchain remains some problems that need to be considered to make it well suitable for integrating with CoT. For example, how to achieve energy efficiency for blockchain in BCoT applications is an important issue. The decentralized consensus algorithms in blockchains often require extensive processing power and high computing energy to mine blocks and maintain the blockchain network. This makes blockchain infeasible to resource-constrained IoT devices in CoT applications. Although we can perform energy-intensive blockchain mining in a centralized cloud, this would essentially negate the advantages of a distributed CoT system. Another issue is the throughput of blockchain systems. In fact, blockchain has much lower throughput in comparison to non-blockchain applications. For example, Bitcoin is able to execute a maximum of only four transactions/second, and the throughput of Ethereum achieved is about 20 transactions/second, while Visa can process up to 1667 transactions/second [24]. Clearly, the existing blockchain networks still remain scalability bottlenecks in terms of the number of replicas and limited throughput. Many current blockchain systems suffer from high block generation time which in turn reduces the overall blockchain throughput. Further, if all transactions are stored in a chain, the blockchain size will become very large [41]. Considering real-world CoT scenarios, e.g., smart cities, the IoT data volume is enormous and thus will result in a rapid growth in the IoT blockchain size. These factors thus should be taken into account in designing blockchain platforms for sustainable BCoT applications.

2) *Cloud of Things:* Nowadays, IoT has constituted a fundamental part of the future Internet and drawn increasing attention from academics and industries thanks to its great potentials to deliver exciting services across various applications. IoT seamlessly interconnects heterogeneous devices and objects to create a physical environment where sensing, processing and communication processes are implemented automatically without human involvement. However, massive volumes of data generated from a large number of devices in current IoT systems become a bottleneck in guaranteeing the desired Quality of Service (QoS) because of constrained power and storage resources of IoT devices. Meanwhile, cloud computing has unlimited resources in terms of storage and computation power, which can provide on-demand, powerful and efficient services for IoT use domains. Especially, the convergence of cloud computing with IoT paves the way for a new paradigm as CoT, which can empower both worlds. Indeed, the wealth of resources available on the cloud is highly beneficial to IoT systems, while cloud can gain more popularity in real-life applications from integrating with IoT platforms [61]. Moreover, CoT can transform current IoT service provision models with minimal management effort, high system performance and service availability. The general concept of CoT is shown in Fig. 5 with a network architecture of IoT devices, cloud computing, analytic services and application layer. In this hierarchy, IoT devices are used to sense and collect data from local environments. However, due to their limited computing resources, IoT devices will transmit recorded data to the cloud for data acquisition. Cloud computing can provide a powerful capability of data processing

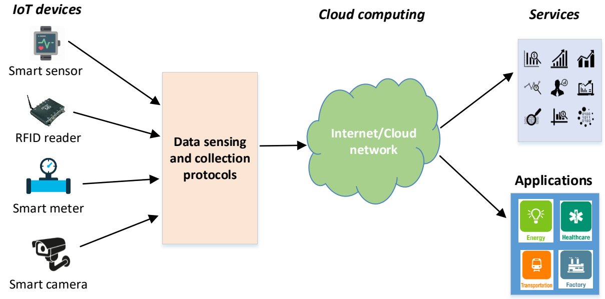

Fig. 5: The general concept of CoT.

and storage. Analytic services can be provided to support IoT systems, such as historic data monitoring, information storage or statistical analysis. The results of cloud data processing are used to serve end applications, aiming to facilitate IoT service provisions and meet requirements of end users.

In general, the CoT platform can offer instant services to users anywhere and anytime thanks to automatic resource provision capabilities of cloud computing. It enables autonomous service delivery without the need for human engagement. With unlimited virtual processing capabilities of cloud computing, CoT open up new opportunities to enhance IoT computation by enabling data offloading and executing data remotely. This not only improves computation abilities of local devices, but also addresses effectively issues of IoT systems in terms of energy-saving and bandwidth preservation. Importantly, CoT can offer simplified and automatic IT maintenance and management solutions by exploiting cloud servers, virtual machines and resource infrastructure. IoT users can interact easily with cloud computing to implement functionalities without any requirement for software installation as well as human involvement. Moreover, the provision of system management models available on clouds also supports well boundless communications and interconnections between IoT devices together, between things and users to empower ubiquitous applications, which would promote the comprehensive collaborations of multiple IoT ecosystems in the future Internet.

B. Motivation of the Integration of Blockchain and CoT

In this subsection, we highlight the motivation of the integration which comes from the security challenges of CoT, technical limitations of blockchain and the promising opportunities brought by the incorporation of such two technologies.

1) Security Challenges in CoT: CoT support ubiquitous computing services with large data storage and high system performance, but still remains some critical challenges [42], [43] as below.

Data availability: In the current cloud network architectures, cloud services are provided and managed centrally by the centralized authority. However, this configuration is vulnerable to single-point failures, which bring threats to the availability of cloud services for on-demand IoT access. A centralized cloud IoT system does not guarantee seamless provisions of IoT services when multiple users request simultaneously data or cloud servers are disrupted due to software bugs or cyber-attacks.

Privacy management: Although the centralized cloud IoT can provide convenient services, this paradigm raises critical data privacy concerns, considering a large amount of IoT data being collected, transferred, stored and used on the dynamic cloud networks. In fact, IoT users often place their trust in cloud providers managing the applications while knowing very little about how data is transmitted and who is currently using their information [44]. Even in the distributed cloud IoT paradigms with multiple clouds, IoT data are not fully distributed but stored in some cloud data centres at high density [45]. In this context, IoT data may be leaked if one of the cloud servers is attacked.

Data integrity: The storage and analysis of IoT data on clouds may give rise to integrity concerns. Indeed, due to having to place trust on the centralized cloud providers, outsourced data is put at risks of being modified or deleted by third parties without user consent. Moreover, adversaries can tamper with cloud data resources for financial or political purposes [46], all of which can breach data integrity. For these reasons, many solutions using public verification schemes based on a third-party auditor have been proposed, but they potentially raise several issues, including irresponsible verification to generate bias data integrity results or invalidated verification due to malicious auditors. Therefore, developing new solutions to solve efficiently data integrity challenges is vitally necessary for CoT systems.

2) Technical Limitations of Blockchain: Although blockchain has its unique promise to disrupt services like CoT, it still remains several critical challenges in its development in terms of complexity, and security flaw.

Complexity: In IoT networks, in order to implement validation on transactions, IoT devices act as blockchain participants to run the consensus process to solve complex mathematical puzzles, which requires powerful computation hardware. Unfortunately, this is challenging to meet such requirements due to the constraints of IoT resources. Even in the case of IoT devices with relatively high computing capacities, running complex blockchain process may require intensive resources involving electricity and human management. This would raise concerns of users about high operational costs which would hinder wide deployment of blockchain-based systems.

Security flaw: The final limitation of current blockchains may be an unavoidable security flaw. If more than half of computers working as blockchain nodes to control computing power, attackers may modify consensus architectures and prevent new transactions from obtaining confirmations for malicious access. This is also called as 51% attack which is highlighted in the Bitcoin concept. Without having a comprehensive transaction management, blockchain can be put at risks of data breach and system damage.

In short, the decentralization of CoT lays the ground for blockchain as data security and privacy solutions, and blockchain can leverage the cloud resources in CoT for intensive mining computations and reliable data storage.

3) The Opportunities of Integration of Blockchain and CoT: Based on complementary roles of blockchain and CoT as well as their potential advantages, the incorporation of such disruptive technologies opens up a wide range of BCoT opportunities, as summarized in the following.

Decentralization management: Motivated by the fully decentralized nature of blockchain, it is possible to build a decentralized BCoT management architecture under the distributed control of peer-to-peer network of cloud nodes and IoT devices. All blockchain peers maintain identical replicas of the ledger data records through decentralized consensus, and trustfulness is shared and distributed equally among the network entities. This decentralized structure eliminates totally single point failure bottlenecks, prevents efficiently disruption of BCoT services, and enhances significantly data availability.

Improved data privacy: The dynamic process of outsourcing IoT data to clouds and data exchange between cloud providers and IoT users are vulnerable to information disclosure and attacks caused by adversaries or third parties. Blockchain with its immutability, integrity and transparency properties is highly suitable for data protection in CoT networks. In fact, to launch a data modification attack in a BCoT system, an adversary would try to modify the records or alter data placed in blockchain. However, this is nearly impossible in practical scenarios where blockchain is preserved and controlled by secure and immutable consensus mechanisms. As a result, properties inherent to blockchain can significantly enhance data privacy for BCoT applications.

Improved system security: Blockchain can provide solutions to improve security for CoT, through the ability to offer important security properties such as confidentiality and availability inherent in blockchain. Indeed, in BCoT networks, all records on the blockchain are cryptographically hashed and transactions are signed by participants so that all user interactions with clouds remain confidential under blockchain-enabled signatures. Furthermore, with the decentralization feature inherent in blockchain, data is replicated across all network members with no single of failure bottlenecks, and thus BCoT promises to provide improved availability. Specially, the resourceful cloud computing can provide off-chain storage solutions to support data availability of the on-chain storage mechanisms once the main BCoT network is interrupted due to external attacks. On the other side, the implementation of blockchain algorithms on clouds may enhance security of the blockchain system itself. For example, clouds can use their available network security tools to maintain and preserve blockchain software, e.g., mining mechanism, against potential threats. The advantage of cloud computing for blockchain is proven through recent successful integration cloud-blockchain projects, such as Oracle blockchain (2017) and iExec blockchain (2018) projects [47].

Reduced system complexity: By integrating blockchain with cloud computing, BCoT can reduce significantly complexity of system implementations. This integration is known as blockchain-as-a-service, where well-defined platforms are available to set up and run blockchain for BCoT projects without worrying about underlying hardware technologies [48]. Moreover, blockchain algorithms now can be run online using cloud infrastructure, which is promising to reduce resource costs for running blockchain. Obviously, the convergence of blockchain and CoT opens up various opportunities to accelerate BCoT deployments on the large scale with simple and cheap implementations.

4) Feasibility of the BCoT Integration: At present, more and more large companies implement BaaS projects to assess the feasibility of the integration of blockchain in cloud computing. Large companies such as Amazon, Microsoft, IBM, Oracle have responded by launching BaaS platforms for IoT on cloud computing. The Amazon cloud provider develops a BaaS platform [49] for IoT business models. For example, an IoT healthcare system was developed in [50] by using Amazon BaaS architecture. In this project, the Ethereum blockchain platform hosted on Amazon cloud helps to implement a health data sharing framework on mobile clouds with high security and privacy. Moreover, IBM cloud [51] also introduces a well-developed BaaS platform for IoT users. The platform has been showcased in a vehicular network [206]. In this project, the IBM IoT platform is integrated with IBM BaaS services to manage vehicle sensor data (vehicle-to-vehicle messages and vehicle monitoring data) and ensure security during data sharing within the vehicular network. Meanwhile, the BaaS platform of Oracle cloud [52] has proven its great potentials through a wide range of BCoT projects, such as banking, healthcare data management, and payment industry. Such above examples have shown high feasibility of the blockchain adoption in cloud computing for solving complex issues in terms of security, network performance for IoT applications. We will detail the development of BaaS models in various IoT domains in the following sections.

III. The Architecture of Integration of Blockchain and CoT

In this section, we review thoroughly the literature studies towards the integrated BCoT models of blockchain and CoT. We then propose a conceptual BCoT architecture with the fundamental concept and basic ideas of the integration which would be applicable to various scenarios.

A. Related Works

With the current growing interest in the blockchain and CoT, many new integrated BCoT platforms and systems have been proposed in the literature studies to provide security solutions and applications [53], [54], [55], [56], [57]. The study [58] proposed a cloud-centric IoT framework enabled by smart contracts and blockchain for secure data provenance. Blockchain incorporates in cloud computing to build a comprehensive security network where IoT metadata (e.g., cryptographic hash) is stored in blockchain while actual data is kept in cloud storage, which makes it highly scalable for dense IoT deployments. Another work in [59] introduced a blockchain-cloud network for access control with four main components: IoT devices, a data owner, a blockchain network and a cloud computing platform. Similarly, a hierarchical access control structure for BCoT was investigated in [60]. The blockchain network topology involves distributed side blockchains deployed at fog nodes and a multi-blockchain operated in the cloud, which would speed up access verification offer flexible storage for scalable IoT networks. In addition, to protect

BCoT in security-critical applications, a forensic investigation framework is proposed using decentralized blockchain [61]. Following by the advantages of BCoT conjunction, [62], [63] provided secure identity management solutions which allow cloud service providers to autonomously control and authenticate user identity in BCoT. Blockchain is combined with virtual clouds to support identity verification in a fashion there is no prior requirements on trust between cloud users and cloud providers. On the other side, data management is also critical in interconnected CoT where IoT data is enormous and thus requires careful management for data privacy objectives. Motivated by this, the work [64] presented a blockchain-based data protection mechanism which can prevent effectively inappropriate IoT data movement due to malicious tampering during Virtual Machine (VM) migration on cloud computing. Also, a Mchain construction method is applied to integrity evaluation on VM measurements data [65]. In this architecture, a two-layer blockchain network, which includes a data validation layer and a PoW task layer, is integrated with IaaS cloud to enhance system integrity [66].

Moreover, the work in [67] also considered an integrated blockchain-CoT architecture where the focus was on solving the mining issue by offloading mining tasks to cloud nodes from IoT devices. Then, a joint problem of user access association and cloud resource allocation is formulated that is then solved by deep reinforcement learning (DRL). In the same direction, the authors in [68], [69] also considered the offloading issue in BCoT networks, in order to optimize the economic cost of IoT devices. The study in [70] paid attention to the cloud service quality in the BCoT systems. In this case, the blockchain plays an important role in providing trust and reliability for high-quality cloud service provisions. The combination of cloud computing with blockchain was also considered in [71]. Here, the computing resources of remote cloud are allocated at the network edge to provide low-latency and real-time computing services for IoT devices. Meanwhile, the resource management in BCoT systems was studied in [72] where the blockchain is able to preserve data privacy during the resource trading between cloud providers and IoT users.

In general, most of the above BCoT platforms are based on a single cloud and may be enough for some applications. However, with complex IoT systems which require huge network resources to serve numerous IoT users, inter-cloud BCoT integration would be more efficient and convenient [18]. As a result, BCoT architectures have been extended to multi-cloud models for complex collaborative scenarios [73], [74]. As an example, a BCoT framework was proposed in a joint cloud collaboration environment where multiple clouds are interconnected securely by a peer-to-peer ledge network [75]. Further, the single cloud can offer instant services for IoT users via blockchain which also mitigates risks of malicious attacks [76]. Moreover, [45] proposed a cloud federation model which enable distributed resource provisions using an individual cloud under the management of blockchain network. Besides, a BCoT model with micro-clouds was introduced by [77] using blockchain-enabled distributed ledgers.

B. The Conceptual BCoT Architecture

Motivated by extensive literature review, we propose a conceptual BCoT architecture as shown in Fig. 6, including three main layers: IoT layer, cloud blockchain layer and application layer. Details of each layer and the general concept will be presented as the following.

1) IoT Layer: IoT devices are responsible for harvesting data from local environments and transmitting wirelessly it to nearby gateways such as base station, router or wireless access point. An IoT device holds a blockchain account (like a wallet in Bitcoin) which allows it to join the blockchain network to perform transactions (e.g., offloading data) and interactions with cloud services. Specially, each resource-limited IoT device (e.g., a wearable sensor) may act as a lightweight node that can participate in the validation process of a transaction through its representative gateway. It is feasible in blockchain-based sensor network scenarios such as [105], [209], [214] where small sensors are connected with blockchain via its gateway (e.g., a smartphone or a fog node). All interactions of sensors with blockchain such as creating transactions, offloading data or even mining tasks, are performed by the gateway [58]. Meanwhile, for IoT devices with relatively large resources such as computers or powerful smartphones, they have enough capacities to serve other lightweight IoT sensors and maintain the full blockchain. IoT devices can also interact each other through IoT gateways to achieve corporative communication (e.g., device to device (D2D) communication in collaborative networks). Such a hybrid communication concept offers highly flexible services for IoT users in a secure and efficient manner.

2) Cloud Blockchain Layer: This plays as a middleware between the IoT network and industrial applications in the BCoT architecture. For a generic architecture, we pay attention to a blockchain platform with multiple clouds, but it also reflects comprehensively technical aspects of a single-cloud BCoT architecture. This model exhibits two merits: 1) ensuring highly secure network management via blockchain and 2) providing on-demand and reliable computing services for large-scale IoT applications. The integrated cloud blockchain layer consists of blockchain services and cloud computing services.

- *Blockchain services:* The main purpose of blockchain in the proposed architecture is to provide secure network management. The blockchain network is deployed and hosted on a cloud platform as Blockchain as a Service (BaaS). In particular, BaaS can offer a number of blockchain-enabled services to support IoT applications.

- Shared ledger: It represents the database that is shared and distributed among BCoT members (e.g., IoT users, cloud nodes and blockchain entities). The shared ledger records transactions, such as information exchange or data sharing among IoT devices and cloud. It enables industrial networks where cloud users can control and verify their own transactions when communicating with blockchain cloud.
- Consensus: It provides verification services on user transactions by using consensus mechanisms such as PoW,

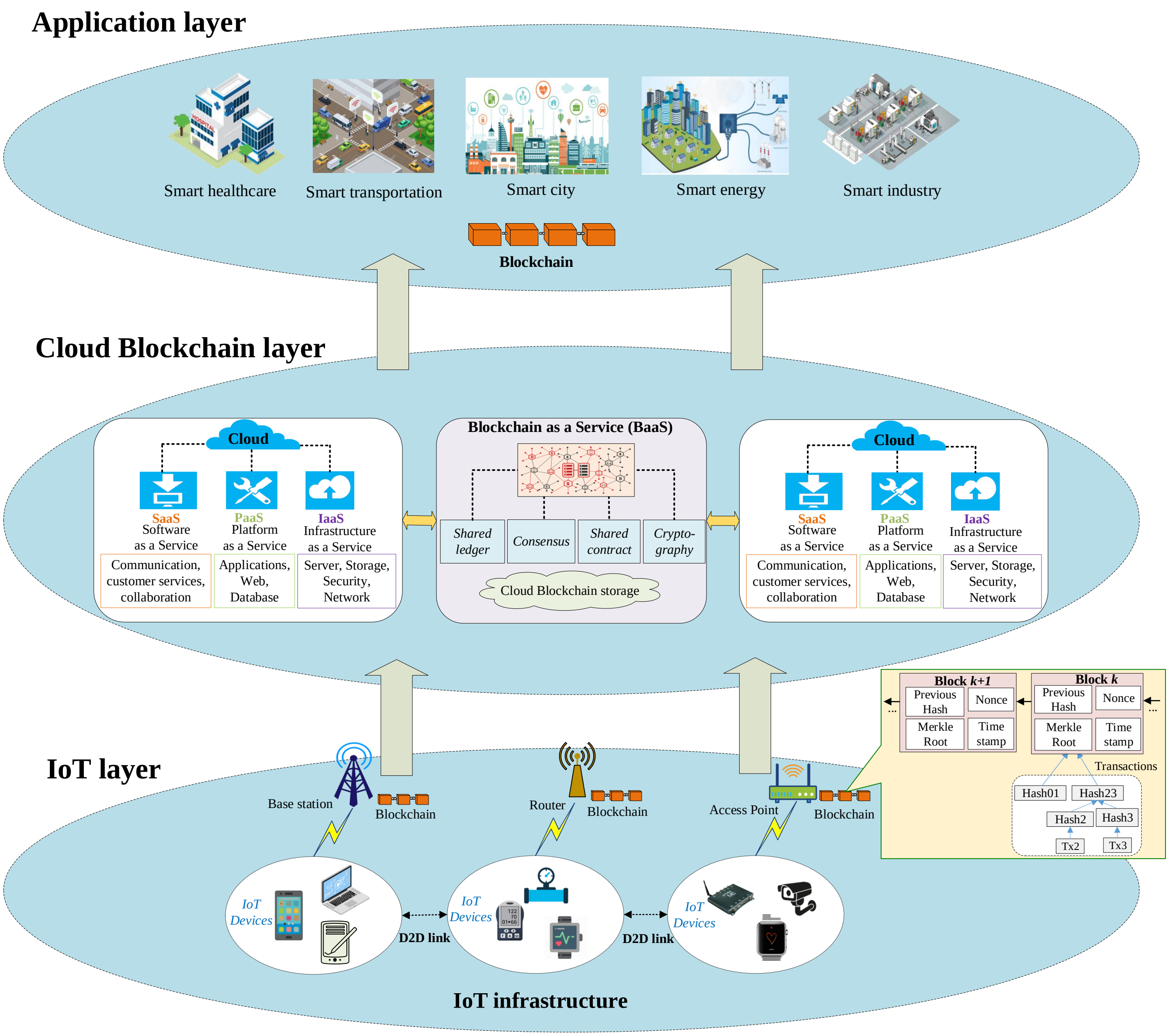

Fig. 6: The conceptual BCoT architecture.

PoS run by a network of miners. This service is highly necessary for BCoT in improving blockchain consistency and ensuring high security for the system. Interestingly, IoT users can use their virtual cloud machines to join the consensus process in order to receive rewards as a result of their efforts (e.g., cryptocurrency in Bitcoin).

- Shared contract: BCoT also offer smart contract services to applications. With its self-executing and independent features, smart contracts are highly beneficial to build business logic and trust in the BCoT system. Furthermore, smart contracts provide security services on user access authentication or data sharing verification once the IoT peer nodes perform transactions, which also supports to maintain security over the cloud blockchain.
- Cryptography: This is responsible for providing public-key cryptography to secure all information and storage of data among IoT and cloud entities. Digital signatures ensure any data being recorded in blockchain is true and untampered with, and this improves immutability and security for user transactions.

In addition to such services, BaaS also offers cloud blockchain storage. The decentralized cloud storage based on blockchain can be built on the cloud platform. Blockchain-based storage manages IoT data through its hash values and implements verification periodically to detect any data modification potentials. For example, InterPlanetary File System (IPFS) [78] is a blockchain-based storage system which is now available on cloud, allowing to store securely among storage nodes. This has also been proven to solve effectively data storage issues brought by centralized cloud models in terms of data leakage and storage management.

- *Cloud computing services:* In the BCoT architecture, cloud computing uses its full services to support applications, including Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). Data aggregated by IoT gateways will be received by cloud servers and kept in the cloud blockchain storage. The cloud server also offers intelligent services on offloaded IoT data using available tools such as data mining or machine learning. IoT data can be stored off-chain in cloud database or on-chain in blockchain. On the other hand, multiple clouds can be incorporated to implement functionalities such as data sharing or collaborative system management. In this context, as a middle layer, blockchain layer plays an important role in handling and controlling cloud interactions to facilitate cloud service delivery to IoT users and avoid conflicts among clouds.

3) Application Layer: Many industrial applications can gain benefits from the BCoT integration in different areas where IoT scenarios are involved, like smart healthcare, smart transportation, smart city, smart energy, and smart industry. BCoT not only provides useful services to industrial applications, such as network management and QoS improvement but also guarantees security and privacy properties for applied domains. For example, in smart healthcare, BCoT can support data processing services thanks to computation ability of cloud, which can assist healthcare providers in analysing intelligently patient information for better medical care. In the meantime, network security of healthcare is ensured with blockchain which offers traceability and verification services during the medical data exchange and data processing. The application of BCoT integration and its benefits to IoT use case domains such as smart industry, smart energy, smart transportation will be extensively analyzed in the next section.

IV. Research and Technology Development of BCoT

In this section, we will present recent advances of BCoT technology. The impacts of BCoT on a wide range of industrial applications are reviewed from the latest research results. Then, we survey recent BCoT developments with platforms, services, and research projects around blockchain and CoT technologies.

A. BCoT Applications

In this sub-section, we will provide readers with a summary of key BCoT applications across different scenarios, such as smart healthcare, smart city, smart transportation, and smart industry as shown in Fig. 7. In particular, we highlight the research findings of the state-of-the-art studies in the use of BCoT paradigms in such applications. Besides, main lessons learned from the review are also discussed.

1) Smart Healthcare: Healthcare is an industrial sector where organizations and medical institutions provide healthcare services, medical equipment, medical insurance to facilitate healthcare delivery to patients. The adoption of BCoT models can offer great potentials to solve critical issues in terms of security and service efficiency, and thus is possible to advance medical services and transform current healthcare systems [79], [80], [81], [82]. The BCoT integration in healthcare promises to provide new smart services, including efficient health data sharing, healthcare data storage and secure system management, which will be summarized from the literature studies as the following.

1.1) Health data sharing

CoT enable efficient healthcare data sharing environments where EHRs can be processed and stored online on the cloud storage while users can use their mobile devices (e.g., smartphones) to access their medical information for health monitoring. This promises to offer on-demand healthcare services, save healthcare costs, and improve quality of experience [83]. However, healthcare data sharing based on such dynamic cloud IoT environments is always vulnerable to security and privacy risks due to attack potentials and the lack of trust between healthcare cloud providers, cloud storage, and users. Blockchain plays a significant role in solving security issues in health data sharing by decentralized data verification of all peers and message validation based on consensus mechanisms. Specially, the traceability of blockchain allows healthcare entities (e.g., healthcare providers, insurance companies, and patients) to trace user access behaviours and detect data attacks, aiming to improve the security of health data sharing in BCoT networks.

The work [84] introduces a privacy-preserved data sharing scheme which is enabled by the conjunction of a tamper-proof consortium blockchain, cloud storage and medical IoT network. In order to protect medical data, original electrical medical records (EMRs) are stored securely in the cloud under the management of smart contracts while data indexes are kept in blockchain. This ensures that EMRs cannot be modified or altered arbitrarily. A user-centric health data sharing solution is also proposed in [85] using permissioned blockchain on a mobile cloud platform where health data from wearable sensors is synchronized to cloud for data sharing with healthcare providers and insurance institutions. Another work in [86] presents a data sharing framework with fine-grained access control, by combining a decentralized storage system interplanetary file system (IPFS), an Ethereum blockchain, and attribute-based encryption technology. An access control design based on smart contract is also proposed to implement keyword search in decentralized cloud storage for sharing services.

Although BCoT can help achieve secure data sharing, the storage of all health data on blockchain will slow down transaction operations and put sensitive patient information at risks of data leakage and sharing security concerns. Motivated by such challenges, [87] proposes a conceptual scheme for exchanging personal continuous dynamic health data using cloud storage and blockchain. In particular, large health datasets are encrypted and stored as off-the-chain in cloud storage, while only metadata (e.g., hash values) of raw data is kept in blockchain, which would overcome the size limitation of the large data storage in BCoT systems.

In line of discussion, the authors in [88] propose a trust-less medical data sharing, called MeDShare, to enable data exchange among untrusted cloud service providers (CSP) using the blockchain. The focus is on an access control design based on smart contracts to trace access behaviours of data users, but access control issues associated with sensitive data in the cloud

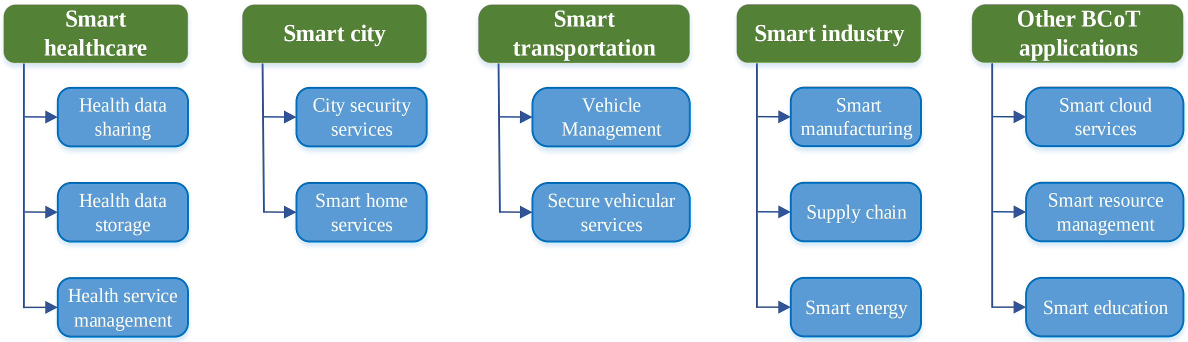

Fig. 7: BCoT application domains.

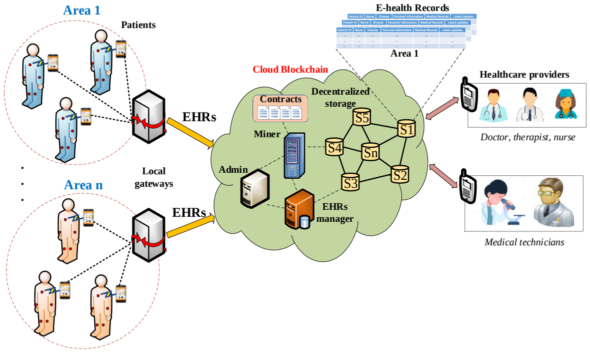

Fig. 8: A smart e-health data sharing system [50].

data pool remains unsolved. Therefore, the work [89] proposes secure cryptographic approaches (including encryption and digital signatures) to provide efficient access control which acts as a monitoring system layer to achieve data user authentication for cloud data sharing. More interesting, in our recent work [50], a mobile cloud blockchain platform is proposed to implement dynamic EHRs sharing where blockchain is integrated with cloud computing to manage user transactions for data access enabled by smart contracts. In particular, a decentralized storage IPFS run by blockchain is combined with cloud computing to make data sharing more efficient in terms of low latency, easy data management and improved data privacy. The concept of the proposed scheme can be seen in Fig. 8.

1.2) Health data storage

Blockchain is able to enhance data integrity and traceability for healthcare data storage. Encrypted health records are stored in cloud blockchain under the control of smart contracts. By using blockchain, the system provides the full data integrity to patients and data users. Vulnerabilities regarding data preservation are addressed effectively by using cryptographic functions along with blockchain, improving integrity, accountability, and security for cloud data storage [90]. For example, the work [91] introduces a secure cloud-based EHR system on blockchain with five entities: key generation centre, hospitals, patients, medical clouds, and data consumers like insurance company. In this network, medical data is stored in the blockchain associated with a complete copy of the timestamp, consequently increasing the integrity and traceability of healthcare records. The work in [92] integrates the medical data into the infrastructure of cloud blockchain called Blockcloud. Blockchain has distributed ledger where encrypted medicine data transactions are stored on cloud storage as a blockchain entity. Any modifications on medical records in cloud storage will be identified by blockchain via the P2P network.

In [93], a modified BCoT scheme is proposed for decentralized health data privacy. The architecture consists of overlay network, cloud storage servers, healthcare providers, smart contracts and patients. Specially, blockchain is interconnected with cloud storage via a P2P network where each cloud storage keeps medical records into blocks and the hash value of these blocks is stored in blockchain. This makes any changes in data possible to be easily traced.

1.3) Healthcare service management

The BCoT paradigm may offer unprecedented breakthroughs with new smart medical services, such as decentralized healthcare, secure user management or medical operation control [94]. Blockchain can be used to build a secure healthcare communication environment among the purchasing manager, device supplier and health users under the control of smart contracts for data traceability and access authentication. In [95], a secure cloud-assisted e-health system based on blockchain is proposed to protect the operation of outsourcing EHRs among medical users. This can be done by an Ethereum blockchain platform to manage user transactions without requiring any trusted entity. Meanwhile, the study in [96] uses blockchain for building a healthcare remedy evaluation system on cloud. In this context, the decentralized replication of blockchain can improve the information credibility and the quality of crowdsourcing systems. Recently, a healthcare project is implemented in Peru using the BCoT platform for purchase management in private health sector [97]. In this project, blockchain hosted inside the Amazon cloud is used to organize a secure communication network of purchasing manager, the supplier and the transporter. Sensor data will be authorized by smart contracts available on blockchain to avoid data alternation risks.

Meanwhile, the authors in [98] highlight the efficiency of BCoT models in health monitoring services that are enabled by IoT devices, cloud computing and blockchain. Cloud connectivity offers substantial medical computing services, such as storage and intelligent computation. In a recent work [99], we also introduce a conceptual BCoT framework for health diagnosis and monitoring. In particular, we integrate the data management system with a data sharing framework in a mobile blockchain network. Data is ensured security through an access control layer managed by smart contracts for access verification and data integrity.

1.4) Lessons learned

The main lessons acquired from the review of BCoT applications in healthcare are highlighted in the following.

- BCoT can achieve secure data sharing on cloud IoT-enabled healthcare networks where blockchain and cloud play a significant role in controlling user access and implementing data sharing. Smart contracts available on blockchain are particularly useful to track automatically transactions and implement access verification which ensures reliability and security for untrusted healthcare environments.
- The integration of blockchain in cloud computing significantly improves security for cloud healthcare storage services. Cloud storage acts as a peer in the P2P network under the management of blockchain. In this context, original health data can be encrypted and kept in cloud storage, while metadata (e.g., hash values) of such data records is stored in blockchain, which enables data traceability and detects easily data modification threats on cloud.
- BCoT can offer innovative healthcare services with high security and efficiency. BCoT has the potentials to improve the quality of medical services such as health monitoring, patient diagnosis or healthcare remedy evaluation.

2) Smart City: With recent advances of cloud computing and IoT technology, smart city has been emerged as a new paradigm to dynamically exploit the resources in cities from ubiquitous devices and provide a wide range of services for citizens. Smart cities involve a variety of components, including ubiquitous IoT devices, heterogeneous networks, large-scale data storage, and powerful processing centres such as cloud computing for service provisions. Despite the potential vision of smart cities, how to provide smart city services with high efficiency and security remains a challenging problem. In this scenario, BCoT can be a promising candidate to empower smart city services by using attractive technical features of cloud computing and blockchain. A number of recently proposed solutions suggest to adopt BCoT architectures to enable ubiquitous connectivity between citizens and industrial applications for smart cities. We summarize recent research efforts in the adoption of BCoT in smart cities via two main services: security services for smart city and smart home services.

2.1) Security services for smart city

Due to the ubiquitous nature of data-based services, smart city architectures remain security bottlenecks such as privacy, integrity, trust, and so on [100]. The BCoT model with high security capabilities enabled by blockchain promises to help overcome such challenges as well as offer new smart city services. In such contexts, blockchain plays an important role in providing high-quality security services for smart city scenarios. In fact, blockchain is possible to provide five main cryptographic primitives, including integrity, authenticity, confidentiality and non-repudiation, by building decentralized security architectures for smart cities.

The work [101] introduces a decentralized big data integrity auditing framework in cloud environments for smart cities. The proposed architecture consists of two main entities: data owners and cloud service providers (CSPs). An innovative blockchain instantiation named the data auditing blockchain (DAB) is proposed to investigate auditing requests between users and CSPs to verify data integrity. Also, the study [102] considers an authorization and delegation architecture for the cloud IoT based on blockchain in smart city projects. The mechanism is conducted in a single smart contract which enables access control functionalities to ensure trustfulness and auditing for operations between IoT devices, cloud and data users.

Furthermore, blockchain is adopted in [103] to build an IoT-based smart city architecture which includes three main layers: smart block, P2P network and cloud. Since blockchain is inefficiently for a large number of network nodes, e.g., IoT devices in smart city, the proposed scheme suggests a lightweight blockchain with low computation and resource demands. All communications between IoT devices, cloud storage and P2P nodes are tagged as transactions which are recorded and stored securely on blockchain in a tamper-proof manner. A blockchain-based infrastructure is also considered in [104] to support secure smart contract services for sharing economy in smart cities. Multimedia payload from IoT devices is offloaded and stored securely in distributed IPFS-based cloud repositories as immutable ledgers.

2.2) Smart home services

In the context with smart cities, home automation gives shape to a smart home which is the main feature of a smart city. A smart home is a network of IoT devices configured with automated devices, intelligent sensors and detectors, which will collect information from the environment to be processed by a control server such as a computer or a cloud computing platform. Despite many potentials to benefit citizens, smart homes remain unsolved issues in terms of security, threats, attacks, and data privacy. BCoT run by blockchain that owns distributed, secure and private properties would be the promising solution to these security issues [105]. In this context, blockchain is used to build a decentralized data integrity architecture for ensuring high stability and reliability of the whole system without the requirement of third-party auditors.

The work in [106] propose a smart home architecture using a BCoT model which includes three main tiers: cloud storage, overlay (blockchain-based P2P network), and smart home. Resourceful devices act as blockchain miners to handle transactions within the smart home and ensure security objectives in terms of confidentiality, integrity, and availability. The storage of data within a smart home is implemented by cloud computing under the management of blockchain miners through a transaction authentication process which enables high security for smart home operations.

In [107], a secure and efficient IoT smart home architecture is proposed by taking advantage of cloud computing and blockchain technology. The general structures contain four components, namely smart home layer, blockchain network, cloud computing, and service layer. Blockchain with its decentralized nature is integrated in distributed cloud storage for data usage traceability. Besides, it also serves processing services and makes the transaction copy of the collected user data from smart home. Moreover, the study in [108] also presents a conceptual access control scheme for smart home where private blockchain is used to store records of user transactions and large-size access data is stored in off-chain storage, such as cloud storage.

2.3) Lessons learned

The main lessons acquired from the review of BCoT applications in smart city are highlighted in the following.

- BCoT can offer advanced security services for smart city applications. Cloud computing is capable of providing powerful computing capacities to handle large data streams from ubiquitous IoT devices to offer real-time applications for citizens. Meanwhile, with high security properties, blockchain proves its high efficiency in controlling smart city operations in a distributed and secure manner. The integration of blockchain and CoT thus transforms smart city architectures to overcome challenges in terms of security and system performance.
- As a significant component of smart city, smart home also gains benefits from the BCoT integration. BCoT can enable intelligent services, such as user monitoring, home management and access control in smart home scenarios. Specially, blockchain can be integrated with distributed cloud computing to make data storage and transaction processing more flexible and secure among IoT devices, home owner and external users.

3) Smart Transportation: With the rapid development of modern sensing, communicating, computing technologies, recent years have witnessed tremendous growth in intelligent transportation systems (ITS), which impose significant impacts on various aspects of our lives with smarter transport facilities and vehicles as well as better transport services. Smart transportation is regarded as a key IoT application which refers to the integrated architectures of communication technologies and vehicular services in transportation systems. One critical issue in smart transportation is security risks resulted by dynamic vehicle-to-vehicle (V2V) communication in untrusted vehicular environments and reliance on centralized network authorities. Blockchain has the potential to help establish a secured, trusted and decentralized ITS ecosystem. The combination of cloud computing with limitless data management capabilities and blockchain with high security features is able to enhance security and quality of services in smart transportation, including vehicular communication management and secure vehicular services.

3.1) Vehicular Communication Management

In vehicular communication management, blockchain is used in information and energy interaction processes to achieve high security levels such as user authentication with contracts and data confidentiality with cryptography. During the information and energy interactions, the vehicular records are encrypted and appended into the blocks by a consensus mechanism in the blockchain network. Also, blockchain is able to create a secure peer-to-peer network to enable seamless communications among ubiquitous vehicles for service management, value exchange and collaborative trust. The work [109] proposes a collaboration network of multiple vehicle clouds where blockchain is applied to establish a coordination scheme. Vehicles from different car manufacturers can achieve efficient interconnection through their private cloud based on a decentralized mechanism which enables service management, value exchange and collaborative trust within the vehicle-to-vehicle (V2V) communication network. Blockchain is adopted to support peer-to-peer collaboration among different clouds of vehicles with high security levels [110].

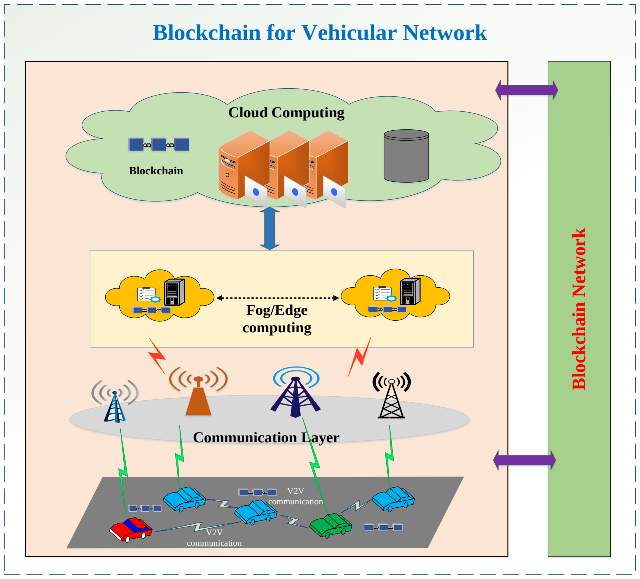

Fig. 9: Blockchain and cloud for security of VANET system [111].

In [111], a distributed blockchain cloud architecture is proposed to preserve privacy of vehicle drivers with on-demand and low-cost access in vehicular ad-hoc networks (VANETs). To solve issues related to limitations of storage, computation and spectrum bandwidth in VANETs, a cloud computational hierarchical architecture is proposed with three interconnected cloud platforms, consisting of vehicular cloud, road side cloud and central cloud. The joint cloud network is interconnected securely with vehicles, service providers through a P2P network run by blockchain which enables the vehicular ecosystem to be resistant to cyber-attacks and privacy bottlenecks. Another research effort [112] shows a security architecture of VANETs based on blockchain and edge-cloud computing. The architecture consists of three main layers, namely perception layer with a network of vehicles, edge computing layer and service layer as illustrated in Fig. 9. Here, the service layer is established by the integration of cloud computing and blockchain to build a secure decentralized vehicular management architecture. Therefore, cloud-based huge data storage and blockchain-based data privacy are ensured for efficient and secure vehicular communication [113].

3.2) Secure vehicular services

Blockchain with its decentralization and traceability also facilitates secure vehicular IoT services, from task scheduling, data carpooling, insurance management to vehicular report and trust control services. In [114], a BCoT architecture is developed to build a vehicular ecosystem where smart vehicles, equipment manufacturers and cloud storage providers can communicate together. The system operates under the management of a public blockchain which is possible to protect the privacy of users and to increase the security of the vehicular network. Two applications including wireless remote software updates and dynamic vehicle insurance fees are considered to demonstrate the efficiency of the architecture.

The authors in [115] consider the privacy issues of carpooling services. To achieve high security and privacy of the service, they propose an efficient and privacy-preserved scheme by using blockchain-enabled vehicular fog computing. Particularly, carpooling data is encrypted and kept at the cloud server, while its hash value is stored on the private blockchain, which enables data traceability and reliability. The work [116] uses the BCoT model to build a mechanism of task scheduling in a vehicular cloud computing environment. An autonomous vehicular cloud (AVC) ecosystem is established where non-repudiation of task execution between task senders and task runners (vehicles) is guaranteed by secure transaction management of blockchain. Meanwhile, the study [117] presents a fine-grained transportation prototype for insurance services enabled by the blockchain and CoT. The system consists of two main parts, namely an IoT based data collection and processing scheme for driving behaviour analytics and a collaborative blockchain network of Ethereum and Hyperledger Fabric platform for vehicular operation management.

Furthermore, security for vehicular IoT services has become a critical challenge. The work [118] proposes a blockchain-based security framework to support vehicular IoT services, e.g., real-time cloud-based video report and trust management on vehicular messages. A software-defined networking architecture is incorporated into the VANET to enable global information collection and network management. A blockchain platform is employed to build a semi-decentralized trust management architecture in which encrypted videos or messages are uploaded to the cloud for large storage while trusted traffic information is stored securely in the blockchain.

3.3) Lessons learned

The main lessons acquired from the review of BCoT applications in smart transportation are highlighted in the following.

- BCoT paradigms can offer advanced solutions by combining cloud computing and blockchain in vehicular networks to achieve efficient and secure vehicular communication. Blockchain can create secure peer-to-peer network environments to enable limitless communications among ubiquitous vehicles for service management, value exchange and collaborative trust.
- CoT also enable a new set of vehicular services with better efficiency and security. The combination of autonomous vehicular cloud and blockchain opens up new opportunities to facilitate vehicular IoT services, from task scheduling, data carpooling, insurance management to vehicular report and trust control services, which promise to transform intelligent transportation systems.

4) Smart Industry: Blockchain has emerged as an enabling technology enabled by the decentralized P2P network structure to drive smart industries, and the convergence of CoT and blockchain as a BCoT paradigm promises to empower industry ecosystems with enhanced security and improved industrial operation efficiency. There is a vast body of research works in the combination of BCoT in smart industry and we can categorize them into three areas: smart manufacturing, smart energy, and smart supply chain.

4.1) Smart manufacturing

Smart manufacturing is a broad category of manufacturing that employs cloud manufacturing, IoT enabled technologies and service-oriented manufacturing, which benefit the manufacturing industry. However, all existing paradigms still face the main problem related to centralized industrial network and third part-based authority. In a nutshell, centralized manufacturing architectures exist limitations with low flexibility, efficiency, and security. The use of BCoT in manufacturing systems can be a promising solution to overcome such critical challenges with the support of cloud computing and blockchain as shown in Fig. 10. BCoT is possible to enhance and optimize manufacturing processes and reduce operation costs [120]. Particularly, blockchain can improve the security of smart manufacturing process, by offering efficient security services for trust and privacy establishment among different manufacturing enterprises.

In [119], a distributed P2P network architecture named BCmfg is proposed with five key layers, namely resource layer, perception layer, manufacturing layer, infrastructure layer and application layer. Blockchain is integrated in the manufacturing industry to facilitate cloud manufacturing and establish a new trustable platform as blockchain cloud manufacturing. Service providers and customers can share data and information over the cloud blockchain network which helps improve the security of industry system. Smart contracts act as agreements between the end users and the service providers to provide on-demand manufacturing services.

The work [121] introduces a decentralized framework called BPIIoT for industrial IoT based on blockchain. The BPIIoT platform is regarded as a technical enabler for cloud-based manufacturing (CBM) which offers ubiquitous and on-demand network access to manufacturing resources. Blockchain is deployed to establish a peer-to-peer network for BPIIoT in which smart contracts are deployed. Here, the smart contracts work as agreements between the service consumers and the manufacturing resources to provide on-demand manufacturing services.

4.2) Smart supply chain

In addition to manufacturing applications, BCoT is also beneficial to industrial supply chain that is the key component in the vertical smart industry ecosystem. Indeed, BCoT with high decentralized and immutable natures of blockchain can ensure faster and more secure corporation between companies and manufacturers in supply chain and logistic activities. [122]. Besides, it also enables secure support planning, scheduling, and monitoring supply chain operations.

For example, the work in [123] investigates the use of blockchain for transaction processing to provide different

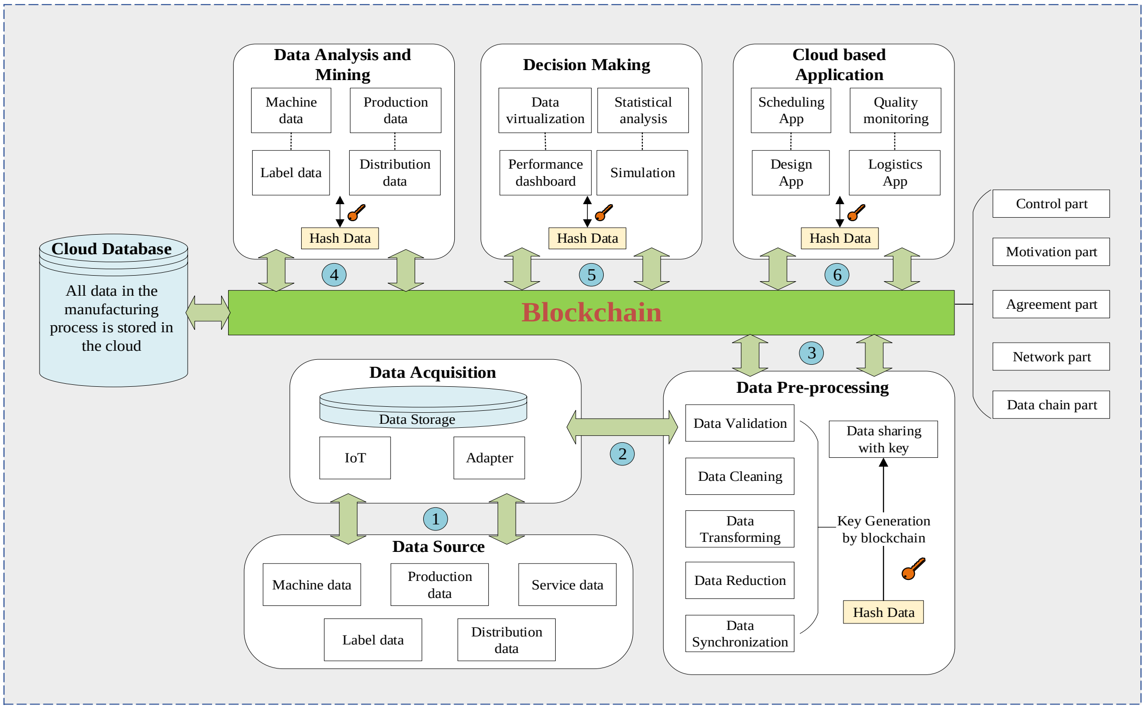

Fig. 10: The blockchain cloud manufacturing system [119].

cloud-blockchain platforms for supply chain applications. Blockchain systems are divided into three categories, including private versus public, centralized versus decentralized and peer-to-peer cloud-based systems. Cloud computing can offer a number of flexible solutions for blockchain-based supply chain, from a single repository for the blockchain to multiple peer-to-peer capabilities with broad accessibility. Blockchain ensures trust among companies and businesses during supply chain operations via consensus mechanisms and smart contracts.

4.3) Smart energy

With the increasing demands of energy usage to support industrial and manufacturing operations, smart energy continues to play an integral part in industry ecosystems. The overall purpose of the energy system is to provide energy services to customers and companies, in a sustainable, reliable, and cost efficient manner. Information and communication technology (ICT) will be an enabler in the transition of electricity, gas and heating grids into the smart energy system. In such a context, BCoT empowered by immutable blockchain has emerged as a promising technique to improve the security and privacy of energy exchange and transmission.

The work [124] considers the potential of cloud-blockchain technologies for decentralized operations in energy internet environments. Centralized energy management systems (EMS) tend to be inefficient to work well with a large quantity of prosumers and thus, a decentralized architecture based on blockchain is necessary to achieve high quality of services for the decentralized institutions of various energy entities. Blockchain can integrate with cloud computing to offer effective methods for information sharing and model updating in cloud-based EMS platforms. Specially, cloud computing operations for energy management are optimized and ensured high security with a decentralized verification mechanism which is made by blockchain-based consensus among energy users.

In [125], a blockchain-based architecture is proposed to manage the operation of crowdsourced energy systems, enabling P2P energy trading at the distribution level, where ubiquitous distribution-level asset owners can trade with each other. The platform is implemented by the IBM Hyperledger Fabric network deployed in cloud to offer blockchain services. Moreover, smart contracts are used to run the pricing mechanism and control energy trading transactions and crowdsources. The work in [126] also implement an intelligent energy-aware resource management in cloud datacentre. With the support of blockchain, the enery management scheme does not require any scheduler, reducing extra energy cost and increasing the robustness of DCs. Smart contracts are also employed and stored in each datacentre to verify transactions from request migration to the DC.

4.4) Lessons learned

The main lessons acquired from the review of BCoT applications in smart industry are highlighted in the following.

- BCoT demonstrates its potentials in the improvement of smart industry for better efficient manufacturing, lower operational costs and minimum management efforts through the use of controlling capabilities of blockchain and service support of cloud computing.
- BCoT with blockchain as a middle communication layer can enable faster and more efficient corporation between companies, manufacturers and users in supply chain and logistic activities. Security and information privacy during supply chain operations can also be ensured by

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.3020092, IEEE Communications Surveys & Tutorials

consensus mechanisms over the peer-to-peer network enabled by cloud-blockchain integration.

- BCoT architectures can empower energy systems which are regarded as a key component of smart industry. Blockchain has potentials to improve security and privacy of energy exchange and transmission, while cloud computing offers storage and management services as well as supports blockchain in achieving decentralized energy operations.

5) Other BCoT Applications: The application of BCoT paradigms has been investigated in other scenarios, including smart cloud services, smart resource management and smart education.

5.1) Smart cloud services

Cloud computing offers a diverse range of outsourcing services, including storage and computation to serve individuals and enterprises. Basically, outsourcing services usually include online payment and security issues. However, most traditional service solutions have to rely on a trusted third-party to realize fairness to complete payments. Therefore, the realization of secure and fair payment of outsourcing services is of paramount importance for cloud-based applications. In this regard, blockchain has emerged as a strong candidate to solve security issues of cloud services and simplify the cloud service management thanks to its traceable and immutable nature. The works [127], [128] introduce a blockchain based fair payment architecture for outsourcing services in cloud computing. The proposed system ensures to provide soundness and robust fairness capabilities by using a service management protocol run by blockchain. Fair payment can be achieved between users and outsourcing service providers on clouds through transactions which are stored and verified by blockchain without the involvement of any third party.

During the process of outsourcing data on clouds, when a user wants to delete the outsourced data, he sends a deletion command to the cloud server so that the server delete the data. However, the cloud server is semi-trusted and it may not delete the requested data honestly due to financial incentives. To solve this issue, the study in [129] presents a new publicly verifiable data deletion scheme for cloud computing enabled by blockchain, which not only supports public verification on deletion requests but also eliminates totally the need of trusted third parties. Blockchain offers fairness verification services which enable all users can authorize transactions for data deletion requests and control malicious behaviours on their cloud data with equal verification rights. This blockchain-base scheme helps reduce the dependence on cloud servers in user data management and makes the deletion operation much more transparent.

Meanwhile, the authors in [130] propose a building information modeling system model called bcBIM to address information security challenges in mobile cloud environments. Specially, blockchain is employed to facilitate BIM data audit for historical modifications of big data sharing. BIM data integrity and provenance are guaranteed by integrating blockchain in BIM database, and system management can be achieved by BIM cloud. The BIM model based on cloud blockchain promises to foster industrial applications, such as engineering machines and construction robots. For data record management on clouds, [131] and [132] use blockchain to build decentralized cloud storage ecosystems for security improvements. Blockchain-based distributed storage is different from traditional cloud storage services because it utilizes the disk space of a network of computers and storage facilities to decentralize the database, which ensures that any data owners can verify and check data integrity via the P2P network on blockchain. This advanced storage concept also improves trustworthiness and data availability on cloud during data long-term preservation.

5.2) Smart resource management

Computing resource management for CoT in blockchain network is also attracting increasing attention. Many approaches have been proposed to enhance computation resources and security services for BCoT applications in various types of tasks such as real-time processing, resource-intensive applications, and consensus process with the help of immutable blockchain and smart contracts for monitoring resource usage and data authenticity in cloud computing.

The work [133] introduces an optimal computing resource allocation based on an auction scheme for edge-cloud-enabled IoT in the blockchain network. A pure P2P computing resource trading system on clouds is built to establish computing resource trading between resource sellers and buyers. Meanwhile, a lightweight infrastructure of the PoW-based blockchains are proposed [134] so that the workload of mining process is offloaded to the cloud/fog for computation. The computation resource management in the blockchain consensus process is formulated as a two-stage Stackelberg game, where the profit of the cloud/fog providers (CFPs) and the utilities of individual miners are jointly optimized.

Further, the authors in [135] introduce a resource management system called Saranyu which adopts smart contracts to control tenant and service accounts as well as monitor resource usage in a cloud computing data center. Saranyu is capable of offering four different services: identity management, authentication, authorization on service resource exploitations, and charging.

5.3) Smart education

The application of BCoT to the education domain is still in its early stages. Only a small number of educational institutions have started to utilize BCoT technology. Most of current solutions use BCoT for the purpose of validating and securely sharing academic certificates and personal information of students as well as learning database of educational institutions [136]. Immutable blockchain ledgers and cloud computing can be combined to develop secure and trusted educational environments for promoting educational collaboration.

For example, the study in [137] proposes an online identity verification system using blockchain to implement cloud educational collaboration. To achieve time authentication on transactions, blockchain is adopted to provide proofs of data content originality, which also maintains system integrity. Some case studies were conducted at Chuo University in Japan to verify the efficiency of the proposal. Additionally, blockchain ledgers and cloud computing are considered to support computer science education in [138]. A new decentralized P2P-cloud model is also proposed using Bitcoin and Torrent models to build proof-of-concept platforms to support service providers in education.

5.4) Lessons learned

The main lessons acquired from the review of the above BCoT applications are highlighted in the following.

- The BCoT architecture has great potentials to transform cloud-based services with better efficiency and security levels. Blockchain can be involved in cloud management processes by autonomous consensus mechanisms and control capabilities of smart contracts, which ensure data integrity, data availability and trustfulness. Importantly, blockchain helps to build peer-to-peer architectures and integrate them in cloud platforms to enable decentralized cloud services with advantages over conventional cloud ecosystems in terms of no single points of failure for better system robustness and low communication overheads.
- BCoT also proves its benefits to network resource management with a wide range of services on real-time processing, resource-intensive applications, blockchain mining, and consensus process. With the support of BCoT and smart contracts available on blockchain, resource management systems can achieve high transparency, trustfulness and ensure robust access control in collaborative networks of resource providers and customers.
- Besides, BCoT can be useful to education management ecosystems. Blockchain ledgers are able to provide secure and trusted educational environments for promoting educational collaboration.

In summary, we list BCoT applications in the taxonomy Table III and Table IV to summarize the contributions and limitations of each reference work.

B. BCoT Platforms and Services

The integration of blockchain and CoT can lead to develop unprecedented architectures to enable smart services across IoT domains. In this section, we review the latest research efforts to integrated BCoT models with cloud blockchain storage platforms and cloud services for BCoT applications.

1) Cloud Blockchain Platforms: The data storage of traditional CoT applications have mainly relied on cloud computing which is a completely central environment. This centralized storage architecture shows a number of critical limitations, such as the lack of user control on IoT data as well as security and privacy concerns. Further, centralized cloud storage service providers charge a significant fee for their services. For example, Amazon cloud charges $23 a month for the storage service they provide, which may pose a burden on small cloud IoT projects. On the other hand, conventional blockchain seems to be very expensive for storing large amounts of IoT data on chain. In fact, blockchain platforms like Bitcoin are restricted data storage only one megabyte. To overcome such challenges, decentralized storage based on cloud blockchain would be a promising solution which offer highly flexible, secure, trustful and super cheap storage services for BCoT applications [86], [50].

In this regard, we survey the most popular decentralized storage platforms and summarize them in Table V. Key information of these platforms is also highlighted, and the open sources of software for ready usage are also released. With these advanced storage solutions, the BCoT applications do not rely on a central service provider, allowing users to store IoT data to a distributed set of storage nodes, e.g., computers, based on the peer-to-peer network on blockchain. In fact, many of these systems have proven their efficiency in IoT scenarios. For example, the decentralized IPFS [139] and Storj [140] storage platforms are applied in IoT systems on cloud blockchain [50], [131] and shows their efficiency in terms of low access latency and improved security levels, compared to traditional centralized storage solutions. Additionally, Swarm [143] works as the distributed data storage platform running on Ethereum which has the potential to manage and share securely IoT data against distributed denial of service (DDoS) attacks and malicious access [147]. Recently, some cloud giants have launched initiatives to integrate decentralized storage for large-scale cloud blockchain deployments, such as IPFS storage on Amazon and Microsoft Azure clouds [50], [148], for secure and efficient data storage. These interesting integrations have the potentials to disrupt both blockchain and cloud computing worlds to enable new infrastructures for future BCoT applications.

2) BaaS Services for CoT: In BCoT ecosystems, blockchain can be regarded as a Blockchain-as-a-Service (BaaS) which is integrated with cloud computing to offer full IT services in order to help researchers and enterprises develop, verify and deploy blockchain for cloud IoT applications. Specially, BaaS services are capable of providing foundation architecture and technical support to ensure that BCoT systems can achieve robust and efficient operations. Nowadays, there is a large number of BaaS providers on commercial markets to enable customers to adopt services without worrying about infrastructure installation and system investment, which can accelerate their BCoT deployments.

Reviewing thoroughly the state-of-the-art BaaS platforms available on the market, in this subsection, we introduce the leading BaaS platforms which are ready to use for BCoT applications. The key technical characteristics of each platform are described briefly in Table VI. The source code for BaaS examples and templates are also available on the code sharing platform Github. In fact, many research projects have employed such BaaS platforms to develop their BCoT applications. For example, the Amazon Blockchain service [49] is adopted to build an IoT healthcare system [50]. In this project, the Ethereum blockchain platform hosted on Amazon cloud helps to implement a health data sharing framework on mobile clouds with high security and privacy. Moreover, IBM cloud [51] also introduces a well-developed BaaS platform for IoT users. The platform has been showcased in a vehicular network [156]. In this project, the IBM IoT platform is integrated with IBM BaaS services to manage vehicle sensor data (vehicle-to-vehicle messages and vehicle monitoring data) and ensure security during data sharing within the vehicular network. Meanwhile, the BaaS platform of Oracle cloud [52] has proven its great potentials through a wide range of BCoT projects,

TABLE III: Taxonomy of BCoT applications.

Category	Ref.	Use case	Blockchain platform	Main contributions	Limitations
Smart healthcare	[84]	EMRs sharing	Ethereum	An EMRs sharing scheme to ensure data privacy on cloud.	The real prototype is not implemented between cloud, blockchain and medical users.
	[85]	Health data sharing	Hyperledger Fabric	A user-centric health data sharing solution for cloud healthcare with a focus on scalability and data integrity evaluation.	Security issues on healthcare IoT devices, e.g., malicious attacks, are not considered.
	[86]	Data sharing, access control	Ethereum	A data sharing with access control in decentralized loud storage.	Issues on data confidentiality and access control latency are not discussed in detail.
	[87]	Data sharing	-	A lightweight data sharing scheme in cloud blockchain.	The real prototype is not investigated between cloud, blockchain and medical users.
	[88]	Trust-less data sharing	-	An access control mechanism to track data access behaviours of cloud providers.	Implementation results on access control efficiency is not investigated.
	[50]	E-health data sharing	Ethereum	A mobile cloud blockchain platform for e-health sharing with an access control design.	Data confidentiality and scalability are not considered in detail.
	[90]	healthcare data management	Ethereum	A privacy-preserved platform for data storage in cloud.	Comparisons between smart contract-based scheme and conventional schemes have not been done.
	[91]	Cloud data storage	-	A blockchain-based cloud storage scheme for data integrity and traceability.	Smart contract implementation on data storage has not been considered.
	[92]	Cloud data storage	-	A EMRs storage scheme on blockchain-based cloud.	Investigations on blockchain prototype has not been done.
	[93]	Security for EMRs storage	-	A security scheme for EMRs storage.	Real experiments on the proposed security scheme has not been done.
	[95]	Secure healthcare service	Ethereum	A secure cloud-assisted e-health system.	Smart contract design for service management has not been considered.
	[96]	Healthcare remedy service	-	A healthcare remedy evaluation system.	Performance for blockchain implementation on cloud has not been done.
	[97]	Medical supply chain	Hyperledger	Purchase management in private health sector.	Data privacy has not been considered.
	[98]	Health monitoring services	-	A concept of health monitoring services using BCoT approach.	Performance evaluation on the proposed scheme has not been done.
	[99]	Health diagnosis and assessment	Ethereum	A conceptual framework on health assessment and monitoring using cloud blockchain	System scalability and communication costs have not been considered.
Smart city	[101]	Data auditing	-	A decentralized data auditing framework on cloud for smart cities.	Smart contract design, experiment on security evaluation have not been done.
	[102]	Service authorization and delegation	Ethereum	An authorization and delegation scheme for BCoT-enabled smart city.	Privacy is not taken into consideration.
	[103]	Secure smart city architecture	Ethereum	A BCoT smart city platform for high security.	Access control for cloud storage has not been considered.
	[104]	Sharing economy services	Ethereum and Hyper-ledger	A blockchain-based infrastructure for secure sharing economy services.	Data privacy has not been analysed.
	[106]	Smart home services	-	A BCoT architecture for security and privacy in smart homes.	Blockchain implementation has not been done.
	[107]	Smart home services	-	A smart home architecture for security services.	Real blockchain implementation has not been investigated.

such as banking, healthcare data management, and payment industry [157]. Recently, the Hewlett Packard cloud provider [150] collaborates with the automotive manufacturing giant Continental to launch a blockchain-based platform for car manufacturers to share and sell vehicle data [158]. This project allows customers, including vehicle drivers, car manufacturers and service providers can share securely vehicle data in untrusted vehicular networks, making mobility safer, greener, and more accessible. Although the development of BaaS platforms is still in progress, the success of such initial projects on BaaS platforms is expected to open up new opportunities for future BCoT deployments as well as disrupt global industries.

V. Research Challenges and Discussion

From the extensive review on BCoT integrations, we identify possible research challenges and open issues in the field. We also discuss some potential solutions to encourage more research efforts in this promising area.

A. Research Challenges

We highlight five major challenges in BCoT research, namely standardization, security vulnerability, privacy leakage, intelligence, and resource management.

1) Standardization: Since its inception, the blockchain technology has revolutionized industries by offering new network models with its decentralized and secure natures. The

TABLE IV: Taxonomy of BCoT applications (continued).

Category	Ref.	Use case	Blockchain platform	Main contributions	Limitations
Smart transportation	[109]	Vehicle collaboration	-	A joint cloud collaboration scheme between vehicle clouds based on blockchain	Blockchain implementation has not been done.
	[110]	Information and energy interactions	-	An electric vehicles cloud and edge computing network paradigm for secure vehicular communication with blockchain.	Network performance has not been evaluated in experiments.
	[111]	Secure vehicular communication	-	A distributed vehicular network based on cloud blockchain for data privacy.	Blockchain implementation for the proposed approach has not been done.
	[112]	Secure vehicular communication	-	A multi-layer decentralized VANET architecture for secure vehicular communication.	Implementation to investigate the system efficiency is lacked.
	[114]	Secure vehicle services	-	A BCoT platform for secure vehicular services, e.g., remote software updates and vehicle insurance fees.	Blockchain and smart contract implementations have not been done.
	[115]	Carpooling services	-	A privacy-preserving carpooling scheme using blockchain with cloud-fog computing.	Scalability of the proposed scheme has not been verified.
	[116]	Vehicular task scheduling	Ethereum	A strategy for task scheduling in autonomous vehicular cloud system.	The performance of the proposed framework has not been simulated.
	[117]	Fine-grained transportation insurance	Ethereum and Hyperledger	A fine-grained transportation scheme for insurance services on cloud blockchain.	Privacy issues in vehicular transactions is not taken into consideration.
	[118]	Vehicular IoT services	-	A blockchain-based security framework for vehicular IoT services.	Scalability of the proposed scheme and access control have not been verified.
Smart industry	[119]	Smart manufacturing	Ethereum	A blockchain cloud manufacturing system for secure manufacturing industry.	Access control to the data storage in cloud database has not been considered.
	[121]	Manufacturing platform	Ethereum	A decentralized framework for manufacturing applications with cloud blockchain.	The performance of the proposed framework has not been simulated.
	[123]	Supply chain	-	A conceptual cloud blockchain framework for supply chain.	BCoT implementation for supply chain scenarios has not been done.
	[124]	Smart energy	-	A cloud-blockchain scheme for decentralized operations in energy internet.	Only conceptual analysis is provided and simulation to evaluate the proposal is lacked.
	[125]	Smart grids	Hyperledger Fabric	A crowdsourced energy system for energy trading on cloud blockchain.	Scalability of the cloud-blockchain based solution in smart grids has not been considered.
	[126]	Smart energy	Ethereum	An intelligent energy aware resource management in cloud datacentre (DC) using blockchain.	Mining cost, privacy of energy data in cloud data centre have not been considered.
Cloud services	[127]	Smart payment	Ethereum	A blockchain based fair payment architecture named BCPay for outsourcing services.	Data privacy has not been investigated.
	[129]	Data delection	-	A new publicly verifiable data deletion scheme on cloud using blockchain.	The feasibility of the proposed model has not been investigated on real world cloud platforms.
	[133]	Resource management	-	An optimal computing resource allocation scheme on cloud blockchain in IoT.	Smart contracts for access control among resource users have not been investigated.
	[135]	Cloud service management	Ethereum	A service management system based on smart contracts for cloud resource provisions.	Data privacy on service exchanges has not been investigated.
	[137]	Smart education	-	An online identity verification system based on blockchain for educational collaboration.	Real implementation results have not been reported to verify the proposal.

arrival of this emerging technology is potential to change the current shape of CoT markets and transform industrial network architectures with advanced BCoT paradigms. Although the convergence of blockchain and CoT can bring various benefits to IoT applications, the BCoT technology has developed without standards and is limited to a few service providers. Importantly, each service provider mainly designs and offers BCoT for specific applications rather than generic schemes which can be applicable to diverse use-case domains. The lack of system standard can restrict potential collaborations between services providers and make customers feel difficult in changing providers as each provider has their own rules [27]. Furthermore, non-standard heterogeneous communication protocol between different blockchain platforms and CoT systems is still a critical issue for the BCoT market. For example, three cloud blockchain projects considered in [27] including Golem, SONM and iExec have different visions in terms of service provision, system configuration, and customer targets. Such a lack of standard arises from three main reasons: different service definitions, different network management concepts and different operational hypothesis. Consequently, they are unable to meet a standard service level agreement, which is very important for their project developments in a long run.

2) Security Vulnerability: Although blockchain can bring security benefits to CoT thanks to its distributed nature,

TABLE V: Decentralized storage platforms based on cloud blockchain.

Platforms	Key features	Cloud support	Latest version	Last update	Ready to use?	Open source?
IPFS	Data file is hashed cryptographically for immutability.	Yes	v0.4.21	May 2019	Yes	Yes [139]
Storj	End-to-end encryption security is provided.	Yes	v04	Apr. 2019	Yes	Yes [140]
Filecoin	End-to-end encryption security is provided. Users can stored files with preferences based on cost budgets, redundancy, and file retrieval speeds	Yes	v 0.2.2	May 2019	Yes	Yes [141]
Sia	Stored files are encrypted. Storage is supper cheap with $2/ terabyte.	Yes	v1.3.3	Aug. 2018	Yes	Yes [142]
Swarm	Users can use local HTTP proxy API to interact with Swarm. Ethereum support is provided.	-	v 0.4.3	Jun. 2019	Yes	Yes [143]
Maidsafe	Data file is uploaded to a safe network and is fully encrypted for privacy.	-	v4.18.2	2018	Yes	Yes [144]
BigchainDB	It combines the key benefits of distributed databases and traditional blockchains.	Yes	v2.0	2018	Yes	Yes [145]
Datum	Users can offload data to decentralized nodes via mobile application with smart contracts.	-	v0.1.33	2018	Yes	Yes [146]

immutability, verifiability, and encryption, security issues in BCoT still remain due to the vulnerabilities of both CoT and blockchain systems. In CoT, there has been an increasing demand of outsourcing IoT data to clouds for storage and computation services due to the constrained resources of IoT devices. This dynamic incorporation has brought a series of new challenging security concerns such as identity and access control, authentication, system integrity [42]. Further, there are a number of critical security attacks to CoT, such as eavesdropping, malicious IoT attacks, unsecured communication channels, and degradation of connection quality. Cloud services for BCoT also suffer from serious security threats, from storage and computation attacks, virtual machine (VM) migration attacks to malware injection and DoS attacks [159].

On the other side, recent studies also have revealed inherent security weaknesses in blockchain operations which are mostly related to BCoT systems [160]. A serious security bottleneck is 51% attack which means that a group of miners controls more than 50% of the network's mining hash rate, or computing power, which prevents new transactions from gaining confirmations and halts payments between service providers and IoT users. Seriously, attackers can exploit this vulnerability to perform attacks, for example, they can modify the ordering of transactions, hamper normal mining operations or initiate double spending attack, all of which can degrade the blockchain network [160]. In addition, the security aspect of smart contract, which is regarded as core software on blockchain, is also very important since a small bug or attack can result in significant issues like privacy leakage or system logic modifications [161], [162]. Some of critical security vulnerabilities can include timestamp dependence, mishandled exceptions, reentrancy attacks on smart contracts in BCoT applications.

3) Privacy Leakage: The privacy of IoT data in BCoT can be compromised accidentally and hence the disclosure of data is respectively beneficial for the attacker and harmful to the users. In current BCoT systems, data can be stored off-chain in cloud storage to reduce the burden on blockchain. However, this storage architecture can arise new privacy concerns. Specifically, an autonomous entity can act as a network member to honestly perform the cloud data processing, but meanwhile obtains personal information without the consent of users, which leads to serious information leakage issues. External attacks can also gain malicious access to retrieve cloud data, or even alter and modify illegally outsourced IoT records on cloud. Besides, privacy leakage on blockchain transactions is another significant problem. Although blockchain uses encryption and digital signature to preserve transactions, recent measure results [163] show that a certain amount of transaction is leaked during blockchain operations and data protection of blockchain is not very robust in practice. Furthermore, criminals can leverage smart contracts for illegal purposes, facilitating the leakage of confidential information, theft of cryptographic keys. Importantly, the privacy of BCoT users can not be ensured once they join the network. Indeed, by participating in the blockchain network, all information of users such as the addresses of sender and receiver, amount values is publicly available on the network due to the transparency of blockchain. Consequently, curious users or attacks can analyse such information and keep track of activities of participants, which can lead to leakage of information secrets such as personal data.

4) Intelligence: Currently, BCoT systems are mainly used for data storage, data sharing and security services. However, there has been a lack of research attention in integrating intelligent services in BCoT applications. In fact, modern industries have increasing demands in intelligent services such as smart data analytics, smart decision making systems or automatic management tools to facilitate user service delivery. For example, a smart clinical support system based on cloud computing in healthcare can make diagnosis and treatment much easier. Further, an intelligent traffic analytic tool in cloud-based vehicular networks can help vehicle drivers to adjust their route for reducing possibilities of traffic congestion. All such intelligent services will be promising in BCoT-enabled applications to satisfy quality of user experience and enhance system efficiency. Therefore, we consider intelligence in BCoT as an important open issue where research efforts are strongly necessary.

5) Resource Management: In BCoT applications, to achieve sustainable profit advantage, cost reduction, and flexibility in cloud service provision, the resource management in cloud blockchain is vitally important and needs more research efforts. In fact, resource management in cloud blockchain

TABLE VI: BaaS platforms for BCoT applications.

BaaS Services	Descriptions	Blockchain	Launch Year	Source code
Microsoft Azure Blockchain	Microsoft Blockchain on Azure is a BaaS platform hosted on the Microsoft Azure cloud computing for creating and configuring consortium blockchain infrastructure quickly. It is now available in two tiers: Basic for cost-optimized services to test blockchain apps and Standard for running real BCoT applications.	Ethereum, Hyperledger Fabric or R3 Corda	2016	[149]
IBM Blockchain	IBM blockchain is an enterprise-ready blockchain application development platform. It enables businesses to develop, govern, and operate blockchain systems with seamless software and network updates on IBM cloud. Some biggest banking and commercial industries have used IBM blockchain.	Hyperledger Fabric	2017	[51]
Amazon Blockchain	Amazon blockchain service makes it easy to setup, deploy, and manage scalable blockchain networks. It can be useful in many IoT use cases, such as manufacturing, insurance, trading, retail, and banking systems.	Ethereum and Hyperledger Fabric	2018	[49]
Oracle Blockchain	BaaS on Oracle cloud provides an enterprise-grade distributed ledger platform that can assist businesses to increase trust and provide agility in transactions across their business networks. Oracle BaaS can seamlessly connects with a number of popular Oracle solutions such as Oracle Supply Chain Management (SCM) Cloud and Oracle Enterprise Resource Planning (ERP) Cloud.	Hyperledger Fabric	2018	[52]
Hewlett-Packard (HP)	Blockchain HP launched its BaaS called HPE Mission Critical Blockchain, which enables customers to execute distributed-ledger workloads in industrial environments with high security. It also guarantees massive scalability of HP-based blockchain projects to support business.	Ethereum	2017	[150]
Alibaba Blockchain	Alibaba BaaS is an enterprise-level PaaS (Platform as a Service) which is built on Alibaba Cloud Container Service for Kubernetes clusters. It brings benefits such as high security, ease-of-use, high stability, openness and efficient sharing services for blockchain-based applications.	Ethereum and Hyperledger Fabric	2017	[151]
Baidu Blockchain	Baidu BaaS is a commercialized platform, to simplify Dapp development. It provides developers with services such as multi-chain and middle-tier frameworks, as well as smart contract and DApp templates on Baidu cloud computing. Its applications consists of IoT with BCoT, finance, and data sharing.	Ethereum, Hyperledger Fabric, and Baidu XuperChain	2018	[152]
Huawei Blockchain	Huawei BaaS is a cloud service that capitalizes on the advantages of Huawei clouds container and security technologies. It offers key advantages such as open, easy-to-use, flexible and efficient features as well as robust security and privacy protections.	Hyperledger	2018	[153]
Google Blockchain	Google BaaS is based on Ethereum platform with important features such as API integration, configurable consensus algorithms, and the ability to use a traditional SQL databases to query and report on blockchain data.	Ethereum	2018	[154]
SAP	SAP BaaS provides an easiest and lowest-risk gateway to experimenting with distributed ledger technology. It is hosted on SAP cloud platform, enabling to prototype, test, and build blockchain applications (both private and consortium) and smart contracts.	MultiChain and Hyperledger Fabric	2018	[155]

networks requires adaptive and robust designs to solve series of technical problems, from resource allocation, bandwidth reservation to task allocation and workload allocation. A set of issues, challenges, and future research directions on resource management in cloud-based networks is discussed in [164], for example, the optimization of cloud resource allocation to computation demands and the adaption to dynamic service usage patterns. Such issues would become more complex when integrating cloud computing in blockchain where the resource usage is divided to serve multiple purposes, including resource for user demands and resource for mining mechanisms to maintain blockchain. Therefore, there is an urgent need to seek innovative solutions to overcome challenges in terms of resource management in integrated BCoT networks.

B. Discussion

Different BCoT service providers should achieve a service agreement on the incorporation of blockchain and CoT. Technical details such as network settings, blockchain deployment, IoT device integration, and service payment schemes should be considered carefully. Federation of service providers can be necessary to standardise the BCoT technology. Many standardization efforts have been made with the participation of a number of organizations such as ISO, ISTIC Europe, IEEE [165] to build a general functional architecture for blockchain platforms. Moreover, international BCoT standards will have to be developed simultaneously among multiple service suppliers in cloud blockchain design, market creation and customer service support, which promises to facilitate current BCoT-related industries [166].

Meanwhile, security problems in BCoT can be solved by security improvements in both CoT and blockchain systems. From the CoT point of view, security evaluations and appropriate solutions are vitally important. For example, the work in [167] proposed a trust assessment framework for cloud services named STRAF which takes into account security as a crucial feature to investigate trustworthiness of cloud computing to ensure security of cloud-based IoT applications. Furthermore, a cloud IoT architecture was also presented in [168] in which the trust evaluation mechanism guarantees high security for IoT and enhance system trustworthiness. In the perspective of blockchain, there are also some security enhancements. For instance, a mining pool system called SmartPool [169] was proposed to improve transaction verification in blockchain mining to mitigate security bottlenecks, such as 51% vulnerability, ensuring that the ledger cannot be hacked by increasingly sophisticated attackers. Particularly, recent works [170], [171] introduced efficient security analysis tools to investigate and prevent threat potentials in order to ensure trustful smart contract execution on blockchain. Such research efforts make contributions to addressing security issues in BCoT environments and improving the overall performance of the system.

Moreover, many innovative approaches have been considered to enhance privacy for BCoT systems such as encryption methods, trusted cloud computing, efficient user identification, access control, and intention hiding solutions [172]. Recently, an access control architecture was proposed in [173] to improve privacy of IoT data in cloud computing with better data reliability levels inherited by a consensus mechanism. From the blockchain view, anonymity plays a crucial role in ensuring robust privacy for BCoT users. In this regard, user information on blockchain can be hidden efficiently and attackers cannot guess identity of transactions and thus preserve private user information. For example, a recent work in [174] proposes a new solution with the ability to provide anonymity and unlinkability of senders, the privacy of transaction on the blockchain platform. Additionally, the authors in [175] present an anonymous reporting scheme which can ensure the reliability of anonymous reporting information without revealing the identities of IoT users, then preserving the privacy of blockchain systems.

The adoption of expert systems and intelligent tools available on cloud computing may be a good solution to provide intelligence in BCoT-related applications. For example, in BCoT-based smart healthcare, machine learning for smart health assessment systems is useful to support doctors in medical processes [176], [177]. Meanwhile, in smart cities, big data analytic software available on cloud is very helpful to solve data-related issues such as data collection, processing and visualization for smart services from city environment, citizens and various departments and agencies in the city scale [178]. Specially, a recent research effort [179] was put on the integration of machine learning and blockchain to enable decision making services in a fashion the intelligence of the system is improved while security and reliability are guaranteed.

Some intelligent approaches have been proposed recently to enhance efficiency of resource management in BCoT. For example, the authors in [126] presented a framework for energy-aware resource management in cloud datacentres with blockchain. Machine learning is embedded to smart contracts to optimize energy consumption according to user requests. This solution also has the potentials to achieve significant cost savings in respect with request scheduling and request migration on cloud blockchain. Meanwhile, the issue of resource management for mining blockchain in BCoT is considered in [180] in which resource for computation in the blockchain consensus process is optimized to achieve minimum prices of service usage. It also demonstrates that cloud providers can gain benefits from the optimal resource management with better profits in the proposed public cloud blockchain networks.

VI. Future Directions

As BCoT has attracted widespread attention of both academics and industries, its developments are likely to be affected by other technologies. The convergence of BCoT and these technologies can open up a wide range of opportunities to future services and applications. In this section, we will provide insights of such technologies and present the future research directions of integrating BCoT in such technologies to empower both worlds.

A. Improving Blockchain Performance for Future BCoT

To realize the full potential of blockchain in future BCoT applications, improving blockchain efficiency is highly important. Due to the security features of blockchain, each blockchain node is often required to verify transactions and authenticate user messages, which may require large computing and storage resources. Blockchain also requires network bandwidth and energy resources from cloud services to implement the mining process. Moreover, current blockchain designs still remain scalability issues from the perspectives of throughput, storage and networking. For example, many current blockchain platforms suffer from a long queueing time for transaction processing due to the block size restriction, which results in high block generation latency [22]. In addition to that, each blockchain node often has to store a copy of complete transaction data which poses a storage burden on the blockchain system. The integration of blockchain into CoT, therefore, will introduce new technical challenges that can negatively affect the overall performance of BCoT systems. Recently, many solutions have been proposed to improve these problems. A research direction is to provide lightweight consensus mechanisms, in order to enhance the blockchain performance by compressing consensus storage [181] or designing lightweight block validation schemes [182]. These approaches would help simplify the blockchain mining process to achieve energy savings and latency improvement. Another potential solution is to build off-chain blockchain platforms [183] by cooperating cloud services with hybrid consensus protocols on top of BCoT networks [184]. These techniques are capable of mitigating the data processing and storage burden posed on CoT devices and improving the scalability issues of BCoT platforms.

B. Machine Learning with BCoT

The main vision of future BCoT is to provide ubiquitous IoT services with system performance improvements and security enhancements to meet the ever-growing demands of user traffic and emerging services in the future networks, i.e., 5G and beyond. To achieve these goals, strategies for critical BCoT network issues such as networking optimization, system management, resource scheduling are vitally necessary. However, most current solutions have been based on traditional optimization algorithms or centralized designs, which remains some critical challenges [185]. For example, the explosion of IoT data volumes in future BCoT ecosystems can make traditional data processing techniques inefficient, and the high dynamics of IoT data traffic make computation and service management become challenging. To overcome these challenges, machine learning has emerged as a highly efficient solution for supporting future BCoT. As an important enabling technology for artificial intelligence, machine learning has been successfully applied in many areas, including computer vision, medical diagnosis, and speech recognition. The revolution of machine learning technology transforms current BCoT services by enabling its ability to learn from data and provide data driven insights, decision support, and predictions for improving network performances. For example, the work in [178] demonstrates the efficiency of machine learning tools in improving intelligence of BCoT applications. Specially, DRL [186] has recently emerged as one of the most attractive machine learning techniques to solve many critical issues in BCoT networks. Indeed, the integration of DRL can overcome security challenges brought by the dynamic data exchanges among blockchain users and information flow over untrusted mobile environments in cloud-blockchain systems. Our recent works verify that DRL-based offloading for consensus mechanisms in mobile blockchain networks can achieve security improvements for BCoT systems [187]. Obviously, the adoption of machine learning provides more perspectives to evaluate, analyse and deal with existing issues in BCoT scenarios, enabling to boost QoS, security and performance of the whole network.

C. Big Data in BCoT

With the rapid development of BCoT applications, big data has emerged as a significant data analytic tool for realizing the potential of the knowledge discovery from huge blockchain IoT data. In the future networks, it is expected that BCoT will witness an exponential growth of data traffic, from the volume, velocity, and variety of blockchain data. Big data can support a number of solutions to facilitating BCoT systems, including storage, data cleaning, and analytics [188]. Furthermore, big data also supports cleaning services which are understood as a pre-processing phase before big data analytics, mainly used to integrate and improve the quality of big data. More specific, the cleaning service includes two main phases: data integration (data fusion or data aggregation) and data quality management which address issues related to low-quality data such as corrupted data detection in the blockchain data, data redundancy reduction in BCoT data collection services (e.g., blockchain-based sensor networks). Then the analytics service includes all the methods and models for data analysis and processing such as data clustering algorithms and MapReduce processing [189]. For example, data clustering has been applied to characterize the usage and performance characteristics of large peer-to-peer consensus-based systems where blockchain datasets (e.g., Bitcoin data) are aggregated, analysed and visualized to discover unanticipated patterns in blockchain networks.

In return, BCoT also support big data in terms of better data integrity and privacy preservation to make sure that data analytics in big data is secure. In such contexts, blockchain in BCoT appears as the ideal candidate to solve big data-related issues [190]. Indeed, the decentralized management associated with authentication and reliability of blockchain can provide high security guarantees to big data resources. Specially, blockchain can offer transparency and trustworthiness for sharing of big data among service providers and data owners. By eliminating fear of security bottlenecks, BCoT can enable universal data exchange which empowers large-scale BCoT deployments. Recently, some big data models enabled by blockchain are proposed, such as data sharing with smart contracts [191] or data tracing solutions using blockchain transaction [192]. Such preliminary results show that blockchain can bring various advantages in terms of security and performance to big data applications, which will be promising to the development of both worlds.

D. BCoT in 5G Networks and Beyond

The next generations of mobile network (5G and beyond) have revolutionized industry and society by providing an unimaginable level of innovation with some key advantages such as high data rate, low network latency, energy savings, reduced operational costs, higher system throughput, and massive device connectivity. However, the development of new technology architectures in 5G wireless networks such as software defined networking (SDN), network functions virtualisation (NFV), network slicing, device-to-device (D2D) communications, and cloud computing has also raised many security issues [193]. For example, SDN remains some security issues such as forged or faked traffic flows, attacks on vulnerabilities in switches, control plane communications, and controllers, and the lack of trust mechanisms between controllers and management applications [194]. Moreover, how to provide the integrity between the service providers and platforms to avoid data leakage risks in resource sharing among NFV users and servers is still an open issue [195]. In such contexts, the blockchain is able to provide viable security solutions. For example, blockchain can build decentralized authentication mechanisms for SDN to implement decentralized access authorization with smart contracts [196]. By using shared ledgers, blockchain can also build trust among network entities, e.g., SDN controllers and network users, for reliable communications and secure data exchange. In NFV, blockchain can secure the delivery of network functions and ensure the system integrity against data threats, e.g., malicious VM modifications and data attacks [197].

To support future IoT applications, 5G also relies on the network slicing concept, which enables multiple tenants to share the same physical hardware. However, the network slicing operation also remains inter-slice security issues. For example, if the communication link is shared between multiple slices, then a malicious user on one slice could impact other slices, e.g., exploiting the resources or compromising data of the target slice [198]. Blockchain can be exploited to build reliable end-to-end network slices and allow network slide providers to manage their resource [199]. When a slice provider receives a request to establish an end-to-end slice, this request is submitted to the blockchain for authentication using smart contracts. In this way, the resource providers can perform resource trading on contracts with sub-slice components, and the information of sub-slice deployment is immutably recorded and stored in the blockchain. In terms of D2D communications in 5G networks, blockchain is able to build trust between D2D users and ensure transparent and reliable data exchange among different users [200]. In this blockchain-based D2D scenario, only resourceful devices (e.g., laptops, powerful smartphones) or edge servers participate in the blockchain mining process, while other lightweight D2D devices only join the network for communications without requiring blockchain mining [201].

Moreover, blockchain can support well 5G services. As an example, blockchain has been used to achieve trust management for 5G mobile vehicular communication due to its decentralized and immutable characteristics [118]. By using blockchain, the 5G-VANET scheme can detect network attacks and prevent data threats from accessing vehicular ecosystems. Besides, it is proven that blockchain can support secure and flexible key management in 5G IoT networks [202] thanks to its ability to reduce computational complexity and enhance communication security. Moreover, the blockchain along with cloud computing can bring great opportunities to 5G network management. For example, the blockchain can be exploited to build reliable end-to-end network slices and allow network slide providers to manage their resources. The work in [203] uses blockchain for dynamic control of vehicle-to-vehicle and vehicle-to-everything communications in vehicular network slices. Meanwhile, the cloud-native architecture with its programmable networking potentially improves 5G network slicing functions. For instance, the study in [204] demonstrates that the cloud-native model can enable life-cycle slice management to create, orchestrate and optimize the performances of network slices in terms of network resources, end-to-end delay, and data throughput. These research findings are expected to pave the way for the next generation of BCoT-5G networks.

VII. Conclusions

In this paper, we have presented an extensive and up-to-date review of the integration of two disruptive technologies: blockchain and CoT, referred to as BCoT, which is becoming increasingly important in industrial applications due to its advantages in security, privacy, and service support. This survey is motivated by the lack of a comprehensive literature review on the development of BCoT systems. We have first discussed the recent advances of BCoT along with the integration motivations and the conceptual BCoT integrated architecture. In particular, we have presented a comprehensive survey on the use of BCoT models in various applied scenarios, ranging from smart healthcare, smart city, smart transportation to industry applications and cloud services. We have further surveyed the emerging BCoT platforms and services that would be useful to application developers and researchers. From the extensive literature review on BCoT applications, we have highlighted some key technical challenges and pointed out possible future directions in BCoT research.

References

[1] J.-H. Lee and M. Pilkington, "How the blockchain revolution will reshape the consumer electronics industry [future directions]," *IEEE Consumer Electronics Magazine*, vol. 6, no. 3, pp. 19–23, 2017.

[2] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and beyond networks: A state of the art survey," *Journal of Network and Computer Applications*, vol. 166, 2020.

[3] P. Treleaven, R. G. Brown, and D. Yang, "Blockchain technology in finance," *Computer*, vol. 50, no. 9, pp. 14–17, 2017.

[4] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renewable and Sustainable Energy Reviews*, vol. 100, pp. 143–174, 2019.

[5] A. Alketbi, Q. Nasir, and M. A. Talib, "Blockchain for government servicesuse cases, security benefits and challenges," in *2018 15th Learning and Technology Conference (L&T)*, 2018, pp. 112–119.

[6] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[7] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016.

[8] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[9] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[10] M. Aazam, I. Khan, A. A. Alsaffar, and E.-N. Huh, "Cloud of things: Integrating internet of things and cloud computing and the issues involved," in *Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th-18th January, 2014*, 2014, pp. 414–419.

[11] M. S. Karunarathne, S. A. Jones, S. W. Ekanayake, and P. N. Pathirana, "Remote monitoring system enabling cloud technology upon smart phones and inertial sensors for human kinematics," in *2014 IEEE Fourth International Conference on Big Data and Cloud Computing*, 2014, pp. 137–142.

[12] B. Kantarci and H. T. Mouftah, "Sensing services in cloud-centric internet of things: A survey, taxonomy and challenges," in *2015 IEEE International Conference on Communication Workshop (ICCW)*, 2015, pp. 1865–1870.

[13] H. F. Atlam, A. Alenezi, A. Alharthi, R. J. Walters, and G. B. Wills, "Integration of cloud computing with internet of things: challenges and open issues," in *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2017, pp. 670–675.

[14] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26–33, 2017.

[15] K. Gai, K.-K. R. Choo, and L. Zhu, "Blockchain-enabled reengineering of cloud datacenters," *IEEE Cloud Computing*, vol. 5, no. 6, pp. 21–25, 2018.

[16] A. S. e. a. Yining Hu, "Blockchain-based smart contracts - applications and challenges," [Online]. Available: https://arxiv.org/abs/1810.04699.

[17] M. Ma, G. Shi, and F. Li, "Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario," *IEEE Access*, vol. 7, pp. 34 045–34 059, 2019.

[18] Y. Li, L. Zhu, M. Shen, F. Gao, B. Zheng, X. Du, S. Liu, and S. Yin, "Cloudshare: Towards a cost-efficient and privacy-preserving alliance cloud using permissioned blockchains," in *International Conference on Mobile Networks and Management*. Springer, 2017, pp. 339–352.

[19] D. F.-C. JOANNA KOLODZIEJ, ANDRZEJ WILCZYNSKI and A. FERNNDEZ-MONTES, "Blockchain secure cloud: a new generation integrated cloud and blockchain platforms general concepts and challenges," in *https://www.awilczynski.me/wp-content/uploads/2018/09/ECJvol4issue2.pdf.*

[20] T. Hardjono and N. Smith, "Cloud-based commissioning of constrained devices using permissioned blockchains," in *Proceedings of the 2nd ACM international workshop on IoT privacy, trust, and security*. ACM, 2016, pp. 29–36.

[21] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, 2018.

[22] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2018.

[23] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, pp. 32 979–33 001, 2018.

[24] H. 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.

[25] 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.

[26] J. Park and J. Park, "Blockchain security in cloud computing: Use cases, challenges, and solutions," *Symmetry*, vol. 9, no. 8, p. 164, 2017.

[27] R. B. Uriarte and R. De Nicola, "Blockchain-based decentralized cloud/fog solutions: Challenges, opportunities, and standards," *IEEE Communications Standards Magazine*, vol. 2, no. 3, pp. 22–28, 2018.

[28] 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.

[29] Bitcoin Platform. [Online]. Available: https://bitcoin.org/en/release/v0.18.0.

[30] Ethereum Platform. [Online]. Available: https://github.com/ethereum/go-ethereum/releases.

[31] Hyperledger Platform. [Online]. Available: https://github.com/hyperledger.

[32] IBM Blockchain Platform. [Online]. Available: https://github.com/IBM-Blockchain.

[33] MultiChain Platform. [Online]. Available: https://github.com/MultiChain.

[34] Hydrachain Platform. [Online]. Available: https://pypi.org/project/hydrachain/.

[35] Ripple Blockchain Platform. [Online]. Available: https://github.com/ripple/rippled/releases/tag/1.2.4.

[36] Corda Platform. [Online]. Available: https://docs.corda.net/head/release-notes.html.

[37] Bigchain Platform. [Online]. Available: https://github.com/bigchaindb/bigchaindb/releases/tag/v2.0.0b9.

[38] Openchain Platform. [Online]. Available: https://github.com/openchain.

[39] 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.

[40] J. Liu and Z. Liu, "A survey on security verification of blockchain smart contracts," *IEEE Access*, 2019.

[41] F. Lin and M. Qiang, "The challenges of existence, status, and value for improving blockchain," *IEEE Access*, vol. 7, pp. 7747–7758, 2018.

[42] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26–33, 2017.

[43] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in IoT: The challenges, and a way forward," *Journal of Network and Computer Applications*, 2018.

[44] J. Li, J. Wu, and L. Chen, "Block-secure: Blockchain based scheme for secure p2p cloud storage," *Information Sciences*, vol. 465, pp. 219–231, 2018.

[45] M. Yang, A. Margheri, R. Hu, and V. Sassone, "Differentially private data sharing in a cloud federation with blockchain," *IEEE Cloud Computing*, vol. 5, no. 6, pp. 69–79, 2018.

[46] Y. Zhang, C. Xu, X. Lin, and X. S. Shen, "Blockchain-based public integrity verification for cloud storage against procrastinating auditors," *IEEE Transactions on Cloud Computing*, 2019.

[47] Blockchain-Based Decentralized Cloud Computing. [Online]. Available: https://iex.ec/wp-content/uploads/pdf/iExec-WPv3.0-English.pdf.

[48] K. Gai, K.-K. R. Choo, and L. Zhu, "Blockchain-enabled reengineering of cloud datacenters," *IEEE Cloud Computing*, vol. 5, no. 6, pp. 21–25, 2018.

[49] AWS Blockchain. [Online]. Available: https://github.com/aws-samples/non-profit-blockchain.

[50] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure EHRs sharing of mobile cloud based e-health systems," *IEEE Access*, vol. 7, pp. 66 792–66 806, 2019.

[51] IBM Blockchain. [Online]. Available: https://github.com/IBM-Blockchain.

[52] Oracle Blockchain. [Online]. Available: https://github.com/oracle.

[53] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proceedings of the 17th IEEE/ACM international symposium on cluster, cloud and grid computing*. IEEE Press, 2017, pp. 468–477.

[54] J. Li, Z. Liu, L. Chen, P. Chen, and J. Wu, "Blockchain-based security architecture for distributed cloud storage," in *2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC)*, 2017, pp. 408–411.

[55] Y. Zhao and B. Duncan, "The impact of crypto-currency risks on the use of blockchain for cloud security and privacy," in *2018 International Conference on High Performance Computing & Simulation (HPCS)*, 2018, pp. 677–684.

[56] C. Yang, X. Chen, and Y. Xiang, "Blockchain-based publicly verifiable data deletion scheme for cloud storage," *Journal of Network and Computer Applications*, vol. 103, pp. 185–193, 2018.

[57] I. Sukhodolskiy and S. Zapechnikov, "A blockchain-based access control system for cloud storage," in *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, 2018, pp. 1575–1578.

[58] S. Ali, G. Wang, M. Z. A. Bhuiyan, and H. Jiang, "Secure data provenance in cloud-centric internet of things via blockchain smart contracts," in *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, 2018, pp. 991–998.

[59] Y. Zhang, D. He, and K.-K. R. Choo, "Bads: Blockchain-based architecture for data sharing with abs and cp-abe in IoT," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[60] M. Ma, G. Shi, and F. Li, "Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario," *IEEE Access*, vol. 7, pp. 34 045–34 059, 2019.

[61] M. Hossain, Y. Karim, and R. Hasan, "Fif-IoT: A forensic investigation framework for IoT using a public digital ledger," in *2018 IEEE International Congress on Internet of Things (ICIoT)*, 2018, pp. 33–40.

[62] N. M. Ahmad, S. F. A. Razak, S. Kannan, I. Yusof, and A. H. M. Amin, "Improving identity management of cloud-based IoT applications using blockchain," in *2018 International Conference on Intelligent and Advanced System (ICIAS)*, 2018, pp. 1–6.

[63] K. Bendiab, N. Kolokotronis, S. Shiaeles, and S. Boucherkha, "Wip: A novel blockchain-based trust model for cloud identity management," in *2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*, 2018, pp. 724–729.

[64] T. Uchibayashi, B. Apduhan, T. Suganuma, and M. Hiji, "Toward a secure vm migration control mechanism using blockchain technique for cloud computing environment," in *International Conference on Computational Science and Its Applications*. Springer, 2018, pp. 177–186.

[65] B. Zhao, P. Fan, and M. Ni, "Mchain: a blockchain-based vm measurements secure storage approach in iaas cloud with enhanced integrity and controllability," *IEEE Access*, vol. 6, pp. 43 758–43 769, 2018.

[66] Y. Zhang, C. Xu, X. Lin, and X. S. Shen, "Blockchain-based public integrity verification for cloud storage against procrastinating auditors," *IEEE Transactions on Cloud Computing*, 2019.

[67] C. Qiu, H. Yao, C. Jiang, S. Guo, and F. Xu, "Cloud computing assisted blockchain-enabled internet of things," *IEEE Transactions on Cloud Computing*, 2019.

[68] 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.

[69] X. Qiu, L. Liu, W. Chen, Z. Hong, and Z. Zheng, "Online deep reinforcement learning for computation offloading in blockchain-empowered mobile edge computing," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 8, pp. 8050–8062, 2019.

[70] M. Taghavi, J. Bentahar, H. Otrok, and K. Bakhtiyari, "A blockchain-based model for cloud service quality monitoring," *IEEE Transactions on Services Computing*, 2019.

[71] D. Wu and N. Ansari, "A cooperative computing strategy for blockchain-secured fog computing," *IEEE Internet of Things Journal*, 2020.

[72] 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.

[73] P. Zheng, Z. Zheng, W. Chen, J. Bian, and J. E. Yang, "Ethershare: Share information in jointcloud environment using blockchain-based smart contracts," in *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*, 2019, pp. 233–2335.

[74] Y. H. Ho, Z. Cheng, P. M. F. Ho, and H. C. Chan, "Mobile intercloud system with blockchain," in *Proceedings of the International Multi-Conference of Engineers and Computer Scientists*, vol. 1, 2018.

[75] W. Chen, M. Ma, Y. Ye, Z. Zheng, and Y. Zhou, "IoT service based on jointcloud blockchain: The case study of smart traveling," in *2018 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, 2018, pp. 216–221.

[76] O. O. Malomo, D. B. Rawat, and M. Garuba, "Next-generation cybersecurity through a blockchain-enabled federated cloud framework," *The Journal of Supercomputing*, vol. 74, no. 10, pp. 5099–5126, 2018.

[77] F. Freitag, "On the collaborative governance of decentralized edge microclouds with blockchain-based distributed ledgers," in *2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI)*, 2018, pp. 709–712.

[78] Y. Chen, H. Li, K. Li, and J. Zhang, "An improved p2p file system scheme based on ipfs and blockchain," in *2017 IEEE International Conference on Big Data (Big Data)*, 2017, pp. 2652–2657.

[79] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," *Applied Sciences*, vol. 9, no. 9, p. 1736, 2019.

[80] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, p. 470, 2018.

[81] H.-T. Pham and P. N. Pathirana, "Measurement and assessment of hand functionality via a cloud-based implementation," in *International Conference on Smart Homes and Health Telematics*. Springer, 2015, pp. 289–294.

[82] S. Li and P. N. Pathirana, "Cloud-based non-invasive tele-rehabilitation exercise monitoring," in *2014 IEEE Conference on Biomedical Engineering and Sciences (IECBES)*, 2014, pp. 385–390.

[83] H. Jin, Y. Luo, P. Li, and J. Mathew, "A review of secure and privacy-preserving medical data sharing," *IEEE Access*, vol. 7, pp. 61 656–61 669, 2019.

[84] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, "Bpds: A blockchain based privacy-preserving data sharing for electronic medical records," in *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 1–6.

[85] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2017, pp. 1–5.

[86] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, pp. 38 437–38 450, 2018.

[87] X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere, "Blockchain-based personal health data sharing system using cloud storage," in *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, 2018, pp. 1–6.

[88] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "Medshare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14 757–14 767, 2017.

[89] Q. Xia, E. Sifah, A. Smahi, S. Amofa, and X. Zhang, "Bbds: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, 2017.

[90] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment," *Journal of medical systems*, vol. 42, no. 8, p. 156, 2018.

[91] A. Al Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future Generation Computer Systems*, vol. 95, pp. 511–521, 2019.

[92] H. Wang and Y. Song, "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain," *Journal of medical systems*, vol. 42, no. 8, p. 152, 2018.

[93] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, 2019.

[94] Y. Du, J. Liu, Z. Guan, and H. Feng, "A medical information service platform based on distributed cloud and blockchain," in *2018 IEEE International Conference on Smart Cloud (SmartCloud)*, 2018, pp. 34–39.

[95] S. Cao, G. Zhang, P. Liu, X. Zhang, and F. Neri, "Cloud-assisted secure ehealth systems for tamper-proofing EHR via blockchain," *Information Sciences*, vol. 485, pp. 427–440, 2019.

[96] J. Park, S. Park, K. Kim, and D. Lee, "Corus: Blockchain-based trustworthy evaluation system for efficacy of healthcare remedies," in *2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, 2018, pp. 181–184.

[97] R. C. Celiz, Y. E. De La Cruz, and D. M. Sanchez, "Cloud model for purchase management in health sector of peru based on IoT and blockchain," in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 2018, pp. 328–334.

[98] C. G. Number, "Recent patient health monitoring platforms incorporating internet of things-enabled smart devices," *UROLOGY JOURNAL*, vol. 19, no. 2, 2015.

[99] D. C. Nguyen, K. D. Nguyen, and P. N. Pathirana, "A mobile cloud based IoMT framework for automated health assessment and management," in *2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, 2019, pp. 6517–6520.

[100] M. Sookhak, H. Tang, Y. He, and F. R. Yu, "Security and privacy of smart cities: a survey, research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1718–1743, 2018.

[101] H. Yu, Z. Yang, and R. O. Sinnott, "Decentralized big data auditing for smart city environments leveraging blockchain technology," *IEEE Access*, vol. 7, pp. 6288–6296, 2018.

[102] N. Tapas, G. Merlino, and F. Longo, "Blockchain-based IoT-cloud authorization and delegation," in *2018 IEEE International Conference on Smart Computing (SMARTCOMP)*, 2018, pp. 411–416.

[103] R. Paul, P. Baidya, S. Sau, K. Maity, S. Maity, and S. B. Mandal, "IoT based secure smart city architecture using blockchain," in *2018 2nd International Conference on Data Science and Business Analytics (ICDSBA)*, 2018, pp. 215–220.

[104] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city," *IEEE Access*, vol. 7, pp. 18 611–18 621, 2019.

[105] M. AbuNaser and A. A. Alkhatib, "Advanced survey of blockchain for the internet of things smart home," in *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, 2019, pp. 58–62.

[106] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*, 2017, pp. 618–623.

[107] S. Singh, I.-H. Ra, W. Meng, M. Kaur, and G. H. Cho, "Sh-blockcc: A secure and efficient internet of things smart home architecture based on cloud computing and blockchain technology," *International Journal of Distributed Sensor Networks*, vol. 15, no. 4, p. 1550147719844159, 2019.

[108] J. Xue, C. Xu, and Y. Zhang, "Private blockchain-based secure access control for smart home systems." *KSII Transactions on Internet & Information Systems*, vol. 12, no. 12, 2018.

[109] B. Yin, L. Mei, Z. Jiang, and K. Wang, "Joint cloud collaboration mechanism between vehicle clouds based on blockchain," in *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*, 2019, pp. 227–2275.

[110] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Network*, vol. 32, no. 3, pp. 78–83, 2018.

[111] S. Nadeem, M. Rizwan, F. Ahmad, and J. Manzoor, "Securing cognitive radio vehicular ad hoc network with fog node based distributed blockchain cloud architecture," *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS*, vol. 10, no. 1, pp. 288–295, 2019.

[112] X. Zhang, R. Li, and B. Cui, "A security architecture of vanet based on blockchain and mobile edge computing," in *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, 2018, pp. 258–259.

[113] M. Singh and S. Kim, "Introduce reward-based intelligent vehicles communication using blockchain," in *2017 International SoC Design Conference (ISOCC)*, 2017, pp. 15–16.

[114] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119–125, 2017.

[115] M. Li, L. Zhu, and X. Lin, "Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing," *IEEE Internet of Things Journal*, 2018.

[116] J. Fan, R. Li, and S. Li, "Research on task scheduling strategy: Based on smart contract in vehicular cloud computing environment," in *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, 2018, pp. 248–249.

[117] Z. Li, Z. Xiao, Q. Xu, E. Sotthiwat, R. S. M. Goh, and X. Liang, "Blockchain and IoT data analytics for fine-grained transportation insurance," in *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)*, 2018, pp. 1022–1027.

[118] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy internet of things in SDN-enabled 5G -vanets," *IEEE Access*, vol. 7, pp. 56 656–56 666, 2019.

[119] Z. Li, A. V. Barenji, and G. Q. Huang, "Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform," *Robotics and Computer-Integrated Manufacturing*, vol. 54, pp. 133–144, 2018.

[120] N. Mohamed, J. Al-Jaroodi, and S. Lazarova-Molnar, "Leveraging the capabilities of industry 4.0 for improving energy efficiency in smart factories," *IEEE Access*, vol. 7, pp. 18 008–18 020, 2019.

[121] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial internet of things," *Journal of Software Engineering and Applications*, vol. 9, no. 10, p. 533, 2016.

[122] G. Perboli, S. Musso, and M. Rosano, "Blockchain in logistics and supply chain: A lean approach for designing real-world use cases," *IEEE Access*, vol. 6, pp. 62 018–62 028, 2018.

[123] D. E. O'Leary, "Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems," *Intelligent Systems in Accounting, Finance and Management*, vol. 24, no. 4, pp. 138–147, 2017.

[124] T. Yang, Q. Guo, X. Tai, H. Sun, B. Zhang, W. Zhao, and C. Lin, "Applying blockchain technology to decentralized operation in future energy internet," in *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*, 2017, pp. 1–5.

[125] S. Wang, A. F. Taha, J. Wang, K. Kvaternik, and A. Hahn, "Energy crowdsourcing and peer-to-peer energy trading in blockchain-enabled smart grids," *arXiv preprint arXiv:1901.02390*, 2019.

[126] C. Xu, K. Wang, and M. Guo, "Intelligent resource management in blockchain-based cloud datacenters," *IEEE Cloud Computing*, vol. 4, no. 6, pp. 50–59, 2017.

[127] Y. Zhang, R. H. Deng, X. Liu, and D. Zheng, "Blockchain based efficient and robust fair payment for outsourcing services in cloud computing," *Information Sciences*, vol. 462, pp. 262–277, 2018.

[128] D. R. H. L.-X. Zhang, Yinghui and D. Zheng, "Blockchain based efficient and robust fair payment for outsourcing services in cloud computing," *Information Sciences*, vol. 462, pp. 262–277, 2018.

[129] C. Yang, X. Chen, and Y. Xiang, "Blockchain-based publicly verifiable data deletion scheme for cloud storage," *Journal of Network and Computer Applications*, vol. 103, pp. 185–193, 2018.

[130] R. Zheng, J. Jiang, X. Hao, W. Ren, F. Xiong, and Y. Ren, "bcbim: A blockchain-based big data model for bim modification audit and provenance in mobile cloud," *Mathematical Problems in Engineering*, vol. 2019, 2019.

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

[132] Y. Ren, Y. Liu, X. Yin, Z. Shen, and H.-J. Kim, "Blockchain-based trusted electronic records preservation in cloud storage," *Computers, Materials & Continua*, vol. 58, no. 1, pp. 135–151, 2019.

[133] Z. Li, Z. Yang, and S. Xie, "Computing resource trading for edge-cloud-assisted internet of things," *IEEE Transactions on Industrial Informatics*, 2019.

[134] 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*, 2018.

[135] S. Nayak, N. C. Narendra, A. Shukla, and J. Kempf, "Saranyu: Using smart contracts and blockchain for cloud tenant management," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 2018, pp. 857–861.

[136] A. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-based applications in education: A systematic review," *Applied Sciences*, vol. 9, no. 12, p. 2400, 2019.

[137] M. Hori and M. Ohashi, "Adaptive identity authentication of blockchain system-the collaborative cloud educational system," in *EdMedia+ Innovate Learning*. Association for the Advancement of Computing in Education (AACE), 2018, pp. 1339–1346.

[138] I. Purdon and E. Erturk, "to the cloud and its potential role in computer science education," *Engineering, Technology & Applied Science Research*, vol. 7, no. 6, pp. 2340–2344, 2017.

[139] IPFS Storage Platform. [Online]. Available: https://github.com/ipfs/ipfs.

[140] Storj Platform. [Online]. Available: https://github.com/Storj/.

[141] Filecoin Platform. [Online]. Available: https://github.com/filecoin-project.

[142] Sia Platform. [Online]. Available: https://github.com/NebulousLabs/Sia.

[143] Swarm Platform. [Online]. Available: https://swarm.ethereum.org/.

[144] Maidsafe Platform. [Online]. Available: https://maidsafe.net/.

[145] BigchainDB Platform. [Online]. Available: https://github.com/bigchaindb/bigchaindb.

[146] Datum Platform. [Online]. Available: https://github.com/Datum.

[147] K. R. Ozyilmaz and A. Yurdakul, "Designing a blockchain-based IoT with ethereum, swarm, and lora: the software solution to create high availability with minimal security risks," *IEEE Consumer Electronics Magazine*, vol. 8, no. 2, pp. 28–34, 2019.

[148] Microsoft Azure - IPFS. [Online]. Available: https://ipfs.io/ipfs/wiki/Microsoft Azure.html.

[149] Azure Blockchain. [Online]. Available: https://github.com/Azure-Samples/blockchain.

[150] Hewlett Packard Blockchain. [Online]. Available: https://github.com/HewlettPackard/catena/wiki/Ethereum.

[151] Alibaba Blockchain. [Online]. Available: https://github.com/AliyunContainerService/solution-blockchain-demo.

[152] Baidu Blockchain. [Online]. Available: https://github.com/baidu.

[153] Huawei Blockchain. [Online]. Available: https://github.com/Huawei.

[154] Google Blockchain. [Online]. Available: https://github.com/blockchain-etl/ethereum-etl-airflow.

[155] SAP Blockchain. [Online]. Available: https://github.com/SAP/cloud-blockchain-odometer-example.

[156] Use vehicle sensor data to execute smart transactions in Blockchain. [Online]. Available: https://developer.ibm.com/articles/cl-blockchain-for-cognitive-IoT-apps2/.

[157] Oracle Blockchain Use Cases. [Online]. Available: https://blogs.oracle.com/blockchain/blockchain-use-cases.

[158] HPE and Continental to launch blockchain platform for vehicle data sharing. [Online]. Available: https://www.cio.com.au/article/658229/hpe-continental- launch-blockchain-platform-vehicle-data-sharing/.

[159] M. A. Khan, "A survey of security issues for cloud computing," *Journal of network and computer applications*, vol. 71, pp. 11–29, 2016.

[160] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, 2017.

[161] S. Rouhani and R. Deters, "Security, performance, and applications of smart contracts: A systematic survey," *IEEE Access*, vol. 7, pp. 50 759–50 779, 2019.

[162] M. Wohrer and U. Zdun, "Smart contracts: security patterns in the ethereum ecosystem and solidity," in *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, 2018, pp. 2–8.

[163] A. Miller, M. Möser, K. Lee, and A. Narayanan, "An empirical analysis of linkability in the monero blockchain.(2017)," 2017.

[164] N. C. Luong, P. Wang, D. Niyato, Y. Wen, and Z. Han, "Resource management in cloud networking using economic analysis and pricing models: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 954–1001, 2017.

[165] V. Gramoli and M. Staples, "Blockchain standard: Can we reach consensus?" *IEEE Communications Standards Magazine*, vol. 2, no. 3, pp. 16–21, 2018.

[166] A. Anjum, M. Sporny, and A. Sill, "Blockchain standards for compliance and trust," *IEEE Cloud Computing*, vol. 4, no. 4, pp. 84–90, 2017.

[167] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang, and D. Chen, "Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach," *IEEE Access*, vol. 7, pp. 9368–9383, 2019.

[168] T. Wang, G. Zhang, A. Liu, M. Z. A. Bhuiyan, and Q. Jin, "A secure IoT service architecture with an efficient balance dynamics based on cloud and edge computing," *IEEE Internet of Things Journal*, 2018.

[169] L. Luu, Y. Velner, J. Teutsch, and P. Saxena, "Smartpool: Practical decentralized pooled mining," in *26th {USENIX} Security Symposium ({USENIX} Security 17)*, 2017, pp. 1409–1426.

[170] R. Cheng, F. Zhang, J. Kos, W. He, N. Hynes, N. Johnson, A. Juels, A. Miller, and D. Song, "Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts," 2018.

[171] P. Tsankov, A. Dan, D. Drachsler-Cohen, A. Gervais, F. Buenzli, and M. Vechev, "Securify: Practical security analysis of smart contracts," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2018, pp. 67–82.

[172] C. Stergiou, K. E. Psannis, B. B. Gupta, and Y. Ishibashi, "Security, privacy & efficiency of sustainable cloud computing for big data & IoT," *Sustainable Computing: Informatics and Systems*, vol. 19, pp. 174–184, 2018.

[173] R. Saha, G. Kumar, M. K. Rai, R. Thomas, and S.-J. Lim, "Privacy ensured ehealthcare for fog-enhanced IoT based applications," *IEEE Access*, vol. 7, pp. 44 536–44 543, 2019.

[174] K. Singh, N. Heulot, and E. B. Hamida, "Towards anonymous, unlinkable, and confidential transactions in blockchain," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, pp. 1642–1649.

[175] S. Zou, J. Xi, S. Wang, Y. Lu, and G. Xu, "Reportcoin: A novel blockchain-based incentive anonymous reporting system," *IEEE Access*, vol. 7, pp. 65 544–65 559, 2019.

[176] D. N. Khoa, N. P. Pubudu, and et al., "An instrumented measurement scheme for the assessment of upper limb function in individuals with friedreich ataxia," in *Proc. 41th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc., Berlin, Germany*, 2019.

[177] M. S. Karunarathne, S. A. Jones, S. W. Ekanayake, and P. N. Pathirana, "Remote monitoring system enabling cloud technology upon smart phones and inertial sensors for human kinematics," in *2014 IEEE Fourth International Conference on Big Data and Cloud Computing*, 2014, pp. 137–142.

[178] Z. Khan, A. Anjum, and S. L. Kiani, "Cloud based big data analytics for smart future cities," in *2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing*, 2013, pp. 381–386.

[179] S. Vyas, M. Gupta, and R. Yadav, "Converging blockchain and machine learning for healthcare," in *2019 Amity International Conference on Artificial Intelligence (AICAI)*, 2019, pp. 709–711.

[180] 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*, 2018.

[181] T. Kim, J. Noh, and S. Cho, "Scc: Storage compression consensus for blockchain in lightweight IoT network," in *2019 IEEE International Conference on Consumer Electronics (ICCE)*, 2019, pp. 1–4.

[182] Y. Liu, K. Wang, Y. Lin, and W. Xu, "Lightchain: A lightweight blockchain system for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3571–3581, 2019.

[183] Y. Tang, Q. Zou, J. Chen, K. Li, C. A. Kamhoua, K. Kwiat, and L. Njilla, "Chainfs: Blockchain-secured cloud storage," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 2018, pp. 987–990.

[184] S. S. Hazari and Q. H. Mahmoud, "A parallel proof of work to improve transaction speed and scalability in blockchain systems," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 2019, pp. 0916–0921.

[185] D. C. Nguyen, P. Cheng, M. Ding, D. Lopez-Perez, P. N. Pathirana, J. Li, A. Seneviratne, Y. Li, and H. V. Poor, "Wireless AI: Enabling an AI-governed data life cycle," *arXiv preprint arXiv:2003.00866*, 2020.

[186] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Privacy-preserved task offloading in mobile blockchain with deep reinforcement learning," [Online]. Available: https://arxiv.org/abs/1908.07467.

[187] D. C. Nguyen, P. Pathirana, M. Ding, and A. Seneviratne, "Secure computation offloading in blockchain based IoT networks with deep reinforcement learning," [Online]. Available: https://arxiv.org/abs/1908.07466.

[188] M. Ge, H. Bangui, and B. Buhnova, "Big data for internet of things: a survey," *Future Generation Computer Systems*, vol. 87, pp. 601–614, 2018.

[189] O. Nasraoui and C.-E. B. N'Cir, *Clustering Methods for Big Data Analytics: Techniques, Toolboxes and Applications*. Springer, 2018.

[190] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," in *IEEE EUROCON 2017-17th International Conference on Smart Technologies*, 2017, pp. 763–768.

[191] L. Yue, H. Junqin, Q. Shengzhi, and W. Ruijin, "Big data model of security sharing based on blockchain," in *2017 3rd International Conference on Big Data Computing and Communications (BIGCOM)*, 2017, pp. 117–121.

[192] Z. Wang, Y. Tian, and J. Zhu, "Data sharing and tracing scheme based on blockchain," in *2018 8th International Conference on Logistics, Informatics and Service Sciences (LISS)*, 2018, pp. 1–6.

[193] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2017.

[194] D. Fang and Y. Qian, "5G wireless security and privacy: Architecture and flexible mechanisms," *IEEE Vehicular Technology Magazine*, vol. 15, no. 2, pp. 58–64, 2020.

[195] A. M. Alwakeel, A. K. Alnaim, and E. B. Fernandez, "A survey of network function virtualization security," in *SoutheastCon 2018*, 2018, pp. 1–8.

[196] 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.

[197] R. V. Rosa and C. E. Rothenberg, "Blockchain-based decentralized applications for multiple administrative domain networking," *IEEE Communications Standards Magazine*, vol. 2, no. 3, pp. 29–37, 2018.

[198] S. Zhang, "An overview of network slicing for 5G," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 111–117, 2019.

[199] 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.

[200] V. A. Siris, D. Dimopoulos, N. Fotiou, S. Voulgaris, and G. C. Polyzos, "Trusted D2D-based IoT resource access using smart contracts," in *2019 IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, 2019, pp. 1–9.

[201] H. Cui, Z. Chen, N. Liu, and B. Xia, "Blockchain-driven contents sharing strategy for wireless cache-enabled D2D networks," in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2019, pp. 1–5.

[202] V. Adat, I. Politis, C. Tselios, P. GalIoTos, and S. Kotsopoulos, "On blockchain enhanced secure network coding for 5G deployments," in *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 1–7.

[203] 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, 2018.

[204] S. Sharma, R. Miller, and A. Francini, "A cloud-native approach to 5G network slicing," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 120–127, 2017.

Dinh C. Nguyen (Graduate Student Member, IEEE) is currently pursuing the Ph.D. degree at the School of Engineering, Deakin University, Victoria, Australia. He is also affiliated with the Information Security and Privacy Research Group, CSIRO Data61, Docklands, Melbourne, Australia. His research interests focus on blockchain, deep reinforcement learning, mobile edge/cloud computing, Internet of Things, network security and privacy. He is currently working on blockchain and reinforcement learning for Internet of Things and 5G networks. He has been a recipient of the prestigious Data61 PhD scholarship, CSIRO, Australia.

Pubudu N. Pathirana (Senior Member, IEEE) was born in 1970 in Matara, Sri Lanka, and was educated at Royal College Colombo. He received the B.E. degree (first class honors) in electrical engineering and the B.Sc. degree in mathematics in 1996, and the Ph.D. degree in electrical engineering in 2000 from the University of Western Australia, all sponsored by the government of Australia on EMSS and IPRS scholarships, respectively. He was a Postdoctoral Research Fellow at Oxford University, Oxford, a Research Fellow at the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia, and a Consultant to the Defence Science and Technology Organization (DSTO), Australia, in 2002. He was a visiting professor at Yale University in 2009. Currently, he is a full Professor and the Director of Networked Sensing and Control group at the School of Engineering, Deakin University, Geelong, Australia and his current research interests include Bio-Medical assistive device design, human motion capture, mobile/wireless networks, rehabilitation robotics and radar array signal processing.

Ming Ding (Senior Member, IEEE) received the B.S. and M.S. degrees (Hons.) in electronics engineering and the Ph.D. degree in signal and information processing from Shanghai Jiao Tong University (SJTU), Shanghai, China, in 2004, 2007, and 2011, respectively. From April 2007 to September 2014, he worked as a Researcher/Senior Researcher/Principal Researcher at the Sharp Laboratories of China, Shanghai. He also served as the Algorithm Design Director and the Programming Director for a system-level simulator of future telecommunication networks in Sharp Laboratories of China for more than seven years. He is currently a Senior Research Scientist with the CSIRO Data61, Sydney, NSW, Australia. His research interests include information technology, data privacy and security, machine learning and AI. He has authored over 100 articles in IEEE journals and conferences, all in recognized venues, and around 20 3GPP standardization contributions, and a Springer book Multi-Point Cooperative Communication Systems: Theory and Applications. He holds 21 U.S. patents and co-invented another more than 100 patents on 4G/5G technologies in CN, JP, KR, EU. He is an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and the IEEE Wireless Communications Letters. Besides, he is or has been a Guest Editor/CoChair/Co-Tutor/TPC Member of several IEEE top-tier journals/conferences, such as the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, IEEE Communications Magazine, and the IEEE GLOBECOM Workshops.

Aruna Seneviratne (Senior Member, IEEE) is currently a Foundation Professor of telecommunications with the University of New South Wales, Australia, where he holds the Mahanakorn Chair of telecommunications. He has also worked at a number of other Universities in Australia, U.K., and France, and industrial organizations, including Muirhead, Standard Telecommunication Labs, Avaya Labs, and Telecom Australia (Telstra). In addition, he has held visiting appointments at INRIA, France. His current research interests are in physical analytics: technologies that enable applications to interact intelligently and securely with their environment in real time. Most recently, his team has been working on using these technologies in behavioral biometrics, optimizing the performance of wearables, and the IoT system verification. He has been awarded a number of fellowships, including one at British Telecom and one at Telecom Australia Research Labs.