Blockchain for Internet of Things: A Survey

Hong-Ning Dai , *Senior Member, IEEE*, Zibin Zheng , *Senior Member, IEEE*,
and Yan Zhang , *Senior Member, IEEE*

Abstract—Internet of Things (IoT) is reshaping the incumbent industry to smart industry featured with data-driven decision-making. However, intrinsic features of IoT result in a number of challenges, such as decentralization, poor interoperability, privacy, and security vulnerabilities. Blockchain technology brings the opportunities in addressing the challenges of IoT. In this paper, we investigate the integration of blockchain technology with IoT. We name such synthesis of blockchain and IoT as blockchain of things (BCoT). This paper presents an in-depth survey of BCoT and discusses the insights of this new paradigm. In particular, we first briefly introduce IoT and discuss the challenges of IoT. Then, we give an overview of blockchain technology. We next concentrate on introducing the convergence of blockchain and IoT and presenting the proposal of BCoT architecture. We further discuss the issues about using blockchain for fifth generation beyond in IoT as well as industrial applications of BCoT. Finally, we outline the open research directions in this promising area.

Index Terms—Blockchain, industrial applications, Internet of Things (IoT), smart contract.

I. INTRODUCTION

THE RECENT advances in information and communication technology (ICT) have promoted the evolution of conventional computer-aided industry to *smart industry* featured with data-driven decision making [1]. During this paradigm shift, Internet of Things (IoT) plays an important role of connecting the physical industrial environment to the cyberspace of computing systems consequently forming a cyber-physical system (CPS). IoT can support a wide diversity of industrial applications, such as manufacturing, logistics, food industry, and utilities. IoT aims to improve operation efficiency and production throughput, reduce the machine downtime and enhance product quality.

In particular, IoT has the following features: 1) decentralization of IoT systems; 2) diversity of IoT devices and systems; 3) heterogeneity of IoT data; and 4) network complexity. All of them result in the challenges including heterogeneity of IoT system, poor interoperability, resource constraints of IoT devices, and privacy and security vulnerabilities.

The appearance of blockchain technologies brings the opportunities in overcoming the above challenges of IoT. A blockchain is essentially a distributed *ledger* spreading over the whole distributed system. With the decentralized consensus, blockchains can enable a transaction to occur and be validated in a mutually distrusted distributed system without the intervention of the trusted third party. Unlike incumbent transaction-management systems where the centralized agency needs to validate the transaction, blockchains can achieve the *decentralized* validation of transactions, thereby greatly saving the cost and mitigating the performance bottleneck at the central agency. Moreover, each transaction saved in blockchains is essentially *immutable* since each node in the network keeps all the committed transactions in the blockchain. Meanwhile, crytographic mechanisms (such as asymmetric encryption algorithms, digital signature, and hash functions) guarantee the integrity of data blocks in the blockchains. Therefore, the blockchains can ensure nonrepudiation of transactions. In addition, each transaction in blockchains is traceable to every user with the attached historic timestamp.

Blockchain is essentially a perfect complement to IoT with the improved interoperability, privacy, security, reliability, and scalability. In this paper, we investigate a new paradigm of integrating blockchain with IoT. We name such synthesis of blockchain and IoT as blockchain of things (BCoT). In particular, BCoT has the following merits.

1) *Interoperability* across IoT devices, IoT systems and industrial sectors, where the interoperability is the ability of interacting with physical systems and exchanging information between IoT systems. It can be achieved through the *blockchain-composite layer* built on top of an overlay peer-to-peer (P2P) network with uniform access across different IoT systems.

2) *Traceability* of IoT data, where the traceability is the capability of tracing and verifying the spatial and temporal information of a data block saved in the blockchain. Each data block saved in a blockchain is attached with a historic timestamp consequently assuring the data traceability.

3) *Reliability* of IoT data is the quality of IoT data being trustworthy. It can be ensured by the integrity

enforced by crytographic mechanisms including asymmetric encryption algorithms, hash functions and digital signature, all of which are inherent in blockchains.

4) *Autonomic interactions* of IoT system refer to the capability of IoT systems interacting with each other without the intervention of a trusted third party. This autonomy can be achieved by *smart contracts* enabled by blockchains. In particular, contract clauses embedded in smart contracts will be executed automatically when a certain condition is satisfied (e.g., the user breaching the contract will be punished with a fine automatically).

Though BCoT can benefit IoT, there are also a number of challenges to be addressed before the potentials of BCoT can be fully unleashed. Therefore, this paper aims to present an in-depth survey on the state-of-the-art advances, challenges, and open research issues in BCoT.

A. Comparison Between This Paper and Existing Surveys

There are several published papers discussing the convergence of blockchain with IoT. For example, the work of [2] presents a smart home application of using blockchains for IoT. Zhang and Wen [3] proposed a business model to support P2P trading based on smart contracts and blockchains. However, these studies are too specific to a certain scenario of incorporating blockchain with IoT (e.g., a smart home application).

Recently, several surveys on the convergence of blockchain with IoT have been published. In particular, [4] gives a systematic literature review on blockchain for IoT with the categorization of a number of use cases. The work of [5] presents a survey on IoT security and investigates the potentials of blockchain technologies as the solutions. Reyna *et al.* [6] investigated the possibility and research issues of integrating blockchain with IoT. The work of [7] presents a review on integrating blockchain with IoT in the application aspect. Ali *et al.* [8] attempted to give a comprehensive survey on application of blockchain in IoT. The work of [9] gives a categorization of applications of blockchain for IoT.

However, most of the existing surveys suffer from the following limitations: 1) there is no general architecture proposed for BCoT; 2) there is no study explicitly discussing blockchain for fifth generation (5G) beyond networks for IoT (however, this topic is of great importance for the development of IoT); and 3) other important issues like life cycle of smart contracts are missing in most of the existing surveys.

B. Contributions

In view of prior work, we aim to: 1) provide a conceptual introduction on IoT and blockchain technologies; 2) present in-depth analysis on the potentials of incorporating blockchains into IoT; and 3) give insightful discussions of technical challenges enabling BCoT. In summary, the main contributions of this paper are highlighted as follows.

1) A brief introduction on IoT is first given and then accompanied by a summary of key characteristics of IoT. Meanwhile, research challenges of IoT are outlined.
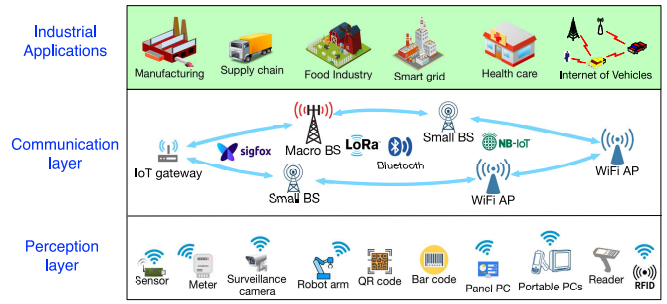

Fig. 1. IoT consists of perception layer, communication layer, and industrial applications.

2) An overview of key blockchain technologies is then given with a summary of key characteristics of blockchains and a taxonomy of the incumbent blockchain systems.

3) The core part of this paper is focused on the convergence of blockchain and IoT. In this respect, the opportunities of integrating blockchain with IoT are first discussed. An architecture of BCoT is then proposed and illustrated.

4) The 5G-beyond networks play an important role in constructing the infrastructure for BCoT. Research issues about blockchain for 5G-beyond networks in IoT are also discussed.

5) Furthermore, this paper summarizes the applications of BCoT and outlines the open research issues in BCoT.

The remainder of this paper is organized as follows. Section II first presents an overview on IoT. Section III then gives the introduction of blockchain technology. The convergence of blockchain and IoT is discussed in Section IV. Section V discusses the research issues about blockchain for 5G-beyond networks. Section VI next summarizes the applications of BCoT. Open research issues are discussed in Section VII. Finally, this paper is concluded in Section VIII.

II. INTERNET OF THINGS

In this section, we briefly introduce IoT in Section II-A and summarize the challenges of IoT in Section II-B.

A. Introduction to Internet of Things

Today's industry is experiencing a paradigm shift from conventional computer-aided industry to *smart industry* driven by recently advances in IoT and big data analytics (BDA). During this evolution, IoT plays a critical role of bridging the gap between the physical industrial environment and the cyberspace of computing systems while BDA can help to extract hidden values from massive IoT data so as to make intelligent decisions.

IoT is essentially a network of smart objects (i.e., things) with provision of various industrial services. A typical IoT system consists of the following layered subsystems (from bottom to up) as shown in Fig. 1.

1) *Perception Layer:* There is a wide diversity of IoT devices including sensors, actuators, controllers, bar code/quick response code (QR code) tags, RFID tags,

smart meters, and other wireless/wired devices. These devices can sense and collect data from the physical environment. Meanwhile, some of them (like actuators and controllers) can make actions on the environment.

2) *Communication Layer:* Various wireless/wired devices, such as sensors, RFIDs, actuators, controllers, and other tags can then connect with IoT gateways, WiFi access points (APs), small base stations (BSs), and macro BS to form an industrial network. The network connection is enabled by a diverse of communication protocols, such as Bluetooth, near field communications (NFCs), low-power wireless personal area networks (6LoWPANs), wireless highway addressable remote transducer (WirelessHART) [10], low power wide area networks (LPWANs) technologies including Sigfox, LoRa, narrowband IoT (NB-IoT), and industrial Ethernet [11].

3) *Industrial Applications:* IoT can be widely used to support a number of industrial applications. The typical industrial applications include manufacturing, supply chain, food industry, smart grid, health care, and Internet of Vehicles (IoV).

B. Challenges of Internet of Things

In this paper, we mainly focus on Industrial IoT. We denote Industrial IoT by IoT thereafter without loss of generality. The IoT ensures the connection of various *things* (smart objects) mounted with various electronic or mechanic sensors, actuators, and software systems which can sense and collect information from the physical environment and then make actions on the physical environment. The unique features of IoT pose a number of research challenges exhibiting in the following aspects.

1) *Heterogeneity* of IoT systems exhibits in the heterogeneous IoT devices, heterogeneous communication protocols and heterogeneous IoT data types (i.e., structured, semi-structured, and nonstructured). The heterogeneity is also the root of other challenges, such as interoperability, privacy, and security (to be explained as follows).

2) *Complexity* of networks. There are a number of communication/network protocols coexisting in IoT. Typical network protocols include NFC, Bluetooth, 6LoWPAN, WirelessHART, Sigfox, LoRa, and NB-IoT, all of which offer different network services. For example, 6LoWPAN and WirelessHART have typically short communication coverage (e.g., less than 100 m) while LPWAN technologies can provide the coverage from 1 to 10 km [12], [13].

3) *Poor interoperability* is the capability of IoT systems (both hardware and software) to exchange, make use of information and collaborate with each other. Due to the decentralization of IoT systems and the heterogeneity of IoT systems, it is challenging to exchange the data between different industrial sectors, strategic centers, and IoT systems. As a result, the interoperability of IoT is difficult to be achieved.

4) *Resource Constraints of IoT Devices:* IoT devices, such as sensors, actuators, RFID tags, and smart meters suffer, from limited resources including computing resource, storage resource, and battery power. For example, there is no battery power for passive RFID tags that can only harvest the energy from RFID readers or from ambient environment [14]. Moreover, the resource constraints also result in the vulnerability of IoT devices to malicious attacks.

5) *Privacy Vulnerability:* Privacy is to guarantee the appropriate usage of IoT data while there is no disclosure of user private information without user consent. It is challenging to preserve data privacy in IoT due to the complexity and the decentralization of IoT systems, the heterogeneity of IoT systems. Moreover, it becomes a trend to integrate IoT with cloud computing since cloud computing can empower IoT with extra computing and storage capabilities. However, uploading the confidential IoT data to the third-party cloud servers may also compromise the vulnerable privacy of IoT [15].

6) *Security Vulnerability:* The decentralization and the heterogeneity of IoT systems also result in the difficulty in ensuring the security of IoT while the security is extremely important for an enterprise. The typical solutions, such as authentication, authorization, and communication encryption, may not be appropriate to IoT due to the difficulty in implementing the security countermeasures in resource-constrained IoT systems. Moreover, IoT systems are also vulnerable to malicious attacks due to the failure of security firmware updates in time [16].

Discussion: Some intrinsic limitations of IoT can be overcome via recent ICT advances. For example, ambient backscatter assisted communications [14] can help IoT nodes obtain extra energy from ambience. Meanwhile, mobile edge computing (MEC) can extend the capability of IoT nodes via offloading the computationally intensive tasks to edge servers [17]. Moreover, the recent advances in blockchain technologies offer potential solutions to the challenges, such as poor interoperability and privacy and security vulnerabilities. In addition, blockchain is also beneficial to improve heterogeneity of IoT systems. We will discuss these opportunities brought by blockchain to IoT in Section IV-A after giving a briefing on blockchain technologies in Section III.

III. BLOCKCHAIN TECHNOLOGIES

In this section, we first give an overview on blockchain technologies in Section III-A, then summarize the key blockchain characteristics in Section III-B and present a taxonomy of blockchain platforms in Section III-D.

A. Overview of Blockchain Technologies

1) Blockchain: A blockchain is essentially a distributed *ledger* spreading over the whole blockchain system [18]. Fig. 2 shows an exemplary blockchain consisting of a number of consecutively connected blocks. Each block (with the exception of the first block) in a blockchain points to its immediately previous block (called parent block) via an *inverse* reference
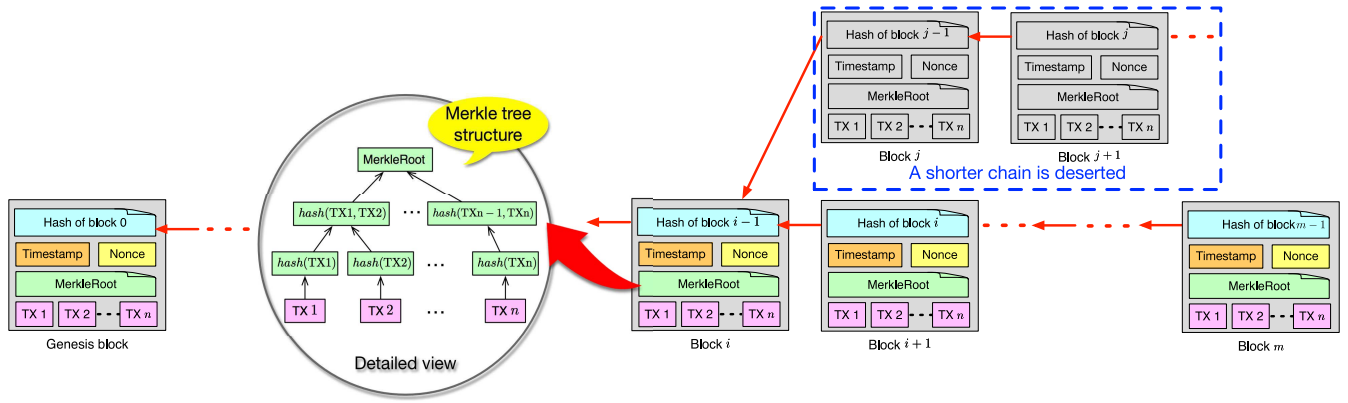
Fig. 2. Blockchain consists of a number of consecutively connected blocks and the detailed view represents a Merkle tree structure (where TX represents a transaction).

that is essentially the *hash* value of the parent block. For example, block i contains the hash of block $i - 1$ as shown in Fig. 2. The first block of a blockchain is called the *genesis* block having no parent block. In particular, a block structure consists of the following information: 1) block version (indicating the validation rules to follow); 2) the hash of parent block; 3) timestamp recording the current time in seconds; 4) nonce staring from 0 and increasing for every hash calculation; 5) the number of transactions; and 6) MerkleRoot (i.e., the hash value of the root of a Merkel tree with concatenating the hash values of all the transactions in the block) as shown in the detailed view of Fig. 2.

A blockchain is continuously growing with the transactions being executed. When a new block is generated, all the nodes in the network will participate in the block validation. A validated block will be automatically appended at the end of the blockchain via the inverse reference pointing to the parent block. In this manner, any unauthorized alterations on the previously generated block can be easily detected since the hash value of the tampered block is significantly different from that of the unchanged block. Moreover, since the blockchain is distributed throughout the whole network, the tampering behavior can also be easily detected by other nodes in the network.

a) Data integrity guarantee in blockchain: Blockchains leverage cryptographic techniques to guarantee data integrity. In particular, there are two mechanisms in blockchains to ensure the data integrity.

1) *An ordered link list structure of blocks*, in which each newly appended block must include the hash value of the preceding block. In this manner, a falsification on any of the previous blocks will invalidate the subsequent blocks.

2) *Merkel tree structure*, in which each block contains a root hash of a Merkel tree of all the transactions. Each nonleave node is essentially a hash value of two concatenated values of its two children. Therefore, a Merkel tree is typically a binary tree. In this way, any falsification on the transactions will lead to a new hash value in the above layer, consequently resulting in a falsified root hash. As a result, any falsification can be easily detected.

2) Consensus Algorithms: One of the advantages of blockchain technologies is to validate the block trustfulness in a decentralized trustless environment without the necessity of the trusted third-party authority. In distributed environment, it is challenging to reach a *consensus* on a newly generated block as the consensus may be biased in favor of malicious nodes. This trustfulness validation in a decentralized environment can be achieved by *consensus* algorithms. Typical consensus algorithms include proof of work (PoW), proof of stake (PoS), and practical Byzantine fault tolerance (PBFT) [19].

Take PoW as an example. The creation of a newly generated block is equivalent to the solution of a computationally difficult problem. This computationally difficult problem (also know as a puzzle) can nevertheless be verifiable without difficulty [20]. Each node in the distributed P2P network can participate in the validation procedure. The first node who solves the puzzle can append the validated block to the blockchain; this node is also called a *miner*. It then broadcasts the validation results in the whole blockchain system, consequently other nodes validating and updating the new results in the blockchain. A small portion of bonus will then be given to this node as a compensation for solving the puzzle.

a) Discrepancy solution: In a distributed system, multiple nodes may validate blocks nearly at the same time. Meanwhile, the network latency can somehow result in bifurcated (or forked) chains at the same time. To solve the discrepancy, most of existing blockchain systems typically maintain the longest chain as the valid chain because the longest chain implies the most tolerant of being compromised by adversaries. If so, a shorter chain is automatically deserted (i.e., the blue dashed-line box as shown in Fig. 2) and the future validation work will continue on the longest chain.

b) Trustfulness of PoW: The trustfulness of PoW is based on the assumption that a majority of blockchain nodes is trustful. Generally, 51% of computational capability is regarded as the threshold of PoW being tolerant of malicious attacks. The incentive mechanisms can encourage miners to be honest against compromising. Meanwhile, solving the puzzle typically requires extensive computing power. The probability of solving the puzzle at a miner is often proportional to the computational capability and resource of a miner [21].

TABLE I
TAXONOMY OF TYPICAL CONSENSUS ALGORITHMS

	Probabilistic Consensus	Deterministic Consensus
Consensus procedure	Saving first and then consenting	Consenting first and then saving
Bifurcation (fork)	Yes	No
Arbitration mechanism	Choosing the longest chain when there are multiple forked chains	Voting to solve discrepancy through multiple communication-rounds
Adversary tolerance	< 50% computing or stakes	< 1/3 voting nodes
Complexity	High computational-complexity	High network-complexity
Examples	PoW, PoS, DPOS	PBFT and PBFT variants, Tendermint

Fig. 3. Working flow of blockchains.

PoW schemes require extensive computation to solve the puzzle, thereby resulting in the extensive energy consumption. Unlike PoW, PoS requires the proof of ownership to validate the trustfulness of a block since the users with more cryptocurrencies (i.e., more stakes) are more trustful than those with fewer cryptocurrencies. In PBFT, each node who has the equal right to vote for the consensus will send its voting state to other nodes. After multiple rounds of voting procedure, the consensus reaches.

We roughly categorize typical consensus algorithms into two types: 1) probabilistic consensus algorithms and 2) deterministic consensus algorithms. Table I gives the taxonomy. Probabilistic consensus algorithms including PoW, PoS, and delegated POS (DPOS) typically first save the validated block to the chain and then seek the consensus of all the nodes while deterministic consensus algorithms first consent to the block and then saved the validated block to the chain. Moreover, probabilistic consensus algorithms often result in multiple bifurcate chains and the discrepancy is solved by choosing the longest chain. In contrast, deterministic consensus algorithms solve the discrepancy through multiple rounds of communications in the overlay network.

There are many attempts to improve incumbent consensus algorithms, such as Ripple [22], Algorand [23], Tendermint, proof of authority (PoA) [24], proof of elapsed time (PoET) [25]. Instead of choosing single consensus algorithm, there is a trend of integrating multiple consensus algorithms to fulfill the requirements from different applications.

3) Working Flow of Blockchains: We next show how a blockchain works in an example. Take a money transfer as an example as shown in Fig. 3. Alice wants to transfer an amount of money to Bob. She first initiates the transaction at a computer through her Bitcoin (BTC) wallet (i.e., step ①). The transaction includes the information, such as the sender's wallet, the receiver's address, and the amount of money. The transaction is essentially signed by Alice's private key and can be accessible and verifiable by other users via Alice's public key thereafter. Then, the computer broadcasts the initiated transaction to other computers (or nodes) in the P2P network (i.e., step ②). Next, a validated transaction is then appended
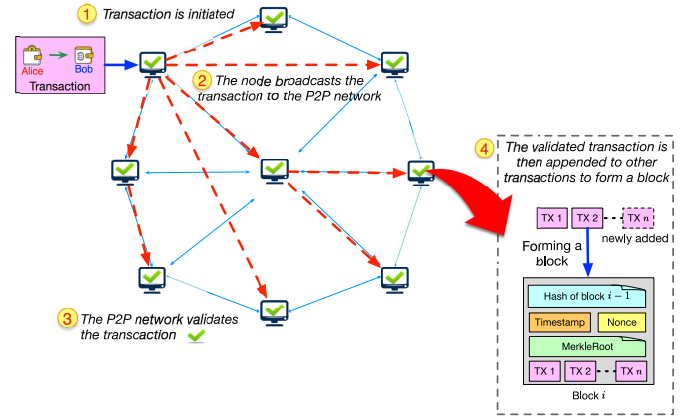
to the end of the chain of transactions consequently forming a new block in the blockchain once a miner successfully solves the puzzle (i.e., step ③). Finally, every node saves a replica of the updated blockchain when the validated transaction is appended to the blockchain (i.e., step ④).

B. Key Characteristics of Blockchain

In summary, blockchain technologies have the following key characteristics.

1) *Decentralization:* In traditional transaction management systems, the transaction validation has been conducted through a trusted agency (e.g., a bank or government). This centralization manner inevitably results in the extra cost, the performance bottleneck, and the single-point failure (SPF) at centralized service providers. In contrast, blockchain allows the transaction being validated between two peers without the authentication, jurisdiction, or intervention done by the central agency, thereby reducing the service cost, mitigating the performance bottleneck, lowering the SPF risk.

2) *Immutability:* A blockchain consists of a consecutively linked chain of blocks, in which each link is essentially an inverse hash point of previous block. Any modification on the previous block invalidates all the consequently generated blocks. Meanwhile, the root hash of the Merkle tree saves the hash of all the committed transactions. Any (even tiny) changes on any transactions generates a new Merkle root. Therefore, any falsification can be easily detected. The integration of the inverse hash point and the Merkle tree can guarantee the data integrity.

3) *Nonrepudiation:* Recall the fact that the private key is used to put the signature to the transaction, which can then be accessible and verified by others via the corresponding public key. Therefore, the crytographically signed transaction cannot be denied by the transaction initiator.

4) *Transparency:* For most of public blockchain systems (like BTC and Ethereum), every user can access and interact with the blockchain network with an equal right. Moreover, every new transaction is validated and saved

in the blockchain, consequently being available for every user. Therefore, the blockchain data is essentially transparent to every user who can access and verify the committed transactions in the blockchain.

5) *Pseudonymity:* Despite the transparency of blockchain data, blockchain systems can preserve a certain level of the privacy via making blockchain addresses anonymous. For example, the work of [26] presents an application of blockchain to preserve the privacy of personal data. However, blockchain can only preserve the privacy at a certain level since blockchain addresses are essentially traceable by inference [8]. For example, it is shown in [27] that the analysis of blockchain data can help to detect fraud and illegal transactions. Therefore, blockchain can only preserve the pseudonymity instead of full privacy.

6) *Traceability:* Each transaction saved in the blockchain is attached with a timestamp (recorded when the transaction occurs). Therefore, users can easily verify and trace the origins of historical data items after analyzing the blockchain data with corresponding timestamps.

C. Smart Contract

Smart contracts are a great advance for blockchain technology [28]. In 1990s, smart contracts were proposed as a computerized transaction protocol that executes the contractual terms of an agreement [29]. Contractual clauses that are embedded in smart contracts will be enforced automatically when a certain condition is satisfied (e.g., one party who breaches the contract will be punished automatically).

Blockchains are enabling smart contracts. Essentially, smart contracts are implemented on top of blockchains. The approved contractual clauses are converted into executable computer programs. The logical connections between contractual clauses have also been preserved in the form of logical flows in programs (e.g., `if-else-if` statement). The execution of each contract statement is recorded as an immutable transaction stored in the blockchain. Smart contracts guarantee appropriate access control and contract enforcement. In particular, developers can assign access permission for each function in the contract. Contract enforcement ensures that the contract execution is deterministic. Once any conditions in a smart contract are satisfied, the triggered statement will automatically execute the corresponding function in a predictable manner. For example, Alice and Bob agree on the penalty of violating the contract. If Bob breaches the contract, the corresponding penalty (as specified in the contract) will be automatically paid from Bob's deposit.

The whole life cycle of smart contracts consists of four consecutive phases as illustrated in Fig. 4.

1) *Creation* of smart contracts. Several involved parties first negotiate on the obligations, rights and prohibitions on contracts. After multiple rounds of discussions and negotiations, an agreement can reach. Lawyers or counselors will help parties to draft an initial contractual agreement. Software engineers then convert this agreement written in natural languages into a smart contract
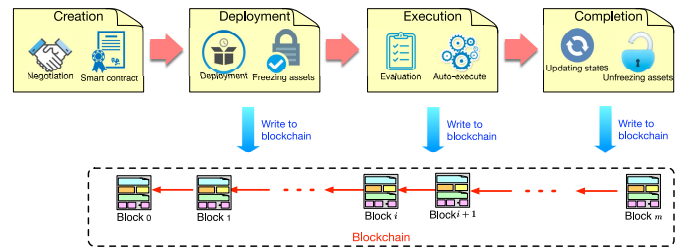

Fig. 4. Life cycle of smart contracts consisting of four consecutive phases: creation, deployment, execution, and completion.

written in computer languages including declarative language and logic-based rule language [30]. Similar to the development of computer software, the procedure of the smart contract conversion is composed of design, implementation, and validation (i.e., testing). It is worth mentioning that the creation of smart contracts is an iterative process involving with multiple rounds of negotiations and iterations. Meanwhile, it is also involved with multiple parties, such as stakeholders, lawyers, and software engineers.

2) *Deployment* of smart contracts. The validated smart contracts can then be deployed to platforms on top of blockchains. Contracts stored on the blockchains cannot be modified due to the immutability of blockchains. Any emendation requires the creation of a new contract. Once the smart contracts are deployed on blockchains, all the parties can access the contracts through the blockchains. Moreover, digital assets of both involved parties in the smart contract are locked via freezing the corresponding digital wallets [31]. For example, the coin transfers (either incoming or outgoing) on the wallets relevant to the contract are blocked. Meanwhile, the parties can be identified by their digital wallets.

3) *Execution* of smart contracts. After the deployment of smart contracts, the contractual clauses have been monitored and evaluated. Once the contractual conditions reach (e.g., product reception), the contractual procedures (or functions) will be automatically executed. It is worth noting that a smart contract consisting of a number of declarative statements with logical connections. When a condition is triggered, the corresponding statement will be automatically executed, consequently a transaction being executed and validated by miners in the blockchains [32]. The committed transactions and the updated states have been stored on the blockchains thereafter.

4) *Completion* of smart contracts. After a smart contract has been executed, new states of all involved parties are updated. Accordingly, the transactions during the execution of the smart contracts as well as the updated states are stored in blockchains. Meanwhile, the digital assets have been transferred from one party to another party (e.g., money transfer from the buyer to the supplier). Consequently, digital assets of involved parties have been unlocked. The smart contract has completed the whole life cycle.

TABLE II
COMPARISONS OF BLOCKCHAIN SYSTEMS

	Public	Private	Consortium
Decentralization	Decentralized	Centralized	Partially Decentralized
Immutability	Immutable	Alterable	Partially Immutable
Non-repudiation	Non-refusable	Refusable	Partially Refusable
Transparency	Transparent	Opaque	Partially Transparent
Traceability	Traceable	Traceable	Partially Traceable
Scalability	Poor	Superior	Good
Flexibility	Poor	Superior	Good
Permission	Permissionless	Permissioned	Permissioned
Consensus	PoW, PoS	Ripple	PBFT, PoA, PoET
Examples	Bitcoin [34], Ethereum [35]	GemOS [36], Multichain [37]	Hyperledger [38] Ethereum [35]

It is worth mentioning that during deployment, execution and completion of a smart contract, a sequence of transactions has been executed (each corresponding to a statement in the smart contract) and stored in the blockchain. Therefore, all the three phases need to write data to the blockchain as shown in Fig. 4.

D. Taxonomy of Blockchain Systems

We classify blockchain systems into three types: 1) public blockchains; 2) private blockchains; and 3) consortium (or community) blockchains [38]. Most digital currencies such as BTC (i.e., the ticker symbol of BTC cryptocurrency) and ETH (i.e., the ticker symbol of Ethereum cryptocurrency) are implemented on public blockchains, thereby being accessible by anyone in the P2P network. Differently, private blockchains can be managed or controlled by a single organization while consortium blockchains sit in limbo between public and private blockchains. Table II presents a comparison of three types of blockchains.

In particular, we summary the comparison among public, private, and consortium blockchains in the following aspects.

1) *Key Characteristics:* Public blockchains are fully decentralized while private and consortium blockchains are partially decentralized or fully controlled by a single group or multiple groups. Moreover, it is nearly impossible to tamper transactions in public blockchains as every node keeps a replica of the blockchain (containing all the transactions) while the dominant organization or multiple parties of consortium and private blockchains can modify the blockchain. Similarly, public blockchains can fully ensure the nonrepudiation, transparency, and traceability of transactions while private and consortium blockchains cannot or can only partially ensure these properties.

2) *Scalability:* Although public blockchains can guarantee the decentralization, immutability, transparency, nonrepudiation, and traceability, the merits are obtained in the cost of low transaction-validation rate, high latency and extra storage space consumption, consequently limiting the scalability of public blockchains. Compared with public blockchains, private and consortium blockchains have a better scalability since blockchains are fully controlled by a single group or multiple organizations and the consensus can be easily reached.

3) *Flexibility:* Similarly, public blockchains have the less flexibility than private and consortium blockchains since configurations of private and consortium blockchains are more adjustable.

4) *Permission:* Permission refers to consent or authorization to access the blockchains. In public blockchains, public participation is allowed, thereby being permissionless. However, private and consortium blockchains can allow one or more users to access and interact with blockchains with different permission levels. For example, some users can only read the blockchain data while others can either read or initiate transactions.

5) *Consensus:* Public blockchains usually use PoW and PoS as the consensus algorithms, which are Byzantine-failure tolerant while resulting in extensive resource consumption. Private blockchains can easily achieve the consensus among the authenticated users. Typical consensus algorithms used for private blockchains include PBFT, PoA, and PoET. Moreover, consortium blockchains are a hybrid type of public blockchains and private blockchains. In particular, Ripple [22] is a variant of PBFT typically used for consortium blockchains.

6) *Exemplary Platforms:* BTC [33] and Ethereum [34] are two typical public blockchain platforms, which are mainly used for digital currency. With regard to private blockchains, GemOS [35] is a private blockchain platform for healthcare and supply chain. In addition, MultiChain [36] is an open source platform granting the implementation of private blockchains. As for consortium blockchains, Hyperledger [37] is developing business consortium blockchain frameworks. Moreover, Ethereum also provides tools for building consortium blockchains [39].

IV. CONVERGENCE OF BLOCKCHAIN AND IoT

In this section, we first discuss the opportunities of integrating blockchain with IoT in Section IV-A. We then present the architecture of the integration of blockchain and IoT (namely BCoT) in Section IV-B. We next discuss the deployment issues on BCoT in Section IV-C.

A. Opportunities of Integrating Blockchain With IoT

As summarized in Section II-B, IoT systems are facing many challenges, such as heterogeneity of IoT systems, poor interoperability, resource constraints of IoT devices, and privacy and security vulnerabilities. Blockchain technologies
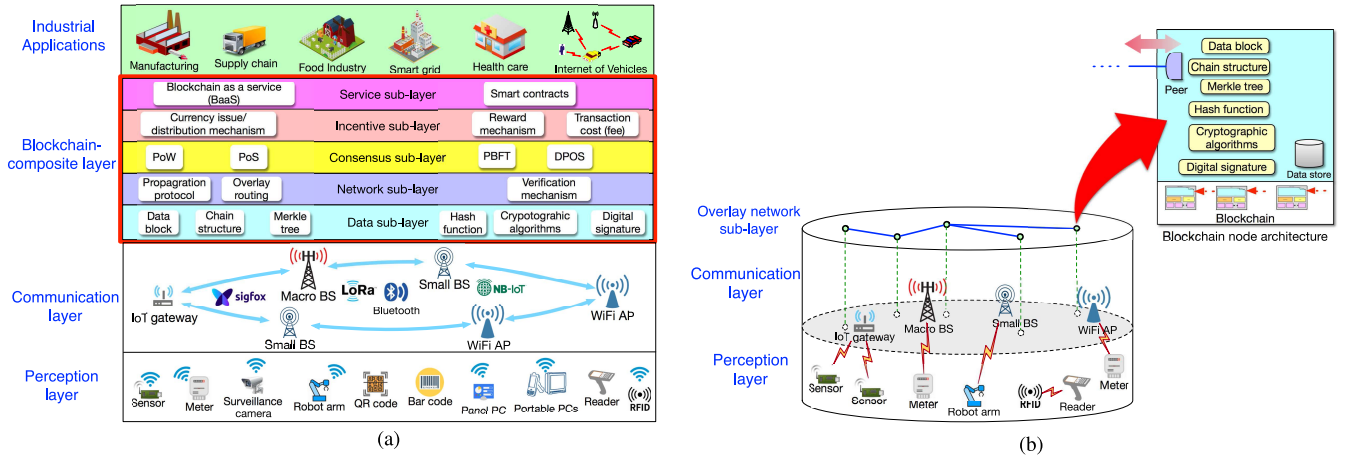
Fig. 5. Overview of BCoT architecture. (a) Blockchain-composite layer. (b) P2P overlay network and blockchain node architecture.

can complement IoT systems with the enhanced interoperability and the improved privacy and security. Moreover, blockchain can also enhance the reliability and scalability of IoT systems [6]. In short, we name such integration of blockchain with IoT as BCoT. BCoT has the following potential benefits in contrast to incumbent IoT systems.

1) *Enhanced interoperability* of IoT systems. Blockchain can essentially improve the interoperability of IoT systems via transforming and storing IoT data into blockchains. During this procedure, heterogeneous types of IoT data are converted, processed, extracted, compressed and finally stored in blockchains. Moreover, the interoperability also exhibits in easily passing through different types of fragmented networks since blockchains are established on top of the P2P overlay network that supports universal Internet access.

2) *Improved security* of IoT systems. On one hand, IoT data can be secured by blockchains since they are stored as blockchain transactions which are encrypted and digitally signed by cryptographic keys (e.g., elliptic curve digital signature algorithm (ECDSA) [40]). Moreover, the integration of IoT systems with blockchain technologies (like smart contracts) can help to improve the security of IoT systems by automatically updating IoT device firmwares to remedy vulnerable breaches thereby improving the system security [41].

3) *Traceability* and *Reliability* of IoT data. Blockchain data can be identified and verified anywhere and anytime. Meanwhile, all the historical transactions stored in the blockchains are *traceable*. For example, the work of [42] has developed a blockchain-based product traceability system, which provide suppliers and retailers with traceable services. In this manner, the quality and originality of the products can be inspected and verified. Moreover, the immutability of blockchains also assures the reliability of IoT data since it is nearly impossible to alter or falsify any transactions stored in blockchains.

4) *Autonomic* interactions of IoT systems. Blockchain technologies can grant IoT devices or subsystems to interact with each other automatically. For example, the work of [43] proposes distributed autonomous

corporations (DACs) to automate transactions, in which there are no traditional roles like governments or companies involved with the payment. Being implemented by smart contracts, DACs can work automatically without human intervention consequently saving the cost.

B. Architecture of Blockchain of Things

We propose the architecture of BCoT as shown in Fig. 5. In this architecture, the blockchain-composite layer plays as a middleware between IoT and industrial applications. This design has two merits: 1) offering an abstraction from the lower layers in IoT and 2) providing users with blockchain-based services. In particular, the blockchain-composite layer hides the heterogeneity of lower layers (like perception layer and communication layer in IoT). On the other hand, the blockchain-composite layer offers a number of blockchain-based services, which are essentially application programming interfaces (APIs) to support various industrial applications. As a result, the difficulty of developing industrial applications can also be lowered down due to the abstraction achieved by the blockchain-composite layer.

In particular, the blockchain-composite layer consists of five sublayers as shown in Fig. 5(a) (from bottom to up).

1) *Data Sublayer:* Collects the IoT data from the lower layers (e.g., perception layer) and wraps up the encrypted data with digital signature via asymmetric cryptographic algorithms and hash functions. These consecutively connected data blocks then form the blockchain after the distributed validation. Different blockchain platforms may choose different cryptographic algorithms and hash functions. For example, BTC blockchain chooses SHA-256 as the hash function and ECDSA as the signature algorithm.

2) *Network Sublayer:* It is essentially an overlay P2P network running on top of the communication layer. The overlay network consists of either virtual or physical links connecting nodes in the underlying communication networks (i.e., wired/wireless communication networks). One node only simply broadcasts the block of transactions to its connected peers. Once receiving the
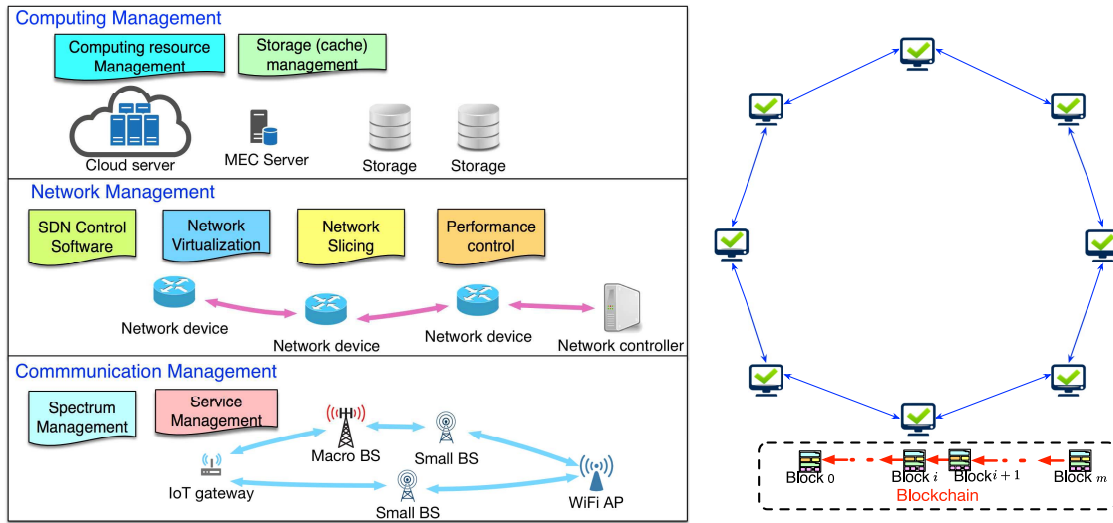
Fig. 6. Deployment scenario of BCoT.

block of transactions, other peers will verify it locally. If it is valid, the block will be further propagated to other nodes through the overlay network.

3) *Consensus Sublayer:* It is mainly involved with the distributed consensus for the trustfulness of a block. The consensus can be achieved by various consensus algorithms like PoW, PoS, PBFT, and DPOS (as explained in Section III-A2). It is worth mentioning that block propagation mechanisms (such as relay network propagation and advertisement-based propagation [20]) are the prerequisite for the distributed consensus protocols.

4) *Incentive Sublayer:* It is responsible for the following tasks: a) digital currency issuing; b) digital currency distribution; c) designing reward mechanism (especially for miners); and d) handling transaction cost. In particular, it is important to design appropriate monetary policy of digital currency (i.e., money creation and distribution), distribute rewards to participants who contribute to distributed consensus (i.e., mining).

5) *Service Sublayer:* It provides users with blockchain-based services for various industrial sectors include manufacturing, logistics, supply chains, food industry and utilities. The blockchain as a service (BaaS) can be achieved by smart contracts, which can be automatically triggered when a special event occurs. For example, a payment contract is automatically executed when a product is well received by a consumer.

It is worth mentioning that the network sublayer that is established on top of the communication layer is the abstraction of underneath communication networks, consequently offering a universal network access across different networks as shown in Fig. 5(b). Fig. 5(b) also shows the architecture of a blockchain node, which essentially includes blockchain data and other elements in the data sublayer.

C. Deployment of BCoT

The realistic deployment of BCoT is of great importance. However, due to the constraints of IoT devices, it is challenging to store the whole blockchain at IoT devices. In

particular, there are two modes to store the blockchain data [6]: 1) *full storage*, in which the entire blockchain is stored and 2) *partial storage*, in which only a subset of data blocks are stored locally. Accordingly, we name the nodes with full storage of blockchain data as *full nodes* and the nodes with partial storage of blockchain data as *lightweight nodes*. In practice, a full node can be a cloud server or an edge server with adequate computing resources since it requires a large storage space to save the entire blockchain (e.g., the whole BTC blockchain occupies nearly 185 GB at the end of September 2018 according to the statistic report)[1] and strong computing capability of solving consensus puzzles (i.e., mining). On the other hand, resource-constrained IoT devices (e.g., sensors, IoT objects) can be lightweight nodes that can validate the trustfulness of a transaction without downloading or saving the whole blockchain (i.e., only saving partial blockchain data such as hash values). It is worth mentioning that the lightweight nodes highly rely on the full nodes.

Fig. 6 presents a possible deployment scenario of BCoT, in which cloud servers and edge servers may store the whole blockchain (or partial blockchain) data while IoT devices may only save the partial blockchain data. In addition to the deployment of BCoT, there are also several possible interaction manners between IoT and blockchain [8]: 1) direct interaction between IoT and blockchain, in which IoT devices can directly access blockchain data saved at edge servers co-located with IoT gateways, Macro BSs (MBSs) or small BS; 2) direct interaction between IoT nodes, in which IoT nodes can directly exchange/access partial blockchain data via D2D links; and 3) hybrid interaction of cloud and edge servers with IoT devices, in which IoT devices can interact with blockchain data through edge/cloud servers.

There are several initiatives addressing the configuration and initialization of blockchain at edge servers or at IoT devices. For example, Raspnode[2] is a project mainly for installing

---

[1]https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/

[2]http://raspnode.com/

Fig. 7. Blockchain for 5G beyond networks in IoT.

BTC and other blockchains at Raspberry Pi micro computers. EthArmbian[3] offers the customized Ubuntu Linux image for ARM devices, each of which can serve as an Ethereum node. Despite these initiatives, most of IoT devices are still lightweight nodes due to the limited storage.

V. BLOCKCHAIN FOR 5G BEYOND IN IOT

Although blockchain technology is promising to IoT, there are still many research issues to be addressed before the integration of blockchain with IoT, especially for the next-generation networks (i.e., 5G-beyond or 6G networks), which play a critical role in constructing the infrastructure for blockchains. Fig. 7 illustrates the potentials brought by blockchain to 5G-beyond networks in the perspectives from communications, network management, and computing management. We explain them in details as follows.

A. Blockchain for Communications

The growing demands of mobile data traffic are driving the more efficient resource management in the 5G communication systems. For example, radio spectrum is one of the most important resources [44]. Radio spectrum management typically includes spectrum auction and spectrum sharing. It is shown in the latest speech [45] given by Federal Communications Commission (FCC) commissioner Rosenworcel that blockchain technology could be used to achieve the dynamic and secure spectrum management in 5G and 5G beyond (also known as 6G) communication systems [46], [47]. The benefits of using blockchains for 5G-beyond networks lie in the secure and traceable transaction-management without the necessity of a central intermediary, consequently saving the management cost. Yrjölä [48] gave several use cases to illustrate that using blockchain technology can benefit radio spectrum sharing in terms of trustfulness, consensus, and cost reduction. Moreover, Kotobi and Bilen [49] put forth a blockchain-based protocol

[3]http://raspnode.com/

to secure spectrum sharing between primary users and cognitive users in wireless communication systems. In addition, blockchain may potentially help to share link conditions to multiple IoT nodes with privacy preservation consequently improving spectral efficiency via traffic optimization [50].

In addition to the radio spectrum management, blockchains also have the potentials to provide users with the improved mobile services. For example, 5G networks typically consist of a number of fragmented heterogeneous networks. Blockchains that are built on top of the network layer can help to integrate different networks with the provision of seamless access between different networks. Moreover, smart contracts can automate the procedure of provisions and agreements between network operators and subscribers while operational cost can be greatly saved [51]. The work of [52] also shows that a blockchain-based system can help operating nodes to improve their operational and service capabilities. In the future, the synthesis of blockchains and BDA can help service providers to extract valuable insights from transactions of subscribers and offer the better services for users.

B. Blockchain for Network Management

Recently, software defined networking (SDN) technology can bestow the flexibility and scalability for distributed IoT [53]. However, it is shown in [54] that the centralization of SDN can also result in the single-point-of-failure. Moreover, incumbent SDN devices (such as gateways) are also incapable of conducting computational-intensive analysis on data traffic. The integration of blockchain technology with SDN can overcome the disadvantages of SDN. For example, the work of [55] proposes a secure blockchain-based SDN framework for IoT. In particular, a blockchain-based scheme has been developed to update the flow rule table in a secure way without the necessity of the intermediary. In addition, blockchain can also help to secure the network management of network function visualization (NFV). In particular, it is shown in [56] that the integration of blockchain with NFV can ensure that the configuration of NFV is immutable, auditable,

nonrepudiable, consistent and anonymous. A prototype of the proposed architecture was also developed and implemented in this paper.

In addition to SDN and NFV, the appearance of network slicing technologies [57] brings the agility and flexibility of networks to support different functional and performance requirements. As mentioned in Section IV, different industrial sectors have diverse application demands on blockchains. For example, a single blockchain is typically used in digital-currency like applications while an enterprise may maintain several blockchains to serve for different purposes. In particular, four isolated blockchains are dedicate to enterprise resource planning (ERP), product lifecycle management (PLM), manufacturing execution systems (MESs), and customer relationship management (CRM), respectively, [58]. Network slicing can essentially offer a solution to the diverse demands of blockchain applications in MEC. For example, each of network instances can be created for the provision of a specific blockchain service on top of network slicing and network visualization. However, it is necessary to optimize and allocate both network and computing resources to fulfill the diverse demands in the composite environment of MEC and cloud computing. Moreover, the integration of blockchain and network slicing technologies can also support the reliable content sharing in content-centric networks (CCNs) [59] and privacy preservation in data sharing in 5G networks [60].

C. Blockchain for Computing Management

Due to the resource constraints of IoT devices, massive IoT data has been typically uploaded to remote cloud servers for further processing. However, the pure cloud-based computing paradigm also causes the network traffic bottlenecks, long latency, context unawareness, and privacy exposure [61], thereby limiting the scalability of IoT. Recently, MEC [62] is becoming a crucial complement to cloud computing by offloading computing tasks from distant cloud servers to MEC servers typically installed at IoT gateways, WiFi APs, Macro BS, and Small BS, which are close to users. In this manner, the context-aware, latency-critical, and less-computing-intensive tasks can be migrated from remote cloud servers to local MEC servers, thereby improving the response, privacy-preservation, and context-awareness.

Blockchain technology has been applied in a variety of fields due to its capability of establishing trust in a decentralized fashion. There are still a number of issues needed to be solved before MEC can be used in BCoT [63]. In contrast to cloud servers with strong computing capability and extensive storage space, mobile edge servers usually have inferior capability. Moreover, mobile edge servers are heterogeneous in terms of computing capability, main memory, storage space, and network connection. As a result, mobile edge servers cannot accommodate the computational demands alone. For example, a mobile edge server may not be able to solve the consensus puzzle in blockchains while a cloud server can serve for this goal. Therefore, it is worthwhile to investigate the orchestration of MEC and cloud computing for the provision of blockchain services [64].

D. Orchestration of Cloud and Edge Computing With Blockchain

During the orchestration of cloud and edge computing with blockchain, there are several challenges including computational task offloading and incentivizing resource sharing.

Offloading the computational tasks to edge servers can significantly reduce the delay. Therefore, it is crucial to conduct edge-cloud interoperation [65]. Nevertheless, it can cause a performance bottleneck and a single-point-of-failure if all the nodes offload their tasks to the same MEC server. The work of [66] presents an offloading method with consideration of load balancing among multiple MEC servers. Meanwhile, it is worthwhile to investigate how to incentivize both edge severs and cloud servers. For example, [67] presents a contract-match approach to allocate computational resource and assign tasks while incentivizing edge severs and cloud servers effectively. Moreover, it is challenging to design an optimal solution to the offloading tasks with consideration of spectrum, computation, and energy consumption together. The work of [68] essentially provides a solution to optimize the offloading energy consumption with consideration of feasible modulation schemes and tasks scheduling. However, most of existing studies only consider a task is either done at an edge sever or at a cloud. In realistic application, a task can be partitioned into multiple subtasks with task dependency and those subtasks can be either executed at the edge server or at the cloud server. It is worthwhile to investigate the task partition with consideration of subtask dependency in blockchains in the future.

VI. APPLICATIONS OF BLOCKCHAIN OF THINGS

There is a growing trend in applying blockchain in IoT since blockchain technologies can help to overcome the challenges of IoT. We then provide an overview of the applications of BCoT. It is worth mentioning that there is a wide diversity of applications of blockchains [ranging from smart manufacturing to IoV and unmanned aerial vehicles (UAVs)]. In this paper, we mainly focus on the industrial applications of BCoT. We roughly categorize the applications of BCoT into six types as shown in Fig. 8.

A. Smart Manufacturing

The manufacturing industry is experiencing an upgrading from automated manufacturing to "smart manufacturing" [69]. BDA on manufacturing data plays an important role during this upgrading process. Massive data is generated during every phase of the product life cycle consisting of product designing, raw material supply, manufacturing, distribution, retail, and after-sales service. However, the manufacturing data is highly fragmented, consequently leading to the difficulty in data aggregation and data analytics. BCoT can address the interoperability issue by interconnecting IoT systems via P2P network and allowing data sharing across industrial sectors. For example, several distributed blockchains can be constructed to serve for different sectors and each blockchain is serving for a sector or more than one sector.

BCoT can also improve the security of smart manufacturing. One of major bottlenecks limiting the upgrading of factories
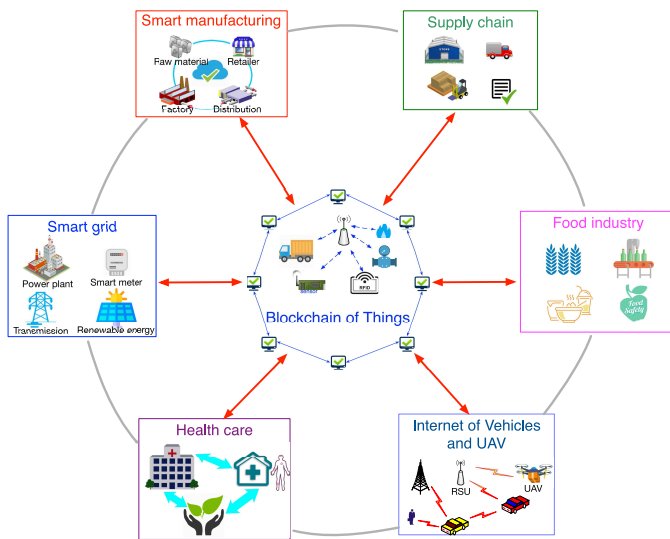
Fig. 8. Applications of BCoT.

is that the IoT systems have been maintained in a centralized way. For example, IoT firmware needs to be upgraded regularly to remedy security breaches. However, most of the firmware updates are downloaded from a central server and then are manually installed at IoT devices. It is expensive and in-efficient to install and upgrade the firmware updates in distributed IoT. The work of [41] presents an automatic firmware upgrading solution based on smart contract and blockchains. In particular, smart contracts describing the firmware upgrading manners (e.g., when and where to upgrade firmwares) are deployed across the whole industrial network. Devices can then download and install the firmware hashes via smart contracts being automatically executed. As a result, the security maintenance cost can be greatly saved. In addition, a decentralized blockchain-based automatic production platform was proposed in [70] to offer a better security and privacy protection than conventional centralized architecture.

B. Supply Chain Management

A product often consists of multiple parts provided by different manufacturers across countries. However, some forged (or low-quality) parts may seep into the supply chain. It is quite expensive to apply anti-fraud technologies in every part of a product. The integration of blockchain and IoT can solve this problem. In particular, every part will be associated with a unique ID with the creation. Meanwhile, an immutable timestamp is also attached with this ID. The identification of every part can then be saved into a blockchain, which is tamper-resistant and traceable. For example, the work of [71] shows that the part ownership of a product can be authenticated through a blockchain-based system. Moreover, the work of [72] presents a traceability ontology with the integration of IoT and blockchain technologies based on Ethereum blockchain platform. The proposed framework has demonstrated to guarantee data provenance of supply chain.

On the other hand, BCoT can also be used to reduce the costs in after-sale services in the supply chain management.

The work of [73] shows a user case of a motor insurance, in which the settlement of claims can be automated via smart contracts based on blockchains, thereby improving the efficiency and reducing the claim-processing time. Moreover, it is shown in [74] that integrating blockchain with IoT can help to reduce the cost, fasten the speed and reduce the risk in the supply chain management. Furthermore, a blockchain-based machine learning platform [75] was proposed to secure the data sharing among different enterprises to improve the quality of customer service.

C. Food Industry

BCoT can enhance the visibility of the product life cycle especially in food industry. In particular, the traceability of food products is a necessity to ensure food safety. However, it is challenging for the incumbent IoT to guarantee the food traceability in the whole food supply chain [76]. For example, a food company may be provisioned by a number of suppliers. The traceability requires digitizing the information of raw materials from sources to every sector of food manufacturing. During this procedure, blockchain technologies can ensure the traceability and the provenance of food industry data.

There are several proposals in this aspect. For example, the work of [77] proposed to use RFID and blockchain technology to establish a supply chain platform from agriculture to food production in China. This system has demonstrated to guarantee the traceability of food supply chain data. Meanwhile, the work of [78] shows that blockchain technologies can help to improve food safety via the provision of the traceable food products. Moreover, it is shown in [79] that the integration of blockchain in food supply chain can allow customers to track the whole process of food production. Authors also gave a user case of using blockchain for the organic coffee industry in Colombian. Furthermore, [80] proposes a food safety traceability system based on the blockchain and electronic product code (EPC) IoT tags. In particular, this system can prevent data tampering and privacy exposure via smart contracts. A prototype of the proposed architecture has been implemented to demonstrate the effectiveness.

D. Smart Grid

The appearance of distributed renewable energy resources is reshaping the role of energy consumers from pure consumers to *prosumers* who can also generate energy (e.g., from renewable energy resources) in addition to consuming energy only [81]. Energy prosumers who have extra energy can sell it to other consumers. We name the energy trading between a prosumer and a consumer (i.e., peers) as P2P energy trading. However, it is challenging to ensure the secured and trusted energy trading between two trading parties in the distributed environment.

The appearance of blockchain technology brings the opportunities to ensure the secured P2P energy trading. Some of recent studies proposed using blockchain technologies to tackle these challenges. For example, the work in [82] developed a secure energy trading system based on consortium

blockchains. This system can greatly save the trading cost without going through a central broker via the distributed consensus of blockchains. Moreover, Aitzhan and Svetinovic [83] developed a decentralized energy-trading system based on blockchain technology. This system demonstrated the effectiveness in protecting confidential energy-trading transaction in decentralized smart grid systems. Furthermore, the work of [84] proposed a blockchain-based mechanism to provide a secure and transparent energy demand-side management on smart grid.

E. Health Care

Health care becomes one of the major social-economic problems due to the aging population; it poses new challenges in traditional healthcare services because of the limited hospital resources. The recent advances in wearable health-care devices as well as BDA in health-care data bring the opportunities in promoting the remote health-care services at home or at clinic. As a result, the burden of the hospital resources can be potentially released [85]. For example, senior citizens staying at their homes are wearing the health-care devices at their bodies. These wearable devices continuously measure and collect health-care data including heart beat rate, blood sugar, and blood pressure readings. Doctors and health-care teams can access health-care data at any time and anywhere via the health-care networks. However, assessing health-care data also brings privacy and security concerns. The vulnerability of health-care devices and the heterogeneity of health-care networks pose the challenges in preserving privacy an ensuring security of health-care data.

Incorporating blockchains into health-care networks can potentially overcome the challenges in privacy preservation and security assurance of health-care data. For example, the work of [86] shows that using blockchain technology can protect health-care data stored in cloud servers. Meanwhile, Griggs *et al.* [87] developed a blockchain-based system to assure the private health-care data management. In particular, the health-care data generated by medical sensors can be automatically collected and transmitted to the system via executing smart contracts, consequently supporting the real-time patient monitoring. During the whole procedure, the privacy can be preserved via underneath blockchains. Moreover, the work of [88] proposed a blockchain-based solution to manage individual health-care data and support data-sharing across different hospitals, medical centers, insurance companies and patients. During the whole process, the privacy and security of health-care data can be assured. Furthermore, Sun *et al.* [89] put forth an attribute-based signature scheme in decentralized health-care blockchain systems. On one hand, this scheme can verify the authenticity of health-care data and identification of the health-care data owner. On the other hand, this scheme can also preserve the privacy of the health-care data owner. The recent work [90] presents an in-home therapy management framework integrating IoT and blockchain-based MEC scheme to provide secrecy and anonymity assurance. The experimental results on a prototype demonstrate the effectiveness of the proposed system.

F. Internet of Vehicles and Unmanned Aerial Vehicles

IoV essentially integrates vehicle-to-vehicle networks, vehicle-to-roadside networks, vehicle-to-infrastructure networks, and vehicle-to-pedestrian networks. The decentralization, heterogeneity and nontrustworthiness of IoV pose the challenges in securing message-transmission and transaction-execution. Integrating blockchain with IoV can tackle the above challenges. For example, the work of [91] developed a trust-management platform in IoV on top of blockchains. In particular, the trustworthiness of messages can be validated via PoW/PoS consensus executed by roadside units (RSUs). Moreover, blockchain technologies can be used to protect both the energy and information interactions between electric vehicles [92] and hybrid electric vehicles in smart grids [93], [94]. In the future, incorporating artificial intelligence, MEC, and blockchain can further optimize the resource allocation in IoVs [95].

Recently, UAVs communication networks can compensate in-sufficient coverage of wireless communication networks [96]. Meanwhile, UAVs can also be used to deliver product items [97] and acquire real-time traffic flow data [98]. Moreover, the recent study of [99] also shows that UAVs can be used to support content-centric networking and MEC. However, it is challenging to assure the trustworthiness in decentralized nontrusted UAV-networks and restrict the misbehaving UAVs [102]. The integration of blockchain technology with UAV-networks can guarantee the mutual-confidence among UAVs. The work of [100] developed an autonomous platform based on Ethereum blockchain to provide the trust-management of UAVs. Moreover, IBM [101] recently applied for a patent to develop a blockchain-based system to preserve privacy and assure security of UAV data. In particular, blocks in blockchains will store the information related to UAVs including model type, manufacturer, proximity to restricted region. Consequently, the misbehavior of UAVs can be detected and identified in time.

Summary: Table III summarizes major BCoT applications. In particular, it is shown in Table III that incorporating blockchain with IoT can bring a number of benefits in the aforementioned applications. In summary, BCoT has merits like reducing the cost for trusted third party, assuring security, improving data traceability, and verifying the data authenticity and preserving privacy.

VII. OPEN RESEARCH ISSUES OF BLOCKCHAIN OF THINGS

Although the convergence of blockchain and IoT brings a number opportunities in upgrading the industry, there are many challenges to be addressed before the potentials of BCoT can be fully unleashed. In this section, we identify several major challenges in incorporating blockchain into IoT and discuss the potential solutions. Fig. 9 summarizes the open research issues for BCoT.

A. Resource Constraints

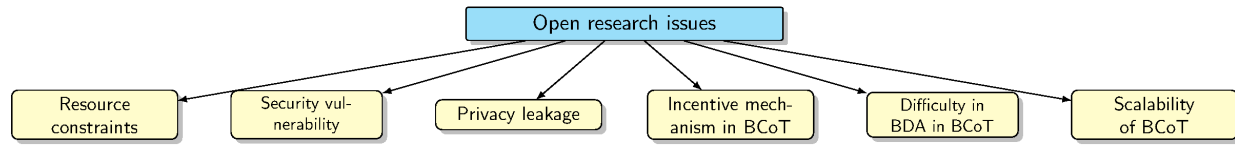Most of IoT devices are resource-constrained. For example, sensors, RFID tags and smart meters have inferior computing

Fig. 9. Open research issues for BCoT.

TABLE III
COMPARISON OF APPLICATIONS OF BCoT.

Application	Benefits
Smart manufacturing [42], [70], [71]	✓Improving interoperability
	✓Automating P2P business trading
	✓Reducing cost for trusted third party
Supply chain management [72]–[76]	✓Assuring data provenance
	✓Reducing the costs in after-sale services
	✓Mitigating the supply chain risk
Food industry [77]–[81]	✓Improving data traceability
	✓Enhancing food safety
Smart grid [82]–[85]	✓Securing energy trading
	✓Improving transparency
	✓Preserving privacy
Health care [86]–[91]	✓Assuring security
	✓Preserving privacy
	✓Verifying authenticity
IoV and UAVs [92]–[102]	✓Assuring trustworthiness of messages
	✓Securing energy-trading in electric vehicles
	✓Guaranteeing mutual-confidence among UAVs

capability, limited storage space, low battery power, and poor network connection capability. However, the decentralized consensus algorithms of blockchains often require extensive computing power and energy consumption. For example, PoW in BTC is shown to have high energy consumption [6]. Therefore, the consensus mechanisms with huge energy consumption may not be feasible to low-power IoT devices.

On the other hand, the bulky size of blockchain data also results in infeasibility of fully deploying blockchains across IoT. For example, the BTC blockchain size almost reaches 185 GB by the end of September 2018. It is impossible to fully store the whole blockchain at each IoT device. Meanwhile, the massive IoT data generated in nearly real time manner makes this status quo even worse. Moreover, blockchains are mainly designed for a scenario with the stable network connection, which may not be feasible for IoT that often suffers from the poor network connection of IoT devices and the unstable network due to the failure of nodes (e.g., battery depletion).

Potential Solutions: Incorporating MEC and cloud computing technologies into BCoT may potentially overcome resource constraints of IoT devices. For example, cloud servers or some MEC servers may serve as full nodes that store the whole blockchain data and participate in most of blockchain operations, such as initiating transactions, validating transactions (i.e., mining) while IoT devices may serve as lightweight nodes that only store partial blockchain data (even hash value of blockchain data) and undertake some less-computational-intensive tasks (such as initiating transactions) [103]. The orchestration of MEC and cloud computing becomes an important issue in the sense of allocating resource in BCoT [104].

B. Security Vulnerability

Although incorporating blockchain technologies into IoT can improve the security of IoT via the encryption and digital signature brought by blockchains, the security is still a major concern for BCoT due to the vulnerabilities of IoT systems and blockchain systems.

On one hand, there is a growing trend in deploying wireless networks into industrial environment due to the feasibility and scalability of wireless communication systems. However, the open wireless medium also makes IoT suffering from the security breaches, such as passive eavesdropping [105], jamming, and replaying attacks [106]. Moreover, due to the resource constraints of IoT devices, conventional heavy-weighted encryption algorithms may not be feasible to IoT [107]. In addition, it is also challenging to manage the keys (which are crucial to encryption algorithms) in distributed environment.

Meanwhile, blockchain systems also have their own security vulnerabilities such as program defects of smart contracts [20]. In particular, it is shown in [108] that the malicious users can exploit border gateway protocol (BGP) routing scheme to hijack blockchain messages, thereby resulting in the higher delay of block broadcasting. The work of [109] also shows that a decentralized autonomous organization (DAO) attack stole $50 million worth of Ethereum by leveraging the vulnerability of smart contracts.

Potential Solutions: Security vulnerabilities of BCoT can be remedied via either the security enhancement of IoT systems or loophole repairing of blockchain. For example, cooperative jamming scheme [110] was explored to improve the security of IoT systems while no extra hardware is required for existing IoT nodes. Meanwhile, [111] exploits key generations based on reciprocity and randomness of wireless channels in long range (LoRa) IoT network. In the perspective of repairing blockchain loopholes, there are also some advances. In particular, the recent work of [112] proposes a secure relaying-network for blockchains, namely SABRE, which can prevent blockchain from BGP routing attacks. Regarding DAO attacks, Corda and Stellar trade the expressiveness for the verifiability of smart contracts [113] so as to avoid DAO attacks.

C. Privacy Leakage

Blockchain technologies have some mechanisms to preserve a certain data privacy of transaction records saved in blockchains. For example, transactions are made in BTC via IP addresses instead of users' real identities thereby ensuring a certain anonymity. Moreover, one-time accounts are generated in BTC to achieve the anonymity of users. However, these protection schemes are not robust enough. For example, it is shown in [21] that user pseudonyms can be cracked via learning and inferring the multiple transactions associated with one common user. In addition, the full storage of transaction data on blockchain can also lead to the potential privacy leakage as indicated in [114].

Potential Solutions: Recently, mixed coins are proposed to confuse attackers so that they cannot infer the exact number of real coins spent by a transaction. However, recent study [115] demonstrates the weakness of the coin-mixed schemes via extensive realistic experiments based on Monero.[4] Moreover, the actual transaction can be deduced by leveraging the vulnerability of the coin-mixed schemes. The work of [114] presents a memory optimized and flexible blockchain data storage scheme, which can somewhat reduce the privacy leakage risk.

D. Incentive Mechanism in BCoT

An appropriate incentive mechanism is a benign stimulus to blockchain systems. For example, a number of BTCs will be rewarded to a miner who first solves the computationally difficult task. Meanwhile, a transaction in Ethereum will be charged with a given fee (i.e., gas) to pay the miners for the execution of contracts. Therefore, there are two issues in designing incentive mechanisms in blockchains: 1) the reward for proving (or mining) a block and 2) the compensation for processing a transaction (or a contract).

However, it is challenging to design a proper incentive mechanism for BCoT to fulfill the requirements of different applications. Take digital currency platforms as an example, where miners are keen on the price of digital currency. For instance, the BTC reward for a generated block will be halved every 210 000 blocks [116]. The reward decrement will discourage miners to contribute to the solution of the puzzle consequently migrating to other blockchain platforms. How to design a proper rewarding and publishing mechanism of digital currency is necessary to ensure the stability of blockchain systems.

Potential Solutions: On the other hand, the reputation and honesty is an impetus to users in private or consortium blockchain systems. Therefore, going beyond digital currency, reputation credits can be used as incentives in the scenarios like personal reputation systems [117], sharing economy [118], data provenance [119], and the medication supply chain [120]. The recent work [121] presents RepChain, which exploits the reputation of each node to develop the incentive mechanism.

[4]A private digital currency platform (https://getmonero.org/).

E. Difficulty in BDA in BCoT

There is a surge of big volume of IoT data generated in nearly real time fashion. The IoT data exhibits in massive volume, heterogeneity and huge business value. BDA on IoT data can extract hidden values and make intelligent decisions. However, it is challenging for apply conventional BDA schemes in BCoT due to the following reasons.

1) *Conventional BDA Schemes Cannot Be Applied to IoT Devices Due to the Resource Limitations:* Since IoT devices have inferior computing capability, the complicated BDA schemes cannot be deployed at IoT devices directly. Moreover, the bulky size of blockchain data also leads to the infeasibility of the local storage of blockchain data at IoT devices. Although cloud computing can address these issues, uploading the data to remote cloud servers can also result in the privacy-breach and the long-latency [122].

2) *It Is Difficult to Conduct Data Analytics on Anonymous Blockchain Data:* Blockchain technologies can protect data privacy via encryption and digital signature on data records. However, it often requires the data decryption before conducting data analytics. Nevertheless, the decryption process is often time-consuming thereby resulting in the inefficiency of data analytics [123]. It is challenging to design data analytics schemes on blockchain data without decryption.

Potential Solutions: MEC is serving as a crucial complement to cloud computing by offloading computing tasks from distant cloud servers to MEC in approximation to users. As a result, MEC can improve the response, privacy-preservation and context-awareness in contrast to cloud computing. Therefore, offloading BDA tasks to MEC servers can potentially solve the privacy-leakage and long latency issue of cloud computing with blockchain [124]. Regarding data analytics on anonymous blockchain data, there are some recent advances: 1) complex network-based community detection [125] to identify multiple addresses associated with an identical user; 2) feature extraction of transaction patterns of BTC blockchain data to identify payment relationships [126]; and 3) analysis of user accounts and operation codes on Ethereum to detect Ponzi fraud behavior [127].

F. Scalability of BCoT

The scalability of incumbent blockchains also limits the wide usage of blockchains in large-scale IoT. The scalability of blockchains can be measured by the *throughput* of transactions per second against the number of IoT nodes and the number of concurrent workloads [25], [113]. Many blockchain systems are suffering from the poor throughput. For example, it is shown in [128] that BTC can only process seven transactions per second. In contrast, VISA can process nearly 2000 transactions per second and PayPal has the throughput of 170 transactions per second [129], [130]. Conoscenti *et al.* [4] showed that BTC blockchain may not be suitable for IoT due to the poor scalability. In summary, the incumbent blockchain systems may not be suitable for the applications with a large volume of transactions especially for IoT.

Potential Solutions: There are two possible directions in improving the scalability of blockchains in IoT: 1) designing more scalable consensus algorithms and 2) constructing private or consortium blockchains for IoT. Regarding 1), we can choose the consensus-localization strategy to improve the throughput of transactions. Meanwhile, we may implement some new blockchain structures such as directed acyclic graph (DAG) [131] to allow the nonconflicting blocks from the side-chain to be assembled with the main chain, consequently reducing the cost for resolving bifurcation. In addition, we may consider integrating PoW with PBFT to improve the throughput of PoW similar to sharding protocol proposed in [132], in which less computational-extensive puzzle is first solved in PoW and consensus is then reached in multiple small groups.

Regarding 2), transactions in private and consortium blockchains can be processed much faster than public blockchains due to the fully controlled systems and the limited number of permitted users. Meanwhile, the consensus can also be easily reached in private and consortium blockchains. Moreover, the fully controlled blockchains also fulfill the requirement that an enterprise needs to have a control on different strategic sectors, e.g., ERP, MES, PLM, and CRM systems [58], [113]. Though there are some attempts, such as GemOS [35], Multichain [36], and Hyperledger [37], more mature private and consortium blockchain platforms serving for specific industrial sectors are still expected in the future.

VIII. CONCLUSION

The incumbent IoT systems are facing a number of challenges including heterogeneity, poor interoperability, resource constraints, and privacy and security vulnerability. The recent appearance of blockchain technologies essentially offers a solution to the issues with the enhanced interoperability, privacy, security, and traceability and reliability.

In this paper, we investigate integrating blockchain with IoT. We name such synthesis of blockchain and IoT as BCoT. We provide a comprehensive survey on BCoT. In particular, we first briefly introduce IoT and blockchain technology. We then discuss the opportunities of BCoT and depict the architecture of BCoT. We next outline the research issues in blockchain for next-generation networks. We further discuss the potential applications of BCoT and outline the open research directions in BCoT.

ACKNOWLEDGMENT

REFERENCES

[1] P. Lade, R. Ghosh, and S. Srinivasan, "Manufacturing analytics and industrial Internet of Things," *IEEE Intell. Syst.*, vol. 32, no. 3, pp. 74–79, May/Jun. 2017.

[2] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Kailua, HI, USA, Mar. 2017, pp. 618–623.

[3] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the Internet of Things," *Peer Peer Netw. Appl.*, vol. 10, no. 4, pp. 983–994, Jul. 2017. [Online]. Available: https://doi.org/10.1007/s12083-016-0456-1

[4] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Agadir, Morocco, Nov./Dec. 2016, pp. 1–6.

[5] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for Internet of Things security: A position paper," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 149–160, 2018.

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

[7] 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. 32979–33001, 2018.

[8] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2019. [Online]. Available: https://doi.org/10.1109/COMST.2018.2886932

[9] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, 2018, Art. no. E2575. [Online]. Available: http://www.mdpi.com/1424-8220/18/8/2575

[10] S. Petersen and S. Carlsen, "WirelessHART versus ISA100.11a: The format war hits the factory floor," *IEEE Ind. Electron. Mag.*, vol. 5, no. 4, pp. 23–34, Dec. 2011.

[11] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Exp.*, vol. 5, no. 1, pp. 1–7, 2019.

[12] M. Chen, Y. Miao, Y. Hao, and K. Hwang, "Narrow band Internet of Things," *IEEE Access*, vol. 5, p. 20557, 2017.

[13] O. Khutsoane, B. Isong, and A. M. Abu-Mahfouz, "IoT devices and applications based on LoRa/LoRaWAN," in *Proc. 43rd Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Beijing, China, Oct./Nov. 2017, pp. 6107–6112.

[14] X. Lu, D. Niyato, H. Jiang, D. I. Kim, Y. Xiao, and Z. Han, "Ambient backscatter assisted wireless powered communications," *IEEE Wireless Commun.*, vol. 25, no. 2, pp. 170–177, Apr. 2018.

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

[16] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, Jul. 2013.

[17] J. He, J. Wei, K. Chen, Z. Tang, Y. Zhou, and Y. Zhang, "Multitier fog computing with large-scale IoT data analytics for smart cities," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 677–686, Apr. 2018.

[18] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[19] C. Miguel and L. Barbara, "Practical Byzantine fault tolerance," in *Proc. 3rd Symp. Oper. Syst. Design Implement.*, vol. 99. New Orleans, LA, USA, 1999, pp. 173–186.

[20] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, to be published. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17318332

[21] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018.

[22] B. Chase and E. MacBrough, "Analysis of the XRP ledger consensus protocol," *arXiv preprint arXiv:1802.07242*, 2018. [Online]. Available: https://arxiv.org/pdf/1802.07242.pdf

[23] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling Byzantine agreements for cryptocurrencies," in *Proc. ACM 26th Symp. Oper. Syst. Principles*, Shanghai, China, 2017, pp. 51–68.

[24] F. R. Yu, J. Liu, Y. He, P. Si, and Y. Zhang, "Virtualization for distributed ledger technology (vDLT)," *IEEE Access*, vol. 6, pp. 25019–25028, 2018.

[25] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "BLOCKBENCH: A framework for analyzing private blockchains," in *Proc. ACM Int. Conf. Manag. Data (SIGMOD)*, Chicago, IL, USA, 2017, pp. 1085–1100. [Online]. Available: http://doi.acm.org/10.1145/3035918.3064033

[26] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Security Privacy Workshops*, San Jose, CA, USA, May 2015, pp. 180–184.

[27] S. S. Chawathe, *Clustering Blockchain Data*. Cham, Switzerland: Springer, 2019, pp. 43–72.

[28] J. Ream, Y. Chu, and D. Schatsky, *Upgrading Blockchains: Smart Contract Use Cases in Industry*. London, U.K.: Deloitte Press, 2016. [Online]. Available: https://www2.deloitte.com/insights/us/en/focus/signals-for-strategists/using-blockchain-for-smart-contracts.html

[29] N. Szabo, "The idea of smart contracts," Rep., 1997. [Online]. Available: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

[30] F. Idelberger, G. Governatori, R. Riveret, and G. Sartor, "Evaluation of logic-based smart contracts for blockchain systems," in *Proc. Int. Symp. Rules Rule Markup Lang. Semantic Web (RuleML)*, Stony Brook, NY, USA, 2016, pp. 167–183.

[31] C. Sillaber and B. Waltl, "Life cycle of smart contracts in blockchain ecosystems," *Datenschutz und Datensicherheit - DuD*, vol. 41, no. 8, pp. 497–500, Aug. 2017.

[32] R. Koulu, "Blockchains and online dispute resolution: Smart contracts as an alternative to enforcement," *SCRIPTed*, vol. 13, no. 1, p. 40, 2016.

[33] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[34] *Ethereum: Blockchain APP Platforms*. Accessed: Aug. 19, 2018. [Online]. Available: https://www.ethereum.org/

[35] *GemOS: The Blockchain Operating System*. Accessed: Aug. 19, 2018. [Online]. Available: https://enterprise.gem.co/

[36] *MultiChain: Open Platform for Building Blockchains*. Accessed: Aug. 19, 2018. [Online]. Available: https://www.multichain.com/

[37] (2015). *Hyperledger Project*. [Online]. Available: https://www.hyperledger.org/

[38] X. Xu *et al.*, "A taxonomy of blockchain-based systems for architecture design," in *Proc. IEEE Int. Conf. Softw. Archit. (ICSA)*, Gothenburg, Sweden, 2017, pp. 243–252.

[39] *Consortium Chain Development*. Accessed: Aug. 19, 2018. [Online]. Available: https://github.com/ethereum/wiki/wiki/Consortium-Chain-Development

[40] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Security*, vol. 1, no. 1, pp. 36–63, 2001.

[41] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[42] Q. Lu and X. Xu, "Adaptable blockchain-based systems: A case study for product traceability," *IEEE Softw.*, vol. 34, no. 6, pp. 21–27, Nov./Dec. 2017.

[43] Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of bitcoin," in *Proc. 18th Int. Conf. Intell. Next Gener. Netw. (ICIN)*, Paris, France, 2015, pp. 184–191.

[44] M. Massaro, "Next generation of radio spectrum management: Licensed shared access for 5G," *Telecommun. Policy*, vol. 41, nos. 5–6, pp. 422–433, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0308596117301416

[45] J. Eggerton, *FCC's Rosenworcel Talks Up 6G*, Future Publ. Ltd., Bath, U.K., Sep. 2018. [Online]. Available: https://www.multichannel.com/news/fccs-rosenworcel-talks-up-6g

[46] R. Saracco, *Let's Start Talking About 6G!* IEEE, Piscataway, NJ, USA, Jan. 2018. [Online]. Available: http://sites.ieee.org/futuredirections/2018/01/25/lets-start-talking-about-6g/

[47] A. Gatherer, *What Will 6G Be?* IEEE Commun. Soc., New York, NY, USA, Jun. 2018. [Online]. Available: https://www.comsoc.org/publications/ctn/what-will-6g-be

[48] S. Yrjölä, "Analysis of blockchain use cases in the citizens broadband radio service spectrum sharing concept," in *Cognitive Radio Oriented Wireless Networks*. Cham, Switzerland: Springer Int., 2018, pp. 128–139.

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

[50] E. H. H. Kure, P. Engelstad, S. Maharjan, S. Gjessing, and Y. Zhang, "Distributed uplink offloading for IoT in 5G heterogeneous networks under private information constraints," *IEEE Internet Things J.*, to be published. [Online]. Available: https://doi.org/10.1109/JIOT.2018.2886703

[51] E. Langberg, "Blockchains in mobile networks," Wireless Access Dept., Huawei Technol. Company Ltd., New York, NY, USA, Rep. 21, Mar. 2017. [Online]. Available: https://e.huawei.com/hk/publications/global/ict_insights/201703141505/

[52] S. He, C. Xing, and L.-J. Zhang, "A business-oriented schema for blockchain network operation," in *Blockchain—ICBC 2018*, S. Chen, H. Wang, and L.-J. Zhang, Eds. Cham, Switzerland: Springer Int., 2018, pp. 277–284.

[53] S. Bera, S. Misra, and A. V. Vasilakos, "Software-defined networking for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1994–2008, Dec. 2017.

[54] K. Kalkan and S. Zeadally, "Securing Internet of Things with software defined networking," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 186–192, Sep. 2018.

[55] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, Sep. 2017.

[56] I. D. Alvarenga, G. A. F. Rebello, and O. C. M. B. Duarte, "Securing configuration management and migration of virtual network functions using blockchain," in *Proc. IEEE/IFIP Netw. Oper. Manag. Symp. (NOMS)*, Taipei, Taiwan, Apr. 2018, pp. 1–9.

[57] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2429–2453, 3rd Quart., 2018.

[58] C. Esposito, A. Castiglione, B. Martini, and K.-K. R. Choo, "Cloud manufacturing: Security, privacy, and forensic concerns," *IEEE Cloud Comput.*, vol. 3, no. 4, pp. 16–22, Jul./Aug. 2016.

[59] V. Ortega, F. Bouchmal, and J. F. Monserrat, "Trusted 5G vehicular networks: Blockchains and content-centric networking," *IEEE Veh. Technol. Mag.*, vol. 13, no. 2, pp. 121–127, Jun. 2018.

[60] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," *IET Commun.*, vol. 12, no. 5, pp. 527–532, Mar. 2018.

[61] C.-H. Chen, M.-Y. Lin, and C.-C. Liu, "Edge computing gateway of the industrial Internet of Things using multiple collaborative microcontrollers," *IEEE Netw.*, vol. 32, no. 1, pp. 24–32, Jan./Feb. 2018.

[62] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: A survey," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 450–465, Feb. 2018.

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

[64] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, "Computation offloading and content caching in wireless blockchain networks with mobile edge computing," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11008–11021, Nov. 2018.

[65] P. Yang, N. Zhang, Y. Bi, L. Yu, and X. S. Shen, "Catalyzing cloud-fog interoperation in 5G wireless networks: An SDN approach," *IEEE Netw.*, vol. 31, no. 5, pp. 14–20, Sep. 2017.

[66] Y. Dai, D. Xu, S. Maharjan, and Y. Zhang, "Joint load balancing and offloading in vehicular edge computing and networks," *IEEE Internet Things J.*, to be published. [Online]. Available: https://doi.org/10.1109/JIOT.2018.2876298

[67] Z. Zhou, P. Liu, J. Feng, Y. Zhang, S. Mumtaz, and J. Rodriguez, "Computation resource allocation and task assignment optimization in vehicular fog computing: A contract-matching approach," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3113–3125, Apr. 2019. [Online]. Available: https://doi.org/10.1109/TVT.2019.2894851

[68] Y. Yang, K. Wang, G. Zhang, X. Chen, X. Luo, and M. Zhou, "Meets: Maximal energy efficient task scheduling in homogeneous fog networks," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 4076–4087, Oct. 2018.

[69] A. Kusiak, "Smart manufacturing," *Int. J. Prod. Res.*, vol. 56, nos. 1–2, pp. 508–517, 2018.

[70] J. Wan, J. Li, M. Imran, and D. Li, "A blockchain-based solution for enhancing security and privacy in smart factory," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3652–3660, Jun. 2019. [Online]. Available: https://doi.org/10.1109/TII.2019.2894573

[71] I. Konstantinidis, G. Siaminos, C. Timplalexis, P. Zervas, V. Peristeras, and S. Decker, "Blockchain for business applications: A systematic literature review," in *Business Information Systems*, W. Abramowicz and A. Paschke, Eds. Cham, Switzerland: Springer Int., 2018, pp. 384–399.

[72] H. M. Kim and M. Laskowski, "Toward an ontology-driven blockchain design for supply-chain provenance," *Intell. Syst. Account. Finance Manag.*, vol. 25, no. 1, pp. 18–27, 2018.

[73] A. Tapscott and D. Tapscott, "How blockchain is changing finance," *Harvard Bus. Rev.*, vol. 1, Mar. 2017. [Online]. Available: https://hbr.org/2017/03/how-blockchain-is-changing-finance

[74] N. Kshetri, "1 blockchain's roles in meeting key supply chain management objectives," *Int. J. Inf. Manag.*, vol. 39, pp. 80–89, Apr. 2018.

[75] Z. Li *et al.*, "A blockchain and AutoML approach for open and automated customer service," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3642–3651, Jun. 2019. [Online]. Available: https://doi.org/10.1109/TII.2019.2900987

[76] D. Tse, B. Zhang, Y. Yang, C. Cheng, and H. Mu, "Blockchain application in food supply information security," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manag. (IEEM)*, Singapore, Dec. 2017, pp. 1357–1361.

[77] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *Proc. 13th Int. Conf. Service Syst. Service Manag. (ICSSSM)*, Kunming, China, 2016, pp. 1–6.

[78] F. Sander, J. Semeijn, and D. Mahr, "The acceptance of blockchain technology in meat traceability and transparency," *Brit. Food J.*, vol. 120, no. 9, pp. 2066–2079, 2018.

[79] R. Bettín-Díaz, A. E. Rojas, and C. Mejía-Moncayo, "Methodological approach to the definition of a blockchain system for the food industry supply chain traceability," in *Computational Science and Its Applications—ICCSA 2018*. Cham, Switzerland: Springer Int., 2018, pp. 19–33.

[80] Q. Lin, H. Wang, X. Pei, and J. Wang, "Food safety traceability system based on blockchain and EPCIS," *IEEE Access*, vol. 7, pp. 20698–20707, 2019.

[81] C. Zhang, J. Wu, Y. Zhou, M. Cheng, and C. Long, "Peer-to-peer energy trading in a microgrid," *Appl. Energy*, vol. 220, pp. 1–12, Jun. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0306261918303398

[82] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.

[83] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Depend. Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep./Oct. 2018.

[84] C. Pop *et al.*, "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors*, vol. 18, no. 1, 2018, Art. no. E162.

[85] K. Wang, Y. Shao, L. Shu, C. Zhu, and Y. Zhang, "Mobile big data fault-tolerant processing for eHealth networks," *IEEE Netw.*, vol. 30, no. 1, pp. 36–42, Jan./Feb. 2016.

[86] C. Esposito, A. D. Santis, G. Tortora, H. Chang, and K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan./Feb. 2018.

[87] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *J. Med. Syst.*, vol. 42, no. 7, p. 130, Jun. 2018. [Online]. Available: https://doi.org/10.1007/s10916-018-0982-x

[88] M. Z. A. Bhuiyan, A. Zaman, T. Wang, G. Wang, H. Tao, and M. M. Hassan, "Blockchain and big data to transform the healthcare," in *Proc. ACM Int. Conf. Data Process. Appl. (ICDPA)*, 2018, pp. 62–68.

[89] Y. Sun, R. Zhang, X. Wang, K. Gao, and L. Liu, "A decentralizing attribute-based signature for healthcare blockchain," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, 2018, pp. 1–9.

[90] M. A. Rahman *et al.*, "Blockchain-based mobile edge computing framework for secure therapy applications," *IEEE Access*, vol. 6, pp. 72469–72478, 2018.

[91] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019. [Online]. Available: https://doi.org/10.1109/JIOT.2018.2836144

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

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

[94] J. Kang *et al.*, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, to be published.

[95] Y. Dai, D. Xu, S. Maharjan, G. Qiao, and Y. Zhang, "Artificial intelligence empowered edge computing and caching for Internet of Vehicles," *IEEE Wireless Commun. Mag.*, to be published.

[96] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36–42, May 2016.

[97] G. Kimchi *et al.*, "Unmanned aerial vehicle delivery system," U.S. Patent 9 573 684, 2017.

[98] L. Wang, F. Chen, and H. Yin, "Detecting and tracking vehicles in traffic by unmanned aerial vehicles," *Autom. Construction*, vol. 72, pp. 294–308, Dec. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0926580516300887

[99] N. Cheng *et al.*, "Air-ground integrated mobile edge networks: Architecture, challenges, and opportunities," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 26–32, Aug. 2018.

[100] A. Kapitonov, S. Lonshakov, A. Krupenkin, and I. Berman, "Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of UAVs," in *Proc. Workshop Res. Educ. Develop. Unmanned Aerial Syst. (RED-UAS)*, Linköping, Sweden, 2017, pp. 84–89.

[101] A. Kumar, A. Kundu, C. A. Pickover, and K. Weldemariam, "Unmanned aerial vehicle data management," U.S. Patent Appl. 15 463 147, 2018.

[102] B. Li, Z. Fei, and Y. Zhang, "UAV communications for 5G and beyond: Recent advances and future trends," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2241–2263, Apr. 2019. [Online]. Available: https://doi.org/10.1109/JIOT.2018.2887086

[103] Y. Dai, D. Xu, S. Maharjan, and Y. Zhang, "Joint computation offloading and user association in multi-task mobile edge computing," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12313–12325, Dec. 2018.

[104] T. X. Tran, A. Hajisami, P. Pandey, and D. Pompili, "Collaborative mobile edge computing in 5G networks: New paradigms, scenarios, and challenges," *IEEE Commun. Mag.*, vol. 55, no. 4, pp. 54–61, Apr. 2017.

[105] X. Li, H. Wang, H.-N. Dai, Y. Wang, and Q. Zhao, "An analytical study on eavesdropping attacks in wireless nets of things," *Mobile Inf. Syst.*, vol. 2016, Dec. 2016, Art. no. 4313475.

[106] 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 Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[107] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[108] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies," in *Proc. IEEE Symp. Security Privacy (SP)*, San Jose, CA, USA, 2017, pp. 375–392.

[109] S. Adhami, G. Giudici, and S. Martinazzi, "Why do businesses go crypto? An empirical analysis of initial coin offerings," *J. Econ. Bus.*, vol. 100, pp. 64–75, Nov./Dec. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0148619517302308

[110] L. Hu *et al.*, "Cooperative jamming for physical layer security enhancement in Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 219–228, Feb. 2018.

[111] W. Xu, S. Jha, and W. Hu, "LoRa-Key: Secure key generation system for LoRa-based network," *IEEE Internet Things J.*, to be published.

[112] M. Apostolaki, G. Marti, J. Müller, and L. Vanbever, "SABRE: Protecting bitcoin against routing attacks," in *Proc. Netw. Distrib. Syst. Security Symp.*, 2019, pp. 1–15.

[113] 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 Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, Jul. 2018.

[114] A. Dorri, S. S. Kanhere, and R. Jurdak, "MOF-BC: A memory optimized and flexible blockchain for large scale networks," *Future Gener. Comput. Syst.*, vol. 92, pp. 357–373, Jan. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17329552

[115] M. Möser *et al.*, "An empirical analysis of traceability in the Monero blockchain," *Proc. Privacy Enhanc. Technol.*, vol. 2018, no. 3, pp. 143–163, 2018.

[116] K. Saito and M. Iwamura, "How to make a digital currency on a blockchain stable," *Future Gener. Comput. Syst.*, vol. 100, pp. 58–69, 2019. [Online]. Available: https://doi.org/10.1016/j.future.2019.05.019

[117] A. Yasin and L. Liu, "An online identity and smart contract management system," in *Proc. 40th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 2. Atlanta, GA, USA, 2016, pp. 192–198.

[118] A. Bogner, M. Chanson, and A. Meeuw, "A decentralised sharing app running a smart contract on the Ethereum blockchain," in *Proc. 6th Int. Conf. Internet Things*, 2016, pp. 177–178.

[119] 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 *Proc. 17th IEEE/ACM Int. Symp. Clust. Cloud Grid Comput. (CCGRID)*, Madrid, Spain, 2017, pp. 468–477.

[120] D. G. Glover and J. Hermans, "Improving the traceability of the clinical trial supply chain," *Appl. Clin. Trials*, vol. 26, no. 11, pp. 36–38, Nov. 2017. [Online]. Available: https://search.proquest.com/docview/1984377517?accountid=28120

[121] C. Huang *et al.* (2019). *RepChain: A Reputation Based Secure, Fast and High Incentive Blockchain System Via Sharding*. [Online]. Available: https://arxiv.org/pdf/1901.05741.pdf

[122] P. Wang, R. X. Gao, and Z. Fan, "Cloud computing for cloud manufacturing: Benefits and limitations," *J. Manuf. Sci. Eng.*, vol. 137, no. 4, pp. 1–9, 2015.

[123] N. Wang *et al.*, "PrivTrie: Effective frequent term discovery under local differential privacy," in *Proc. IEEE Int. Conf. Data Eng. (ICDE)*, 2018, pp. 1–12.

[124] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5G beyond," *IEEE Netw. Mag.*, vol. 33, no. 3, pp. 10–17, May/Jun. 2019.

[125] C. Remy, B. Rym, and L. Matthieu, "Tracking bitcoin users activity using community detection on a network of weak signals," in *Complex Networks & Their Applications VI*. Cham, Switzerland: Springer Int., 2018, pp. 166–177.

[126] P. Tasca, A. Hayes, and S. Liu, "The evolution of the bitcoin economy: Extracting and analyzing the network of payment relationships," *J. Risk Finance*, vol. 19, no. 2, pp. 94–126, 2018.

[127] W. Chen, Z. Zheng, J. Cui, E. Ngai, P. Zheng, and Y. Zhou, "Detecting Ponzi schemes on Ethereum: Towards healthier blockchain technology," in *Proc. World Wide Web Conf. (WWW)*, Lyon, France, 2018, pp. 1409–1418. [Online]. Available: https://doi.org/10.1145/3178876.3186046

[128] K. Croman *et al.*, "On scaling decentralized blockchains," in *Proc. Int. Conf. Financ. Cryptography Data Security*, 2016, pp. 106–125.

[129] J. Vermeulen, *Bitcoin and Ethereum vs Visa and Paypal—Transactions Per Second*, Altcoin Today, London, U.K., Apr. 2017. [Online]. Available: http://www.altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/

[130] S. Albrecht, S. Reichert, J. Schmid, J. Strüker, D. Neumann, and G. Fridgen, "Dynamics of blockchain implementation—A case study from the energy sector," in *Proc. 51st Hawaii Int. Conf. Syst. Sci.*, 2018, p. 10.

[131] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, "Inclusive block chain protocols," in *Proc. Int. Conf. Financ. Cryptography Data Security*, 2015, pp. 528–547.

[132] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS)*, Vienna, Austria, 2016, pp. 17–30. [Online]. Available: http://doi.acm.org/10.1145/2976749.2978389

Zibin Zheng (SM'16) received the Ph.D. degree in computer science and engineering with the Chinese University of Hong Kong, Hong Kong, in 2011.

He is currently a Professor with the School of Data and Computer Science, Sun Yat-sen University, Guangzhou, China. His current research interests include service computing, cloud computing, and blockchain.

Dr. Zheng was a recipient of the Outstanding Ph.D. dissertation Award of the Chinese University of Hong Kong in 2012, the Association for Computing Machinery's Special Interest Group on Software Engineering Distinguished Paper Award at the International Conference on Science and Engineering, in 2010, the Best Student Paper Award at the International Conference on Web Services, in 2010, and the IBM Ph.D. Fellowship Award at 2010. He served as a Program Committee Member for the IEEE International Conference on Cloud Computing, the International Conference on Web Services, the International Conference on Service Computing, the International Conference on Service-Oriented Computing, and the International Symposium on Service-Oriented System Engineering.

Hong-Ning Dai (SM'16) received the Ph.D. degree in computer science and engineering from the Department of Computer Science and Engineering, Chinese University of Hong Kong, Hong Kong.

He is an Associate Professor with the Faculty of Information Technology, Macau University of Science and Technology, Macau, China. He has published over 90 peer-reviewed papers in top-tier journals and conferences, including *ACM Computing Surveys*, the IEEE Transactions on Industrial Informatics, the IEEE Transactions on Vehicular Technology, the IEEE Transactions on Intelligent Transportation Systems, the IEEE Transactions on Computational Social Systems, *ACM/Springer Wireless Networks*, and IEEE INFOCOM. He is also the holder of one U.S. patent. His research interests include Internet of Things, BDA, and blockchains.

Dr. Dai was a recipient of the One ESI Highly Cited Paper Award by Clarivate Analytics, the BOC Excellent Research Award of the Macau University of Science and Technology in 2015 for his outstanding research performance. He has served as a Guest Editor for the IEEE Transactions on Industrial Informatics and an Editorial Board Member in several peer-reviewed journals, such as IEEE Access, the *International Journal of Industrial Engineering Computations*, and the *International Journal of Wireless and Mobile Communication for Industrial Systems*. He is a professional member of ACM.

Yan Zhang (SM'10) received the Ph.D. degree form the School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore.

He is a Full Professor with the Department of Informatics, University of Oslo, Oslo, Norway. His current research interests include next-generation wireless networks leading to 5G and green and secure CPSs (e.g., smart grid, healthcare, and transport).

Dr. Zhang was a recipient of the 2018 Highly Cited Researcher (top 1% by citations) Award according to Clarivate Analytics. He is an Associate Technical Editor of the *IEEE Communications Magazine*, an Editor of the IEEE Transactions on Green Communications and Networking, the IEEE Communications Surveys and Tutorials, and the IEEE Internet of Things Journal, and an Associate Editor of IEEE Access. He serves as chair positions in a number of conferences, including IEEE GLOBECOM 2017, IEEE VTC-Spring 2017, IEEE PIMRC 2016, IEEE CloudCom 2016, IEEE ICCC 2016, IEEE CCNC 2016, IEEE SmartGridComm 2015, and IEEE CloudCom 2015. He serves as a TPC member for numerous international conference including IEEE INFOCOM, IEEE ICC, IEEE GLOBECOM, and IEEE WCNC. He is the IEEE Vehicular Technology Society (VTS) Distinguished Lecturer. He is also a senior member of IEEE ComSoc, IEEE CS, IEEE PES, and IEEE VTS. He is a fellow of IET.