A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges

Junfeng Xie, Helen Tang, Tao Huang, F. Richard Yu, *Fellow, IEEE*, Renchao Xie, Jiang Liu, and Yunjie Liu

***Abstract*—In recent years, the rapid urbanization of world's population causes many economic, social, and environmental problems, which affect people's living conditions and quality of life significantly. The concept of "smart city" brings opportunities to solve these urban problems. The objectives of smart cities are to make the best use of public resources, provide high-quality services to the citizens, and improve the people's quality of life. Information and communication technology plays an important role in the implementation of smart cities. Blockchain as an emerging technology has many good features, such as trust-free, transparency, pseudonymity, democracy, automation, decentralization, and security. These features of blockchain are helpful to improve smart city services and promote the development of smart cities. In this paper, we provide a comprehensive survey on the literature involving blockchain technology applied to smart cities. First, the related works and background knowledge are introduced. Then, we review how blockchain technology is applied in the realm of smart cities, from the perspectives of smart citizen, smart healthcare, smart grid, smart transportation, supply chain management, and others. Finally, some challenges and broader perspectives are discussed.**

***Index Terms*—Smart cities, blockchain.**

I. Introduction

IN THE past few decades, the world's population lived in urban areas is growing explosively. According to the report from United Nations [1], over the next 30 years, an additional 2.5 billion people are predicted to move to urban areas and more than 70% of the world's population will live in the urban areas by 2050. The urbanization level of developing countries in Asia and Africa grows at a higher growth rate than other regions of the world. From 2001 to 2015, the urbanization level of China has increased from 38% to 56% [2]. The world's urbanization process has greatly improved citizens' living standard in many aspects, such as health, education, transportation, economy, as well as living and working environments [3]. However, the rapid increase of the world's urban population also brings new challenges and problems. Due to the high density of population in urban areas, citizens' quality of life has been affected by environmental resource constraints, traffic congestion, air pollution, greenhouse gas emission and waste disposal [4]. All these challenges and problems force participants in cities (e.g., governments and citizens) to pay attention to smarter approaches for the sustainable development of cities and the improvement of citizens' quality of life. In this case, the concept of "Smart City" is proposed [4]–[7].

What is a smart city? Although there are many definitions of "Smart City", a commonly accepted definition is that a smart city aims to improve the citizens' quality of life and build a sustainable urban environment by using modern advanced Information and Communication Technology (ICT). A smart city has many good characteristics, such as increased openness of public government, encouraged involvement of citizens, effective management of traffic and public transport, optimal resource utilization, better environmental protection, intelligent device control, and improved health, energy and education services. ICT plays a key role in the implementation of smart cities. In this paper, we focus on an emerging technology called *blockchain* [8]–[10], which has a huge potential to promote the development of smart cities and to enhance smart city services.

Blockchain is a distributed ledger technology evolved from Bitcoin [11] and other crypto currencies. Blockchain is first applied to Bitcoin, which is created by Satoshi Nakamoto in 2008. The blockchain is basically an immutable, decentralized and public available shared database. In the blockchain, all transactions are recorded and anyone in the system is allowed to access, send and verify these transactions. Applying blockchain technology to smart cities can bring many good features, such as trust-free, transparency, pseudonymity, democracy, automation, decentralization and security. Trust-free means that the blockchain system can run normally in a peer-to-peer manner without a reliable third party. Blockchain technology enables everyone to access all transaction records, which makes it transparent. The pseudonymity can be realized by recording transactions using public pseudonymous addresses and keeping nodes' real-world identities hidden. In the blockchain system, decisions are made by all nodes in a peer-to-peer manner, which makes it democratized. Smart contracts on the blockchain have the ability to perform transaction generation, decision making and data

Manuscript received March 9, 2018; revised July 31, 2018, November 18, 2018, and December 23, 2018; accepted January 16, 2019. Date of publication February 15, 2019; date of current version August 20, 2019. This work was supported by the National Science and Technology Major Project of China under Grant 2018ZX03001019-003. *(Corresponding author: Tao Huang.)*

J. Xie is with the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China, and also with the School of Information Science and Engineering, Guangxi University for Nationalities, Nanning 530006, China.

H. Tang is with the Centre for Security Science, Defence Research and Development Canada, Ottawa, ON K1A 0K2, Canada.

T. Huang, R. Xie, J. Liu, and Y. Liu are with the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: htao@bupt.edu.cn).

F. R. Yu is with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6, Canada.

Digital Object Identifier 10.1109/COMST.2019.2899617

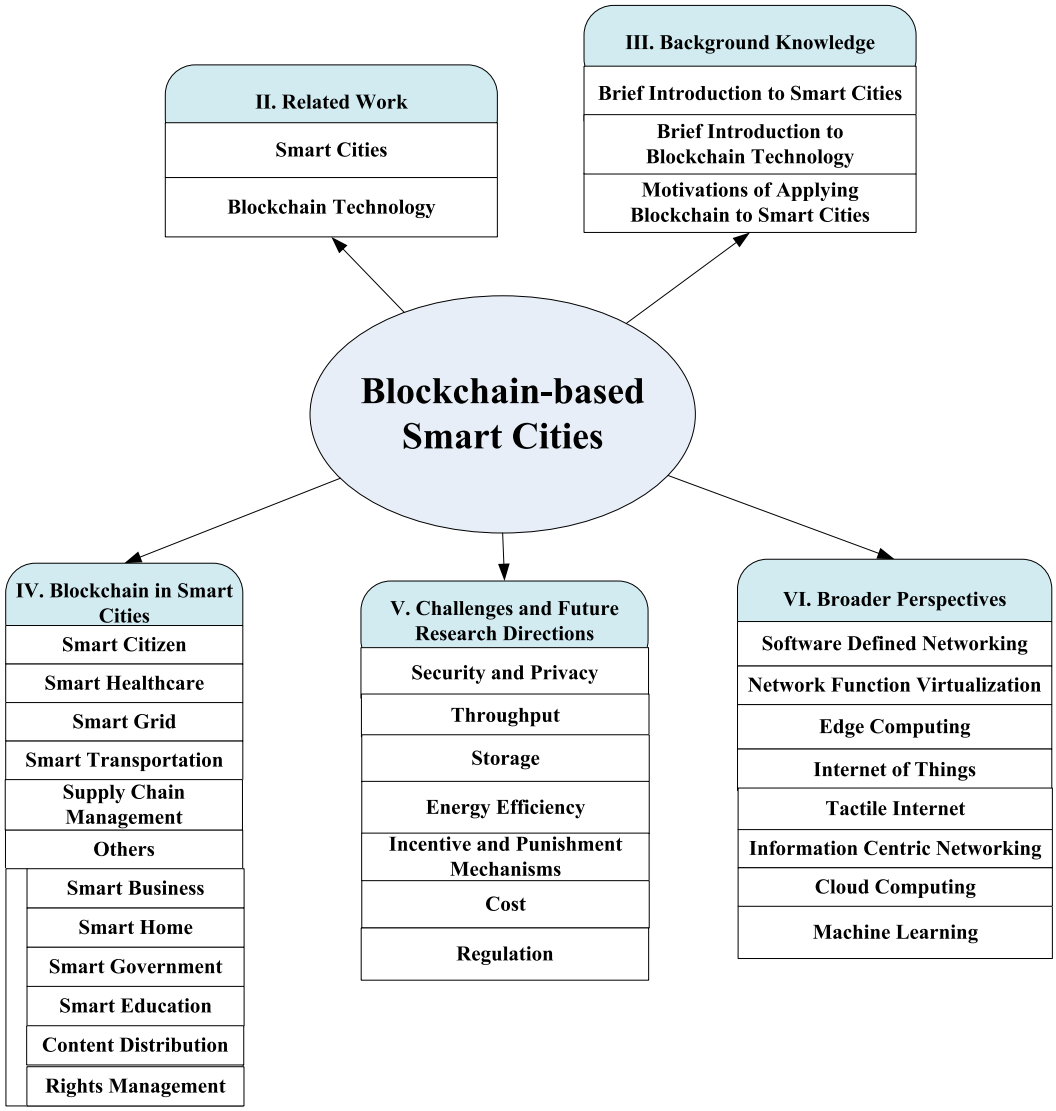


Fig. 1. Road map of blockchain-based smart cities.

storage automatically. The decentralization of the blockchain system makes it necessary to ensure consistency by running consensus algorithms among decentralized nodes. Security in the blockchain system is related to integrity, confidentiality and authorization.

Although smart cities and blockchain have been studied extensively in previous works, these two important areas have traditionally been researched separately in the existing studies. To the best of our knowledge, there is no existing work to survey the conjunction of these two important areas. To fill this gap, in this paper, we survey the state-of-the-art blockchain technology that can be applied in smart cities. Research on adopting blockchain technology to improve the performance, smartness, efficiency and security of smart cities is presented. In addition, we discuss future research directions in related areas with proper depth and sufficient breadth. A road map of our approach is given in Fig. 1. As shown in the figure, we identify five aspects of the blockchain-based smart cities, on which we would like to focus: related work, background knowledge, blockchain in smart cities, challenges and broader perspectives. We believe that our discussion and exploration can give readers an overall understanding of this field, and foster more subsequent studies on this issue.

The rest of the article is organized as follows. First, the related work is presented in Section II. Then, background knowledge of smart cities and blockchain are briefly introduced in Section III. Section IV reviews how blockchain technology is applied in the realm of smart cities, from the perspectives of smart citizen, smart healthcare, smart grid, smart transportation, supply chain management and others, and provides a detailed explanation of how blockchain efforts can be applied within each category. Some challenges and future research directions are discussed in Section V. In Section VI, we present some broader perspectives. Finally, we conclude this study in Section VII.

II. Related Work

In this section, we present the related work, including smart cities and blockchain technology.

A. Smart Cities

The topic of smart cities has attracted a lot of attention from academia. Various definitions of smart cities have been presented in [12]. Batty *et al.* [13] have presented a comprehensive survey on smart cities, from research goals, research challenges, scenarios and project areas. Yin *et al.* [14] have presented a comprehensive survey on smart cities, from the definition, application domains, architectures, key enabling technologies and research challenges. The functional requirements for smart cities have been discussed in [15]. Issues and solutions regarding the information security in smart cities have been studied in [16]. Pan *et al.* [17] have surveyed the research issues, methods, and application domains in trace analysis and mining for smart cities. Shuai *et al.* [18] have surveyed the economic models of electric vehicles' charging process in smart cities considering both unidirectional and bidirectional energy flows, and given some valuable classification and comparison. Other specific areas of smart cities, such as software architectures [19], business models [20] and people movement analytics [21], are also studied respectively.

ICT plays a key role in the implementation of smart cities. Data collection and analysis can help to effectively provide public services to citizens and improve the management of cities. Al Nuaimi *et al.* [22] have studied the applications of *big data technologies* to smart cities, and surveyed the opportunities, challenges and benefits. Djahel *et al.* [23] have presented a comprehensive survey of the technologies (e.g., *machine learning*) used in different phases of modern traffic management systems, from information gathering to service delivery, and discussed innovative approaches to enable a fast, efficient and accurate traffic management system in smart cities. Wang and Sng [24] have surveyed the *deep learning algorithms* applied to video analytics in smart cities. Smart cities have been surveyed in [25] from a data-centric perspective, which gives a detailed discussion on the technologies (e.g., *machine learning and deep learning algorithms*) used in data management, security and privacy. In addition, some networking and computing technologies such as *Software Defined Networking (SDN), Network Function Virtualization (NFV) and Cloud computing* are also studied in [25].

Other promising technologies such as Internet of Things (IoT) and fog computing can also been applied to promote the development of smart cities. *IoT*-enabled smart cities have been surveyed in [26] and [27]. Especially, Zanella *et al.* [26] have researched the enabling technologies, protocols and architecture for an urban IoT system. Anagnostopoulos *et al.* [27] focus on the waste management in smart cities, and discuss the strength and weakness of six IoT-enabled waste management models. Petrolo *et al.* [28] have discussed the impact of *Cloud of Things (CoT)* on smart cities, and surveyed the requirements, benefits and challenges. *Fog computing* for sustainable smart cities has been surveyed in [29], which analyzes the characteristics and functionalities of an ideal fog computing architecture, and discusses some future research challenges and directions. In Section VI, we present some broader perspectives of these technologies applied in smart cities.

B. Blockchain Technology

Several papers have also studied and surveyed blockchain technology (e.g., [30]–[37]). Zheng *et al.* [30], [31] have presented a comprehensive overview on the blockchain, from the architecture, characteristics, consensus algorithms, applications, future research challenges and directions. Security issues and challenges faced by blockchain technology have been surveyed in [32]. Tschorsch and Scheuermann [33] focus on distributed crypto currencies, and describe the most widely known crypto currency Bitcoin, from the characteristics, related concepts, fundamental structures and applications. Mukhopadhyay *et al.* [34] have surveyed the current mining techniques used by crypto currencies, and given some valuable comparison and evaluation. Widely used consensus protocols in blockchain have been studied in [35]. Li *et al.* [36] have presented the attacks on popular blockchain systems, summarized academic achievements for blockchain security enhancement, and discussed future research directions. Christidis and Devetsikiotis [37] have studied how to employ blockchain and smart contracts to promote the development of IoT, and discussed several issues.

III. Background Knowledge

In this section, we first present brief background knowledge about smart cities and blockchain. Then, the motivations of applying blockchain technology to smart cities are described.

A. Brief Introduction to Smart Cities

In [12], a formal definition of smart cities is given: "A smart city is a system that enhances human and social capital wisely using and interacting with natural and economic resources via technology-based solutions and innovations to address public issues and efficiently achieve sustainable development and high quality of life".

Based on the definition, to understand smart cities more clearly, a conceptual framework of smart cities [5]–[7] is proposed. As shown in Fig. 2, there are three core components in smart cities: technology, human and organization.

The key factor of smart cities is information and communication technology, which can be used to improve life and work significantly and fundamentally [38]. Intelligent hardware infrastructures and software applications can achieve a sustainable smart city. In general, the ICT includes smart database systems, smart control systems, and smart interfaces [39], [40]. Information in smart cities is collected and stored in the smart database systems. Smart control systems are responsible for organizing and scheduling resources in smart cities. The smart interfaces are used by citizens to access information and share resources. In mobile environments, mobile, virtual, and ubiquitous technologies, such as WiFi networks, public access points and wireless hot spots, are very important to citizens.

A smart city is a center of high education and smart workforce [41], [42], who can provide innovative ideas, creative works and solutions to promote the development of smart cities. Thus, smart human is an important component of smart cities [43], [44]. Smart human is related to various factors

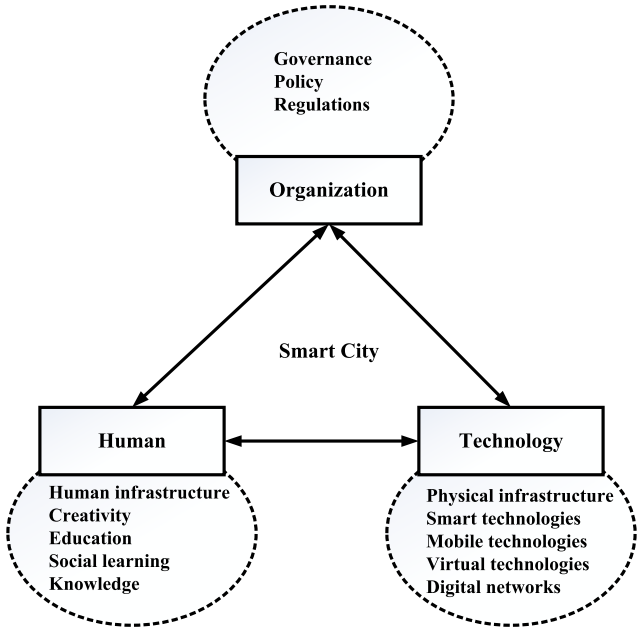


Fig. 2. A conceptual framework of smart cities [5]–[7]. There are three core components in smart cities: technology, human and organization. Technology is the key factor of smart cities. Human can provide innovative ideas, creative works and solutions to promote the development of smart cities. The organization is fundamental to design and implement smart cities.

like creativity, education, and social learning. Human creative capability is helpful to solve problems associated with urban agglomerations. Education makes a city attractive by creating a dynamic learning environment [45]. Collective intelligence and social learning are integrated approaches to build connections among schools, enterprises, governments, nonprofit organizations, and citizens. Based on these factors, smart human can create specific services to address challenges faced by smart cities.

The organization based on governance and policy, is fundamental to design and implement smart cities. The government aims to create a transparent and accountable environment, where citizens can access information related to their daily lives and resources are managed more effectively. In order to promote growth and encourage innovation, the government needs to interconnect with stakeholders such as enterprises, citizens, communities and non-profit organizations [46]. In smart cities, it is necessary for the government to provide interoperable, Internet-based services, which allow effective communications with smart citizens and satisfy their requirements efficiently. In summary, the successful deployment of a smart city is the result of a coalition of ubiquitous infrastructures, technologies, education, government and citizens [47].

B. Brief Introduction to Blockchain Technology

Distributed Ledger Technology (DLT) has attracted widespread attention in recent years. DLT is a transparent, distributed, secure data storage and transfer technology that works without any centralized trusted third party. A distributed ledger is a decentralized database that is maintained by several nodes over a peer-to-peer network. The ledger is verified and replicated by each node. Blockchain is one form of DLT. The blockchain organizes data into blocks, which are chained together using an append-only structure. The chain-based block structure is the most popular data structure of DLT, but it is not the only one. There are other data structures to implement DLT, such as Directed Acyclic Graph (DAG). The DAG-based DLT can be divided into two categories: blockDAG and Transaction DAG (TDAG). BlockDAG is a DAG structure, where each block is allowed to reference multiple previous blocks. Inclusive BlockDAG [48] and Spectre [49] are two examples of blockDAG systems. In the TDAG-based DLT, transactions are directly added to a graph, forming a graph of transactions. Each transaction references multiple previous transactions. IOTA [50] and Byteball [51] are two representative TDAG systems. Blockchain is the most widely used distributed ledger technology, so in this paper, we mainly focus on blockchain technology.

Blockchain systems are typically classified into three categories: public blockchain, consortium blockchain and private blockchain [30]. The public blockchain is permissionless blockchain, while both consortium blockchain and private blockchain are permissioned blockchain. In the public blockchain, anyone is allowed to join the network, participate in the consensus process, read and send transactions, and maintain the shared ledger. Most crypto currencies and some open-source blockchain platforms are permissionless blockchain systems. Bitcoin [11] and Ethereum [52], [53] are two representative public blockchain systems. Bitcoin is the most famous crypto currency that is created by Satoshi Nakamoto in 2008. Ethereum is another representative public blockchain that supports extensive decentralized applications using its Turing-complete smart contract programming languages.

The consortium blockchain systems are generally used in business domain to record cross-organizational business transactions. Different from public blockchain systems, consortium blockchain systems only allow authorized entities to participate in the consensus process. The private blockchain is a distributed but still centralized network that is owned by an organization or entity. Permissioned blockchain systems can be further divided into two categories: public and private permissioned blockchain systems. Both public and private permissioned blockchain systems allow only the authorized entities to participate in the consensus process, send transactions, and maintain the shared ledger. The main difference between them is that public permissioned blockchain systems allow anyone to read transactions in the shared ledger, while in the private permissioned blockchain systems, reading transactions is also restricted to the authorized entities. Most blockchain systems developed for business are permissioned blockchain systems. Hyperledger Fabric [54] is a representative permissioned blockchain system.

Hyperledger Fabric is a Linux Foundation project developed for business. Nodes in the Hyperledger Fabric are divided into validating peers and non-validating peers. The validating peers are responsible for validating transactions, participating in the consensus process and maintaining the ledger by running the Practical Byzantine Fault Tolerance (PBFT) consensus

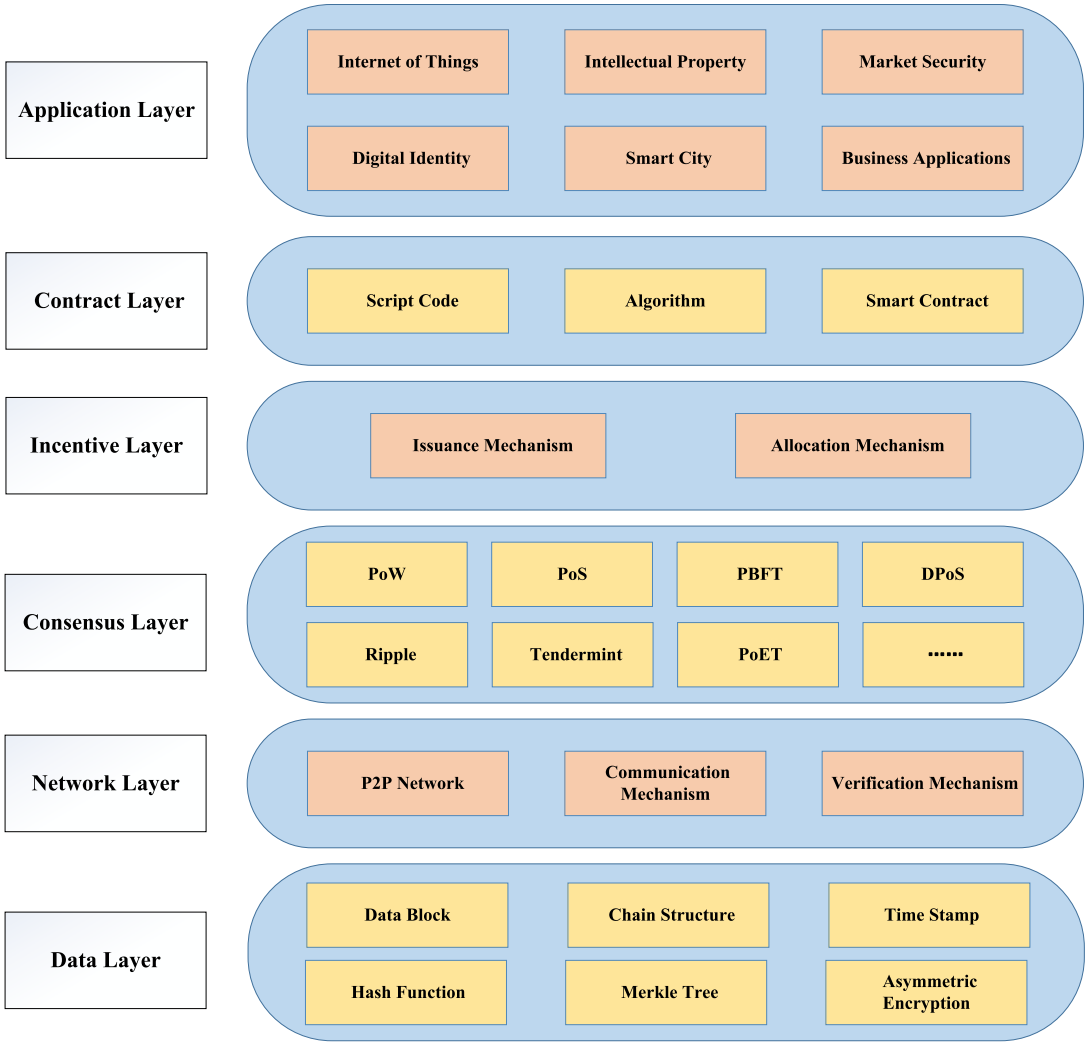


Fig. 3. A general blockchain architecture [8]–[10]. The data layer encapsulates the time-stamped data blocks. The network layer is composed of distributed networking mechanism, data propagation mechanism and data verification mechanism. The consensus layer consists of various consensus algorithms. The incentive layer is the main driving force for blockchain network. The contract layer brings programmability into blockchain. The application layer is composed of blockchain-based business applications.

protocol. The non-validating peers are allowed to read and verify transactions. In Table I, we provide a brief comparison of some well-known blockchain systems.

In the following, we present a brief introduction of blockchain from the perspectives of architecture and workflow of blockchain.

1) Architecture of Blockchain: A basic blockchain architecture is composed of six main layers, including data layer, network layer, consensus layer, incentive layer, contract layer, and application layer [8]–[10], [65], [66]. The architectural components of each layer are shown in Fig. 3. In the following, we will give a detailed description of these layers and their functions.

The lowest layer in blockchain architecture is the data layer, which encapsulates the time-stamped data blocks. Each block contains a small part of transactions and is "chained" back to its previous block, resulting an ordered list of blocks [67]. A typical block structure [8], [10], [33] is shown in Fig. 4. The block structure mainly includes two parts: the block header and the block body. The block body stores verified transactions.

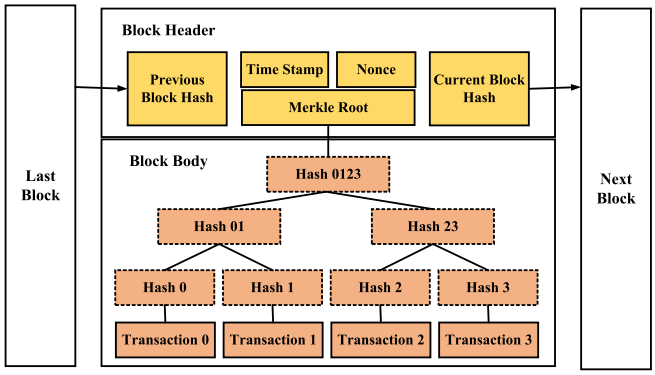


Fig. 4. A typical block structure [8], [10], [33]. The block structure mainly includes two parts: block header and block body. The block body stores verified transactions. The block header specifies the metadata, including hash of previous block, hash of current block, timestamp, Nonce and Merkle root.

The block header specifies the metadata, including hash of previous block, hash of current block, timestamp, Nonce and Merkle root. The hash of previous block is used by the current

TABLE I
A BRIEF COMPARISON OF SOME WELL-KNOWN BLOCKCHAIN SYSTEMS

Blockchain system	Data structure	Permissioned	Consensus	Smart contract language	Turing complete
Bitcoin [11]	blockchain	No	PoW	Golang, C++	No
Litecoin [55]	blockchain	No	PoW	Golang, C++	No
Ripple [56]	blockchain	Yes	Ripple	Golang, C++	No
ZCash [57]	blockchain	No	PoW	C++	No
Hyperledger [54]	blockchain	Yes	PBFT	Golang, Java	Yes
Sawtooth Lake [58]	blockchain	No	PoET	Python	Yes
Ethereum [52], [53]	blockchain	No	PoW/PoS	Solidity, Serpent, LLL	Yes
Quorum [59]	blockchain	Yes	QuorumChain	Golang	Yes
Monax [60]	blockchain	Yes	Tendermint	Solidity	Yes
Tezos [61]	blockchain	No	PoS	Michelson	No
Corda [62]	blockchain	Yes	BFT	Kotlin, Java	No
Kadena [63], [64]	blockchain	Yes	ScalableBFT	Pact	No
IOTA [50]	DAG	No	PoW	Java	No
Byteball [51]	DAG	Yes	Main chain	Node.js	No

block to connect its previous block called parent block. The first block of a blockchain is named as genesis block that has no parent block. Timestamp indicates the creating time of this block. Nonce relates to mining process. The Merkle root is the root of a Merkle tree. The Merkle tree uses a hash binary tree to store the transactions within a specific time period. In this way, the existence and integrity of transactions can be verified rapidly, efficiently and securely.

The network layer is composed of distributed networking mechanism, communication mechanism and data verification mechanism. The goal of this layer is to distribute, forward and verify blockchain transactions. The topology of blockchain network is generally modeled as a P2P network, where peers are equally privileged participants. Once a transaction is generated, it is broadcast to all neighboring nodes. Each node will verify the received transaction according to predefined specifications. If the transaction is valid, it will be forwarded to other nodes. Otherwise, it will be discarded. In this way, only valid transactions are stored by every node in the blockchain network. Digital signature based on asymmetric cryptography mechanism is generally applied to verify the authentication of transactions [68]. The typical digital signature includes two phases: the signing phase and the verification phase. When a node creates a transaction, the transaction is signed by the node's private key. Once other nodes receive the transaction, the initiator's public key is used to verify the authentication of the received transaction.

The consensus layer consists of various consensus algorithms. How to reach consensus efficiently among the untrustworthy nodes in decentralized environments is an important issue [69]. In a blockchain network, there is no trusted central node. Thus, some protocols are needed to ensure a consensus among all decentralized nodes before a block is included into the blockchain. In the existing blockchain systems, there are four major consensus mechanisms: Proof of Work (PoW) [11], Proof of Stake (PoS) [70], [71], PBFT [72], and Delegated Proof of Stake (DPoS) [73]. PoW is a consensus algorithm used in Bitcoin blockchain. Nodes in the PoW algorithm repeatedly run hashing functions to generate a nonce value which is difficult to produce but easy for other nodes to validate. PoS is an energy-saving mechanism, which enables the node with the largest amount of stake (e.g., currency) to generate blocks. PBFT is a replication algorithm to tolerate byzantine faults. DPoS is similar to PoS. The major difference between PoS and DPoS is that PoS is direct democratic while DPoS is representative democratic. There are some other less popular consensus mechanisms such as Ripple [56], Stellar [74], Tendermint [75], Proof of Bandwidth (PoB) [76], Proof of Elapsed Time (PoET) [77], Proof of Authority (PoA) [78], Proof of Retrievability [79], Proof of Burn [80], Proof of Activity [81], Proof of Space [82], Proof of Trust [83], Proof of Luck [84], BFT-SMART [85] and ScalableBFT [86]. Among all consensus mechanisms, PoW, PoS, DPoS and other protocols based on PoW such as Proof of Activity [81], Proof of Space [82] and Proof of Luck [84], are generally used in public blockchain systems. In contrast, Byzantine Fault Tolerance (BFT)-related algorithms (e.g., PBFT, Tendermint, Stellar, Ripple, BFT-SMART and ScalableBFT) are typically suitable for permissioned blockchain systems. For a more insightful discussion on consensus protocols, please refer to [87] and [88].

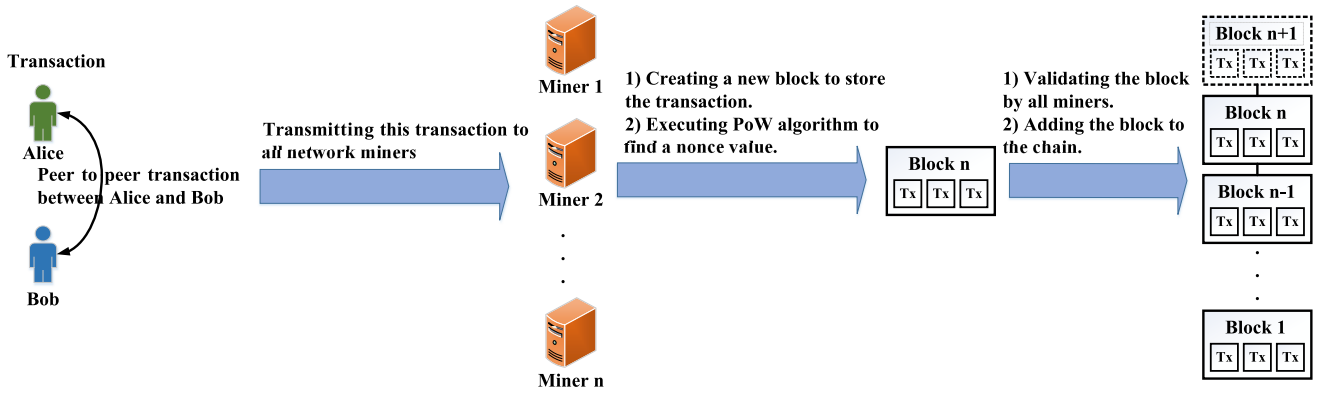


Fig. 5. The general processing procedure of a PoW-based blockchain network. Tx stands for Transaction.

The incentive layer is the main driving force for blockchain network by integrating the economic factors, such as economic incentive issuance and allocation mechanisms, into the blockchain network to motivate the nodes to contribute their efforts to verify data. Specifically, once a new block is generated, some economic incentives (e.g., digital currencies) will be issued as reward and allocated to corresponding nodes according to their contributions.

The contract layer brings programmability into blockchain. Various scripts, algorithms and smart contracts are utilized to enable more complex programmable transactions. Specifically, smart contracts are a group of state-response rules that are securely stored on the blockchain. Smart contracts can control users' digital assets, express business logic, and formulate the participants' rights and obligations. When all terms within a smart contract are agreed by two or more participants, the contract will be signed cryptographically and broadcast to the blockchain network for verification [89]. Once the predefined conditions are triggered, the smart contract will execute independently and automatically according to the prescribed rules.

A smart contract can be regarded as a self-executing procedure stored on the blockchain. Like transactions on the blockchain, the inputs, outputs and states of a smart contract are verified by each node. All blockchain systems have their programming languages to implement transaction logic. Bitcoin and its derived altcoins support non-Turing complete languages to provide limited functionality mainly in charge of validating the ownership and availability of the crypto currencies. For example, Bitcoin provides approximately 200 opcodes that can be used by developers to write stack-based programs. Ethereum is the first open-source blockchain platform that offers Turing-complete smart contract languages. A Turing-complete language refers to a programming language that supports all types of computations including loops. Due to the Turing-complete languages, Ethereum not only enables anyone to design his/her own rules, formats of transactions, and state transition functions, but also supports developers to deploy arbitrary decentralized applications in the form of smart contracts. The most popular programming language for writing smart contracts in Ethereum is Solidity [90]. The smart contracts programmed in high-level programming languages (e.g., Solidity) are compiled into low-level bytecodes by the Ethereum Virtual Machine (EVM). Then, the bytecodes are broadcast to Ethereum blockchain network. Each smart contract has its address. A smart contract can be invoked by sending a contract-invoking transaction to its address. To prevent attackers from attacking blockchain systems using programming bugs, some blockchain systems such as Tezos, Corda and Kadena provide non-Turing complete, but more powerful programming languages than Bitcoin's opcodes. For a more insightful discussion on smart contracts, please refer to [87] and [91].

The highest layer in the blockchain architecture is the application layer, which is composed of business applications, such as Internet of Things, intellectual property, market security, digital identity and so on [92]. These applications can provide new services and perform business management and optimization. Although blockchain technology is still in its infancy, academia and industry are trying to apply the promising technology into many areas.

2) Workflow of Blockchain: To understand the blockchain architecture, it is important to recall its basic operation. Fig. 5 shows the working procedure of the PoW-based blockchain network. First, a transaction related to Alice and Bob is created and signed using their private keys. The signed transaction is broadcast to neighboring nodes. Then this transaction is verified by these neighboring nodes. If the transaction is valid, it will be forwarded to other nodes. Otherwise, it will be discarded. Finally this transaction is spread across the entire network. Each miner bundles this transaction and many other transactions during the time period into a block. PoW algorithm is executed by all miners to find a nonce value which makes the block header hash value less than a "Difficulty Target". Once the nonce value is found by a miner, the miner will add a timestamp to the block and broadcast the time-stamped block to the blockchain network. Other miners need to validate the time-stamped block. If all transactions in the block are proved to be valid, the block will be added to the chain.

C. Motivations of Applying Blockchain Technology to Smart Cities

Nowadays, many countries and cities have presented their smart city projects. For example, the Government of India plans to develop 100 smart cities [93]; Singapore has presented

the Smart Nation initiative, which aims to improve living, create economic opportunities and build closer communities by leveraging networks, big data and information technologies [94]. A number of cities such as Dublin, Amsterdam, Barcelona, Madrid and Manchester, are also actively pursuing their smart city strategies.

In order to promote the simulation and evaluation of smart city solutions, some smart city testbeds have been developed. SmartSantander [95] is the most well-known smart city testbed. The SmartSantander testbed has deployed 2000 IoT devices, 400 parking sensors, 200 GPRS modules and 2000 joint RFID tag/QR code labels in the city of Santander, Spain. Now it has implemented eight use cases, including environmental monitoring, outdoor parking area management, mobile environmental monitoring, traffic intensity monitoring, guidance to free parking lots, parks and gardens irrigation, augmented reality and participatory sensing [96]. City of Things [97] is a smart city testbed located in the city of Antwerp, Belgium, supporting the setup of experiments on three different levels: network level, data level and user level. NYUAD [98] is a smart city testbed developed by the Center for Cyber Security in New York University Abu Dhabi (CCS-AD). The purpose of NYUAD is to provide a realistic and real-time smart city environment for researchers to perform security evaluations. The ParticipAct Living Lab testbed [99] monitored the behaviour of 300 students at the University of Bologna over the course of one year to conduct Mobile Crowd Sensing (MCS) experiments.

Despite these smart city testbeds, a lot of challenges need to be addressed prior to the implementation and deployment of smart cities. In addition to some non-technological factors such as high financial investment and skilled human resource requirement, there are also some technological challenges in developing and implementing smart cities.

- Data collection and analysis can help to effectively provide public services to citizens and improve the management of cities. The data reliability and integrity are of vital importance. Unauthorized modification of data is not allowed [100].
- The number of devices and the complexity of applications in smart cities are increasing as time goes by. Devices and nodes in smart cities can connect or leave the network flexibly. Compared with centralized systems, decentralized systems are more suitable for the dynamic scenarios where the number of devices and the complexity of applications are fluctuant.
- City management is related to everyone. Citizens have a strong desire for participation, democracy and transparency. The government should disclose city management-related information to citizens, such as government affairs information, environmental information, and the decision-making process. In addition, companies also need to disclose how the customer-related information is used.
- The sharing of data such as IoT data, organizational data of companies and personal data of citizens, has the potential to offer high-value smart city services and improve the city management and decision making. However, lack of incentives, market confidence and trust has a bad effect on data sharing among the government, organizations and individuals.

The following features of blockchain make it an attractive technology to address these challenges in smart cities.

- Decentralization: The blockchain systems run normally in a peer-to-peer manner without a centralized third party.
- Pseudonymity: In the blockchain system, each node is linked to a public pseudonymous address, keeping its real-world identity hidden. The inherent pseudonymity is suitable for use cases where the users' identities must be kept private.
- Transparency: Blockchain technology enables everyone to access all transaction records, which makes it transparent.
- Democracy: Consensus algorithms are executed by all decentralized nodes to reach an agreement before a block is included into the blockchain. Thus, in the blockchain system, decisions are made by all nodes in a peer-to-peer manner, which makes it democratized.
- Security: In the blockchain-based decentralized systems, it is difficult to have a single point of failure. Thus, the network security is enhanced.
- Immutability: In the blockchain system, all transactions are signed using digital signatures. Moreover, the data blocks are linked and secured through the one-way cryptographic hash functions. Any small modification generates a different hash and can be detected immediately, which makes the shared ledger immutable.

Due to these good features, applying blockchain technology to smart cities can ensure data integrity, encourage organizations (e.g., companies, schools, hospitals, universities, local and national government) and individuals to share data and perform joint decision making, enable transparent city management, and promote the implementation and deployment of a trusted, secure, transparent and democratized smart city.

Nowadays, many countries and cities such as Dubai, Chile, Toronto, Stockholm and Visakhapatnam have proposed blockchain-based projects. For example, Dubai's government has announced a plan to enable all government transactions and documents on the blockchain, making it the world's first blockchain-powered digital city by 2020 [101]. With the blockchain, Dubai is expected to save 100 million pages of documents every year, generate 25.1 million hours of economic productivity in savings each year, and enable citizens to save 411 million kilometers of city service-related travel every year.

The blockchain technology enhances the smart cities significantly. In the following, we use a general blockchain-based e-voting system as a use case to further elaborate how the blockchain technology can be used to promote the implementation of a trusted, secure, transparent and democratized smart city. As shown in Fig. 6, a blockchain-based e-voting system generally consists of five distinct steps, including election creation, voter registration, vote transaction, vote tallying, and vote verification.

(1) Election creation. The election administrator who manages the lifecycle of an election creates an election

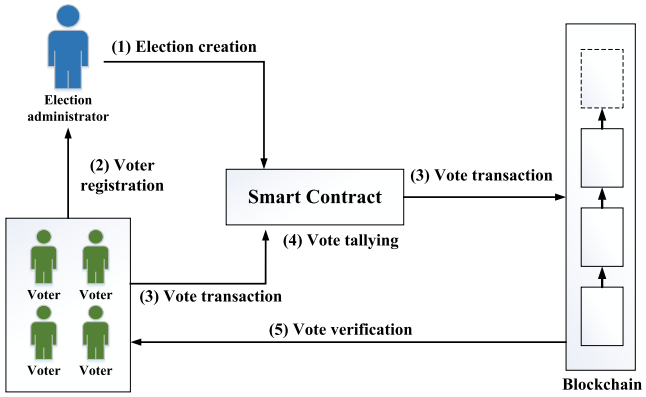


Fig. 6. A use case of applying blockchain technology to smart cities.

using an Admin decentralized application (DApp). The election administrator specifies the election type, sets election policies, defines a list of candidates, and decides the lifetime of the election. Then the Admin DApp creates an election smart contract and deploys it onto the blockchain.

(2) Voter registration. When an election is created, the election administrator must determine a list of eligible voters. Using a government identity verification component, the election administrator can authenticate and authorize eligible voters. If an individual is an eligible voter, he/she is assigned a secure digital key. And then a corresponding wallet is generated for the eligible voter. The wallet is unique for each voter and can be used to cast the vote.

(3) Vote transaction. When a voter selects a candidate and casts his/her vote, the voter proceeds to sign his/her vote using the secure digital key. After the vote data is signed, the voter's wallet will interact with the election smart contract. The smart contract only processes legal votes, which mean that the voter is eligible and has not voted before, and the vote is cast during the election period. If the vote is legal, the smart contract broadcast the vote data as a transaction to all blockchain nodes. If the majority of blockchain nodes agree upon the vote data, consensus for the particular vote is reached. Then the transaction that holds the vote data is appended onto the blockchain permanently and the transaction ID is sent to the corresponding voter.

(4) Vote tallying. The tallying of the election is done automatically by the election smart contract according to the vote transactions that are stored on the blockchain. When the election is finished, the final result is published.

(5) Vote verification. As mentioned earlier, each eligible voter receives the transaction ID of his/her vote data. The transaction ID can be used by voters to access the blockchain and locate the corresponding transaction. The voters can therefore see their vote data, verify the validity of the election tallying process, and confirm the accuracy of the election results.

From the detailed description of a general blockchain-based e-voting system, we conclude that the blockchain technology can be used to create a secure, transparent, traceable, verifiable and democratic voting system. First, the decentralized system makes the voting process less vulnerable to manipulation and attack, and only allows eligible individuals to vote in an election. Second, all vote transactions stored on the blockchain are public to all voters, making the voting process transparent, traceable and verifiable. Third, the vote transactions stored on the blockchain are agreed by all blockchain nodes using consensus algorithms. The election smart contract enables that the vote data storage, the tallying of an election, and the determining of an election result are done automatically. Thus no one entity can control the voting process and manipulate the vote data, which makes the voting process more democratic.

Although the above use case focuses on e-voting system, similar blockchain-based use cases can be derived for other aspects in smart cities, such as transportation, education, healthcare, etc.

IV. Blockchain in Smart Cities

There are many aspects in smart cities, including smart citizen, smart healthcare, smart grid, smart transportation, supply chain management, smart business, smart home, smart government, smart education and others. In this section, we review existing blockchain efforts in each aspect. We will give readers a summary on how blockchain technology is applied in the realm of smart cities.

A. Smart Citizen

Citizens are the core of smart cities. Analyzing citizens' personal data has many benefits, such as providing personalized services, accelerating innovation and economic growth, predicting future market trends, and optimizing companies' decision-making process [102], [103]. In recent years, with the rapid growth of urban population, citizens' personal data increases exponentially. Nowadays, these data is constantly collected, stored and analyzed by centralized service providers such as Facebook and Google. This centralized way causes that citizens have little knowledge about how their personal data is used. However, citizens are willing to control their personal data. The blockchain is a promising technology that allows citizens to collect, store, and control the access to their personal data. In the section, we will summarize these related studies.

1) Personal Data Storage: In recent years, citizens' personal data increases rapidly. How to store these data securely, while ensuring data integrity, is a challenging task. Blockchain's transparency, security and immutability features make it an ideal choice for personal data storage. Many studies have been done to improve the personal data storage by applying blockchain technology.

The work in [104] focuses on the personal archive storage. A blockchain-based personal archive storage system is proposed to realize authenticity, accuracy and transparency. The system consists of various roles, such as subject, certifier, client and stake node. A subject is a person who owns digital artifacts. A certifier is an entity that provides certification to the subject. A client is an organization who wants to gain access to the personal digital artifacts. The stake node is

responsible for maintaining the blockchain by utilizing DPoS as the consensus algorithm.

In [105], a personal data storage framework called BCPDS is proposed to realize notary and autonomy. The BCPDS is based on the existing OpenPDS/SafeAnswers framework. In BCPDS, the blockchain technology is utilized as a notary to store personal metadata securely. In order to improve the autonomy property, the AutoNomy-based Access Control (ANAC) mechanism is presented.

Reference [106] proposes a secure P2P online storage scheme, in which the encrypted user data is divided into some parts, and each part is delivered to a randomly selected P2P storage node via the anonymous communication. In order to restore the stored user data correctly in a dynamic situation where the state of the P2P network varies over time, the blockchain technology is utilized to record the storage node lists periodically. The security of the proposed scheme has been discussed in a qualitative manner to show that the proposed scheme is resistant to many attacks.

Do and Ng [107] focus on the data storage in the federated cloud. A blockchain-based system called BlockDS is proposed to store data securely and ensure the data integrity. The system is composed of three general parties, including data owner, data consumer, and the blockchain nodes. The data owner provides personal documents. Each document contains a set of keywords. A data consumer is a subscriber for the personal documents. A keyword search component is used by the data consumer to retrieve only the required documents. Separate cloud service providers in the federated cloud are blockchain nodes. In the proposed system, the encrypted documents are stored in the off-chain cloud data storage system, while the encrypted keyword tags are stored on the blockchain.

2) Personal Data Access Control: Access control aims to assign permissions to indicate who can access information. In our society, citizens have little knowledge about how their personal data is used. However, citizens are willing to control where their personal data is stored and who can access their data. With the rapid growth of urban population, it becomes difficult to manage the access control of all citizens' personal data relying on a centralized access control server. Some researchers try to enhance the personal data access control using the blockchain technology.

Reference [108] proposes a blockchain-based decentralized personal data access control system. As shown in Fig. 7, the system includes three entities: users, services and nodes. Users are interested in mobile phone applications. Services are the applications' providers who require personal data to improve their business, such as targeted ads and personalized services. The responsibility of nodes is to maintain the blockchain. T_{access} and T_{data} are two types of transactions on the blockchain. T_{access} is used for access control management. T_{data} is used for data storage and retrieval.

In [109] and [110], a decentralized user-centric access control model is proposed, which is shown in Fig. 8. The model is composed of three main components: data management protocol, messaging service, and data store system. The blockchain technology is used in the data store system to store access control data, based on which the data requesters can know whether they are allowed to access the data owners' personal data.

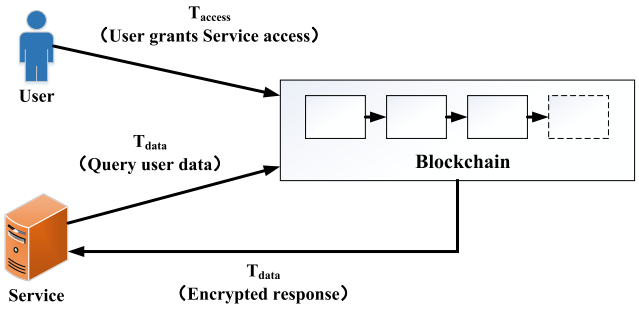


Fig. 7. Overview of a decentralized personal data access control system [108]. The system includes three entities: users, services and nodes. Users are interested in mobile phone applications. Services are the applications' providers who require personal data to improve their business. The responsibility of nodes is to maintain the blockchain. T_{access} and T_{data} are two types of transactions on the blockchain.

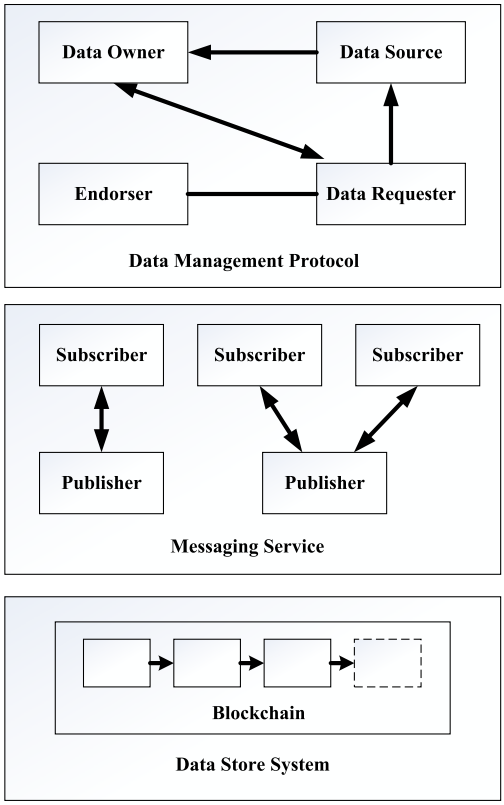


Fig. 8. Overview of a decentralized user-centric access control model [109], [110]. The model is composed of three main components, including data management protocol, messaging service, and data store system. Data management protocol enables the interaction among different roles. Based on the publish-subscribe architecture, the messaging service is able to provide scalable, flexible and reliable communication between senders and receivers. Data store system is designed to store access control data based on the blockchain technology.

3) Personal Data Exchange: In recent years, data is becoming a valuable asset in our society and economy. Therefore, data exchange markets are becoming more popular. In the data exchange markets, the data owners can share or sell their data to the data consumers. However, current data exchange markets are centralized, where all participants have to trust an

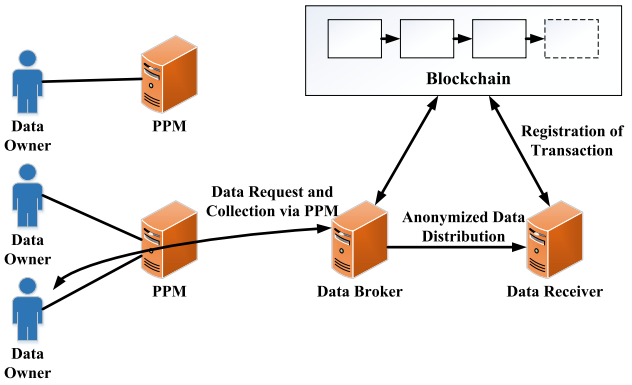


Fig. 9. Overview of an anonymized dataset exchange platform [111]. The platform consists of five entities, including data owner, PPM, data broker, data receiver, and blockchain. A data owner is a person who provides his/her personal data. The PPM is responsible for managing data owners' privacy settings. The data broker aims to collect personal data with the data owner's consent, generate an anonymized dataset and distribute it to the data receivers. The anonymized dataset is used by the data receivers to improve their services. The blockchain is applied to record transactions between the data brokers and the data receivers.

authorized third party. In the centralized markets, the data owners and customers need to pay some management fees to the authorized third party. Moreover, a single point of failure may occur. To overcome these challenges, the blockchain technology can be used by the data owners and customers to build a decentralized data exchange market cooperatively.

In [111], an anonymized dataset exchange platform is proposed, which is shown in Fig. 9. The platform consists of five entities, including data owner, Privacy Policy Manager (PPM), data broker, data receiver, and blockchain. The data broker aims to collect personal data with the data owner's consent, generate an anonymized dataset and distribute it to the data receivers. The anonymized dataset is used by the data receivers to improve their services. The blockchain is applied to record transactions between the data brokers and the data receivers.

Reference [112] proposes a blockchain-based data exchange system, which enables all participants to exchange data in a peer-to-peer way. Transaction logs between the data owners and the data consumers are recorded on the blockchain. Smart contracts are used to ensure the rules in data exchange, such as the data copyright and the use of personal data.

4) Improvement of Citizens' Activities: The blockchain and smart contracts are also used by some researchers to improve citizens' activities, such as will drafting and probating [113], the storage of breeder documents [114], and the volunteer service time management [115].

Reference [113] focuses on will drafting and probating. The blockchain technology is used to keep the will drafting tamper-proof, secure and transparent, as well as to increase the speed of will probating. By using the blockchain-based Smart Will system, the beneficiaries can be freed from the pain of fighting for their rights. The transparency of blockchain technology also lets the government monitor the processing of wills.

The long-term security of breeder documents is studied in [114]. The authors present an efficient conceptual architecture to enhance the long-term security of breeder documents. In the architecture, the breeder documents equipped with biometric information are stored on the blockchain. The biometric information is utilized to establish a strong link between breeder documents and their holders.

In [115], a blockchain-based volunteer time record system is proposed to realize the traceability and transparency of the entire time record process. Smart contracts are utilized to guarantee the effective time recognition without tedious certification rules. The system consists of four entities: volunteer information center, government department, local organization and volunteer. The responsibility of volunteer information center is to manage timecoin, which is used to record volunteer service time and activity information. Government department such as Communist Youth League, needs to apply for the timecoin according to volunteer activities. Local organization such as volunteer association, is in charge of initiating and registering a volunteer activity, and distributing timecoin to volunteers after the completion of the volunteer activity.

5) Lessons Learned: Key lessons learned from the review of the blockchain-based solutions discussed above are summarized below.

- The transparency, security and immutability features of blockchain make it an ideal choice for personal data storage. The ever-increasing personal data is generally stored off the chain, while only the keyword tags [107] or data references [108] are stored on the blockchain. The blockchain-based data storage systems ensure that citizens have the ownership of their personal data.
- There are two ways to enhance the personal data access control by applying the blockchain technology. One way is to store the access control policies on the blockchain securely, according to which a data requester can know his/her permissions to access the personal data. Another way is programming the access control policies as smart contracts, and therefore the access control can be managed automatically. With the two ways, citizens can adjust their access control policies flexibly.
- The blockchain can also be used to build a decentralized, transparent data exchange market, where transactions between the data owners and the data consumers are recorded on the blockchain. Moreover, smart contracts can be used to ensure the rules in data exchange automatically, such as the data copyright and the use of personal data.
- Another application of the blockchain and smart contracts is to improve citizens' activities, such as will drafting and probating, the storage of breeder documents, the volunteer service time management, and so on.

B. Smart Healthcare

Health is the foundation of citizens' happy life. Citizens have gained benefits greatly from the advances in medical technology [116]. However, due to the rapid urbanization of world's population, traditional healthcare is not enough to meet the demands of citizens. The contradiction between the ever-growing demand and the limited resources, makes

it necessary to evolve traditional healthcare into the intelligent, efficient and sustainable healthcare. The realization of smart healthcare is related to many components, such as wearable devices, smart hospitals, smart emergency response and smart ambulance systems. The patient data is very important for the efficient treatment of patients. In smart healthcare, the patient data sharing among different hospitals can help nurses and doctors to judge a patient's condition and make real-time decisions on patient health even in remote locations. Applying blockchain in smart healthcare has several advantages [117], [118]. For example, medical data can be stored on the blockchain in a secure, immutable way. Patients can control the use of their medical data and manage the access to their data flexibly. In the following, the related research on blockchain-based smart healthcare solutions will be summarized.

1) Health Data Sharing and Storage: Healthcare is a data-intensive domain where a large amount of medical data is created, stored and accessed daily. In the traditional healthcare system, a patient's medical data is scattered across different hospitals, resulting that each hospital does not have the patient's complete historical medical data, which has a bad effect on the treatment of patients and the quality of healthcare services. Thus, it is necessary to share patients' medical data among different healthcare providers (e.g., hospitals). On the other hand, patients' medical data is very important for healthcare decisions. Any data tampering is not allowed. How to store the medical data securely, while guaranteeing the data integrity, is a challenging task. The rapid development of blockchain technology promotes the sharing and storage of medical data. Patients' medical data can be shared and stored on the blockchain in an immutable, secure and reliable way.

Reference [119] presents a distributed Electronic Health Records (EHR) storage and processing system that integrates the blockchain, IoT and big data technologies. IoT devices can collect a huge amount of EHR data. The collected data is stored on the blockchain-based BigchainDB [120]. Big data tools are used to process data.

The work in [121] proposes a Healthcare Data Gateway (HDG)-centric healthcare architecture that enables patients to manage and control their own medical data securely. The HDG-centric healthcare architecture (shown in Fig. 10) is composed of three layers: data storage layer, data management layer, and data usage layer. The blockchain is used in the data storage layer to store personal medical data securely and immutably.

In [122], a blockchain-based smart healthcare system is proposed to protect physiological signals from the human body, which is shown in Fig. 11. The system is composed of a Body Sensor Network (BSN) and a health blockchain. The BSN is deployed on a user's body to collect various physiological signals. The collected data is stored on the health blockchain.

Reference [123] proposes a blockchain-based approach to share healthcare information among institutions effectively and securely. In the approach, an emerging standard, called Fast Healthcare Interoperability Resources (FHIR) [124], is chosen as the sharing format of electronic health records. In order to ensure blockchain consistency and interoperability, a Proof of Interoperability mechanism is proposed.

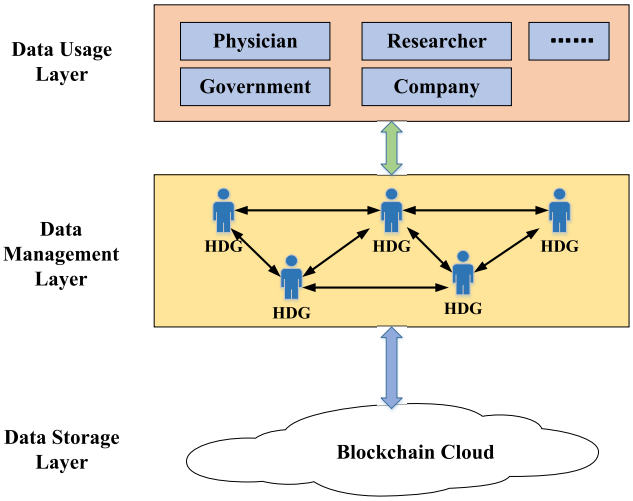


Fig. 10. The HDG-centric healthcare architecture [121]. The responsibility of data storage layer is to store medical data securely and immutably. A set of connected HDGs are included in the data management layer. The data usage layer consists of entities that use the patients' medical data.

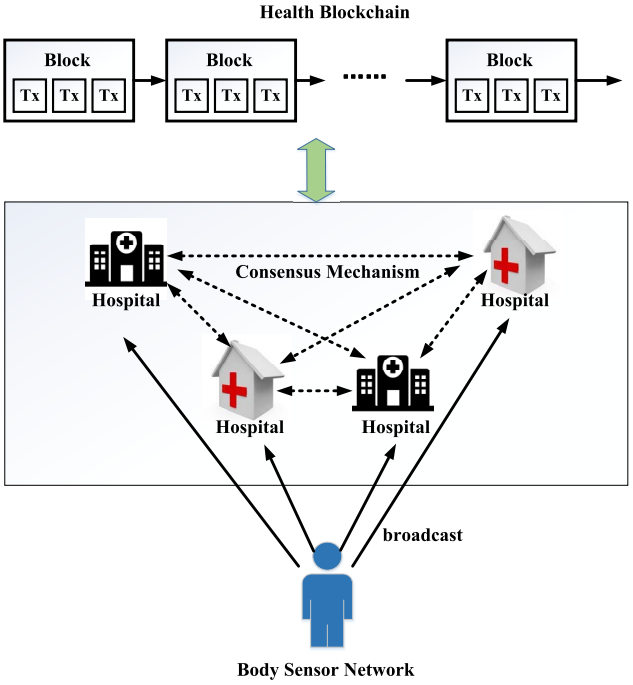


Fig. 11. A smart healthcare system [122]. The system is composed of a BSN and a health blockchain. The BSN is deployed on a user's body and includes many wearable devices and implanted devices. The user's various physiological signals collected by wearable devices and implanted devices are broadcast to some hospitals. Each hospital is a blockchain node. The health blockchain is maintained by all blockchain nodes using consensus mechanism, digital signature and hash chain technologies.

In [125], a blockchain-based healthcare system is proposed to enable secure health data sharing among Pervasive Social Network (PSN) nodes. The system consists of two areas: Wireless Body Area Network (WBAN) area and PSN area. In WBAN area, an improved protocol based on IEEE 802.15.6 is proposed to establish secure links between sensor nodes

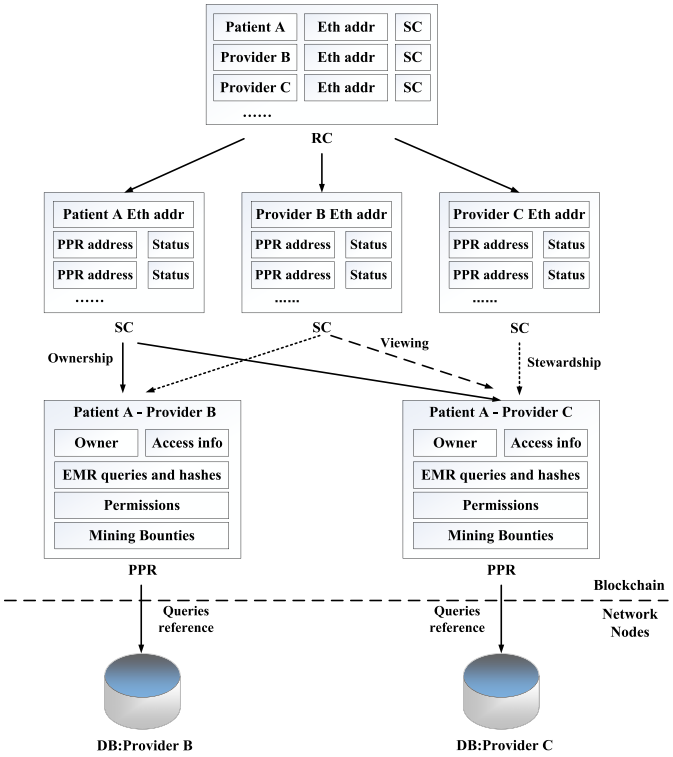


Fig. 12. The contract structures and relationships in MedRec [126], [127]. MedRec consists of three main contracts: RC, PPR and SC. RC stands for Registrar Contract, PPR for Patient-Provider Relationship Contract, SC for Summary Contract. The responsibility of RC is to map participants' identities to their Ethereum addresses. The PPR is issued between the healthcare providers and patients when storing and adjusting the access control policies of medical records. The SC is responsible for locating participants' medical record history by holding a list of references to PPRs.

and mobile devices. In PSN area, the blockchain is utilized to enable health data sharing among PSN nodes.

2) Health Data Access Control: In the traditional healthcare system, patients' medical data is managed by hospitals, whereas patients are deprived of the right to control their own medical data and do not know how their medical data is used. Because the medical data usually contains patients' personal and sensitive information, patients have a strong need to control their own medical data and protect their data from unauthorized access. The blockchain provides a secure, decentralized framework for patients to control the access to their medical data.

In [126] and [127], a blockchain-based decentralized record management system, called MedRec, is proposed to handle Electronic Medical Records (EMRs). Medical stakeholders such as public medical institutions and researchers, are motivated to participate in the blockchain network as "miners". In MedRec, smart contracts are utilized to enable automatic access control of medical records. MedRec consists of three main contracts: Registrar Contract (RC), Patient-Provider Relationship Contract (PPR), and Summary Contract (SC), shown in Fig. 12.

In [128], a public health blockchain is used to control access to personal health data, and enable secure sharing of electronic health data among individuals, healthcare providers and medical researchers. All health records and medical data are stored off the blockchain in a data repository called data lake. Only access control policies and the encrypted links to the health records are stored on the blockchain.

Genestier *et al.* [129] study the consent management in the eHealth environment. A blockchain-based consent management solution is proposed to allow patients to control the access to their personal data. Smart contracts are used by patients to manage their consent policies flexibly.

In [130] and [131], a blockchain-based system called MeDShare is proposed to provide medical data provenance, auditing and access control among cloud service providers. Smart contracts are utilized to monitor the actions performed on the medical data and revoke malicious users' permissions to access medical data automatically.

Reference [132] proposes a blockchain-based framework to share EMR data among healthcare providers for cancer patient care. By collaborating with the Department of Radiation Oncology in a major U.S. hospital, a practical prototype has been developed to ensure security, availability, and fine-grained access control over EMR data. In the prototype, the encrypted patients' data is stored in a cloud service, the metadata and access control policies defined by the patients are stored on the blockchain.

3) Lessons Learned: Key lessons learned from the review of the blockchain-based solutions discussed above are summarized below.

- The blockchain technology promotes the sharing and storage of medical data. Entities (e.g., healthcare providers and medical researchers) who are interested in medical data, are motivated to maintain a blockchain collectively in a decentralized way, based on which patients' complete medical histories can be stored. The volume of medical data is immense, so the raw medical data is generally stored off the chain, while only the pointers to medical data are stored on the blockchain for checking the authenticity and accuracy of the off-chain medical data.
- Another application of the blockchain in the smart healthcare domain is medical data access control. Patients can use the blockchain and smart contracts to specify access control policies flexibly. Only authorized users are allowed to access patients' medical data. In this way, patients become the owners of their medical data and can control the access to their medical data automatically to improve their own lives and health.

C. Smart Grid

Worldwide, most of the electricity energy comes from fossil energy (e.g., coal, oil and natural gas). Over utilization of fossil energy results in environmental pollution and greenhouse gas emission. In order to protect the environment (e.g., atmosphere and water), renewable energy (e.g., solar energy and wind energy) is being used more widely. Moreover, with the development of new battery energy storage, a large number of consumers will evolve into prosumers, which can utilize the renewable energy to generate and store electricity energy. In this scenario, to provide an efficient, secure, economical and sustainable power grid system, smart grid [133], [134] is

proposed. Managing a large number of consumers and prosumers is a challenging issue for the conventional centralized power grid, so decentralized power grid system is a trend of the smart grid. The blockchain technology not only promotes the realization of a trusted, reliable and effective decentralized power grid system [135], [136], but also enhances the stability and data security of smart grid systems. In the following, we will review recent studies that apply blockchain technology to the smart grid.

1) Electricity Energy Trading: The emergence of the prosumers makes the boundary of supply and demand in traditional power systems blurred, and promotes the development of decentralized power systems. In the decentralized power systems, how to build a trusted, reliable and effective electricity energy trading model among a large number of prosumers is an important task. The blockchain technology offers a new opportunity for designing a decentralized market. In the smart grid domain, the blockchain can help to provide a transparent and trusted electricity trading market where the prosumers participate to trade electricity energy in a decentralized approach.

Cheng *et al.* [137] analyze the basic characteristics of a decentralized power system and the blockchain technology. A blockchain-based distributed electricity trading model is presented. The transaction information is stored on the blockchain. In order to maintain the stability of the electricity market and facilitate the balance of electricity production and consumption, an effective pricing mechanism is proposed.

In [138], a blockchain-based electricity trading system with Digitalgrid router is proposed to provide a secure and decentralized control over the electricity exchange between consumers and prosumers. The blockchain is used to ensure the security and accuracy of the electricity exchange transactions. Digitalgrid router is leveraged to control power flow and realize electricity exchange.

Reference [139] focuses on the conceptual implementation of a sustainable local energy trading market. A proof-of-concept model including 100 residential households is implemented on the Ethereum blockchain. In the model, an operational auction mechanism is used to match the demand and supply. The auction mechanism and payment are conducted automatically via smart contracts deployed on the blockchain.

Kvaternik *et al.* [140] study the Transactive Energy System (TES). TES is a decentralized model where end users play an active role in both power consumption and production. A blockchain-based transaction management platform called PETra is presented. As shown in Fig. 13, the PETra is composed of three types of components: Distribution System Operator (DSO), prosumer and smart contract. In [141] and [142], the same authors focus on the communication and transactional anonymity in PETra. Solutions such as garlic routing and ring signatures, can be used to improve the communication and anonymity in PETra.

In [143], a blockchain-based decentralized transactive energy auction system is proposed to enable trustworthy, secure and transparent energy exchange. The system consists of four key entities, including bidders, sellers, smart meters, and smart contracts. When energy is available, sellers initiate new auctions and advertise the available energy to the blockchain. Bidders monitor the new auctions and submit bids. The smart meters are used to report how much energy is sold or consumed during a time period. The auction data from bidders, sellers and smart meters is stored on the blockchain. Then, the Vickrey second price auction and payment functions are executed automatically via smart contracts.

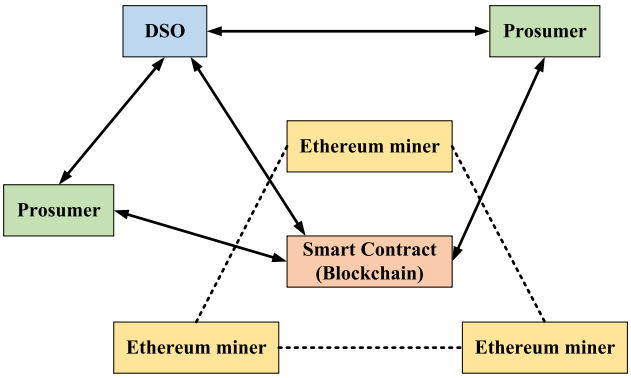


Fig. 13. Components of PETra [140]–[142]. The PETra is composed of three types of components: DSO, prosumer and smart contract. There is only one DSO in PETra, which is responsible for ensuring the microgrid's safe operation and regulating the total load of the microgrid. Each household has a prosumer component, the responsibility of which is to trade energy production and consumption for its household. The smart contracts deployed on Ethereum blockchain are used to keep track of the energy and financial asset transactions among different components.

Reference [144] focuses on the identity privacy and transaction security in the smart grid energy trading system. A decentralized token-based energy trading system called PriWatt has been proposed to enable peers to negotiate energy prices and perform energy trading in an anonymous and secure way, by leveraging blockchain technology, multi-signature approach, and anonymous encrypted messaging streams.

In [145], an electricity energy production and distribution architecture called Helios is proposed to support automatic energy exchange. The Helios model is divided into three layers: the energy grid, the middleware controller, and smart contracts. The energy grid is composed of devices such as solar panels, batteries, smart meters and IoT devices. The energy produced by a prosumer is stored in the user's local battery. Smart contracts are used to monitor and account energy exchange, enabling prosumers to trade energy automatically in a limited geographical area. The middleware controller interconnects the energy grid with the smart contracts.

2) Enhancement of Stability and Data Security in Smart Grid: Recently, Distributed Energy Resources (DERs) such as photovoltaic panels and battery storage systems are deployed to produce electricity energy locally using renewable energy (e.g., solar energy) [146]. DERs can meet part of the local power consumption and reduce the electricity energy transmission loss over long distances. Each individual DER wants to inject all available power into the grid to maximize its revenue. However, the electricity energy produced by renewable energy is erratic [147]. Injecting all DERs' available power into the grid may cause erratic voltage behaviors. In order to

keep the grid stable, [148] proposes a blockchain-based control strategy, in which a subset of DERs act as voltage regulators to decrease their individual power injected into the grid. In order to motivate DERs to participate in the voltage regulation, the DERs that act as voltage regulators are paid a certain amount of credit by other DERs. The credit information of all DERs is recorded on the blockchain. Smart contracts are used to ensure proportional fairness, which means that in the long term, all DERs fairly participate in the voltage regulation.

In smart grid systems, data security is very important for both electricity companies and their customers. On the one hand, customers want to avoid overpaying and know how the electricity is used by their appliances. On the other hand, inaccurate data can mislead the control center of a grid system to make bad decisions that may cause system disturbance and financial loss. Therefore, ensuring the data integrity and accuracy is of critical importance for both electricity companies and their customers. The attractive characteristics of blockchain such as immutability, non-repudiation and decentralization make it suitable for data integrity, accuracy and security in smart grid systems.

In [149], a blockchain-based system is proposed to protect consumer data (e.g., electricity usage) that is recorded and transferred onto the smart grid systems. The blockchain is used to record consumer data in an immutable and decentralized way. Smart contracts are used to monitor all actions performed in the grid systems automatically and identify malicious usage of electrical power and electrical data.

Reference [150] proposes a blockchain-based data protection framework to enhance data security of power systems. In the proposed framework, smart meters as blockchain nodes maintain a distributed ledger storing meter measurement data to ensure the data integrity and consistency.

3) Renewable Energy Finance: The financial system is the main driving force for the generation and trading of renewable energy by introducing economic factors to motivate prosumers and consumers to generate and consume renewable energy. Mihaylov *et al.* [151], [152] introduce a blockchain-based digital currency called NRGcoin for the trading of renewable energy in smart grids. When a prosumer supply 1 kWh of renewable energy to the grid, he can get 1 NRGcoin. In contrast, consumers need to pay NRGcoins for the consumption of renewable energy from the grid. The NRGcoins can be exchanged in an open market at any time using fiat currencies such as Euro, Pound, Dollar, etc. Reference [153] proposes a demonstration platform that uses NRGcoin as the digital currency to exchange renewable energy. SolarCoin [154] is another blockchain-based digital currency that is designed to reward solar energy generation. The solar energy producers are rewarded 1 SolarCoin per 1 MWh of solar electricity generation. In [155], Guarantees of Origins (GoOs) are used as tokens for the trading of renewable energy. The renewable energy producers can get benefit from selling GoOs to consumers.

Green bond is an effective financial way to raise finance for renewable energy projects. A green bond is a type of financial instrument that is issued to fund projects that have positive environmental or climate benefits such as renewable energy utilization, energy efficiency improvement, projects leading to reduced carbon emission and so on. The first green bond was issued by the European Investment Bank (EIB) and the World Bank in 2007. In the last decade, the green bond issuance has grown significantly and in 2017, the green bond issuance reached $163 billion. Green bonds can be issued by a wide range of issuers including the government, financial institutions (e.g., commercial banks) and companies. For example, in 2015, Southern Power in the USA completed the green bond issuance of $1 billion for renewable energy generation projects [156]; in 2016, a Moroccan green bond was issued to fund the world's largest concentrated solar plant Noor PV 1; Italian utility Enel issued a green bond to bid for an 850 MW wind project in Italy; French energy giant EDF issued a corporate green bond to build wind and solar farms [157]; Fiji issued a sovereign green bond to help achieve its target of 100 percent renewable energy by 2030.

However, the rapid development of green bond markets poses some challenges. Stakeholders are still unclear about the entire life cycle of a green bond and associated processes. In other words, tracking the funded money and verifying that the money has indeed gone into the green projects are hard for stakeholders. Kottackal Green Bond [158] has been implemented to enhance the transparency. The use of funded money in Kottackal Green Bond is transparent and autonomous depending on various conditions that have been programmed as smart contracts on the blockchain.

4) Thing-to-Thing Electricity Trading: In the future IoT systems, nearly everything will be connected to the Internet. It is difficult to manage the rapidly increasing number of devices using the traditional centralized approach. Thus, decentralized IoT systems are the future direction. The blockchain technology facilitates thing-to-thing interactions. Reference [159] shows that the blockchain technology has the potential to establish a Machine-to-Machine (M2M) electricity trading market in Industry 4.0.

In [160], a proof-of-concept system is implemented to examine the feasibility of using blockchain for autonomous thing-to-thing electricity payments. In the system, the smart cable can pay the connected smart socket for delivering electricity without any human intervention.

5) Lessons Learned: Key lessons learned from the review of the blockchain-based solutions discussed above are summarized below.

- The blockchain technology can promote the implementation of a decentralized, transparent and trusted electricity trading market, where prosumers as blockchain nodes maintain a distributed ledger to store electricity transaction information. Smart contracts are generally used to enable that the electricity energy trading and payments are conducted automatically.
- In smart grid systems, data security is very important for both electricity companies and their customers. The attractive characteristics of blockchain such as immutability, non-repudiation and decentralization make it suitable for data integrity, accuracy and security in smart grid systems. In general, the blockchain is used to store meter measurement data, while smart contracts are used to monitor the usage of electrical power and electrical data.

- The blockchain can also speed up the development of renewable energy finance. On one hand, the blockchain can be used to record transaction information related to renewable energy digital currencies such as NRGcoin and SolarCoin. On the other hand, the blockchain and smart contracts can be used to track the use of funded money and improve the transparency about the entire life cycle of a green bond.
- Another application of the blockchain is to facilitate thing-to-thing electricity trading and payments in the future IoT systems.

D. Smart Transportation

With the advancement of information communication and technology, smart vehicles have attracted widespread attention in recent years. To enable smart vehicles, it is essential for vehicles to access the Internet and communicate with each other through smart transportation, which is also known as Intelligent Transportation System (ITS) [161]. Smart transportation aims to provide comfort and convenience for drivers and passengers, improve traffic and travel efficiency, and enhance vehicle road safety. In smart transportation, a vehicle usually has multiple network interfaces (e.g., WiFi, DSRC, UMTS, WiMax and Bluetooth) to communicate with Road-Side Units (RSUs) and ambient vehicles. The distributed nature of blockchain technology can enhance the robustness of smart transportation and improve the vehicle communication management and information sharing. With the help of blockchain, a decentralized, trusted and secure smart transportation system can be established. In the following, the related research on blockchain-based smart transportation solutions will be summarized.

1) Decentralized Smart Transportation Architecture: Although the centralized vehicular networks make it easy for governmental institutions to perform surveillance and management, they may result in a single point of failure. To overcome the security risks, the blockchain technology is used by some researchers to build a decentralized vehicular network.

Reference [10] presents a blockchain-based ITS framework. As shown in Fig. 14, the ITS framework is composed of seven layers: physical layer, data layer, network layer, consensus layer, incentive layer, contract layer and application layer.

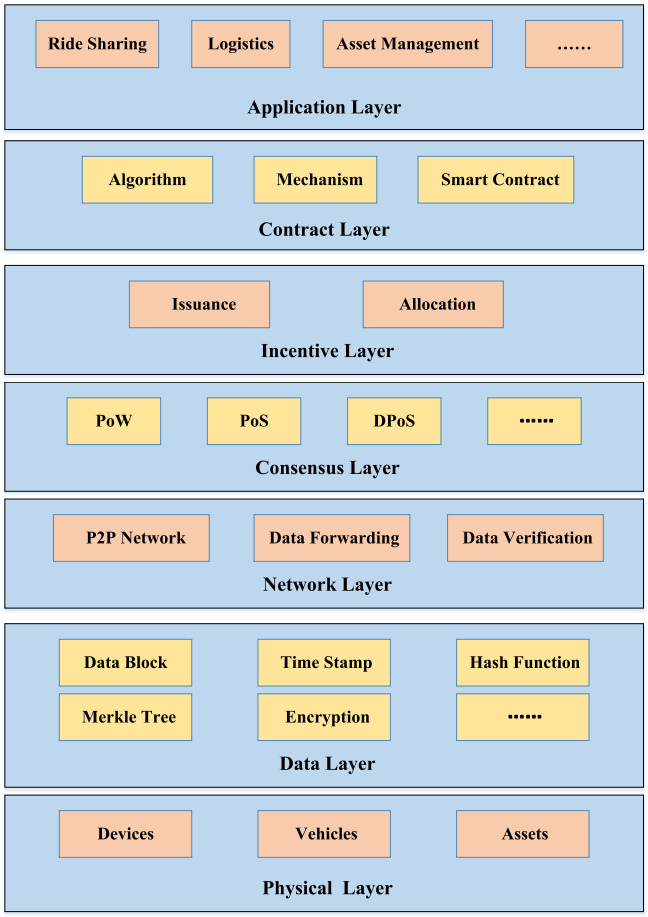


Fig. 14. A blockchain-based ITS framework [10]. The framework is composed of seven layers. The physical layer consists of devices, vehicles and assets. The data layer stores the chained data blocks. The distributed networking, data forwarding and verification mechanisms are specified in the network layer. The consensus layer consists of various consensus algorithms. The reward mechanisms are specified in the incentive layer. The contract layer packages various scripts, algorithms and smart contracts. The application layer is composed of potential ITS-oriented applications.

In [162], a decentralized and self-managed Vehicular Ad-hoc Network (VANET) is proposed. Smart contracts are utilized to promote the development of decentralized VANET applications. The decentralized applications are deployed in RSUs.

Sharma *et al.* [163] propose a blockchain-based vehicular network architecture called Block-VN, the objective of which is to build a reliable, secure and distributed transport management system in smart cities. The service scenarios and design principles for Block-VN are discussed.

Lei *et al.* [164] focus on secure key management in vehicular networks. A novel blockchain-based system (shown in Fig. 15) is proposed to simplify the distributed key management. In the system, the third-party authority (i.e., central manager) is removed and the key transfer processes are authenticated by the decentralized Security Manager (SM) network.

2) Vehicle Communication Management: Sharing road-related messages (e.g., road conditions and traffic congestions) among vehicles can improve the traffic safety and efficiency. However, due to the intrinsic characteristics of vehicular networks such as high mobility of vehicles and dynamic traffic conditions, vehicles usually cannot fully trust with each other. Inaccurate messages shared by malicious vehicles have a bad impact on traffic safety and efficiency. Thus, in the non-trusted environment, it is necessary to design an effective trust management mechanism in vehicular networks. With the rapid deployment of smart vehicles, it is impractical to manage a large number of vehicles using a fully-trusted centralized entity. In this case, decentralized systems are more effective for trust management. The decentralization, transparency and immutability features of blockchain make it an ideal choice for decentralized trust management systems.

In [165], a blockchain-based decentralized trust management scheme is proposed for vehicular networks. In the

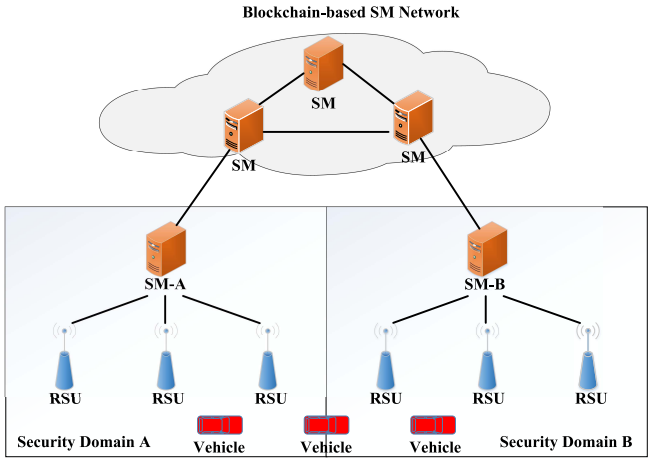


Fig. 15. A blockchain-based dynamic key management system [164]. RSUs offer an interface to route messages from vehicles to SMs. Each SM manages cryptography materials in a security domain. The third-party authority (i.e., central manager) is removed and the key transfer processes are authenticated by the blockchain-based SM network.

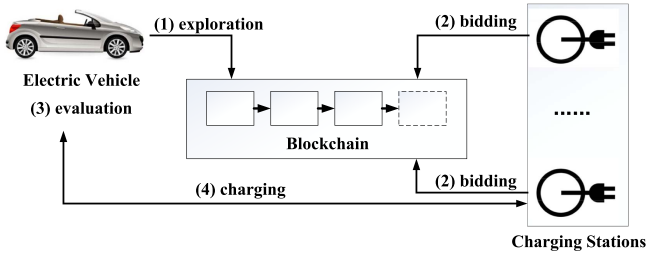


Fig. 16. A blockchain-based electric vehicle charging protocol [167]. The protocol consists of four stages: exploration, bidding, evaluation and charging. In the exploration stage, an electric vehicle sends a request to the blockchain, which contains parameters such as the amount of energy, the time interval and the geographic region. Then, the nearby charging stations send bids for this request in the bidding stage. In the evaluation stage, one optimal charging station is selected by the electric vehicle. In the charging stage, the agreed transaction is executed by the selected charging station to provide the amount of energy for a given price over a given period of time.

scheme, each vehicle first generates a rating for its neighboring vehicles according to the received messages, and then uploads the rating result to its connected RSU. Based on the rating results from vehicles, each RSU calculates the trust values of its involved vehicles and packs these data into a block. PoW and PoS are used as consensus mechanisms to add the block into the blockchain. In this way, all RSUs collaboratively maintain a reliable and consistent public ledger storing the trust values of all vehicles. Each vehicle can easily get other vehicles' trust values from RSUs, which enables vehicles to assess the trustworthiness of received messages.

In addition to trust management, motivating vehicles to share road-related messages is another challenging task. Reference [166] proposes a blockchain-based incentive vehicular announcement network called CreditCoin, in which a vehicular announcement protocol, namely Echo-Announcement, is proposed to guarantee the reliability of announcements. Moreover, a blockchain-based incentive mechanism is proposed to motivate vehicles to share road-related messages by gaining a certain amount of reputation points called the Coins.

3) Electric Vehicle Charging Management: Nowadays, in order to develop green transportation systems, electric vehicles have attracted widespread attention and have been deployed in many countries. To ensure the normal driving of electric vehicles, charging stations as the charging infrastructure are being deployed widely, especially in urban areas. In general, after the charging process from a charging station, the electric vehicle needs to pay the charging station a certain amount of money. The blockchain and smart contracts can be used to facilitate the electricity trading between electric vehicles and charging stations.

In [167], a four-stage protocol for electric vehicle charging is proposed to enable electric vehicles to charge from the optimal charging stations. As shown in Fig. 16, the four stages are exploration, bidding, evaluation and charging.

The work in [168] presents a blockchain-based P2P electricity trading system called PETCON to improve electricity trading among Plug-in Hybrid Electric Vehicles (PHEVs). Electricity transaction information is recorded in a shared ledger. An iterative double auction approach is presented to optimize the electricity prices and the amount of traded electricity among PHEVs, with the objective of social welfare maximization.

Reference [169] proposes a blockchain-based trading model called LNSC, which includes registration, scheduling, authentication and charging phases. The transaction information between electric vehicles and charging stations is stored on the blockchain. Smart contracts are used to enable an automatic trading process.

4) Lessons Learned: Key lessons learned from the review of the blockchain-based solutions discussed above are summarized below.

- The blockchain can promote the deployment of decentralized smart transportation systems, while smart contracts can be utilized to develop decentralized vehicular applications.
- Trust management in vehicular networks enables vehicles to evaluate the trustworthiness of received messages. Due to the decentralization, transparency and immutability features, the blockchain is considered as an ideal choice to deploy a decentralized trust management system in vehicular networks. A general idea is that RSUs work as blockchain nodes to maintain a consistent public ledger storing the trust values of all vehicles. In addition to trust management, the blockchain-based incentive mechanism can be used to motivate vehicles to share road-related messages.
- Nowadays, electric vehicles and charging stations have been deployed in many countries to develop green transportation systems. The blockchain and smart contracts can be used to facilitate the decentralized and transparent electricity trading between electric vehicles and charging stations. The electric vehicles' demand information (e.g., the amount of energy, the time interval and the geographic region) and the charging stations' pricing and location

information are generally stored on the blockchain, based on which each electric vehicle can choose the optimal charging station to charge. Moreover, smart contracts are often used to enable an automatic trading process.

E. Supply Chain Management

Supply chains consist of many entities related to the life cycle of products and services from the upstream and downstream markets [170]. Around the world, billions of products are designed, manufactured, delivered and sold everyday through complex and global supply chains. However, entities in supply chains have very little knowledge about the detailed information related to the life cycle of products. Product information is very useful for the supply chain management. On the one hand, consumers have requirements to obtain more product information to enhance their trust in products. On the other hand, more product information can help entities (e.g., suppliers, transporters, distributors and retailers) in supply chains to predict market trends and make business decisions. Therefore, data sharing is the most important requirement in the supply chain management. Fortunately, recent advances in blockchain technology can achieve secure and transparent data sharing [171]–[173]. In supply chain management, the blockchain can be utilized to track the detailed information of products, and prevent counterfeit products entering the markets. Moreover, the blockchain can also be used to share business information among entities in supply chains. Based on the shared business information, entities can optimize their decision-making process. Many studies have been done to improve the supply chain management by applying blockchain technology. In the section, we will summarize these related studies.

1) Product Traceability: A supply chain is composed of manufacturers and service providers that work together to provide products and services to consumers. In the increasingly globalised markets, supply chains from producers to end consumers are becoming more complex. Nowadays, due to the lack of transparency across supply chains, customers do not have enough information to validate the true value of the products and services they purchase. However, transparency is in high demand from consumers, thereby improving product traceability is a growing trend. One main feature of blockchain is transparency, which makes it a suitable technology to trace the physical flow information of products from producers to end consumers. In the case of supply chains, the blockchain can improve transparency, provide consumers with complete product information, and prevent counterfeit products entering the markets.

a) Agri-food traceability: With the improvement of people's living standards, food safety and quality have drawn much attention. From farm to fork, agri-food needs to go through many steps, such as production, processing, warehousing, distribution and sales. Any improper process in these steps can cause serious food safety risks. Thus, effective agri-food traceability is urgent. Fortunately, the blockchain can help to trace the entire process of agri-food.

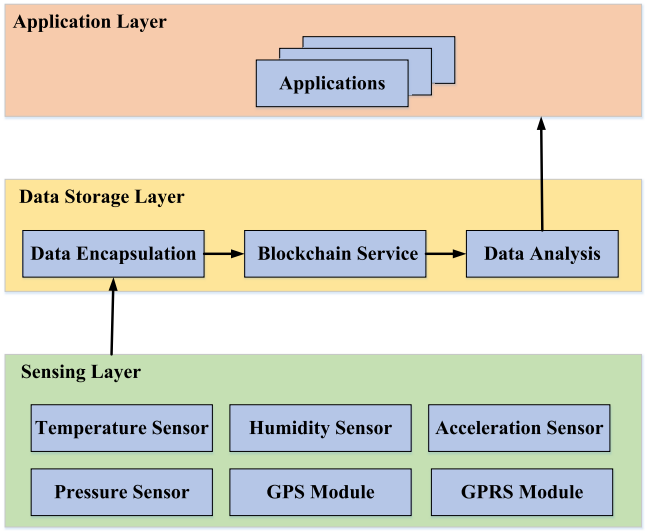


Fig. 17. Overview of a secure data storage system [176]. In sensing layer, various sensor modules are deployed to collect the real-time information of agricultural products. Application layer is composed of applications. Data storage layer is the core of the system, which includes data encapsulation, blockchain service and data analysis modules. The data encapsulation module reassembles the data from sensors. The reassembled data is stored in the blockchain service module and analyzed by the data analysis module.

In [174], an agri-food supply chain traceability system is proposed to guarantee the food safety and quality in China's markets, by leveraging the RFID and blockchain technologies. The RFID technology makes it possible to collect, circulate and share data in all links of agri-food supply chains, such as production, processing, warehousing, distribution and sales links. The blockchain technology is utilized to guarantee the reliability and authenticity of the shared information in the traceability system.

Reference [175] goes a step further and addresses the scalability issue of the blockchain-based food supply chain traceability system in [174]. BigchainDB [120] is used to store relevant data of products in food supply chains. Each participant in food supply chains can add, update and check the product information stored on the BigchainDB.

In [176], a blockchain-based secure data storage system is proposed to store the relevant tracking data of agricultural products. As shown in Fig. 17, in the system, various sensor modules are deployed to monitor the real-time information of agricultural products. Then the tracking data is stored in the blockchain-based storage module. In order to store the data automatically and make the data query more efficient, a double-chain storage structure is proposed, in which blocks including the information of the previous block form a chained structure, and transactions including the information of the parent transaction form another chained structure.

b) Industrial product traceability: Some works also use the blockchain for industrial product traceability. Data tampering is a main risk in product traceability. The immutability feature of blockchain provides tamper-proof product tracing data and enhances data integrity. The product tracing data stored on the blockchain can be used to verify the products'

origin and quality, and prevent counterfeit products entering the markets.

In [177], a novel product ownership management system (POMS) is deployed, with which customers can identify the counterfeit products. The blockchain is applied to track the products' possession information starting from their manufacturers to the current owners. Two contracts, MM (ManufacturersManager) and PM (ProductsManager), are implemented to realize "the possession of products". MM is in charge of managing the information of manufacturers. PM is operated by each manufacturer and is responsible for managing the possession information of products. Based on the Ethereum platform, a proof-of-concept experimental system has been implemented.

Reference [178] proposes a blockchain-based traceability system called originChain. Three parties are involved in originChain: product suppliers, labs, and the traceability service provider. The product suppliers are in charge of managing product and enterprise information. The labs are responsible for managing sample-testing results. The blockchain is used by the traceability service provider to store tamper-proof product information, certificates, and onsite photos.

Ownest [179] is a blockchain-based supply chain management platform that can be used to monitor a product throughout its life cycle. Each time a product is exchanged from one actor of the supply chains to another, the transaction information is recorded on the blockchain. In this way, users can easily prove that the products they own are authentic.

c) Shipment information traceability: The physical product distribution is a phase of complex supply chains that transports the products from suppliers to customers. The real-time reliable shipment tracking information is very important for product traceability. The blockchain can be used to collect and store tamper-proof reliable shipment tracking information.

The medical industry has strict environmental requirements (e.g., humidity and temperature) during the shipment of medical products. Bocek *et al.* [180] focus on the pharmaceutical supply chain management and propose a blockchain-based architecture called Modum.io AG. As shown in Fig. 18, in the Modum.io AG, sensor devices are used to monitor the temperature of each parcel during the shipment. The blockchain and smart contracts are leveraged to collect and store the temperature data automatically in an immutable and verifiable way.

In [181] and [182], a hybrid P2P physical distribution (HP3D) framework is proposed to share shipment tracking information among all stakeholders during the distribution phase of supply chains. Two kinds of blockchain ledgers, a public ledger and a private ledger, are used to record custody events and shipment information. The private ledger mainly stores sensitive information related to specific shipments when transporting high value or hazardous products such as pharmaceutical and chemical products.

2) Business Information Sharing Among Entities in Supply Chains: With the globalization of supply chains, entities have different roles in global supply chains. Each entity's business is closely related to other entities. It becomes more difficult for entities to make decisions using only local information.

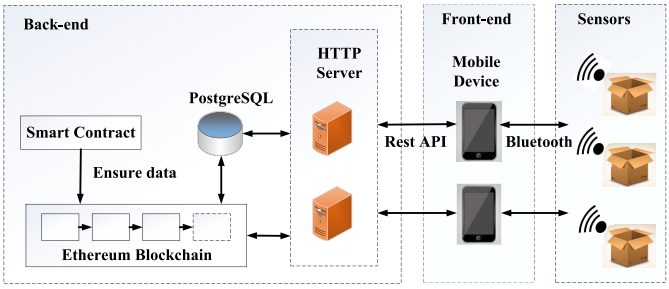


Fig. 18. Blockchain-based Modum.io AG architecture [180]. Modum.io AG consists of six main modules: Ethereum blockchain network, smart contracts, PostgreSQL database, HTTP server, mobile devices and sensors. Ethereum blockchain network and smart contracts are used to verify temperature data. The PostgreSQL database is responsible for storing raw temperature data and user credentials. The HTTP server connects the blockchain network and front-end mobile devices, and provides interfaces for mobile devices to create and modify smart contracts. Using the mobile devices, users can register new shipment and track temperature records. Sensors are in charge of monitoring the temperature data during the transport of medicinal products.

Sharing information among all involved entities in supply chains is an effective way to improve business decision-making process. The blockchain can build a transparent, automatic and trusted information sharing platform for entities.

In [183], the blockchain is used to share product orders and logistics information among companies in supply chains to reduce inventory carrying costs and optimize business decision making. Reference [184] focuses on the aviation industry in which an aircraft consists of many parts (e.g., engine and turbine) produced by multiple manufacturers. Each part has its certain life expectancy, specific requirements and maintenance. The transactions of aviation parts are recorded on the blockchain. Smart contracts are used to monitor the performance and usage of aviation parts automatically. In this way, the quality of aviation products and services is enhanced. Omran *et al.* [185] use the blockchain to share financing related information among all involved partners in supply chains transparently, which can help participants to optimize working capital allocation and reduce corporate financial risks.

3) Lessons Learned: Key lessons learned from the review of the blockchain-based solutions discussed above are summarized below.

- One application of blockchain in supply chain management is product traceability. The blockchain can be utilized to track the detailed information of products. This way not only prevents counterfeit products entering the markets, but also gives customers enough information to validate the true value of the products and services they purchase.
- Sharing business information among all involved entities in supply chains is another application of blockchain. A general idea is that all involved entities work cooperatively to maintain a consistent consortium blockchain storing the shared business information (e.g., product orders, logistics and financial information). Based on the shared information, entities can improve their business decision making such as working capital allocation, inventory management, and the optimization of production and operation activities.

F. Others

Some works also have been done by applying blockchain technology to other fields in smart cities, such as smart business, smart home, smart government, smart education, content distribution and rights management.

1) Smart Business: In recent years, e-business becomes more and more popular in our life. Applying blockchain to e-business has many advantages, such as secure data storage and sharing, decentralized marketplace, and anonymous user identity [186].

Collaborative business processes are typically beneficial for all involved participants. However, the lack of trust among participants is often a challenge. In [187], the blockchain and smart contracts are adopted to enhance the trust among participants in collaborative business processes. Transaction histories are recorded on the blockchain immutably. Smart contracts are used to control business process logic automatically.

In business activities, reputation is very important for participants. A participant's reputation measures how much other participants trust him, and is calculated according to his previous transactions and interactions with other participants. In [188], a blockchain-based P2P reputation system is proposed. When a user's request is satisfied, a transaction including the single dimensional reputation feedback information is sent to the blockchain. All users' reputation scores can be calculated based on the reputation feedback information stored on the blockchain.

Human resource management is a core element of enterprise management. The authenticity of human resource information has a direct impact on human-resource decision making. Reference [189] proposes a blockchain-based human resource management framework to enhance the authenticity of human resource information. The human resource information is stored on a private blockchain that is established by an enterprise and is open to its internal staff.

2) Smart Home: In the future, a smart home will deploy many smart devices. The smart devices need to communicate with each other to offer certain services. For example, in order to turn on the lights automatically when someone enters the home, the light bulb needs to request data from the motion sensor. The blockchain as a decentralized technology promotes the communication among devices and enables that each device in the smart home can request data from other devices directly. In [190]–[192], a private blockchain is used by the owner of a smart home to manage the communication among devices. Communication histories among local devices are recorded as transactions on the blockchain. The owner of the smart home can control the communication among devices. Devices permitted by the owner can only communicate with each other using a shared key.

Home appliances usually consume energy such as gas and electricity. Traditionally, prepaid cards or mobile devices are often used as the payment medium to pay for energy consumption. However, in the future smart home, the automatic payment is a trend without human intervention. The blockchain and smart contracts can promote the realization of automatic payment. Reference [193] proposes a secure blockchain-based smart gas payment system. The system is composed of a smart gas meter and a bitcoin platform server. The responsibility of the bitcoin platform server is to record and verify transactions. The components of the smart gas meter are shown in Fig. 19. Microcontroller and bitcoin secure payment module are two main components. The microcontroller is responsible for measuring gas flow and sending requests to the bitcoin secure payment module when the pre-paid gas is used up. The bitcoin secure payment module communicates with the bitcoin platform server directly to realize the automatic gas payment.

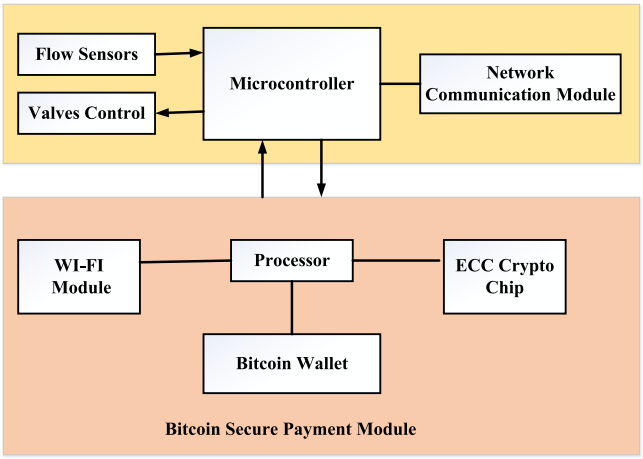


Fig. 19. The components of the smart gas meter [193]. Microcontroller and bitcoin secure payment module are two main components. The microcontroller is responsible for measuring gas flow and sending requests to the bitcoin secure payment module when the pre-paid gas is used up. The bitcoin secure payment module consists of a processor, a bitcoin wallet, an ECC crypto chip, and a WI-FI module.

In [8], the blockchain technology is utilized to enhance the communication trust among users, load aggregators and power grids. Users' electricity information is recorded on the blockchain. Moreover, smart contracts are used by users to control their home appliances automatically.

3) Smart Government: Applying blockchain to e-government has many advantages, such as improving the quality of government services, developing the individual credit system, strengthening the government's credibility, and promoting the integration of resources [194].

Ølnes *et al.* [195], [196] analyze the blockchain technology from an information-infrastructure perspective, and point out that the blockchain technology is suitable for the secure document management in the public sector due to its immutability and transparency features. For example, the Government of Honduras has collaborated with the blockchain company Factom to develop a blockchain-based land registration system for storing land titles-related information, and thereby enhancing the mutual trust between government and citizens [197].

Electronic voting is another potential application of the blockchain technology in smart government domain. Reference [198] proposes a blockchain-based e-voting system to guarantee the authenticity, integrity and non-repudiation of the vote records. In the proposed e-voting system, the vote records are stored on the Ethereum blockchain. Smart contracts

are used to check and count the votes automatically when the voting time is over.

4) Smart Education: In the education domain, the management of students' information such as course records and diplomas is an important task. Nowadays, most of the Higher Education Institutions (HEIs) use their own specialized systems to keep students' information. Students' information in different HEIs is generally stored based on different data formats. Some problems arise from the centralized storage of students' information. For example, detecting the counterfeits and frauds of students' information is a challenge, while exchanging students' information among HEIs is another challenge.

In [199], the blockchain technology is used to guarantee the authenticity of academic diplomas and detect the counterfeits and frauds. Specifically, the hashes of academic diplomas are stored on the blockchain. Digital signatures and chain-based block structure are used to guarantee the authenticity, integrity and non-repudiation of academic diplomas. Reference [200] proposes a blockchain-based global higher education credit platform called EduCTX, where HEIs, students and organizations (e.g., companies as potential employers) are the peers of the blockchain network. EduCTX provides a globally trusted, decentralized platform to process, manage, and store students' course records. A proof-of-concept prototype has been implemented based on the open-source Ark Blockchain Platform [201].

5) Content Distribution: Content distribution is one of the most popular services in people's life. Content distribution optimization can improve user satisfaction. Some works have studied the blockchain-based solutions to optimize the content distribution.

Content integrity is a basic requirement of content distribution systems. Content integrity guarantees that the delivered content has not been modified or tampered. The immutability feature of blockchain can promote the content integrity protection. Reference [202] focuses on the secure content distribution in Information Centric Networking (ICN). A blockchain-based decentralized name-based security mechanism is proposed to distribute content securely. In the mechanism, Hierarchical Identity Based Encryption (HIBE) algorithm is leveraged to provide content storage delegation, content provenance verification and content integrity protection. The system parameters required by the HIBE algorithm are stored on the blockchain. The proposed mechanism is implemented based on an open-source blockchain system called Namecoin.

In [203], a novel watermarking based multimedia blockchain framework is proposed to retrieve the transaction trails and modification histories easily. The unique watermark information contains a cryptographic hash and an image hash. The cryptographic hash can be used to retrieve the information of a multimedia content (e.g., ownership and modification history) that is stored on the multimedia blockchain. The image hash can be used to identify the tampered regions.

A content distribution system is related to multiple stakeholders, such as content owners, content providers, technical enablers and Internet Service Providers (ISPs). Handling the negotiations among these stakeholders to improve the content transmission efficiency and reduce costs is an important issue. The blockchain as a decentralized technology enables multiple stakeholders to deliver content collaboratively. In [204], a collaborative blockchain-based video delivery model is proposed to reduce the overall delivery cost. The model is composed of three blockchains, including content brokering blockchain, delivery monitoring blockchain, and provisioning blockchain. Each blockchain implements a specific function used for content delivery. The responsibility of content brokering blockchain is to handle the negotiation of the optimal content delivery session. The delivery monitoring blockchain is in charge of collecting and processing the delivery contract. The provisioning blockchain is used by content providers to handle the content distribution.

6) Rights Management: Digital rights management tries to control the use, modification, and distribution of copyrighted works (such as software and multimedia content). Traditional centralized copyright management platform such as China copyright protection center, can provide reliable copyright services. However, a large amount of money is spent to maintain the normal operation and security of the system, which leads to the high service fees. The blockchain as a decentralized technology has strong security. The data stored on the blockchain is immutable. These features of blockchain can promote the digital rights management.

In [205], a blockchain-based decentralized rights management system called BRIGHT is proposed to make the rights management more effective and secure. A trial system based on Bitcoin Core software is developed. In the trial system, rights information is stored on the blockchain. In order to reduce the latency of adding the rights information to the blockchain, the puzzle difficulty of the PoW algorithm is adjusted so that the average block interval time is five seconds.

Reference [9] proposes a blockchain-based digital rights management scheme to guarantee the quality of network media and protect the copyrights. In the scheme, consensus algorithms are used to complete the copyrights confirmation, and smart contracts are used to control the copyrights transactions. The reliability of the copyrights transactions is guaranteed by digital signatures and hash chains.

In [206], a blockchain-based digital content distribution system is proposed to enable that right holders can manage their rights by themselves. In order to reduce mining time and control it as 10 seconds, each block's hash value is limited to the condition that first four digits are 0. Furthermore, to balance the encryption/decryption cost and the security level of the proposed content distribution system, only the headers of the high resolution videos (i.e., 4K or 8K) are encrypted and decrypted.

7) Lessons Learned: Key lessons learned from the review of the blockchain-based solutions discussed above are summarized below.

- In the smart business domain, the blockchain and smart contracts can enhance the trust among participants in cross-organizational business processes. The blockchain can be used to record an immutable transaction history. Smart contracts enable that business processes (e.g., payments and escrow) are executed automatically. In

addition, the blockchain can also be used for other business activities such as reputation calculation and human resource management.

- A smart home generally has many smart devices and appliances. On the one hand, a private blockchain can be deployed by the owner of the smart home to record communication histories among local devices. On the other hand, home appliances usually consume energy such as gas and electricity. The blockchain and smart contracts can promote the realization of automatic payments.
- In the smart government domain, the blockchain technology can promote the secure document management in the public sector such as land registration, which will enhance the mutual trust among government, enterprises and citizens. Electronic voting is another potential application of the blockchain technology in the smart government domain. The blockchain is generally used to store the vote records, while smart contracts are used to check and count the votes automatically. In this way, the blockchain and smart contracts can guarantee the authenticity, integrity and non-repudiation of the vote records, and the transparency of the vote counting.
- In the education domain, the public blockchain can be used by multiple stakeholders (e.g., HEIs, students and companies) to manage students' information such as course records and diplomas. The blockchain-based system has some advantages. First, the counterfeits and frauds of students' information can be detected easily. Second, sharing information among HEIs is helpful to maintain students' complete educational information transparently. Third, the blockchain-based system enables organizations (e.g., companies as potential employers) to validate the information provided by students directly.
- For the content distribution, the immutability feature of blockchain can promote the content integrity protection. Users can identify whether the content has been modified or tampered during transmission according to the content-related information stored on the blockchain. On the other hand, the permissioned blockchain and smart contracts can be used by multiple stakeholders (e.g., content owners, content providers, technical enablers and ISPs) in a content distribution system to negotiate with each other to improve the content transmission efficiency and reduce costs.
- Digital rights management is very important for the protection of intellectual properties. In general, the blockchain can promote the copyright management by storing copyrights information on the blockchain. The immutable information stored on the blockchain provides a strong support for solving copyright disputes. Moreover, smart contracts can be used to control the copyrights transactions automatically.

Although these blockchain-based solutions have been presented to promote the development of a decentralized, transparent, secure and trusted smart city, they are still in their infancy and generally have some shortcomings.

- Many blockchain-based solutions are presented based on reasonable concepts, and remain on an idea level.
- In the existing blockchain-based smart city solutions, some details such as the used consensus algorithms and incentive mechanisms have not been discussed.
- Many blockchain-based solutions have only been discussed in a qualitative manner, but have not been analyzed in a quantitative manner.

Finally, the blockchain-based solutions discussed above are summarized in Table II and Table III. Furthermore, we also provide a comparison of pros and cons of all the blockchain-based solutions in Table IV and Table V.

V. Challenges and Future Research Directions

Despite current works being done in the blockchain-based smart cities, with the requirement of robustness and maturity in the area, many significant research challenges remain to be addressed prior to widespread implementation of blockchain-based smart cities in the near future. In this section, we discuss some challenges and present some future research directions.

A. Security and Privacy

Security and privacy are two major challenges in blockchain-based smart city systems [208]. Citizens cannot use a system that does not guarantee the privacy of citizens' data and is not resistant against cyber-attacks [209]. The privacy issue in blockchain is that users cannot stay completely anonymous but just pseudonymous. For anonymity, the objective is unidentifiable and untraceable. Although each user in blockchain is linked to a public pseudonymous address, due to the transparency of blockchain, all transactions are publicly available, and information such as the sender, receiver and amount values is explicitly visible by all network participants. By analyzing the data stored on the blockchain, users' activities can be tracked. Combining the information analyzed from the blockchain and some external information could reveal users' real-world identities. Once a user's real-world identity is revealed, all the activities of the user will be traced and his/her personal information such as some financial secrets (e.g., wealth, income and spending patterns) will be leaked. Therefore, ensuring true anonymity is very important.

Now many schemes have been presented to improve the anonymity of blockchain systems. Using a new address for each transaction is a simple way, which increases the difficulty of finding the relationship among a user's all transactions, and therefore information such as the number of currencies owned by a user cannot be analyzed. Although this remains a best practice, some deanonymization techniques such as multi-input transactions, change addresses and behavior-based clustering, can be used to link different addresses that belong to the same user [210]. Homomorphic commitments, blind signature, ring signature, composite signature, mixing service and zero knowledge proof are other methods to enhance the anonymity. Homomorphic commitments utilize homomorphic encryption technique to commit a piece of data without revealing it to the other parties. The additively homomorphic commitments are used in Confidential Transactions [211] to hide transaction amounts. Blind signature is a form of digital

TABLE II
TAXONOMY OF BLOCKCHAIN-BASED SOLUTIONS IN SMART CITIES

	Ref.	Objective	Blockchain used	Data in the blockchain	Contributions
Smart Citizen	[104]	Personal archive storage	-	Verifiable personal archive information	A blockchain-based personal archive storage system to realize authenticity, accuracy and transparency
	[105]	Personal data storage	-	Personal metadata	A personal data storage framework called BCPDS to realize notary and autonomy
	[106]	Personal data storage	-	Storage node lists information	A secure P2P online storage scheme
	[107]	Personal data storage	-	Encrypted keyword tags	A blockchain-based system called BlockDS to store data in the federated cloud securely
	[108]	Personal data access control	-	Personal data	A blockchain-based decentralized personal data access control system
	[109], [110]	Personal data access control	Bitcoin	Access control data	A decentralized user-centric access control model to enable personal data sharing
	[111]	Anonymized dataset exchange	Hyperledger Fabric	Transactions between data brokers and data receivers	An anonymized dataset exchange platform without any centralized trusted third party
	[112]	Data exchange	-	Transaction logs between data owners and data consumers	A blockchain-based data exchange system that enables all participants to exchange data in a peer-to-peer way
	[115]	Volunteer service time management	-	Volunteer service time and activity information	A blockchain-based volunteer time record system to realize the traceability and transparency of the entire time record process
Smart Healthcare	[121]	Medical data sharing	-	Personal medical data	A HDG-centric healthcare architecture that enables patients to manage and control their own medical data securely
	[122]	Healthcare data storage	-	Physiological signals	A blockchain-based smart healthcare system to protect physiological signals from the human body
	[123]	Healthcare data sharing	-	Healthcare data	A blockchain-based approach to share healthcare information among institutions effectively and securely
	[125]	Healthcare data sharing	-	Healthcare data	A blockchain-based healthcare system to enable secure health data sharing among PSN nodes
	[126], [127]	Medical data access control	Ethereum	Medical records	A blockchain-based decentralized record management system called MedRec to handle EMRs
	[130], [131]	Medical data access control	-	Medical records	A blockchain-based system called MeDShare to provide medical data provenance, auditing, and access control
	[132]	EMR data access control	Hyperledger Fabric	Patients' metadata and access control policies	A blockchain-based framework to share EMR data among healthcare providers for cancer patient care
Smart Grid	[138]	Electricity trading	Ethereum	Electricity exchange information	A blockchain-based electricity trading system with Digitalgrid router to ensure secure and decentralized electricity exchange
	[139]	Electricity trading	Ethereum	Electricity exchange information	A conceptual implementation of a sustainable local energy trading market
	[140]–[142]	Transactive energy system	Ethereum	Electricity exchange information	A blockchain-based transaction management platform called PETra
	[143]	Transactive energy system	Ethereum	Electricity auction information	A blockchain-based decentralized transactive energy auction system to enable trustworthy, secure and transparent energy exchange
	[144]	Electricity trading	Bitcoin	Electricity trading information	A decentralized token-based energy trading system called PriWatt to ensure transaction security and identity privacy
	[145]	Electricity trading	Ethereum	Electricity trading information	A solar energy production and distribution architecture called Helios to enable automatic energy exchange
	[148]	Stability of smart grid	Ethereum	Credit information of all DERs	A blockchain-based control strategy to ensure proportional fairness in the voltage regulation
	[149]	Data security of smart grid	-	Consumer data	A blockchain-based system to protect consumer data (e.g., electricity usage)
	[150]	Data security of smart grid	-	Meter measurement data	A blockchain-based data protection framework to enhance data security of power systems
	[159]	M2M electricity trading	MultiChain [207]	Electricity trading information	A proof-of-concept implementation of a blockchain-based M2M electricity trading system
	[160]	Thing-to-thing electricity payment	Bitcoin	Electricity payment information	A proof-of-concept system to examine the feasibility of using blockchain for autonomous thing-to-thing electricity payment

Continued on next page

signature in which the content of a message is blinded by the message owner using a blinding factor before it is signed. Blind signatures are typically employed in privacy-related applications that allow a participant to sign a message without knowing what the message is. Duffield and Hagan [212] utilizes an ECC-based blind signature scheme to break the links between sender and receiver addresses in a transaction. A ring signature is a digital signature that is created by a

TABLE III
TAXONOMY OF BLOCKCHAIN-BASED SOLUTIONS IN SMART CITIES (CONTINUED)

Continued from previous page

	Ref.	Objective	Blockchain used	Data in the blockchain	Contributions
Smart Transportation	[10]	Intelligent transportation system	-	Transportation-related data	A blockchain-based secure, trusted and decentralized ITS framework
	[164]	Key management	Bitcoin	Vehicle key information	A blockchain-based secure key management system
	[165]	Vehicle communication management	-	Trust values of all vehicles	A blockchain-based decentralized trust management scheme for vehicular networks
	[166]	Vehicle communication management	Bitcoin	Road-related messages	A blockchain-based incentive vehicular announcement network called CreditCoin
	[167]	Electric vehicle charging	-	Charging stations' bids information	A blockchain-based four-stage electric vehicle charging protocol
	[168]	Electric vehicle charging	-	Electricity transaction information	A blockchain-based P2P electricity trading system called PETCON to improve electricity trading among PHEVs
Supply Chain Management	[174]	Agri-food supply chain management	-	Data in all links of agri-food supply chains	An agri-food supply chain traceability system to guarantee the food safety
	[175]	Agri-food supply chain management	BigchainDB	Data in agri-food supply chains	Using BigchainDB to store relevant data of products in food supply chains
	[176]	Secure data storage	Ethereum	Agricultural product data	A blockchain-based system to store the relevant tracking data of agricultural products
	[177]	Product ownership management	Ethereum	Information of products, manufacturers and ownership transfer	A blockchain-based product ownership management system to track the products' possession information
	[180]	Pharma supply chain management	Ethereum	Temperature data	A blockchain-based system called Modum.io AG to collect and store the temperature data automatically
	[181], [182]	Shipment tracking	-	Custody events and shipment information	A framework called HP3D to share shipment tracking information among all stakeholders
	[183]	Business information sharing	-	Product orders and logistics information	A blockchain-based information sharing scheme to reduce inventory carrying costs and optimize business decision making
	[184]	Aviation supply chain management	-	Transactions of aviation parts	Blockchain-based business process in aviation industry to enhance the quality of products and services
	[185]	Supply chain finance	-	Financing related information	A blockchain-based solution to share financing related information among all involved partners transparently
Others	[187]	Collaborative business process	Ethereum	Transaction information	Using the blockchain to enhance the trust among participants in collaborative business processes
	[188]	Reputation system	Bitcoin	Reputation feedback information	A blockchain-based reputation system to reduce the computation complexity of users' reputation scores
	[189]	Human resource management	-	Human resource information	A blockchain-based human resource management framework to enhance the authenticity of human resource information
	[193]	Gas payment system	Bitcoin	Gas payment information	A secure blockchain-based smart gas payment system to enable the automatic gas payment
	[198]	Electronic voting	Ethereum	Vote records	A blockchain-based e-voting system to guarantee the authenticity, integrity and non-repudiation of the vote records
	[199]	Students' information management	Bitcoin	Hashes of academic diplomas	Using the blockchain technology to guarantee the authenticity of academic diplomas
	[200]	Students' information management	Ark Blockchain	Course records	A blockchain-based global higher education credit platform called EduCTX
	[202]	Content distribution	Namecoin	System parameters required by the HIBE algorithm	A blockchain-based decentralized name-based security mechanism to enable the secure content distribution in ICN
	[204]	Video distribution	Hyperledger Fabric	Content brokering, licensing and delivering information	A collaborative blockchain-based video delivery model to reduce the overall delivery cost
	[205]	Rights management	Bitcoin	Rights information	A blockchain-based decentralized rights management system called BRIGHT to make the rights management more effective and secure
	[9]	Rights management	-	Rights information	A blockchain-based digital rights management scheme to guarantee the quality of network media and protect the copyrights
	[206]	Rights management	Bitcoin	Rights information	A blockchain-based digital content distribution system that enables right holders to manage their rights by themselves

member of a group to sign the content of a message. It is computationally infeasible to identify the actual signing member of a group. Monero [213], a privacy-focused cryptocurrency, uses Ring Confidential Transactions [214] which combine Confidential Transactions [211] with ring signatures to hide the senders' addresses, the receivers' addresses and the

TABLE IV
ADVANTAGES AND SHORTCOMINGS OF THE BLOCKCHAIN-BASED SOLUTIONS

	Ref.	Advantages	Shortcomings
Smart Citizen	[104]	Blockchain technology is used in the personal archive storage system.	The performance evaluation of the proposed system in a quantitative manner has not been done.
	[105]	The blockchain technology and ANAC mechanism are used to realize notary and autonomy respectively.	The prototype of the proposed BCPDS framework has not been implemented.
	[106]	The security of the proposed scheme has been discussed in a qualitative manner.	The security evaluation of the proposed scheme in a quantitative manner has not been performed.
	[107]	A keyword search component is used by the data consumers to retrieve only the required documents.	Some complex requirements such as credential revocation and boolean keyword search have not been addressed.
	[108]	The raw personal data is stored on the off-chain DHT, while retaining only the data references on the blockchain.	The services can observe the raw personal data.
	[109], [110]	The blockchain technology is used to store access control data.	DoS attacks in the proposed system are not addressed.
	[111]	A prototype of the proposed platform is implemented based on Hyperledger Fabric.	The economic model for the proposed anonymized dataset exchange platform is not considered.
	[112]	The blockchain is applied to record transaction logs between the data owners and the data consumers.	The prototype of the proposed system has not been implemented.
	[115]	Smart contracts are utilized to guarantee the effective time recognition without tedious certification rules.	The prototype of the proposed system has not been implemented.
Smart Healthcare	[121]	The blockchain is used to store personal medical data securely and immutably.	The consensus algorithm and incentive mechanism are not considered.
	[122]	A health blockchain is used to store physiological signals from the human body.	The performance of the proposed scheme has not been evaluated.
	[123]	FHIR is chosen as the sharing format of electronic health records.	A robust Master Patient Index (MPI) approach to consistently identify a patient among institutions is not provided.
	[125]	An improved protocol based on IEEE 802.15.6 is proposed to establish secure links between sensor nodes and mobile devices.	The performance of a large-scale PSN-based healthcare system has not been tested.
	[126], [127]	Smart contracts are utilized to enable automatic access control of medical records.	Comprehensive experiments have not been done to evaluate the performance of the proposed system.
	[130], [131]	Smart contracts are utilized to monitor the actions performed on the medical data and revoke malicious users' permissions to access medical data automatically.	The consensus algorithm and incentive mechanism are not considered.
	[132]	A practical prototype has been developed to ensure security, availability, and fine-grained access control over EMR data.	Radiology images cannot be shared in the prototype system.
Smart Grid	[138]	Digitalgrid router is leveraged to control power flow and realize power exchange.	The demand-response matching issue has not been considered.
	[139]	A proof-of-concept model including 100 residential households is implemented on the Ethereum blockchain.	Privacy and security in the proposed blockchain-based system are not discussed.
	[140]–[142]	A blockchain-based transaction management platform called PETra is presented.	The limitations of existing smart contract programming languages (e.g., Solidity) complicate the implementation of a full-fledged TES.
	[143]	The Vickrey second price auction and payment functions are executed automatically via smart contracts.	The scalability and performance of the proposed scheme have not been explored.
	[144]	Blockchain technology, multi-signature approach, and anonymous encrypted messaging streams are applied to enhance identity privacy and transaction security.	The replication problem of a large transaction ledger has not been solved.
	[145]	Smart contracts are used to monitor and account energy exchange automatically.	The business model of the proposed system has not been studied.
	[148]	Smart contracts are utilized to ensure proportional fairness.	The mining cost and the communication cost of the blockchain-based control strategy are high.
	[149]	Smart contracts are used to monitor all actions performed in the grid systems automatically.	The prototype of the proposed system has not been implemented.
	[150]	Smart meters as blockchain nodes maintain a distributed ledger storing meter measurement data.	The deployment of the proposed framework needs to upgrade or replace existing sensing devices and communication networks.
	[159]	A proof-of-concept implementation has been done to demonstrate that the blockchain has the potential to establish a M2M electricity trading market.	Only two electricity producers and one electricity consumer are included in the proof-of-concept implementation.
	[160]	A single-fee micro-payment protocol is proposed to reduce the transaction fees.	The prototype system is hard to be deployed in the real world.

Continued on next page

amount values of all transactions. A composite signature combines many individual signatures where there is not any order among them. It is very hard to compute individual signatures from a composite signature. In [215], composite signatures are used to improve the anonymity of Bitcoin-like cryptocurrencies.

TABLE V
ADVANTAGES AND SHORTCOMINGS OF THE BLOCKCHAIN-BASED SOLUTIONS (CONTINUED)

Continued from previous page

	Ref.	Advantages	Shortcomings
Smart Transportation	[10]	A blockchain-based seven-layer conceptual framework is proposed to establish a secure, trusted and decentralized ITS ecosystem.	The technical details for the implementation of the proposed ITS framework are not discussed.
	[164]	An effective transaction collection period optimization scheme is proposed to minimize the key transfer time.	Privacy issue is not taken into consideration.
	[165]	All RSUs collaboratively maintain a reliable and consistent public ledger storing the trust values of all vehicles.	The trade-off between trust management and privacy preservation in the blockchain-based system is not discussed in detail.
	[166]	A blockchain-based incentive mechanism is proposed to motivate vehicles to share road-related messages.	The scalability of the proposed system is not discussed in detail.
	[167]	The blockchain is used to store the charging stations' bids information transparently and verifiably.	The scalability of the proposed protocol to handle a high transaction volume is not investigated.
	[168]	An iterative double auction approach is used to optimize the electricity prices and the amount of traded electricity among PHEVs.	The scalability of the proposed system is not discussed in detail.
Supply Chain Management	[174]	RFID and blockchain technologies are used to guarantee the agri-food safety and quality in China's markets.	The consensus algorithm and incentive mechanism are not considered.
	[175]	BigchainDB is used to store relevant data of products in food supply chains.	The performance of the proposed system has not been simulated.
	[176]	A double-chain storage structure is proposed to store the data automatically and make the data query more efficient.	Access control to the stored information of agricultural products has not been considered.
	[177]	A novel product ownership management system called POMS is proposed to help customers to identify the counterfeit products.	The information of manufacturers is managed by a centralized administrator.
	[180]	Raw temperature data is stored in the PostgreSQL database.	Data security inside the sensors and access control schemes are not taken into account.
	[181], [182]	Both a public ledger and a private ledger are used in HP3D.	The time complexity of queries to the public ledger is not discussed.
	[183]	A new type of transaction is proposed to support the total amount calculation of selected products.	Efficient incentive mechanism needs to be considered.
	[184]	The blockchain and smart contracts are used to enhance the quality of aviation products and services.	The trade-off between privacy and transparency in the blockchain-based system is not discussed.
	[185]	The blockchain is used to share financing related information among all involved partners transparently.	Concrete evaluation on the effectiveness of the proposed blockchain-based solution is lacked.
Others	[187]	Smart contracts are used to control business process logic automatically.	The proposed approach is not suitable for industries that have strong requirements in terms of latency such as automatic financial trading.
	[188]	A blockchain-based P2P reputation system is proposed to reduce the calculation complexity of users' reputation scores.	Privacy of the reputation system has not been considered.
	[189]	The blockchain is used to enhance the authenticity of human resource information.	The consensus algorithm and incentive mechanism are not considered.
	[193]	A bitcoin secure payment module is designed to realize the automatic gas payment.	The scalability and complexity of the proposed system are not discussed.
	[198]	Smart contracts are used to check and count the votes automatically.	The implemented e-voting system is just used for small-sized and less critical kinds of elections.
	[199]	Digital signatures and chain-based block structure are used to guarantee the authenticity of academic diplomas and detect the counterfeits and frauds.	The consensus algorithm and incentive mechanism are not considered.
	[200]	A proof-of-concept prototype has been implemented based on the open-source Ark Blockchain Platform.	The implemented prototype has not been tested in a real-life environment that includes HEIs, students and companies.
	[202]	HIBE algorithm is leveraged to provide content storage delegation, content provenance verification, and content integrity protection.	Content confidentiality and access control are not taken into account.
	[204]	A collaborative blockchain-based video delivery model is proposed to reduce the overall delivery cost.	The governance, security and privacy issues for end users have not been addressed.
	[205]	A trial rights management system based on Bitcoin Core software is developed.	The scalability of the proposed system has not been verified.
	[9]	The blockchain technology is leveraged to guarantee the quality of network media and protect the copyrights.	The performance evaluation of the proposed scheme has not been performed.
	[206]	A prototype system has been demonstrated and a lot of feedbacks have been obtained to optimize the system.	The incentive mechanism is not considered in the proposed system.

In mixing service, instead of payers paying payees directly, a mixer mixes the received currencies from many payers and then returns the same amount of currencies to their respective payees using new addresses. The mixing service makes it difficult to trace the users' activities. TumbleBit [216] is a Bitcoin-compatible mixing system that not only makes

it difficult for malicious observers to track the payers and payees involved in any given Bitcoin transaction, but also prevents the mixer itself from linking the payers and payees. Zero knowledge proof as a cryptographic technology is also used to enhance blockchain anonymity. A zero knowledge proof can prove that a proposition is true without revealing any information about what specifically makes it true. The Zero Knowledge Succinct Non-interactive ARguments of Knowledge (ZK-SNARK) [217], a zero knowledge proof technique, is the underlying cryptographic technique used in ZCash [57] to enhance the privacy of transactions. In ZCash, the creator of a transaction can use the ZK-SNARK to make a proof, which can prove that he owns a certain amount of coins and the transaction is valid without revealing private transaction information such as the sender's address, the receiver's address and the amount values. Although there are many attempts to get closer to full anonymity, achieving complete anonymity while guaranteeing the performance is complicated and needs much more further research. For a more insightful discussion on anonymity and privacy in the blockchain systems, please refer to [210].

In the case of personal data management, it is important to consider the General Data Protection Regulation (GDPR) [218] that is passed by the European Union (EU) in 2016 and becomes enforceable from 25 May 2018. The goal of GDPR is to give EU citizens more rights and control over their personal data. According to GDPR, EU citizens have the right to erase their personal data, which is in conflict with the immutability feature of the blockchain systems [219]. One possible approach to manage personal data based on blockchain technology while maintaining GDPR compliant is that the personal data is stored off the chain, and the reference to the personal data, along with a hash of the personal data and other metadata (e.g., access control policies about the personal data) are stored on the blockchain [220], [221]. The hash can be used to confirm that the personal data stored off the chain has not been tampered. The approach is a GDPR compliant solution, which makes the personal data in the off-chain storage erasable. After the data is erased, its information (e.g., reference and hash) stored on the blockchain becomes completely useless.

In blockchain systems, digital signature based on asymmetric cryptography mechanism is generally applied to verify the authentication of transactions. Currently, the Elliptic Curve Digital Signature Algorithm (ECDSA) is widely used in blockchain systems. The security of ECDSA is based on the intractability of elliptic curve digital logarithm problem. However, ECDSA is vulnerable to quantum computing attacks because solving elliptic curve digital logarithm problem is not hard for quantum computing. Post-quantum cryptography [222] has been proposed to resist quantum computing attacks. In particular, lattice-based cryptography is a main candidate of several post-quantum cryptosystems [223]. In order to enhance the security of blockchain systems, some lattice-based signature schemes [224], [225] have been proposed to resist quantum computing attacks.

B. Throughput

Throughput is another important issue when applying blockchain technology in smart cities. Currently, the throughput of the Bitcoin blockchain is restricted to approximately 7 transactions per second. The Ethereum blockchain achieves 15 transactions per second [226]. In contrast, the conventional VISA system can handle 2000 transactions per second on average [226], [227]. Transaction volumes of the PayPal payment system are 10 million transactions per day. The throughput of blockchain systems is related to the number of transactions in each block and block interval time. Taking Bitcoin blockchain as an example, the block interval time is approximately 10 minutes, and the number of transactions in each block is restricted by the block size, which is one megabyte (MB). This design is a tradeoff between scalability and security [228]. If the block size is increased, the throughput will be higher, but at the same time it will become more difficult to generate and propagate blocks. Regarding the block interval time, although the reduced block interval time can increase the throughput, it also causes the production of stale blocks, which do not contribute to the main chain. High production rate of stale blocks reduces the security of the main chain [229]. Although in this moment the Bitcoin blockchain is the most secure, it cannot be used in smart cities directly because of its throughput. Therefore, in order to support billions of devices in smart cities and sustain the huge volume of real world transactions, proper schemes need to be designed carefully to increase the throughput of blockchain systems, while maintaining enough security.

Now many solutions have been presented to improve the throughput of blockchain systems.

- Reducing the transaction size: Segregated Witness, also known as SegWit [230], separates digital signatures from the rest of the transaction data and moves the digital signatures to the end of the block. In this way, the transaction size is reduced, and one block can contain more transactions.
- Off-chain transactions: The basic idea of off-chain transactions is that if nodes make frequent transactions, off-chain micropayment channels among nodes are created to handle the multi-signature transactions off the chain instantaneously, and only the final settlement transaction is processed on the blockchain. Lightning Network [231] and Duplex Micropayment Channels [232] are two examples of off-chain transactions.
- Sharding: Sharding is an effective technique to improve the horizontal scalability of blockchain systems. With blockchain sharding, nodes are separated into different shards. Each shard only processes a small portion of all transactions. In this way, transactions are processed in parallel. Elastico [233] and OmniLedger [234] are two examples of sharding blockchain systems.
- Reducing the block interval time: In blockchain systems, block generation includes two operations: leader election and transaction serialization. Leader election is responsible for selecting one or some leader nodes. Transaction serialization means that the selected leader nodes validate

transactions and generate new blocks. In order to minimize collisions in leader election, the leader nodes are selected at a low rate. For example, in the Bitcoin blockchain, the leader node is selected every 10 minutes. In traditional blockchain systems, each leader election can only generate one new block. The coupling of leader election and transaction serialization introduces a long delay in transaction validation and block generation. In order to reduce the block interval time and improve the throughput, the slow leader election and the fast transaction serialization should be decoupled. The idea has been adopted by many solutions such as Bitcoin-NG [235], ByzCoin [236] and Solida [237].

- TDAG-based systems: TDAG is considered as the next generation of blockchain development. In the TDAG-based systems, transactions are directly added to a graph, forming a graph of transactions. Each transaction is allowed to reference multiple previous transactions. IOTA is a representative TDAG system. Tangle [50] is the underlying technology of IOTA. In the IOTA Tangle, when a new transaction joins the Tangle, it chooses two previous transactions to approve. A transaction is confirmed when it is approved by many other transactions. Since transactions do not need to wait a long time to be included in blocks, the IOTA outperforms the general blockchain systems in terms of throughput.

C. Storage

Storage is another open research area in blockchain-based smart city systems. In the end of 2017, the whole Bitcoin blockchain size was more than 140 gigabytes (GB) [238]. If the transaction volume of VISA system is processed by the Bitcoin blockchain, the blockchain size will grow rapidly at a speed of 3.9 GB per day [226], [239]. When applying blockchain technology in smart cities, a huge quantity of data will be generated by various devices and be processed by blockchain technology. However, in the traditional blockchain systems, each node must be capable of processing all transactions and maintaining the complete transactions back to the first block (i.e., genesis block). Thus, it is not possible to directly apply the blockchain technology to smart city scenarios where devices have limited storage resources. Therefore, it is necessary to study what information is stored on or off the blockchain, and how to store information in nodes with limited resources effectively.

The general idea to address the storage challenge is to combine the blockchain with the existing P2P storage or database, which is capable of storing large scale of data off the chain. The solution in [108] designs the off-chain storage using the Distributed Hash Table (DHT). The raw data is stored on the off-chain DHT, while retaining only the data references on the blockchain. The references are the SHA-256 hash of the raw data.

The InterPlanetary File System (IPFS) is a P2P distributed file system, which synthesizes successful ideas from previous P2P systems, including DHT, BitTorrent protocol, Git (i.e., a version control system), and Self-Certified Filesystems. On top of IPFS, Filecoin [240] works as an incentive layer to form an entirely distributed file storage system. Based on Ethereum and IPFS, a decentralized service marketplace system called Desema is presented [241]. In the Desema system, service metadata and large data are stored in the off-chain IPFS, and the Ethereum only stores the data references.

BigchainDB [120] is a scalable blockchain database that combines the characteristics of both blockchain and modern distributed databases. Another solution to address the storage challenge of blockchain systems is using a decentralized storage service such as Swarm [242]. Swarm is a distributed storage platform for Ethereum.

D. Energy Efficiency

Energy efficiency is one of smart city goals [243]. With the increasingly rigid environmental standards and rapidly rising energy costs, the "energy efficiency" issue should be taken into account seriously. However, some consensus mechanisms like PoW are computationally expensive. In PoW mechanism, all blockchain nodes perform very hard computations to mine the next block. Due to the redundancy in computation, the PoW is not an energy efficient approach and consumes a large amount of electricity energy [226], [228], [244]. Researchers are developing alternative less computationally expensive consensus mechanisms for blockchain systems. Mechanisms such as PoS, DPoS and some BFT-related algorithms (e.g., PBFT, Tendermint and Ripple) have been presented. However, the security of PoS and DPoS has not been rigorously analyzed. BFT-related algorithms typically lack scalability, and therefore they are not suitable for systems that involve thousands of participants. Reference [83] has proposed a new consensus protocol called Proof of Trust, which leverages a trust model to address the issues of existing consensus protocols, such as high energy consumption, security weakness, low throughput and scalability limitation. Despite the highly promising, these consensus mechanisms are still in their infancy. Therefore, it is interesting to study energy efficient consensus mechanisms for blockchain systems.

E. Incentive and Punishment Mechanisms

In smart cities, we can assume that nodes are self-interested, so that incentive mechanisms are necessary to motivate these nodes to contribute their efforts to verify data. Currency issuance and transaction fees are two common methods. For example, in Bitcoin blockchain, once a miner successfully generates a block, it will earn 12.5 new bitcoins now. In scenarios where blocks are generated by a group of nodes collectively (e.g., PBFT consensus mechanism and mining pools [245]), how to allocate the currencies and transaction fees among these nodes needs to be designed carefully. On the other hand, in order to prevent the double-spending attacks and punish malicious nodes, punishment mechanisms are also necessary for blockchain systems. One approach is to use the confirmation time, which means that the economic incentives of a node can only be spent after a long confirmation time. During the confirmation time, once a poison transaction (i.e., invalid or double-spending transaction) is found, economic incentives of

the malicious node will be invalidated. Another approach is to use the deposit. Before creating new blocks, the nodes are required to make a deposit to blockchain systems. In case of a poison transaction, the nodes are penalized and lose part of their deposit. A suitable amount of deposit is very important to this approach. If the deposit is too low, it has very little effect on malicious nodes. If the deposit is too high, acting as a node to create new blocks is expensive, and a casual node is not capable of performing the task, which will lead to centralization. Therefore, in order to encourage more organizations and citizens to participate in the blockchain-based smart cities, effective incentive and punishment mechanisms need to be designed carefully.

F. Cost

Cost is a sensitive subject for smart city design [208], [246]. In general, the cost includes design cost and operation cost [246]. The design cost is a one-time cost. A small design cost makes it possible to realize a smart city. At the same time, the operation cost is required to maintain the smart city. In order to minimize burden on the city budget and make it easier to operate a smart city system, the operation cost needs to be small. However, the cost of deploying and operating a blockchain-based system is not yet known. At present, there are scarce blockchain systems in full production except for Bitcoin blockchain [247]. It is difficult to forecast the possible cost of deploying and operating a blockchain-based smart city system at scale. Therefore, it is necessary to perform targeted experiments to test the potential cost of a blockchain-based smart city system. One possible solution is to simulate and evaluate the blockchain-based system in real-world smart city testbeds such as SmartSantander [95], City of Things [97] and NYUAD [98].

G. Regulation

Since the decentralized blockchain technology does not need a centralized authority or a trusted intermediary, in order to avoid disputes among the transacting parties, new government and industry regulations are required [247]. On the other hand, in smart cities, data is generated by different devices in different data formats, many of which are unstructured. It is not an effective way to store these unstructured and heterogeneous data in the blockchain-based systems directly. In order to share and exchange data seamlessly among different entities in smart cities, the data format and storage standards for ensuring data quality and integrity should be considered carefully [100]. Therefore, the regulation rules in blockchain-based smart city systems remain an active research direction.

VI. Some Broader Perspectives

Since blockchain-based smart cities have attracted widespread attention and been studied widely, its development can be influenced by a lot of other technologies. In the mean time, blockchain-based smart cities also have an impact on them. In this section, we briefly discuss these technologies and present some broader perspectives of applying blockchain in these technologies to promote the development of smart cities.

A. Software Defined Networking

Software Defined Networking (SDN) [248] is a promising networking paradigm, which decouples the control plane and the data plane. The network resources in SDN are managed by a logically centralized controller, which acts as the Networking Operating System (NOS). The SDN controller can program the network dynamically. Furthermore, the centralized controller has a global view of the network by monitoring and collecting the real-time network state and configuration data, as well as packet and flow-granularity information. These capabilities of SDN can reduce the overall complexity, OPerating EXpenditure (OPEX) and CAPital EXpenditure (CAPEX), and make it easier to coordinate, optimize and configure the smart cities. Network scalability is the critical issue in SDN due to the limited processing capacity of one controller. Distributed multi-controller platforms [249], [250] have been proposed to solve the issue, where the network is partitioned into several domains. Each domain has its own controller. In order to provide a global network view to the upper-layer applications, the communication among multiple controllers is necessary to exchange information. The blockchain as a distributed technology is helpful to enhance the communication among multiple controllers. In [251], a fog node is composed of distributed SDN controllers. The blockchain technology is used to connect the SDN controllers in a distributed manner, making the communication among them reliable and efficient. Reference [252] proposes a distributed blockchain-based secure SDN architecture called DistBlockNet. SDN controllers work as blockchain nodes to manage the forwarding devices' flow tables in the data plane cooperatively.

B. Network Function Virtualization

Network Function Virtualization (NFV) [253] is a promising technology to enable a more flexible and open network architecture, by decoupling network functions from the underlying specialized hardware. NFV makes network reconfiguration quick and adaptive. In addition, it can reduce ISPs' capital expenditures for scaling up the network. NFV and SDN are two closely related technologies to make the network easy to control and manage. The difference between them is that SDN is applied to control network resources, while NFV focuses on the softwarization of network functions by using virtualization technologies. In the NFV systems, Virtualized Network Functions (VNFs) are instantiated as Virtual Machine (VM) instances to provide specific services. Recent advances in blockchain technology can improve the virtual resource management, VM configuration management and VNF integrity verification. In [254], the blockchain is used for the secure configuration management of VNFs by recording the VNF configuration and management information on the blockchain, which ensures non-repudiation, immutability and integrity. Reference [255] uses the blockchain in cloud computing and NFV systems to enhance the authentication and integrity of VM orchestration operation history.

C. Edge Computing

With the popularity of smartphones and wearable gadgets, such as smart glass, smart watch and smart bracelet, Edge Computing as a novel paradigm has attracted widespread attention. In recent years, a few Edge Computing architectures have been presented, such as Cloudlet, Edge Computing, Fog Computing, Mobile Cloud Computing (MCC), Mist Computing and Mobile Edge Computing (MEC) [256]. Edge Computing makes it possible to deploy blockchain in mobile environments. The mining process in blockchain is a computation-intensive task, which requires a lot of computing resources. However, mobile devices in smart cities generally have limited computing resources. Fortunately, Edge Computing can be utilized to address the challenge. Mobile devices can offload the computation-intensive mining task to the edge computing nodes [257].

Now Edge Computing technology has been adopted to promote the implementation of mobile blockchain. In [258] and [259], the edge computing service provider is the seller of computing resources, while the miners (e.g., mobile devices) are buyers. A two-stage Stackelberg game model is used to optimize pricing schemes of the edge computing service provider and to decide on the computing resource demand of each miner. In [260], an auction-based edge computing resource allocation mechanism is proposed to maximize the social welfare. Reference [261] proposes a deep learning-based auction algorithm for edge computing resource allocation to maximize the revenue of the edge computing service provider.

D. Internet of Things

In the future, nearly everything will be connected to the Internet, from traditional communication tools (e.g., laptops and smartphones) to home appliances (e.g., refrigerators and garage doors). The IoT is the foundation of smart cities [262]. The IoT is a network that uses standard communication protocols to interconnect various heterogeneous physical devices (called Things), including smartphones, computers, vehicles, sensors, smart meters, wearable devices and so on. Current IoT systems generally rely on a centralized cloud processing center to identify, authenticate and connect all devices. However, it is difficult for the centralized cloud processing center to manage the rapidly increasing number of devices. Thus, decentralized IoT systems are a future direction. The blockchain technology is an ideal choice to connect, coordinate and control billions of devices.

Now the blockchain technology has been utilized in many aspects of IoT. The works in [263] and [264] focus on the blockchain-based IoT business model. Reference [265] proposes a decentralized key management system that stores the public keys of IoT devices on the blockchain. In [266], the blockchain technology is used to store the identities and attributes of both users and devices. Reference [267] proposes a blockchain-based access control framework for IoT called FairAccess that enables users to own and control their data. The works in [268] and [269] use the blockchain to enhance the security of communication among IoT devices. For a more insightful discussion on the applications of blockchain technology in IoT, please refer to [37].

E. Tactile Internet

Different from IoT which relies on machine-to-machine (M2M) communications with a focus on smart devices (e.g., vehicles, sensors, smart meters and wearable devices), the Tactile Internet adds a new dimension to human-to-machine (H2M) communications by leveraging devices that enable haptic and tactile sensations [270]. As the number of tactile/haptic devices increases in smart cities, the Tactile Internet would help complement citizens by enabling them to remotely steer/control real and virtual tactile/haptic devices of their environment such as robots [271], [272]. This opens up completely new opportunities for existing and new applications in many fields. Potential Tactile Internet applications range from industry automation, autonomous driving, robotics [273], [274], healthcare, virtual and augmented reality, to individualized manufacturing, education, gaming, and unmanned autonomous systems [275]. Most of these envisioned Tactile Internet applications require very low latency, data integrity, accountability, high reliability, availability and security [272]. To meet these design requirements, a distributed (i.e., decentralized) service platform architecture is needed to keep the Tactile Internet applications local, close to the users [270].

The blockchain as a distributed technology has the potential to promote the realization of a trusted, reliable and effective Tactile Internet architecture. Recently the Optical Zeitgeist Laboratory has started a research project [276] which aims to combine the capabilities of emerging blockchain and Tactile Internet technologies to build a truly distributed P2P architecture. The architecture will promote the interaction among humans, machines and smart contracts, and enable a resilient, autonomous, and decentralized control for Tactile Internet applications using smart contracts. Clearly, the integration of blockchain and Tactile Internet will become a main driver for economic growth and innovation, help reshape our society in a more decentralized way, and therefore improve citizens' quality of life.

F. Information Centric Networking

In recent years, data traffic in our world is growing explosively. Mobile video is a major contributor to traffic growth. It is forecasted that mobile video will account for 78% of total mobile data traffic by the end of 2021 [277]. The situation is further aggravated by the emerging trend of adopting higher definition video contents. Thus, how to optimize content distribution over a limited network capacity has become a hot research field in recent years. In this case, Information Centric Networking (ICN) [278], [279] has been presented. Content-centric communication model is the key feature of ICN. Currently, there are a few ICN architectures, such as Named-Data Networking (NDN), Scalable and Adaptive Internet Solutions (SAIL), Architecture and Design for the Future Internet (4WARD), Publish Subscribe Internet Technology (PURSUIT), and Data-Oriented Network

Architecture (DONA). Both the ICN and blockchain are distributed technologies. The integration of these two promising technologies is able to optimize network performance and make the content distribution more effective. Fotiou and Polyzos [202] utilize the blockchain to enhance the security of the name-based content distribution in ICN. In [280], it is proved that NDN is helpful to update the stored block information of each node in blockchain systems.

G. Cloud Computing

Cloud computing has been widely deployed in our modern information systems. Both academy and industry are interested in the cloud computing technology because of its good capabilities, such as high scalability, satisfied availability, expected performance, affordable investment, enhanced fault-tolerance capability and so on [281]. Traditional cloud computing system aims to address the computation explosion issue by integrating large-scale IT resources (i.e., networking, caching and computing resources). Although traditional cloud computing system provides on-demand IT resources dynamically, it cannot meet the requirements of global cloud services. In this case, cloud federation is proposed as a new generation of cloud computing to provide cross-cloud services by enabling the collaboration among independent cloud service providers. In cloud federation system, the provision of cross-cloud services needs to share data among different cloud service providers. Thereby, the stored data is available to both the cloud service provider owning the data and other cloud service providers in the federation system.

To support secure data sharing in the cloud federation system, the blockchain technology is applied for access control in [282] and [283]. The access control policies are programmed as smart contracts stored on the blockchain to enable automatic access control management. In [284], a blockchain-based reputation system called DC-RSF is proposed to evaluate the credibility of cloud service providers. The credit value of each cloud service provider is stored on the blockchain. Reference [285] focuses on data provenance. The blockchain is used to record the data operation history.

H. Machine Learning

Typically, smart cities can provide various applications by leveraging large-scale distributed systems to connect billions of sensors and devices. There is no doubt that devices in smart cities will generate a large amount of data [286]. In order to address the challenges of rapid increasing in data generation and the number of devices, an intelligent, efficient, secure, cost-effective and scalable smart city system needs to be designed. Machine learning techniques can be utilized to promote the implementation of such system and provide intelligent services by processing the generated data effectively.

Recently, there is an increasing trend of integrating machine learning with blockchain. Reference [287] proposes a blockchain-based dynamic access control system, where access control policies are programmed as smart contracts. Reinforcement learning algorithms are used to optimize and adjust access control policies dynamically, based on which smart contracts are updated accordingly. In [288], a blockchain-based decentralized system is proposed for users to evaluate and exchange machine learning models. First, a user who has a problem to solve, creates a smart contract, including a dataset, an evaluation function and a reward amount. Any user can try to train a machine learning model and submit his/her potential solution. Then, all the submitted solutions are verified and evaluated automatically. After the evaluation stage, the user who submits the best machine learning model will get the reward. In this way, machine learning models are evaluated and exchanged automatically.

VII. Conclusion

This article provided a survey of current blockchain technology applied to smart cities. We began our discussion with some related survey papers and background knowledge of smart cities and blockchain. Then, how blockchain technology is applied in the realm of smart cities was discussed in detail, from the perspectives of smart citizen, smart healthcare, smart grid, smart transportation, supply chain management and others. We also discussed some significant research challenges and future research directions in blockchain-based smart cities, including security and privacy, throughput, storage, energy efficiency, incentive and punishment mechanisms, cost and regulation. Finally, we explored some broader perspectives, such as SDN, NFV, edge computing, IoT, ICN, cloud computing and machine learning.

In summary, research on applying blockchain technology in smart cities is quite broad and many challenges lay ahead. Nevertheless, it is favorable for the network community to address the challenges and go forward. This article attempts to briefly explore how blockchain technology works and when it should be used to solve problems in smart cities. We hope that our discussion and exploration may open a new avenue for the development and implementation of smart cities.

References

[1] United Nations. (Dec. 2017). *Population Division*. [Online]. Available: http://www.un.org/en/development/desa/population/

[2] National Bureau of Statistics of China. (Dec. 2017). *China's Population and Its Composition*. [Online]. Available: http://www.stats.gov.cn/english/

[3] K. Davis, "The urbanization of the human population," in *The City Reader*. New York, NY, USA: Routledge, 2011, pp. 2–11.

[4] R. Rivera, J. G. Robledo, V. M. Larios, and J. M. Avalos, "How digital identity on blockchain can contribute in a smart city environment," in *Proc. IEEE ISC2*, Wuxi, China, Sep. 2017, pp. 1–4.

[5] T. Nam and T. A. Pardo, "Conceptualizing smart city with dimensions of technology, people, and institutions," in *Proc. ACM dg.o*, College Park, MD, USA, 2011, pp. 282–291.

[6] E. Tabane, S. M. Ngwira, and T. Zuva, "Survey of smart city initiatives towards urbanization," in *Proc. IEEE ICACCE*, Durban, South Africa, Nov. 2016, pp. 437–440.

[7] J. Sun, J. Yan, and K. Z. K. Zhang, "Blockchain-based sharing services: What blockchain technology can contribute to smart cities," *Financ. Innov.*, vol. 2, no. 1, p. 26, Dec. 2016.

[8] G. Cui *et al.*, "Application of block chain in multi-level demand response reliable mechanism," in *Proc. IEEE ICIM*, Chengdu, China, Apr. 2017, pp. 337–341.

[9] R. Xu, L. Zhang, H. Zhao, and Y. Peng, "Design of network media's digital rights management scheme based on blockchain technology," in *Proc. IEEE ISADS*, Bangkok, Thailand, Mar. 2017, pp. 128–133.

[10] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *Proc. IEEE ITSC*, Rio de Janeiro, Brazil, Nov. 2016, pp. 2663–2668.

[11] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: http://www.ild-group.si/uploads/product/20/bitcoin.pdf

[12] V. Fernandez-Anez, "Stakeholders approach to smart cities: A survey on smart city definitions," in *Proc. Smart-CT*, Málaga, Spain, 2016, pp. 157–167.

[13] M. Batty *et al.*, "Smart cities of the future," *Eur. Phys. J. Spec. Topics*, vol. 214, no. 1, pp. 481–518, 2012.

[14] C. Yin *et al.*, "A literature survey on smart cities," *Sci. China Inf. Sci.*, vol. 58, no. 10, pp. 1–18, 2015.

[15] G. Kakarontzas, L. Anthopoulos, D. Chatzakou, and A. Vakali, "A conceptual enterprise architecture framework for smart cities: A survey based approach," in *Proc. IEEE ICE-B*, Vienna, Austria, Aug. 2014, pp. 47–54.

[16] S. Ijaz, M. A. Shah, A. Khan, and M. Ahmed, "Smart cities: A survey on security concerns," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 2, pp. 612–625, 2016.

[17] G. Pan *et al.*, "Trace analysis and mining for smart cities: Issues, methods, and applications," *IEEE Commun. Mag.*, vol. 51, no. 6, pp. 120–126, Jun. 2013.

[18] W. Shuai, P. Maillé, and A. Pelov, "Charging electric vehicles in the smart city: A survey of economy-driven approaches," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 8, pp. 2089–2106, Aug. 2016.

[19] W. M. da Silva *et al.*, "Smart cities software architectures: A survey," in *Proc. ACM SAC*, Coimbra, Portugal, 2013, pp. 1722–1727.

[20] G. Kuk and M. Janssen, "The business models and information architectures of smart cities," *J. Urban Technol.*, vol. 18, no. 2, pp. 39–52, 2011.

[21] E.-S. Lohan, T. Kauppinen, and S. B. C. Debnath, "A survey of people movement analytics studies in the context of smart cities," in *Proc. IEEE FRUCT*, Jyväskylä, Finland, Nov. 2016, pp. 151–158.

[22] E. Al Nuaimi, H. Al Neyadi, N. Mohamed, and J. Al-Jaroodi, "Applications of big data to smart cities," *J. Internet Services Appl.*, vol. 6, no. 1, p. 25, Dec. 2015.

[23] S. Djahel, R. Doolan, G.-M. Muntean, and J. Murphy, "A communications-oriented perspective on traffic management systems for smart cities: Challenges and innovative approaches," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 125–151, 1st Quart., 2015.

[24] L. Wang and D. Sng, "Deep learning algorithms with applications to video analytics for a smart city: A survey," *arXiv preprint arXiv:1512.03131*, 2015.

[25] A. Gharaibeh *et al.*, "Smart cities: A survey on data management, security, and enabling technologies," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2456–2501, 4th Quart., 2017.

[26] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[27] T. Anagnostopoulos *et al.*, "Challenges and opportunities of waste management in IoT-enabled smart cities: A survey," *IEEE Trans. Sustain. Comput.*, vol. 2, no. 3, pp. 275–289, Jul./Sep. 2017.

[28] R. Petrolo, V. Loscri, and N. Mitton, "Towards a smart city based on Cloud of Things, a survey on the smart city vision and paradigms," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 1, pp. 1–11, 2017.

[29] C. Perera, Y. Qin, J. C. Estrella, S. Reiff-Marganiec, and A. V. Vasilakos, "Fog computing for sustainable smart cities: A survey," *arXiv preprint arXiv:1703.07079*, 2017.

[30] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE BigDataCongress*, Honolulu, HI, USA, Jun. 2017, pp. 557–564.

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

[32] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," *IJ Netw. Security*, vol. 19, no. 5, pp. 653–659, 2017.

[33] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 3rd Quart., 2016.

[34] U. Mukhopadhyay *et al.*, "A brief survey of cryptocurrency systems," in *Proc. IEEE PST*, Auckland, New Zealand, Dec. 2016, pp. 745–752.

[35] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *Proc. IEEE ICACCS*, Coimbatore, India, Jan. 2017, pp. 1–5.

[36] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, Aug. 2017.

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

[38] R. G. Hollands, "Will the real smart city please stand up? Intelligent, progressive or entrepreneurial?" *City*, vol. 12, no. 3, pp. 303–320, 2008.

[39] M. Al-Hader, A. Rodzi, A. R. Sharif, and N. Ahmad, "Smart city components architecture," in *Proc. IEEE CSSim*, Brno, Czech Republic, Sep. 2009, pp. 93–97.

[40] M. Al-Hader, A. Rodzi, A. R. Sharif, and N. Ahmad, "SOA of smart city geospatial management," in *Proc. IEEE EMS*, Athens, Greece, Nov. 2009, pp. 6–10.

[41] E. L. Glaeser and C. R. Berry, *Why Are Smart Places Getting Smarter*, vol. 2, Taubman Center Policy Brief, Bloomfield Hills, MI, USA, 2006.

[42] J. V. Winters, "Why are smart cities growing? Who moves and who stays," *J. Regional Sci.*, vol. 51, no. 2, pp. 253–270, 2011.

[43] R. Giffinger *et al.*, "Smart cities: Ranking of European medium-sized cities," Centre Regional Sci., Vienna Univ. Technol., Vienna, Austria, Rep., 2007.

[44] R. Giffinger and H. Gudrun, "Smart cities ranking: An effective instrument for the positioning of the cities?" *Architecture City Environ.*, vol. 4, no. 12, pp. 7–26, 2010.

[45] "Boise smart city initiative committee report," Boise Smart City Initiative Committee, Rep., 2002.

[46] S. J. Palmisano, *A Smarter Planet: The Next Leadership Agenda*, vol. 6, IBM, New York, NY, USA, Nov. 2008.

[47] H. Lindskog, "Smart communities initiatives," in *Proc. ISOneWorld*, vol. 16, 2004, pp. 83–101.

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

[49] Y. Sompolinsky, Y. Lewenberg, and A. Zohar, "SPECTRE: A fast and scalable cryptocurrency protocol," IACR Cryptol. ePrint Archive, Rep. 2016/1159, 2016.

[50] S. Popov. (Oct. 2017). *The Tangle*. [Online]. Available: http://iotatoken.com/IOTA_Whitepaper.pdf

[51] A. Churyumov. (2016). *Byteball: A Decentralized System for Storage and Transfer of Value*. [Online]. Available: https://byteball.org/Byteball.pdf

[52] (Dec. 2017). *Ethereum*. [Online]. Available: https://www.ethereum.org/

[53] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project, Yellow Paper, pp. 1–32, 2014.

[54] E. Androulaki *et al.*, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. ACM EuroSys*, Porto, Portugal, 2018, pp. 1–15.

[55] (Jun. 2018). *Litecoin: An Open Source P2P Digital Currency*. [Online]. Available: https://litecoin.org/

[56] D. Schwartz, N. Youngs, and A. Britto, "The Ripple protocol consensus algorithm," San Francisco, CA, USA, Ripple Labs Inc., White Paper, 2014.

[57] E. B. Sasson *et al.*, "Zerocash: Decentralized anonymous payments from Bitcoin," in *Proc. IEEE SP*, San Jose, CA, USA, May 2014, pp. 459–474.

[58] (Jun. 2018). *Sawtooth Lake*. [Online]. Available: https://sawtooth.hyperledger.org/docs/core/releases/1.0/introduction.html

[59] J. Morgan. (Jun. 2018). *Quorum*. [Online]. Available: https://www.jpmorgan.com/global/Quorum

[60] (Jun. 2018). *Monax*. [Online]. Available: https://monax.io/

[61] L. Goodman. (Aug. 2014). *Tezos: A Self-Amending Crypto-Ledger Position Paper*. [Online]. Available: https://tezos.com/static/papers/position_paper.pdf

[62] R. Brown, "Introducing R3 Corda^{TM}: A distributed ledger designed for financial services," *R3CEV Blog*, 2016.

[63] (Jun. 2018). *Kadena*. [Online]. Available: http://kadena.io/

[64] W. Martino, "Kadena: The first scalable, high performance private blockchain," White Paper, 2016.

[65] 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.

[66] F. R. Yu, "A service-oriented blockchain system with virtualization," *Trans. Blockchain Technol. Appl.*, vol. 1, no. 1, pp. 1–10, 2019.

[67] X. Xu *et al.*, "A taxonomy of blockchain-based systems for architecture design," in *Proc. IEEE ICSA*, Gothenburg, Sweden, Apr. 2017, pp. 243–252.

[68] "Survey on blockchain technologies and related services," Nomura Res. Inst., Tokyo, Japan, Rep., Dec. 2017. [Online]. Available: http://www.meti.go.jp/english/press/2016/pdf/0531_01f.pdf

[69] T. V. Lakshman and A. K. Agrawala, "Efficient decentralized consensus protocols," *IEEE Trans. Softw. Eng.*, vol. SE-12, no. 5, pp. 600–607, May 1986.

[70] D. Larimer. (Nov. 2013). *Transactions as Proof-of-Stake*. [Online]. Available: https://bravenewcoin.com/assets/Uploads/TransactionsAsProofOfStake10.pdf

[71] S. King and S. Nadal, "PPCoin: Peer-to-peer crypto-currency with proof-of-stake," *Self-Published Paper*, vol. 19, Aug. 2012.

[72] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, vol. 99. New Orleans, LA, USA, 1999, pp. 173–186.

[73] D. Larimer, "Delegated proof-of-stake," Bitshare, White Paper, 2014.

[74] D. Mazieres, *The Stellar Consensus Protocol: A Federated Model for Internet-Level Consensus*, Stellar Develop. Found., San Francisco, CA, USA, 2015.

[75] J. Kwon, "Tendermint: Consensus without mining," *Draft Version 0.6*, 2014.

[76] M. Ghosh, M. Richardson, B. Ford, and R. Jansen, "A TorPath to TorCoin: Proof-of-bandwidth altcoins for compensating relays," Naval Research Lab., Washington, DC, USA, Rep., 2014.

[77] (Dec. 2017). *Proof of Elapsed Time (PoET)*. [Online]. Available: http://consensus.readthedocs.io/en/latest/algos/proof-of-elapsed-time.html

[78] (Dec. 2017). *Proof of Authority Chains*. [Online]. Available: https://github.com/paritytech/parity/wiki/Proof-of-Authority-Chains

[79] A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz, "Permacoin: Repurposing Bitcoin work for data preservation," in *Proc. IEEE SP*, San Jose, CA, USA, May 2014, pp. 475–490.

[80] P4Titan, "Slimcoin: A peer-to-peer crypto-currency with proof-of-burn," May 2014.

[81] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending Bitcoin's proof of work via proof of stake [extended abstract]," *SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 3, pp. 34–37, Dec. 2014.

[82] T. Hønsi, "SpaceMint: A cryptocurrency based on proof of space," M.S. thesis, Norwegian Univ. Sci. Technol., Trondheim, Norway, 2017.

[83] J. Zou *et al.*, "A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services," *IEEE Trans. Services Comput.*, to be published.

[84] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of luck: An efficient blockchain consensus protocol," in *Proc. ACM SysTEX*, Trento, Italy, 2016, pp. 1–6.

[85] A. Bessani, J. Sousa, and E. E. P. Alchieri, "State machine replication for the masses with BFT-SMART," in *Proc. IEEE/IFIP DSN*, Atlanta, GA, USA, Jun. 2014, pp. 355–362.

[86] J. Behl, T. Distler, and R. Kapitza, "Scalable BFT for multi-cores: Actor-based decomposition and consensus-oriented parallelization," in *Proc. HotDep*, 2014, p. 9.

[87] T. T. A. Dinh *et al.*, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, Jul. 2018.

[88] C. Cachin and M. Vukolić, "Blockchains consensus protocols in the wild," *arXiv preprint arXiv:1707.01873*, 2017.

[89] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE SP*, San Jose, CA, USA, May 2016, pp. 839–858.

[90] (Jun. 2018). *Solidity*. [Online]. Available: https://solidity.readthedocs.io/en/develop/

[91] M. Wohrer and U. Zdun, "Smart contracts: Security patterns in the Ethereum ecosystem and solidity," in *Proc. IEEE IWBOSE*, Campobasso, Italy, Mar. 2018, pp. 2–8.

[92] G. Hurlburt, "Might the blockchain outlive Bitcoin?" *IT Prof.*, vol. 18, no. 2, pp. 12–16, Mar. 2016.

[93] Ministry of Urban Development, Government of India. (Jun. 2018). *Smart Cities Mission*. [Online]. Available: http://smartcities.gov.in/content/

[94] (Jun. 2018). *Smart Nation*. [Online]. Available: https://www.smartnation.sg/

[95] J. Lanza *et al.*, "Large-scale mobile sensing enabled Internet-of-Things testbed for smart city services," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 8, 2015, Art. no. 785061.

[96] (Jun. 2018). *Santander Facility*. [Online]. Available: http://www.smartsantander.eu/index.php/testbeds/item/132-santander-summary

[97] S. Latre *et al.*, "City of things: An integrated and multi-technology testbed for IoT smart city experiments," in *Proc. IEEE ISC2*, Trento, Italy, Sep. 2016, pp. 1–8.

[98] (Jun. 2018). *Smart City Testbed NYUAD*. [Online]. Available: http://sites.nyuad.nyu.edu/ccs-ad/about/research-areas-2/research-labs-groups/smart-city-testbed/

[99] G. Cardone, A. Cirri, A. Corradi, and L. Foschini, "The participact mobile crowd sensing living lab: The testbed for smart cities," *IEEE Commun. Mag.*, vol. 52, no. 10, pp. 78–85, Oct. 2014.

[100] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *Proc. IEEE HPCC/SmartCity/DSS*, Sydney, NSW, Australia, Dec. 2016, pp. 1392–1393.

[101] (Jun. 2018). *Dubai Blockchain Strategy*. [Online]. Available: https://smartdubai.ae/en/Initiatives/Pages/DubaiBlockchainStrategy.aspx

[102] A. Lai, C. Zhang, and S. Busovaca, "2-SQUARE: A Web-based enhancement of SQUARE privacy and security requirements engineering," *Int. J. Softw. Innov.*, vol. 1, no. 1, pp. 41–53, 2013.

[103] M. Armbrust *et al.*, "A view of cloud computing," *ACM Commun.*, vol. 53, no. 4, pp. 50–58, Apr. 2010.

[104] Z. Chen and Y. Zhu, "Personal archive service system using blockchain technology: Case study, promising and challenging," in *Proc. IEEE AIMS*, Honolulu, HI, USA, Jun. 2017, pp. 93–99.

[105] Z. Yan, G. Gan, and K. Riad, "BC-PDS: Protecting privacy and self-sovereignty through blockchains for OpenPDS," in *Proc. IEEE SOSE*, San Francisco, CA, USA, Apr. 2017, pp. 138–144.

[106] M. Fukumitsu, S. Hasegawa, J. Iwazaki, M. Sakai, and D. Takahashi, "A proposal of a secure P2P-type storage scheme by using the secret sharing and the blockchain," in *Proc. IEEE AINA*, Taipei, Taiwan, Mar. 2017, pp. 803–810.

[107] H. G. Do and W. K. Ng, "Blockchain-based system for secure data storage with private keyword search," in *Proc. IEEE SERVICES*, Honolulu, HI, USA, Jun. 2017, pp. 90–93.

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

[109] S. H. Hashemi, F. Faghri, and R. H. Campbell, "Decentralized user-centric access control using PubSub over blockchain," *arXiv preprint arXiv:1710.00110*, 2017.

[110] S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell, "World of empowered IoT users," in *Proc. IEEE IoTDI*, Berlin, Germany, Apr. 2016, pp. 13–24.

[111] S. Kiyomoto, M. S. Rahman, and A. Basu, "On blockchain-based anonymized dataset distribution platform," in *Proc. IEEE SERA*, London, U.K., Jun. 2017, pp. 85–92.

[112] J. Chen and Y. Xue, "Bootstrapping a blockchain based ecosystem for big data exchange," in *Proc. IEEE BigDataCongress*, Honolulu, HI, USA, Jun. 2017, pp. 460–463.

[113] P. Sreehari, M. Nandakishore, G. Krishna, J. Jacob, and V. S. Shibu, "Smart will converting the legal testament into a smart contract," in *Proc. IEEE NETACT*, Thiruvanthapuram, India, Jul. 2017, pp. 203–207.

[114] N. Buchmann, C. Rathgeb, H. Baier, C. Busch, and M. Margraf, "Enhancing breeder document long-term security using blockchain technology," in *Proc. IEEE COMPSAC*, vol. 2. Turin, Italy, Jul. 2017, pp. 744–748.

[115] N. Zhou, M. Wu, and J. Zhou, "Volunteer service time record system based on blockchain technology," in *Proc. IEEE IAEAC*, Chongqing, China, Mar. 2017, pp. 610–613.

[116] F. S. Collins, "Exceptional opportunities in medical science: A view from the national institutes of health," *Jama*, vol. 313, no. 2, pp. 131–132, 2015.

[117] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *J. Amer. Med. Informat. Assoc.*, vol. 24, no. 6, pp. 1211–1220, 2017.

[118] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *Proc. IEEE HealthCom*, Munich, Germany, Sep. 2016, pp. 1–3.

[119] M. Simić, G. Sladić, and B. Milosavljević, "A case study IoT and blockchain powered healthcare," in *Proc. ICET*, Novi Sad, Serbia, Jun. 2017.

[120] T. McConaghy *et al.*, "BigchainDB: A scalable blockchain database," White Paper, 2016.

[121] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *J. Med. Syst.*, vol. 40, no. 10, p. 218, 2016.

[122] H. Zhao, Y. Zhang, Y. Peng, and R. Xu, "Lightweight backup and efficient recovery scheme for health blockchain keys," in *Proc. IEEE ISADS*, Bangkok, Thailand, Mar. 2017, pp. 229–234.

[123] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles. (2016). *A Blockchain-Based Approach to Health Information Exchange Networks*. [Online]. Available: http://www.colleaga.org/sites/default/files/12-55-blockchain-based-approach-final.pdf

[124] B. Tim, "Principles of health interoperability HL7 and SNOMED," in *Health Informatics*. London, U.K.: Springer-Verlag, 2010.

[125] J. Zhang, N. Xue, and X. Huang, "A secure system for pervasive social network-based healthcare," *IEEE Access*, vol. 4, pp. 9239–9250, 2016.

[126] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. IEEE OBD*, Vienna, Austria, Aug. 2016, pp. 25–30.

[127] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare: 'MedRec' prototype for electronic health records and medical research data," in *Proc. IEEE Open Big Data Conf.*, 2016, pp. 1–13.

[128] L. Linn and M. Koo, "Blockchain for health data and its potential use in health it and health care related research," in *Proc. ONC/NIST*, Gaithersburg, MD, USA, 2016, pp. 1–10.

[129] P. Genestier *et al.*, "Blockchain for consent management in the eHealth environment: A nugget for privacy and security challenges," *J. Int. Soc. Telemedicine eHealth*, vol. 5, pp. 1–4, Apr. 2017.

[130] Q. Xia *et al.*, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

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

[132] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," *arXiv preprint arXiv:1709.06528*, 2017.

[133] M. E. Peck and D. Wagman, "Energy trading for fun and profit buy your neighbor's rooftop solar power or sell your own-it'll all be on a blockchain," *IEEE Spectr.*, vol. 54, no. 10, pp. 56–61, Oct. 2017.

[134] G. Guérard, B. Pichon, and Z. Nehai, "Demand-response: Let the devices take our decisions," in *Proc. Smart Cities Green ICT Syst.*, 2017, pp. 119–126.

[135] L. Diestelmeier, "Regulating for blockchain technology in the electricity sector: Sharing electricity and opening Pandora's box?" in *Proc. Sci. Technol. Soci. Stud.*, Graz, Austria, May 2017, pp. 1–15.

[136] J. Basden and M. Cottrell, *How Utilities Are Using Blockchain to Modernize the Grid*, Harvard Bus. Rev., Boston, MA, USA, 2017.

[137] S. Cheng, B. Zeng, and Y. Huang, "Research on application model of blockchain technology in distributed electricity market," in *Proc. IOP Conf. Earth Environ. Sci.*, vol. 93, 2017, pp. 12–65.

[138] K. Tanaka, K. Nagakubo, and R. Abe, "Blockchain-based electricity trading with digitalgrid router," in *Proc. IEEE ICCE-TW*, Taipei, Taiwan, Jun. 2017, pp. 201–202.

[139] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: Towards sustainable local energy markets," *Comput. Sci. Research Develop.*, vol. 33, nos. 1–2, pp. 207–214, 2017.

[140] K. Kvaternik *et al.*, "Privacy-preserving platform for transactive energy systems," *arXiv preprint arXiv:1709.09597*, 2017.

[141] A. Laszka, A. Dubey, M. Walker, and D. Schmidt, "Providing privacy, safety, and security in IoT-based transactive energy systems using distributed ledgers," *arXiv preprint arXiv:1709.09614*, 2017.

[142] J. Bergquist *et al.*, "On the design of communication and transaction anonymity in blockchain-based transactive microgrids," *arXiv preprint arXiv:1709.09601*, 2017.

[143] A. Hahn, R. Singh, C. C. Liu, and S. Chen, "Smart contract-based campus demonstration of decentralized transactive energy auctions," in *Proc. IEEE ISGT*, Washington, DC, USA, Apr. 2017, pp. 1–5.

[144] 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.

[145] I. Kounelis *et al.*, "Fostering consumers' energy market through smart contracts," in *Proc. IEEE ES2DE*, Funchal, Portugal, Jul. 2017, pp. 1–6.

[146] E. Münsing, J. Mather, and S. Moura, "Blockchains for decentralized optimization of energy resources in microgrid networks," in *Proc. IEEE CCTA*, Aug. 2017, pp. 2164–2171.

[147] Z. Nehaï and G. Guerard, "Integration of the blockchain in a smart grid model," in *Proc. CYSENI*, Kaunas, Lithuania, May 2017, pp. 127–134.

[148] P. Danzi, M. Angjelichinoski, Č. Stefanović, and P. Popovski, "Distributed proportional-fairness control in microgrids via blockchain smart contracts," *arXiv preprint arXiv:1705.01453*, 2017.

[149] J. Gao *et al.*, "GridMonitoring: Secured sovereign blockchain based monitoring on smart grid," *IEEE Access*, vol. 6, pp. 9917–9925, 2018.

[150] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Trans. Smart Grid*, to be published.

[151] M. Mihaylov, I. Razo-Zapata, R. Rădulescu, and A. Nowé, "Boosting the renewable energy economy with NRGcoin," in *Proc. ICT4S*, 2016, pp. 229–230.

[152] M. Mihaylov *et al.*, "NRGcoin: Virtual currency for trading of renewable energy in smart grids," in *Proc. IEEE EEM*, Krakow, Poland, May 2014, pp. 1–6.

[153] M. Mihaylov *et al.*, "Smart grid demonstration platform for renewable energy exchange," in *Proc. PAAMS*, 2016, pp. 277–280.

[154] *SolarCoin*. (Jun. 2018). [Online]. Available: https://solarcoin.org/fr

[155] J. A. F. Castellanos, D. Coll-Mayor, and J. A. Notholt, "Cryptocurrency as guarantees of origin: Simulating a green certificate market with the Ethereum blockchain," in *Proc. IEEE SEGE*, Oshawa, ON, Canada, Aug. 2017, pp. 367–372.

[156] (Jun. 2018). *Southern Power Green Bonds*. [Online]. Available: https://investor.southerncompany.com/information-for-investors/Green-Bonds/default.aspx

[157] (Jun. 2018). *EDF Green Bonds: Energy for Green Growth*. [Online]. Available: https://www.edf.fr/en/the-edf-group/our-commitments/innovation/edf-green-bonds-energy-for-green-growth

[158] (Jun. 2018). *Kottackal Green Bond*. [Online]. Available: https://www.f6s.com/kottackal

[159] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," *Appl. Energy*, vol. 195, pp. 234–246, Jun. 2017.

[160] T. Lundqvist, A. de Blanche, and H. R. H. Andersson, "Thing-to-thing electricity micro payments using blockchain technology," in *Proc. IEEE GIOTS*, Geneva, Switzerland, Jun. 2017, pp. 1–6.

[161] J. Zhang *et al.*, "Data-driven intelligent transportation systems: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 4, pp. 1624–1639, Dec. 2011.

[162] B. Leiding, P. Memarmoshrefi, and D. Hogrefe, "Self-managed and blockchain-based vehicular ad-hoc networks," in *Proc. ACM UbiComp*, Heidelberg, Germany, 2016, pp. 137–140.

[163] P. K. Sharma, S. Y. Moon, and J. H. Park, "Block-VN: A distributed blockchain based vehicular network architecture in smart city," *J. Inf. Process. Syst.*, vol. 13, no. 1, pp. 184–195, 2017.

[164] A. Lei *et al.*, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.

[165] 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.*, to be published.

[166] L. Li *et al.*, "CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2204–2220, Jul. 2018.

[167] F. Knirsch, A. Unterweger, and D. Engel, "Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions," *Comput. Sci. Res. Develop.*, vol. 33, nos. 1–2, pp. 71–79, 2017.

[168] J. Kang *et al.*, "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.

[169] X. Huang, C. Xu, P. Wang, and H. Liu, "LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE Access*, vol. 6, pp. 13565–13574, 2018.

[170] J. T. Mentzer *et al.*, "Defining supply chain management," *J. Bus. Logist.*, vol. 22, no. 2, pp. 1–25, 2001.

[171] F. Milani, L. Garcia-Banuelos, and M. Dumas, *Blockchain and Business Process Improvement*, BP Trends News Lett., Oct. 2016.

[172] S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," *Int. J. Res. Eng. Technol.*, vol. 5, no. 9, pp. 1–10, 2016.

[173] G. Prockl, V. Bhakoo, and C. Wong, "Supply chains and electronic markets-impulses for value co-creation across the disciplines," *Electron. Markets*, vol. 27, no. 2, pp. 135–140, 2017.

[174] F. Tian, "An agri-food supply chain traceability system for China based on RFID blockchain technology," in *Proc. IEEE ICSSSM*, Kunming, China, Jun. 2016, pp. 1–6.

[175] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain Internet of Things," in *Proc. IEEE ICSSSM*, Dalian, China, Jun. 2017, pp. 1–6.

[176] C. Xie, Y. Sun, and H. Luo, "Secured data storage scheme based on block chain for agricultural products tracking," in *Proc. IEEE BIGCOM*, Chengdu, China, Aug. 2017, pp. 45–50.

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

[178] 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.

[179] (Jun. 2018). *Ownest*. [Online]. Available: https://ownest.io/

[180] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere: A use-case of blockchains in the pharma supply-chain," in *Proc. IEEE INM*, Lisbon, Portugal, May 2017, pp. 772–777.

[181] Z. Li *et al.*, "On the integration of event-based and transaction-based architectures for supply chains," in *Proc. IEEE ICDCSW*, Atlanta, GA, USA, Jun. 2017, pp. 376–382.

[182] H. Wu *et al.*, "A distributed ledger for supply chain physical distribution visibility," *Information*, vol. 8, no. 4, p. 137, 2017.

[183] M. Nakasumi, "Information sharing for supply chain management based on block chain technology," in *Proc. IEEE CBI*, vol. 1. Thessaloniki, Greece, Jul. 2017, pp. 140–149.

[184] Y. Madhwal and P. B. Panfilov, "Industrial case: Blockchain on aircraft's parts supply chain management," in *Proc. AMCIS*, Boston, MA, USA, 2017, pp. 1–6.

[185] Y. Omran, M. Henke, R. Heines, and E. Hofmann, "Blockchain-driven supply chain finance: Towards a conceptual framework from a buyer perspective," in *Proc. IPSERA*, Budapest, Hungary, Apr. 2017, pp. 1–15.

[186] J. Sidhu, "Syscoin: A peer-to-peer electronic cash system with blockchain-based services for e-business," in *Proc. IEEE ICCCN*, Vancouver, BC, Canada, Jul. 2017, pp. 1–6.

[187] I. Weber *et al.*, "Untrusted business process monitoring and execution using blockchain," in *Business Process Management*, M. La Rosa, P. Loos, and O. Pastor, Eds. Cham, Switzerland: Springer Int., 2016, pp. 329–347.

[188] R. Dennis and G. Owen, "Rep on the block: A next generation reputation system based on the blockchain," in *Proc. IEEE ICITST*, London, U.K., Dec. 2015, pp. 131–138.

[189] X. Wang *et al.*, "Human resource information management model based on blockchain technology," in *Proc. IEEE SOSE*, San Francisco, CA, USA, Apr. 2017, pp. 168–173.

[190] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," in *Proc. ACM IoTDI*, Pittsburgh, PA, USA, 2017, pp. 173–178.

[191] 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 PERCOMW*, Kona, HI, USA, Mar. 2017, pp. 618–623.

[192] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and solutions," *arXiv preprint arXiv:1608.05187*, 2016.

[193] A. Xu *et al.*, "A blockchain based micro payment system for smart devices," *Signature*, vol. 256, no. 4936, p. 115, 2016.

[194] H. Hou, "The application of blockchain technology in e-government in China," in *Proc. IEEE ICCCN*, Vancouver, BC, Canada, Jul. 2017, pp. 1–4.

[195] S. Ølnes, "Beyond Bitcoin enabling smart government using blockchain technology," in *Electronic Government*, H. J. Scholl *et al.*, Eds. Cham, Switzerland: Springer Int., 2016, pp. 253–264.

[196] S. Ølnes and A. Jansen, "Blockchain technology as a support infrastructure in e-government," in *Electronic Government*, M. Janssen *et al.*, Eds. Cham, Switzerland: Springer Int., 2017, pp. 215–227.

[197] V. L. Lemieux, "Trusting records: Is blockchain technology the answer?" *Rec. Manag. J.*, vol. 26, no. 2, pp. 110–139, 2016.

[198] E. Yavuz, A. K. Koç, U. C. Çabuk, and G. Dalkılıç, "Towards secure e-voting using Ethereum blockchain," in *Proc. IEEE ISDFS*, Antalya, Turkey, Mar. 2018, pp. 1–7.

[199] F. Bond, F. Amati, and G. Blousson. (Aug. 2015). *Blockchain, Academic Verification Use Case*. [Online]. Available: https://s3.amazonaws.com/signatura-usercontent/blockchain_academic_verification_use_case.pdf

[200] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112–5127, 2018.

[201] (Jun. 2018). *ARK: All-in-One Blockchain Solutions*. [Online]. Available: https://ark.io/

[202] N. Fotiou and G. C. Polyzos, "Decentralized name-based security for content distribution using blockchains," in *Proc. IEEE INFOCOM Workshops*, San Francisco, CA, USA, Apr. 2016, pp. 415–420.

[203] D. Bhowmik and T. Feng, "The multimedia blockchain: A distributed and tamper-proof media transaction framework," in *Proc. IEEE ICDSP*, London, U.K., Aug. 2017, pp. 1–5.

[204] N. Herbaut and N. Negru, "A model for collaborative blockchain-based video delivery relying on advanced network services chains," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 70–76, Sep. 2017.

[205] S. Fujimura *et al.*, "BRIGHT: A concept for a decentralized rights management system based on blockchain," in *Proc. IEEE ICCE Berlin*, Berlin, Germany, Sep. 2015, pp. 345–346.

[206] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, and A. Akutsu, "The blockchain-based digital content distribution system," in *Proc. IEEE BDCloud*, Dalian, China, Aug. 2015, pp. 187–190.

[207] G. Greenspan, "MultiChain private blockchain," White Paper, 2015.

[208] R. Khatoun and S. Zeadally, "Smart cities: Concepts, architectures, research opportunities," *ACM Commun.*, vol. 59, no. 8, pp. 46–57, Jul. 2016.

[209] S. Talari *et al.*, "A review of smart cities based on the Internet of Things concept," *Energies*, vol. 10, no. 4, p. 421, 2017.

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

[211] G. Maxwell. (Dec. 2018). *Confidential Transactions*. [Online]. Available: https://people.xiph.org/g̃reg/confidential_values.txt

[212] E. Duffield and K. Hagan. (Dec. 2018). *Darkcoin: Peer-to-Peer Crypto Currency With Anonymous Blockchain Transactions and an Improved Proof-of-Work System*. [Online]. Available: https://cryptopapers.info/assets/pdf/darkcoin.pdf

[213] (Dec. 2018). *Monero: A Secure, Private, Untraceable Cryptocurrency*. [Online]. Available: https://www.getmonero.org/

[214] S. Noether, "Ring confidential transactions," *IACR Cryptol. ePrint Archive*, Rep., pp. 1–34, 2015.

[215] A. Saxena, J. Misra, and A. Dhar, "Increasing anonymity in Bitcoin," *Financial Cryptography and Data Security* (LNCS 8438). Heidelberg, Germany: Springer, 2014, pp. 122–139.

[216] E. Heilman, L. Alshenibr, F. Baldimtsi, A. Scafuro, and S. Goldberg, "TumbleBit: An untrusted Bitcoin-compatible anonymous payment hub," in *Proc. Netw. Distrib. Syst. Security Symp.*, 2017, pp. 1–14.

[217] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Succinct non-interactive zero knowledge for a von Neumann architecture," in *Proc. USENIX Security Symp.*, San Diego, CA, USA, 2014, pp. 781–796.

[218] (Jun. 2018). *General Data Protection Regulation (GDPR)*. [Online]. Available: https://gdpr-info.eu/

[219] (Jun. 2018). *Will Blockchains Get Blocked in Europe? GDPR and Its Potential Affects on Decentralized Networks*. [Online]. Available: https://irishtechnews.ie/will-blockchains-get-blocked-in-europe-gdpr-and-its-potential-affects-on-decentralized-networks/

[220] (Jun. 2018). *The Blockchain-GDPR Paradox*. [Online]. Available: https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047

[221] (Jun. 2018). *Blockchain and GDPR*. [Online]. Available: http://www.chainfrog.com/wp-content/uploads/2017/08/gdpr.pdf

[222] L. Chen *et al.*, "Report on post-quantum cryptography," U.S. Dept. Commerce, Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep. NISTIR 8105, 2016.

[223] K. Lauter, "Postquantum opportunities: Lattices, homomorphic encryption, and supersingular isogeny graphs," *IEEE Security Privacy*, vol. 15, no. 4, pp. 22–27, Aug. 2017.

[224] Y.-L. Gao *et al.*, "A secure cryptocurrency scheme based on post-quantum blockchain," *IEEE Access*, vol. 6, pp. 27205–27213, 2018.

[225] W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin, "An anti-quantum transaction authentication approach in blockchain," *IEEE Access*, vol. 6, pp. 5393–5401, 2018.

[226] J. Mendling *et al.*, "Blockchains for business process management—Challenges and opportunities," *arXiv preprint arXiv:1704.03610*, 2017.

[227] (Dec. 2017). *Bitcoin Transactions Per Second*. [Online]. Available: http://edupanya.tk/xucyc/bitcoin-transactions-per-second-662.php

[228] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in *Proc. IEEE AICCSA*, Agadir, Morocco, Nov. 2016, pp. 1–6.

[229] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," White Paper, 2014.

[230] E. Lombrozo, J. Lau, and P. Wuille. (Jun. 2018). *Segregated Witness*. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

[231] J. Poon and T. Dryja, "The Bitcoin lightning network: Scalable off-chain instant payments," *Draft Version 0.5*, vol. 9, p. 14, 2016.

[232] C. Decker and R. Wattenhofer, "A fast and scalable payment network with Bitcoin duplex micropayment channels," in *Proc. Symp. Self Stabilizing Syst.*, 2015, pp. 3–18.

[233] L. Luu *et al.*, "A secure sharding protocol for open blockchains," in *Proc. ACM CCS*, Vienna, Austria, 2016, pp. 17–30.

[234] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, and B. Ford, "OmniLedger: A secure, scale-out, decentralized ledger via sharding," IACR Cryptol. ePrint Archive, Rep. 2017/406, 2017.

[235] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-NG: A scalable blockchain protocol," in *Proc. NSDI*, Santa Clara, CA, USA, 2016, pp. 45–59.

[236] E. K. Kogias *et al.*, "Enhancing Bitcoin security and performance with strong consistency via collective signing," in *Proc. USENIX Security*, Austin, TX, USA, 2016, pp. 279–296.

[237] I. Abraham, D. Malkhi, K. Nayak, L. Ren, and A. Spiegelman, "Solida: A blockchain protocol based on reconfigurable Byzantine consensus," *arXiv preprint arXiv:1612.02916*, 2016.

[238] (Jun. 2018). *Does Blockchain Size Matter?* [Online]. Available: https://blocksplain.com/2018/02/22/blockchain-size/

[239] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—A systematic review," *PLoS ONE*, vol. 11, no. 10, pp. 1–27, Oct. 2016.

[240] Protocol Labs. (Jan. 2018). *Filecoin: A Decentralized Storage Network*. [Online]. Available: https://filecoin.io/filecoin.pdf

[241] M. Klems *et al.*, "Trustless intermediation in blockchain-based decentralized service marketplaces," in *Proc. ICSOC*, Málaga, Spain, Nov. 2017, pp. 731–739.

[242] (Jun. 2018). *Swarm Introduction*. [Online]. Available: http://swarm-guide.readthedocs.io/en/latest/introduction.html

[243] S. Pellicer *et al.*, "A global perspective of smart cities: A survey," in *Proc. IEEE IMIS*, Taichung, Taiwan, Jul. 2013, pp. 439–444.

[244] N. Bozic, G. Pujolle, and S. Secci, "A tutorial on blockchain and applications to secure network control-planes," in *Proc. IEEE SCNS*, Dubai, UAE, Dec. 2016, pp. 1–8.

[245] B. Fisch, R. Pass, and A. Shelat, "Socially optimal mining pools," in *Web and Internet Economics*, N. R. Devanur and P. Lu, Eds. Cham, Switzerland: Springer Int., 2017, pp. 205–218.

[246] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything you wanted to know about smart cities: The Internet of Things is the backbone," *IEEE Consum. Electron. Mag.*, vol. 5, no. 3, pp. 60–70, Jul. 2016.

[247] R. Krawiec *et al.*, "Blockchain: Opportunities for health care," in *Proc. NIST Workshop Blockchain Healthcare*, 2016, pp. 1–16.

[248] T. Huang *et al.*, "A survey on large-scale software defined networking (SDN) testbeds: Approaches and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 891–917, 2nd Quart., 2017.

[249] S.-C. Lin, I. F. Akyildiz, P. Wang, and M. Luo, "QoS-aware adaptive routing in multi-layer hierarchical software defined networks: A reinforcement learning approach," in *Proc. IEEE SCC*, San Francisco, CA, USA, Jun. 2016, pp. 25–33.

[250] T. Koponen *et al.*, "Onix: A distributed control platform for large-scale production networks," in *Proc. OSDI*, vol. 10, 2010, pp. 1–6.

[251] P. K. Sharma, M. Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2017.

[252] 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.

[253] J. Matias, J. Garay, N. Toledo, J. Unzilla, and E. Jacob, "Toward an SDN-enabled NFV architecture," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 187–193, Apr. 2015.

[254] 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 NOMS*, Taipei, Taiwan, Apr. 2018.

[255] N. Bozic, G. Pujolle, and S. Secci, "Securing virtual machine orchestration with blockchains," in *Proc. IEEE CSNET*, Rio de Janeiro, Brazil, Oct. 2017, pp. 1–8.

[256] P. Mach and Z. Becvar, "Mobile edge computing: A survey on architecture and computation offloading," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1628–1656, 3rd Quart., 2017.

[257] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing: Challenges and applications," *arXiv preprint arXiv:1711.05938*, 2017.

[258] Z. Xiong, S. Feng, D. Niyato, P. Wang, and Z. Han, "Edge computing resource management and pricing for mobile blockchain," *arXiv preprint arXiv:1710.01567*, 2017.

[259] Z. Xiong, S. Feng, D. Niyato, P. Wang, and Z. Han, "Optimal pricing-based edge computing resource management in mobile blockchain," *arXiv preprint arXiv:1711.01049*, 2017.

[260] Y. Jiao, P. Wang, D. Niyato, and Z. Xiong, "Social welfare maximization auction in edge computing resource allocation for mobile blockchain," *arXiv preprint arXiv:1710.10595*, 2017.

[261] N. C. Luong, Z. Xiong, P. Wang, and D. Niyato, "Optimal auction for edge computing resource management in mobile blockchain networks: A deep learning approach," *arXiv preprint arXiv:1711.02844*, 2017.

[262] P. Liu and Z. Peng, "China's smart city pilots: A progress report," *Computer*, vol. 47, no. 10, pp. 72–81, Oct. 2014.

[263] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the Internet of Things," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 4, pp. 983–994, 2017.

[264] Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of Bitcoin," in *Proc. IEEE ICIN*, Paris, France, Feb. 2015, pp. 184–191.

[265] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. IEEE ICACT*, Bongpyeong-myeon, South Korea, Feb. 2017, pp. 464–467.

[266] D. W. Kravitz and J. Cooper, "Securing user identity and transactions symbiotically: IoT meets blockchain," in *Proc. IEEE GIOTS*, Geneva, Switzerland, Jun. 2017, pp. 1–6.

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

[268] G. C. Polyzos and N. Fotiou, "Blockchain-assisted information distribution for the Internet of Things," in *Proc. IEEE IRI*, San Diego, CA, USA, Aug. 2017, pp. 75–78.

[269] M. Samaniego and R. Deters, "Internet of Smart Things—IoST: Using blockchain and CLIPS to make things autonomous," in *Proc. IEEE ICCC*, Honolulu, HI, USA, Jun. 2017, pp. 9–16.

[270] M. Maier, M. Chowdhury, B. P. Rimal, and D. P. Van, "The Tactile Internet: Vision, recent progress, and open challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 138–145, May 2016.

[271] M. Maier, A. Ebrahimzadeh, and M. Chowdhury, "The Tactile Internet: Automation or augmentation of the human?" *IEEE Access*, vol. 6, pp. 41607–41618, 2018.

[272] G. P. Fettweis, "The Tactile Internet: Applications and challenges," *IEEE Veh. Technol. Mag.*, vol. 9, no. 1, pp. 64–70, Mar. 2014.

[273] M. Chowdhury and M. Maier, "Collaborative computing for advanced Tactile Internet human-to-robot (H2R) communications in integrated FiWi multirobot infrastructures," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 2142–2158, Dec. 2017.

[274] M. Chowdhury, E. Steinbach, W. Kellerer, and M. Maier, "Context-aware task migration for HART-centric collaboration over FiWi based Tactile Internet infrastructures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 29, no. 6, pp. 1231–1246, Jun. 2018.

[275] M. Simsek, A. Aijaz, M. Dohler, J. Sachs, and G. Fettweis, "5G-enabled Tactile Internet," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 460–473, Mar. 2016.

[276] (Nov. 2018). *Scientific Research of the Optical Zeitgeist Laboratory*. [Online]. Available: http://www.zeitgeistlab.ca/research.html

[277] *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021*, Cisco Public Inf., San Jose, CA, USA, 2017.

[278] G. Xylomenos *et al.*, "A survey of information-centric networking research," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 1024–1049, 2nd Quart., 2014.

[279] J. Xie, R. Xie, T. Huang, J. Liu, and Y. Liu, "ICICD: An efficient content distribution architecture in mobile cellular network," *IEEE Access*, vol. 5, pp. 3205–3215, 2017.

[280] T. Jin, X. Zhang, Y. Liu, and K. Lei, "BlockNDN: A Bitcoin blockchain decentralized system over named data networking," in *Proc. IEEE ICUFN*, Milan, Italy, Jul. 2017, pp. 75–80.

[281] S. Patidar, D. Rane, and P. Jain, "A survey paper on cloud computing," in *Proc. IEEE ACCT*, Rohtak, India, Jan. 2012, pp. 394–398.

[282] S. Alansari, F. Paci, and V. Sassone, "A distributed access control system for cloud federations," in *Proc. IEEE ICDCS*, Atlanta, GA, USA, Jun. 2017, pp. 2131–2136.

[283] S. Alansari, F. Paci, A. Margheri, and V. Sassone, "Privacy-preserving access control in cloud federations," in *Proc. IEEE CLOUD*, Honolulu, HI, USA, Jun. 2017, pp. 757–760.
[284] F. Ye, Z. Zheng, C. Chen, and Y. Zhou, "DC-RSF: A dynamic and customized reputation system framework for joint cloud computing," in *Proc. IEEE ICDCSW*, Atlanta, GA, USA, Jun. 2017, pp. 275–279.
[285] X. Liang *et al.*, "ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proc. IEEE CCGRID*, Madrid, Spain, 2017, pp. 468–477.
[286] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.
[287] A. Outchakoucht, E.-S. Hamza, and J. P. Leroy, "Dynamic access control policy based on blockchain and machine learning for the Internet of Things," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 7, pp. 417–424, 2017.
[288] A. B. Kurtulmus and K. Daniel, "Trustless machine learning contracts; evaluating and exchanging machine learning models on the Ethereum blockchain," *arXiv preprint arXiv:1802.10185*, 2018.

Junfeng Xie received the B.S. degree in communication engineering from the University of Science and Technology Beijing, Beijing, China, in 2013. He is currently pursuing the Ph.D. degree with the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing. From 2017 to 2018, he visited Carleton University, Ottawa, ON, Canada, as a visiting Ph.D. student. He has been accepted as a Faculty Member with the Guangxi University for Nationalities. His current research interests include machine learning, content delivery network, smart cities, and blockchain.

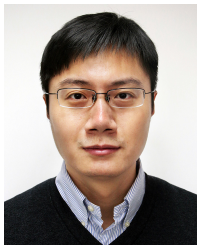
Helen Tang received the Ph.D. degree in electrical engineering from Carleton University in 2005. She is the Portfolio Manager of wireless cyber security with the Center for Security Science, Defence Research and Development Canada (DRDC) Ottawa, working on cyber security related to connected transportations, connected medical devices, and smart cities. From 1999 to 2005, she had worked in several research and development organizations in Canada and USA, including Alcatel-Lucent, Mentor Graphics, and Communications Research Center Canada. In 2005, she was a Defence Scientist with the DRDC-Ottawa on many wireless network security projects, including being the C4ISR SME for the Integrated Soldier System Project for two months. She is also an Adjunct Professor with the School of Information Technology, Carleton University, where she is the Supervisor of several graduate students. She was a recipient of the "Outstanding Achievement Award" at DRDC-CSS in 2017, the "Best Paper Award" at IEEE/IFIP TrustCom in 2009, and the "Outstanding Leadership Award" at IEEE/IFIP TrustCom in 2010.

Tao Huang received the B.S. degree in communication engineering from Nankai University, Tianjin, China, in 2002 and the M.S. and Ph.D. degrees in communication and information systems from the Beijing University of Posts and Telecommunications in 2004 and 2007, respectively, where he is currently a Professor. His current research interests include network architecture, machine learning, smart cities, and blockchain.

F. Richard Yu (S'00–M'04–SM'08–F'18) received the Ph.D. degree in electrical engineering from the University of British Columbia in 2003. From 2002 to 2006, he was with Ericsson, Lund, Sweden, and a start-up in California, USA. He joined Carleton University in 2007, where he is currently a Professor. His research interests include wireless cyber-physical systems, connected/autonomous vehicles, security, distributed ledger technology, and deep learning.

He was a recipient of the IEEE Outstanding Service Award in 2016, the IEEE Outstanding Leadership Award in 2013, the Carleton Research Achievement Award in 2012, the Ontario Early Researcher Award (formerly, Premiers Research Excellence Award) in 2011, the Excellent Contribution Award at IEEE/IFIP TrustCom 2010, the Leadership Opportunity Fund Award from Canada Foundation of Innovation in 2009, and the Best Paper Awards at IEEE ICNC 2018, VTC 2017 Spring, ICC 2014, Globecom 2012, IEEE/IFIP TrustCom 2009, and International Conference on Networking 2005. He serves on the editorial boards of several journals, including the Co-Editor-in-Chief for *Ad Hoc & Sensor Wireless Networks*, and a Lead Series Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, and the IEEE COMMUNICATIONS SURVEYS & TUTORIALS. He has served as the Technical Program Committee Co-Chair of numerous conferences. He is a Distinguished Lecturer, the Vice President (Membership), and an Elected Member of the Board of Governors of the IEEE Vehicular Technology Society. He is a Registered Professional Engineer with the province of Ontario, Canada, and a fellow of the Institution of Engineering and Technology.

Renchao Xie received the Ph.D. degree from the School of Information and Communication Engineering, BUPT in 2012. From 2012 to 2014, he was a Post-Doctoral Researcher with China Unicom. From 2010 to 2011, he visited Carleton University as a Visiting Scholar. He is an Associate Professor with BUPT. He has published over 30 journal and conference papers. His current research interests include content delivery network, machine learning, 5G networks, smart cities, and blockchain. He has served on the Technical Program Committees of Chinacom 2016 and the 2012 IEEE Vehicular Technology Conference-Spring. He has also served for several journals and conferences as a Reviewer, including the IEEE TRANSACTIONS ON COMMUNICATIONS, *ACM/Springer Wireless Networks*, the *EURASIP Journal on Wireless Communications and Networking*, *Wireless Communications and Mobile Computing* (Wiley), the IEEE COMMUNICATIONS LETTERS, and 2011 IEEE GLOBECOM.



Jiang Liu received the B.S. degree in electronics engineering from the Beijing Institute of Technology, China, in 2005, the M.S. degree in communication and information systems from Zhengzhou University, China, in 2009, and the Ph.D. degree from BUPT in 2012, where he is currently an Associate Professor. His current research interests include network architecture, network virtualization, machine learning, smart cities, blockchain, and tools and platforms for networking research and teaching.

Yunjie Liu received the B.S. degree in technical physics from Peking University, Beijing, China, in 1968. He is currently the Academician of the China Academy of Engineering, the Chief of the Science and Technology Committee of China Unicom, and the Dean of the School of Information and Communication Engineering, BUPT. His research interests include next generation networks, and network architecture and management.