JOURNAL OF SOCIAL COMPUTING
ISSN 2688-5255 05/05 pp363−394
Volume 3, Number 4, December 2022
DOI: 10.23919/JSC.2022.0016

# Recent Advances of Blockchain and Its Applications

Xiao Li and Weili Wu*

**Abstract:** Blockchain is an emerging decentralized data collection, sharing, and storage technology, which have provided abundant transparent, secure, tamper-proof, secure, and robust ledger services for various real-world use cases. Recent years have witnessed notable developments of blockchain technology itself as well as blockchain-enabled applications. Most existing surveys limit the scopes on several particular issues of blockchain or applications, which are hard to depict the general picture of current giant blockchain ecosystem. In this paper, we investigate recent advances of both blockchain technology and its most active research topics in real-world applications. We first review the recent developments of consensus and storage mechanisms and communication schema in general blockchain systems. Then extensive literature review is conducted on blockchain-enabled Internet of Things (IoT), edge computing, federated learning, and several emerging applications including healthcare, COVID-19 pandemic, online social network, and supply chain, where detailed specific research topics are discussed in each. Finally, we discuss the future directions, challenges, and opportunities in both academia and industry.

**Key words:** social network; blockchain; edge computing; federated learning; healthcare

## 1 Introduction

Blockchain is a rising data sharing and storage technology and attracts increasing attention from both academia and industry because of its special capabilities and advantages comparing to existing conventional decentralized database storage approaches. Public blockchains which were the most common blockchain type (e.g., Bitcoin), can make the data available on every node which enables transparency to every participant. Since blockchain can work under totally anonymous setting without having to build trust among nodes, privacy of nodes can be preserved. Blockchain is tamper-proof storage, because the blocks are linked together with specific hash values that would cause a violation if any modification is made on block data. Blockchain storage is also free of single-point failure as long as the fraud users hold less than 51% mining power of the whole blockchain system. The comparison between conventional distributed database and blockchain is discussed in Table 1.

With above advantages, blockchain has been proven to be a remarkable success in cryptocurrency applications such as Bitcoin[1], Ethereum[2], and PeerCoin[3]. The adoption of blockchain in many other fields keeps expanding the existing blockchain ecosystem. For instance, blockchain-enabled systems have been developed in areas of financial ledger system[4], Internet of Things (IoT)[5, 6], edge and cloud computing[7], public administration[8, 9], healthcare[10], and supply chain[11].

Current blockchain technology is still not perfect for general adoption and has many deficiencies to be improved. These deficiencies also bring troubles to blockchain-enabled applications. Researchers have devoted tremendous work on improving blockchain system with faster processing speed, more light-weight consensus mechanisms, less storage cost, and lower communication bandwidth requirement. These

• Xiao Li and Weili Wu are with the Department of Computer Science, University of Texas at Dallas, Richardson, TX 75080, USA. E-mail: xiao.li@utdallas.edu; weiliwu@utdallas.edu.
* To whom correspondence should be addressed.
Manuscript received: 2022-09-03; revised: 2022-12-03; accepted: 2022-12-16

**Table 1 Comparison between traditional distributed database storage and blockchain.**

| Comparison factor | Traditional distributed database | Blockchain |
|---|---|---|
| System management | Database is stored on different physical places with multiple copies, however managed by a central server. | Blockchain is maintained by all participants and full copies are stored by every participant. |
| Data accessibility | Common participants have no access to whole database. | Blockchain is public and accessible to all participants. |
| Function execution | Central server performs data collection and calculation. | Each participant is able to generate and record new data following smart contract. |
| Cost | Computation and storage cost are on central server. | Computation and storage cost are on every participant. |
| Communication | Participants mainly communicate only to central server. | Each participant broadcast updates to everyone else. |
| Participants privacy | Need to provide information to central server to build trust. | Fully functional under anonymous setting with no trust been built. |
| Data security | Single-point failure on central server, data can be tampered and destroyed if central server is breached. | No single-point failure, data are not able to be tampered once stored on blockchain. |

advances of blockchain technology can benefit blockchain-enabled applications that are still at the very initial stage. However, there are nature gaps that the advances are hard to propagate among applications. Specifically, in this paper, we depict a blockchain ecosystem that contains several crucial and connected blockchain applications as in Fig. 1, i.e., edge computing, Internet of Things, social network, healthcare, and supply chain. It is highly demanded to bring recent notable works in those application fields together to facilitate future developments of this blockchain ecosystem.

There are extensive survey works in literature related to above applications. Wan et al.[12] and Singh et al.[13] surveyed recent popular blockchain consensus mechanisms. Zhou et al.[14] summarized existing solutions on solving the scalability issue of blockchain. They classified the solutions into three layers: Layer 0 which is about data propagation, Layer 1 which is about on-chain methodologies, and Layer 2 which is

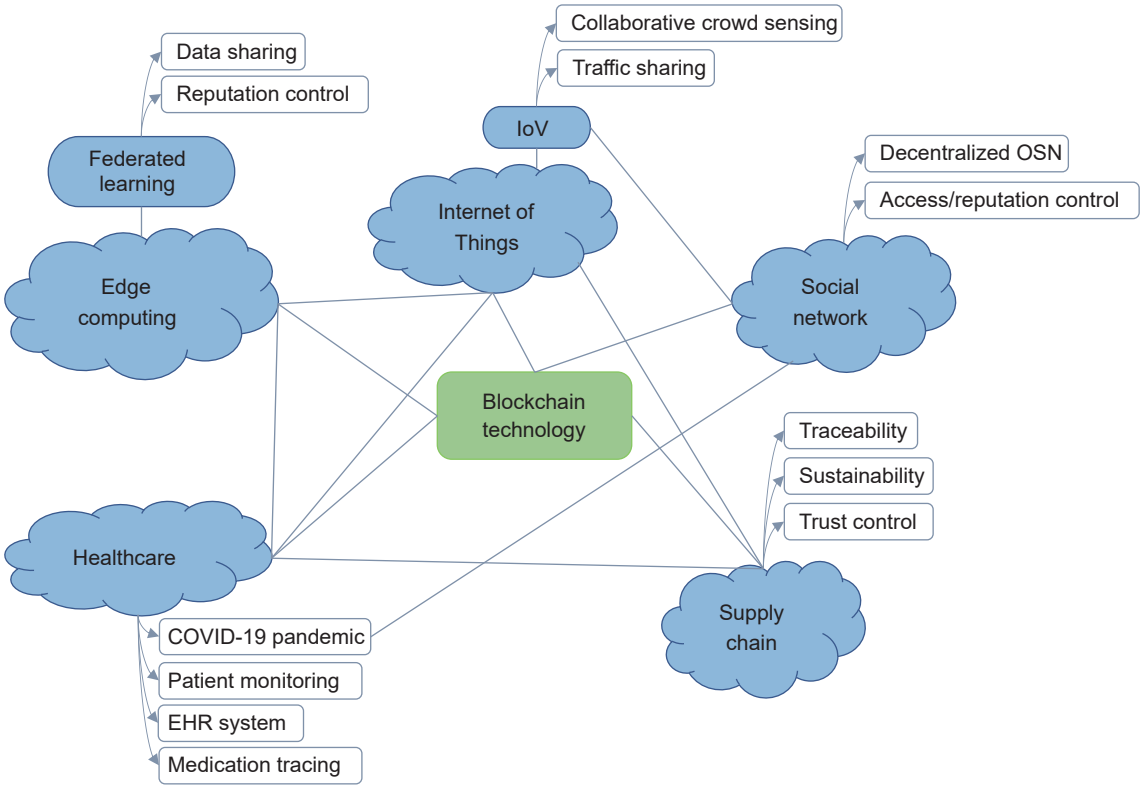


**Fig. 1 Blockchain ecosystem in this paper.**

about external off-chain solutions. Zhang et al.[15] and Feng et al.[16] investigated the security and privacy protocols of blockchain systems. Zhang et al.[15] tried to analyze how well blockchain systems support the privacy and security requirement of transactions and concluded that only a small part of the blockchain platforms can achieve the security goals in practice. Feng et al.[16] summarized methodologies proposed by recent works to tackle the privacy issues in blockchain applications. Gamage et al.[17] introduced several blockchain applications in their survey such as supply chain, however, most the mentioned applications are special use cases of blockchain while some major applications are left behind, for instance, IoT and edge/cloud computing. Huo et al.[18] investigated research topics of blockchain-enabled IoT. They summarized that blockchain is mainly used in IoT for equipment safety and management, data collection and sharing, energy trading, collaborative production, and traceability. Wang et al.[19] and Mollah et al.[20] conducted detailed survey about recent blockchain applications in Internet of Vehicles (IoV) which is a special instance of IoT. Blockchain-enabled IoV is usually studied with more specified use cases than general IoT[21], such as recent emerging electrical vehicle charging and smart parking. Zou et al.[22] extensively reviewed blockchain developments in cloud computing and considered both cloud as a blockchain service where blockchain assists cloud service and blockchain as a cloud service where blockchain service is deployed on cloud. Liao et al.[23] studied the overlapped areas of edge computing and IoT. There are also comprehensive surveys on federated learning[24, 25], which is an emerging distributed machine learning schema to protect data providers' privacy and reduce the data transmission consumption. Sreerakhi et al.[26] reviewed blockchain works in supply chain to discover the possibility of blockchain to help solve challenges including asymmetric information sharing, quality monitoring, and market counterfeiting. Rahman et al.[27] and Shi et al.[28] investigated how blockchain can help healthcare applications collaborating with IoT devices and ensure privacy.

Though hundreds of surveys related to blockchain are published every year, comprehensive surveys that involve multiple applications in above blockchain ecosystem are rather less. In 2022, by the time of this paper was last modified (Nov. 2022), there were totally 160+ blockchain surveys, but none of a survey covers all above mentioned blockchain applications. The distribution of blockchain surveys in last 3 years is shown in Table 2, where only Ref. [29] in 2021 mentioned all the general blockchain applications as this paper but only with brief introductions. Though Refs. [30, 31] in 2022 covered all those blockchain applications except social network, they did not show emerging applications such as federated learning applications in edge computing and COVID-19 applications in healthcare. In this paper, we conduct comprehensive survey of blockchain technology and its applications as in Fig. 1. We first review the recent remarkable improvements of general blockchain technology. Then we choose IoT, edge computing, federated learning, healthcare, social network, and supply chain as the most representative blockchain use cases in whole blockchain ecosystem. Extensive literature review is conducted on those selected use cases by discussing recent active research topics, challenges, and opportunities in each. We finally enumerate several open issues for academia and industry to summarize the survey.

The remainder of this paper is organized as follows. We first present blockchain fundamentals in Section 2. Then in Section 3, we summarize the recent important developments of general blockchain technology. Next in Section 4, we review how blockchain can serve IoT systems and IoV which is a special use case in IoT. Next in Section 5, topics on blockchain-enabled edge computing and federated learning are investigated. In

**Table 2 Amount of blockchain surveys on related topics.**

| Topic | Amount of blockchain surveys | | |
|---|---|---|---|
| | 2020 | 2021 | 2022 |
| Internet of Things | 31 | 33 | 39 |
| Cloud/edge computing | 8 | 12 | 13 |
| Healthcare | 16 | 17 | 20 |
| Social network | 1 | 2 | 0 |
| Supply chain | 14 | 17 | 15 |
| Comprehensive ** | 0 | 1[29] | 0 |
| Total *** | 170 | 187 | 164 |

Note: Data are from DBLP (https://dblp.unitrier.de/db/), with searching keywords: "blockchain survey" and "blockchain review". ** means a survey includes all above topics. *** means the total number of blockchain survey in that year, not limited to listed topics.

Section 6, we study several emerging hot topics that benefit from blockchain, including healthcare, COVID-19 pandemic, social network, and supply chain. Next in Section 7, we discuss our findings on current open issues and challenges of blockchain, then present the suggestions on future work. Finally, this paper is concluded in Section 8.

## 2 Fundamentals of Blockchain

In this section, we review the typical blockchain components and methodologies with Bitcoin blockchain as an typical example. A typical architecture of blockchain systems is illustrated in Fig. 2. For applications in different use cases, modifications are common in order to match different demands which will be described in later sections.

### 2.1 Block storage methodology

In a blockchain system, all data are stored in a data structure called "Block" which are linked together as a chain. At high level, a block contains two parts: block header and block body. Block header contains information for validating a block and linking the current block to previous block. Block body stores data, i.e., transactions.

Figure 3 shows a typical block structure. Block header contains previous block hash, Nonce, timestamp, and Merkle root which is associated with block body. A new block can be generated by finding a valid block header. Let $H_{\text{cur}}$ and $H_{\text{prev}}$ denote the hash values of current generating block and the latest valid on-chain

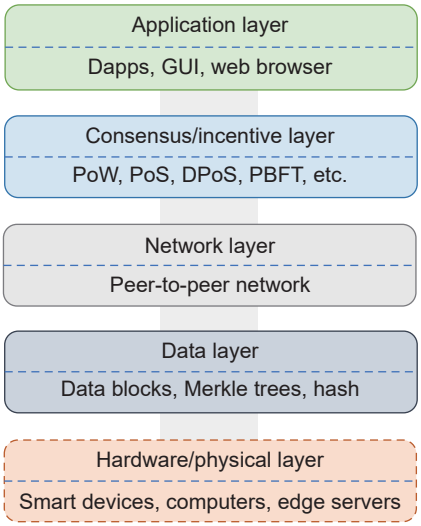


**Fig. 2 A typical architecture of blockchain systems.**

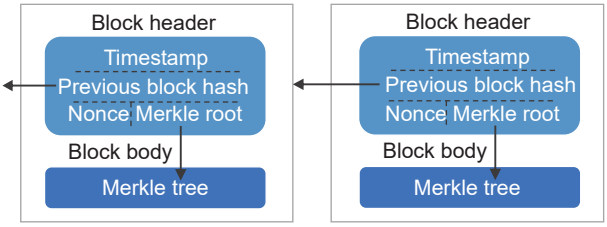


**Fig. 3 A typical block structure in blockchain (e.g., Bitcoin blockchain).**

block, respectively. Let $\mathcal{H}$ be a hash function known by all blockchain nodes. The $H_{\text{cur}}$ can be calculated by

$$H_{\text{cur}} = \mathcal{H}(H_{\text{prev}}, \text{block body}, \text{Nonce}) \tag{1}$$

where $H_{\text{prev}}$ is generated by executing hash function $\mathcal{H}$ on the latest valid on-chain block.

As the Proof of Work mechanism in Bitcoin blockchain, the choose of Nonce is a trial-and-error process to finally make the $H_{\text{cur}}$ satisfy the special requirement, e.g., must start by certain number of zeros. Since the block hash is generated based on previous block, the blocks can be considered as linked together in a chain rule. Any modifications on a block will change the current match of hash values after the modified block, therefore blockchain storage is immutable unless all blocks after the modified block are redone.

In blockchain systems using other consensus mechanisms, the block header and chain role can be slightly different. For example, in Ethereum 2.0, Nonce no longer exists, and blocks are not needed to be validated based on the hash value§.

Block body is the main content in a block where transactions are stored in Merkle tree[1]. Merkle tree (or binary hash tree) is a data structure to securely store and verify information built upon hash functions[32, 33]. A complete Merkle tree maps all the hash values of leave nodes up to a single hash value which is called Merkle root. As in Fig. 4a, $T_i$ denotes a transaction, and the leave nodes of Merkle tree in blockchain systems are transactions. These transactions will first be hashed into a fixed length value $H_i$. Then these $H_i$ will be concatenated pair-wise, and hashed into a new value as Eq. (2). This process continues until the Merkle root is reached, which is the final hash value.

$$H_{ij} = \mathcal{H}(H_i, H_j) \tag{2}$$

§ https://ethereum.org/en/developers/docs/blocks/

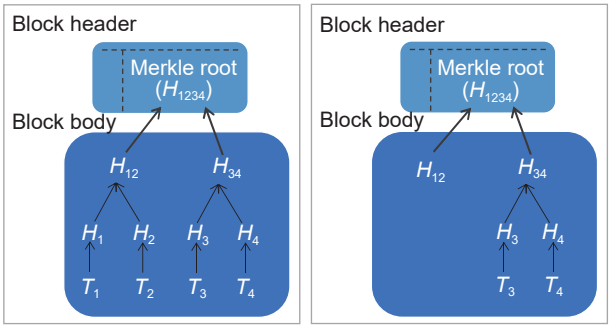


**Fig. 4 Illustration of Merkle tree in a block.**

Merkle tree enables blockchain system to efficiently validate the transactions any later time after the transactions are stored in blockchain, since we can easily check if an unknown transaction matches any recorded hash values in Merkle tree. In addition, it is possible to prune the brunches in Merkle tree to significantly reduce the total storage as shown in Fig. 4b.

In typical blockchain system, every blockchain node keeps the whole copy of blockchain storage which makes blockchain system decentralized in term of storage. Extensive researches have proposed novel storage methods to optimize the blockchain storage cost, which will be discussed in Section 3.2.

### 2.2 Peer-to-peer network and communication schema

A typical public blockchain system works on a Peer-to-Peer (P2P) network. In a P2P network, each peer (also called node) is associated with a client at its local machine. The client stores all the network information of other peers, such as IP address and network port number. In this manner, every peer has direct connections to all other peers, that any message from peer $p_i$ to peer $p_j$ can be directly sent from $p_i$'s client and received by $p_j$'s client without passing through any central server.

Typically, every blockchain node is a peer in the P2P network, works as exactly same role, and performs the same function following particular smart contracts specified in the system. P2P networks allow blockchain systems to broadcast block updates directly to other blockchain nodes. P2P network is the reason that blockchain systems are decentralized in terms of performing functions and can be third-party free.

The major communication between blockchain nodes is for updating blockchain storage. The updates rely on broadcasting and relaying through the P2P network. As illustrated in Fig. 5, once a blockchain node (Node 1) has local update on blockchain storage, the nodes will first broadcast this update to all other blockchain nodes (usually just a few neighbor nodes in practice). Upon receiving the block update, blockchain nodes will verify if the new block is a valid block. For example, in Bitcoin blockchain, nodes recalculate $H_{\text{cur}}$ by the given Nonce in block and justify if $H_{\text{cur}}$ is a satisfied hash value. Because of network delay or failure, some blockchain nodes (Nodes 2 and 3) are able to receive this update earlier than others (Nodes 4 and 5). Later when Nodes 4 and 5 receive another new node, they will understand they missed one block since the hash value will not match. Then they will request the missing block from their neighbors.

### 2.3 Consensus mechanism and miners

Because blockchain systems are decentralized where every node can propose new block and broadcast updates, it is crucial to generate new blocks in an organized way. The consensus mechanisms are the protocols that all the nodes in a blockchain system are required to obey, and carefully give the ledgering right to one of the nodes at a time who is called miner. For example, in Bitcoin blockchain which uses Proof of Work consensus mechanism, a miner is the one who first find the satisfied Nonce in Eq. (1). In Ethereum 2.0 which uses Proof of Stake (PoS) consensus mechanism, the

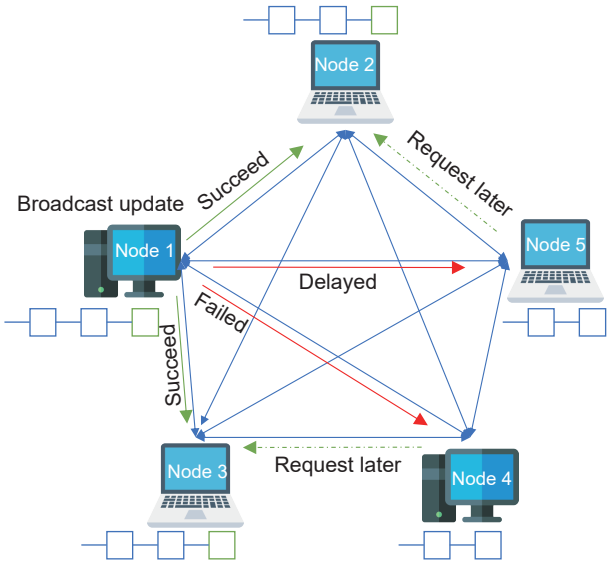


**Fig. 5 Blockchain peer-to-peer network communication schema.**

miner is chosen based on probability that is proportional to nodes' stakes. We will show more consensus mechanism in Section 3.1.

Mining refers to the process that a miner works out a new block for packaging transactions and broadcasts the new block to the whole blockchain network, e.g., Node 1 in Fig. 5. Some time after the broadcasting, all nodes in the network get synchronized and hold the same copies of whole blockchain storage.

Blockchain systems rely on miners to perform data storing function. In many blockchain systems, incentive mechanisms hence commonly exist to distribute the working rewards to the miner and incentive nodes to keep working honestly. Miners in Bitcoin blockchain can earn bitcoins from transaction fees, and miners in Ethereum can earn gas.

## 2.4 Typical blockchain system working flow

Now we summarize a typical blockchain working flow from a transaction being generated to being permanently stored in a blockchain system in Fig. 6. The transaction generator is a network node who has some data needed to store in blockchain. A transaction generator is not necessarily to be one of the blockchain nodes. Let DN be the transaction generator, BN be blockchain nodes, $T$ be a transaction, and $B$ be a block.

**Step 1**: DN generates a new transaction with some data $D$ and promised reward $R$ for the miner.

**Step 2**: After the transaction is formed, the DN broadcasts this transaction to all blockchain nodes. Blockchain nodes will update their transaction pool, memPool, where transactions are waiting to be packaged.

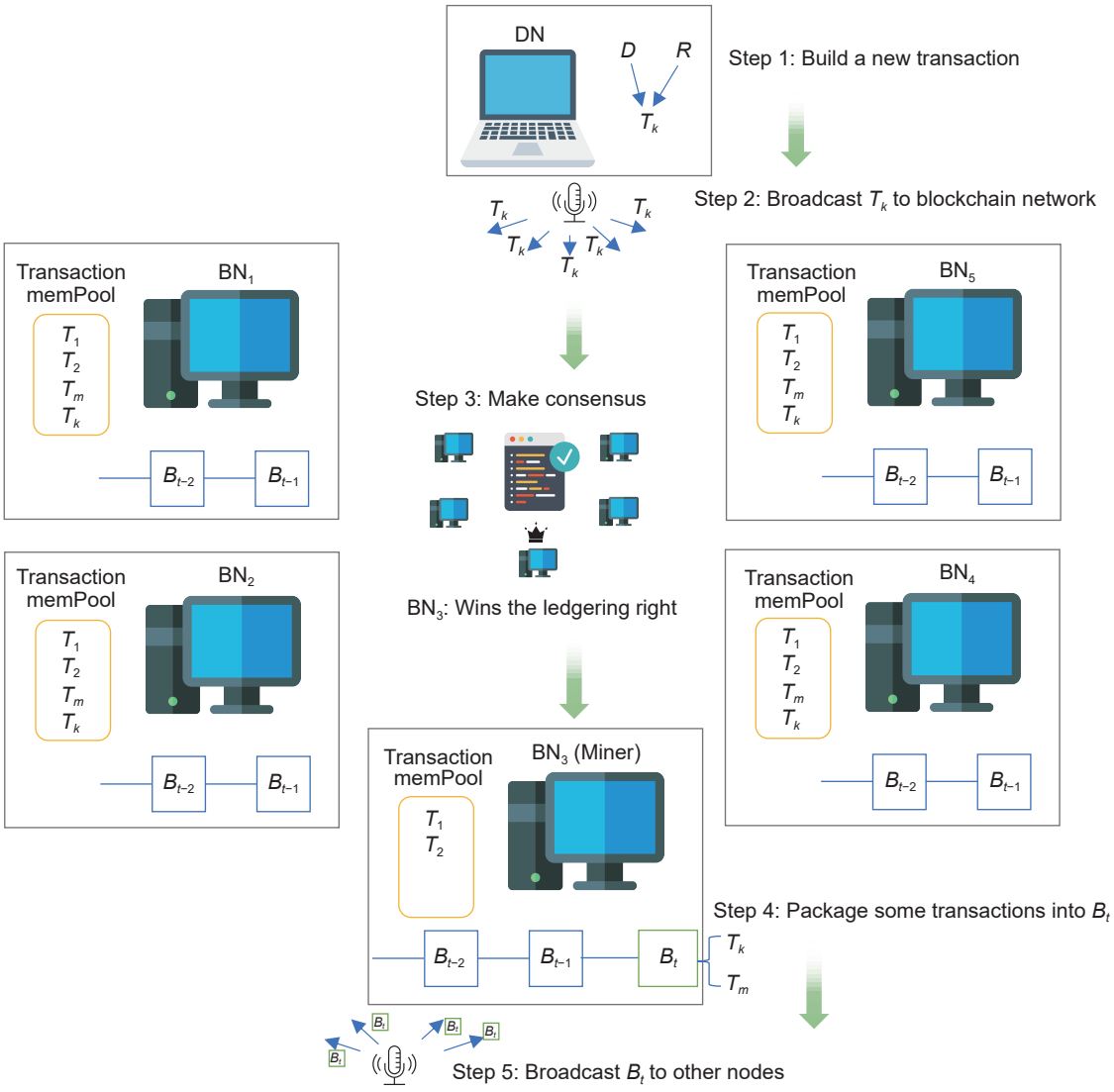


**Fig. 6 A typical data processing flow in blockchain system.**

**Step 3**: The blockchain nodes then conduct consensus mechanism to select one miner for this round. In this example, $BN_3$ wins the ledgering right for generating next block, e.g, the first one who gets the desired Nonce at this round.

**Step 4**: $BN_3$ chooses some transactions in memPool, and stores them into a new block $B_t$. $B_t$ will also be stored locally at $BN_3$ directly and $BN_3$ gets the promised reward $R$.

**Step 5**: $BN_3$ broadcasts this new block through P2P network to all other blockchain nodes. Other block chain nodes will verify $B_t$ and update their local blockchain. The transaction is finally stored in blockchain system which is free of single-point failure, immutable, and accessible from any blockchain nodes.

## 3 Advances in General Blockchain

In this section, we review the recent advances in general blockchain systems. Blockchain technology has been explored from varied directions. Maesa et al.[34, 35] studied blockchain from graph view. Chen and Liu[36] attempted to discover communities in blockchain networks. Pontiveros et al.[37] proposed a centrality measurement for Bitcoin transaction graph. Li et al.[38] discovered topological and geometrical feature of Ethereum blockchain. Banno and Shudo[39] proposed a simulation tool for simulating blockchain systems. Liu et al.[40] designed a neural network that can automatically discover features of blockchain from the blockchain whitepapers. Selfish mining problem was studied in Ethereum and Bitcoin blockchain[41−43]. Chen et al.[44] studied potential phishing scam problem in financial blockchains. Hou et al.[45] proposed SquirRL model that utilizes reinforcement learning method to analyze blockchain incentive mechanisms for vulnerabilities such as selfish mining.

Generally, majority works are focusing on solving the scalability issue of blockchain, that is, to improve the consensus efficiency, increase transaction throughput, and reduce computation and communication cost as well as storage overhead. In this section, we discuss recent advances in consensus mechanisms, storage methods, and communication schemas for general blockchain systems.

### 3.1 Consensus mechanism

Proof of Work (PoW) is the most popular consensus mechanism for blockchain systems. In PoW-based blockchain systems, peers invest powerful machines to solve cryptographic problems to win the right for ledgering. Though it is proven to be secure and stable in some well-known applications, such as Bitcoin[1] (as shown in Section 2.3) and Ethereum[3], it consumes extraordinary power for solving meaningless cryptographic puzzles. PoW limits the throughput of processing transactions and brings increasing computational and storage overhead.

Proof of Stake[3, 46] is a popular consensus mechanism as a competitor of PoW. PoS gives the ledgering right to the peers with the probability as the contribution that the peers have made to the system, namely stake. PoS is less decentralized than PoW, but significantly improves the scalability and consensus efficiency. Delegated Proof of Stake (DPoS)[47] is proposed to give more probability for being a miner than PoS to those who hold small amount of stakes. In DPoS consensus mechanism, whenever there is no candidate miners, every user will vote someone they trust. The weight of the vote is proportional to the stake of the voter. After voting, the peers that received top $k$ votes become candidate miners. DPoS has been applied in many applications[48−51]. DPoS is also a scalable and light weight consensus mechanism but not perfectly decentralized. Various modifications have been proposed for DPoS[52−56]. Xu et al.[57] proposed to improve the DPoS consensus by allowing nodes to vote favor, against, and abstention. Then a vague value of node is calculated based on all three kinds of received votes. Fuzzy value is finally derived as final score on which miners are selected.

We summarize the probability of a blockchain node $BN_i$ to become a miner as follows:

$$P_i \propto \begin{cases} \mathcal{F}_i(\mathcal{H}), & \text{if PoW;} \\ S_i, & \text{if PoS;} \\ \sum_{j \text{ votes } i} S_j, & \text{if DPoS} \end{cases} \tag{3}$$

where $\mathcal{F}_i(\mathcal{H})$ is the hashing power of $BN_i$ for conducting hash function $\mathcal{H}$, and $S_i$ is the current holding stake of $BN_i$.

Practical Byzantine Fault Tolerance (PBFT)[58] is a classic Byzantine fault tolerant protocol and introduced into blockchain systems as consensus mechanism[59, 60]. PBFT consensus mechanism does not produce a single miner, but to make consensus through message

propagation. PBFT consensus mechanism commonly has five phases, namely request, pre-prepare, prepare, commit, and reply. The client sends the message to be confirmed to a selected "primary" at request phase. The "primary" then broadcasts this message to all other peers ("replicas") at pre-prepare phase. Then each "replica" broadcasts received message to all other peers including "primary" and other "replicas" at prepare phase. Next at commit, all peers, including the "primary" and all "replicas" send the message received at last phase to all other peers. Finally all peers send back the message to the "client" at reply phase. PBFT consensus is made through message transmission and commitment, therefore requires notable communication cost.

SCP[61], proposed by Luu et al., constructs two-layer blockchain with committees, where one layer is for data blocks which are proposed by normal committee and another layer is for consensus blocks which are proposed by the final designated committee in SCP to include all data blocks. The committees can make parallel PoW consensus, hence improve the efficiency and transaction throughput. Li et al.[62] proposed ISCP to promote the security level and communication efficiency of SCP. ISCP eliminates the need of final committee in SCP with a decentralized multi-partition consensus model. Amiri et al.[63] proposed a novel OXII distributed diagram allowing transaction to be executed without conflict in permissioned blockchain. ParBlockchain is then proposed based on OXII diagram to achieve better transaction throughput.

In order to adapt to specific applications, various Proof of X (PoX) are developed where "X" can be any metrics defined in those applications, such as Proof of Reputation[64], Proof of Quality Factor[65], and Proof of Event[66]. Bahri and Girdzijauskas[67] studied crypto-currency-free blockchain system. They proposed viable permisionless non-financial blockchain where Proof of Trust (PoT) is designed based on trust graph among peers. In PoT, peers with higher trust level can solve PoW cryptographic puzzle at lower difficulty level, thus reducing overall energy expense of PoW.

### 3.2 Storage method

Classic blockchain systems require every peer to store a full copy of entire blockchain storage. This storage mechanism not only wastes enormous resources, but makes system get centralized gradually. The oversized blockchain increases the bar of storage requirement for participants and also makes the system hard to process data-heavy applications. With the blockchain growing in size, more and more disadvantaged nodes who can not afford the storage cost are gradually leaving the mining game. Finally, the system becomes more and more centralized.

#### 3.2.1 Blockchain sharding

Blockchain sharding technology[68, 69] is explored for reducing the storage overhead. Generally, blockchain sharding is to divide peers into groups where consensus is made within each group so that transactions can be processed concurrently. Peers in each group (shard) maintain their local ledger, therefore in order to derive the full chain, a concurrency control and a commitment mechanism need to be designed[70]. Zamani et al.[71] proposed RapidChain to further reduce the communication cost while maintaining the resistance to Byzantine faults when there are less than $1/3$ fault nodes in all participated nodes. Xu and Huang[72] developed an blockchain sharding mechanism that can tolerate $1/2$ fault nodes. SkyChain is a dynamic sharding method enabled by deep reinforcement learning which can effectively deal with the dynamic environment in the blockchain system, i.e., joining and leaving of nodes, and malicious attacks[73]. Blockchain sharding technology is also developed in many domain-specific applications, such as IoT[74] and Federated Learning[75].

#### 3.2.2 Blockchain segmentation

Xu and Huang[76] proposed segment blockchain where the whole blockchain is broken down into segments, and peers only need to store several segments. The number of blockchain segments is dynamically adjusted to maintain that the minimum number of holders of segments does not exceed 10. The segment adjust function is defined as Eq. (4).

$$\begin{aligned} &n_s = n_s + 10, \\ &\text{if } \exists\, i <= n_s,\ \min(N_i) <= 10 \end{aligned} \tag{4}$$

where $n_s$ is the total number of segments, and $N_i$ is the number of blockchain nodes holding the segment $i$. After readjusting the number of segments and reassigning blockchain nodes for storing the segments, the new block at height $h$ is stored in segment $(h \mod n_s) + 1$. The whole blockchain storage can be recovered from multiple nodes' storage.

Qi et al.[77] proposed a storage partition method

namely BFT-Store for permissioned blockchain reducing the storage complexity per block from $O(n)$ to $O(1)$. Meanwhile, the data availability and data access efficiency are ensured by proposed four-phase re-encoding protocol based on PBFT and multiple replication mechanism with cache structure. The experimental results in Ref. [77] showed that at the same number of nodes, BFT-Store enabled blockchain can store more blocks, with remarkably lower storage overhead.

### 3.3 Blockchain communication protocol

As described in Section 2, the blockchain storage update relies on the broadcasting processes across the whole blockchain P2P network. High broadcasting delay may introduce forks in the blockchain and decrease the throughput of whole blockchain system[78, 79]. The latency of broadcasting is mainly related to three factors: the total number of nodes, the block size for propagation, and the broadcasting protocol. Since the total number of nodes in a blockchain network is not controlled in most public blockchains. In this paper we focus on recent advances related to the later two factors.

#### 3.3.1 Block compression for propagation

Reducing block size can improve the broadcasting speed. Decker and Wattenhofer[79] analyzed that in Bitcoin network, relaying small size blocks brings significant propagation redundancy, and each kilobyte more than 20 kB of a block will cause 80 ms additional delay until majority have updated this block. They proposed three high-level optimizing methods. The first method is to reduce the verification time for blockchain nodes before they can relay the block, so that less time will be wasted before each propagation. The second method is to allow block nodes to request the block body from their neighbors even the block is not yet available at their neighbors, so that blockchain nodes will receive the new block once their neighbors get it. The third method is to re-construct the P2P network with star sub-graphs to shorten the propagation distance. RapidChain[71] and segment blockchain[76] discussed above that reduce the overall blockchain size can also improve communication efficiency meanwhile. PiChu[80] divides one block into multiple chunks, then broadcasts and verifies these chunks in parallel. Though the total size of a block is not reduced and even slightly larger than original due to the extra data required for formatting a chunk, PiChu reduces the message size for a single transmission, and total broadcasting time is reduced with the advantage of parallel broadcasting. Some block compressing methods are proposed to reduce the block size before broadcasting[81, 82]. PoW-BC[82] uses Deflate compression algorithm[83] and incorporates block compress ratio into the mining difficulty in PoW as Eq. (5).

$$D' = D \times \frac{T_{\min} + T_{\text{vrf}} + (\alpha - T_{\text{vrf}}) \times r}{\beta} \tag{5}$$

where $D$ and $D'$ are the original and updated mining difficulty, respectively. $T_{\min}$ is the minimum block interval. $T_{\text{vrf}}$ is the time for verifying the transactions in the generated block, $r$ is the compress ratio, and lower compress ratio means smaller block size after compress. $\alpha$ and $\beta$ are predefined parameters.

#### 3.3.2 Improvements on block propagation schema

New broadcasting schemas are also proposed. Classic P2P network is unstructured where nodes are connected randomly. Structurizing the P2P network and optimizing the message propagation topology are a promising way to alleviate communication cost. Wang et al.[78] proposed new propagation topology in P2P network, namely Swift, that recursively divided the whole P2P network into propagation scopes, and each propagation scope is divided into smaller sub-scopes. Message is also transmitted within each sub-scope recursively. They defined a node $n$ establishes a connection with another peer $p$ with a probability $\Phi(p,n)$ which is greedily defined to maximizing propagation scope given each propagation round. Other classic state-of-the-art propagations optimizing in structured P2P network include Chord[84], CAN[85], Tapestry[86], and Graphene[87]. Kadcast[88] is another recent notable work built upon Kademlia[89] where UDP networking process is utilized to support light-weight transmitting. Perigee[90] maps the propagation process as multi-armed bandit problem that is able to build optimal propagation path considering geography, varying hashing power, and computation power of peers. Nodes in Perigee evaluate its neighbors' connectivity based on propagation history periodically and choose the node with best connectivity to connect.

#### 3.3.3 Joint optimization on consensus mechanism and propagation schema

Some works jointly improve consensus mechanism and block broadcasting[91–94]. Algorand[92] is a blockchain

system using Byzantine Agreement (BA) protocol to reach consensus. The consensus is made during the propagation through the votes on the propatated block. Prism[93] deconstructs the blockchain into transaction blocks, proposal blocks, and voter blocks. The main chain is selected through voter blocks, which vote among the proposal blocks at each level to select a leader block. The three types of blocks form a structured Directed Acyclic Graph (DAG) that allows a very efficient way to vote on leader blocks that eventually give consensus via total ordering. Al-Musharaf et al.[94] first grouped blockchain nodes into clusters where close nodes within a geographical region belong to one cluster. Then each node within one cluster will try different Nonce to solve PoW to avoid repeated work. The mined block will be broadcasted first within one cluster then through cluster header to other clusters. However, this method is not robust to attack because clustered nodes are easily to collaborate with each other to propose false blocks.

## 4 Advances in Blockchain-Enabled Internet of Things (IoT)

Internet of Things (IoT) allows smart devices to connect with each other through internet protocols for a ubiquitous data exchange[95, 96]. The devices or objects working in Internet of Things are mostly sensors and micro-computers that can be easily compromised by malicious attacks. Blockchain technology applied in IoT is a promising solution to improve the data integrity and security[97]. Figure 7 shows a typical structure of blockchain-enabled IoT and edge computing systems which will be discussed in Section 5.

However, there are some challenges for realizing blockchain-enabled IoT systems. Due to the low computation capability, battery life, and memory storage of devices in IoT, the devices are not able to process heavy-weight consensus mechanisms like PoW[98]. On the other side, blockchain systems are mostly not able to produce high throughput which can not meet the demand of tremendous data generating and storage tasks in IoT systems[99].

In this section, we first review the recent blockchain works in general IoT systems, then we investigate an active special use case in IoT, namely Internet of Vehicles (IoV).

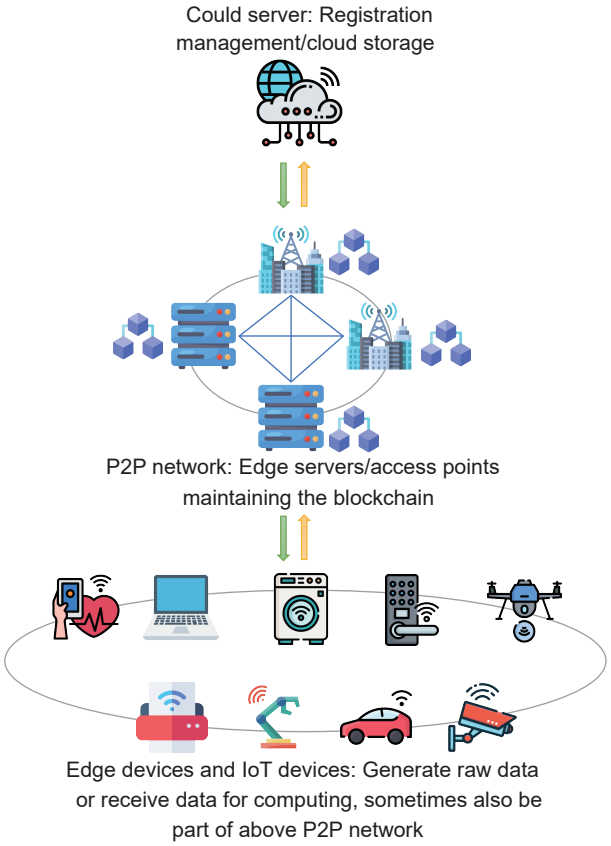


**Fig. 7 General architecture of blockchain-enabled IoT and edge computing systems.**

### 4.1 General IoT

#### 4.1.1 Consensus mechanisms for IoT

Many light-weight consensus mechanisms are designed to make blockchain feasible in IoT, such as credit-based consensus mechanism[100], Proof of Block & Trade (PoBT)[101], PoRX[102], and Proof of Transactions[103]. Huang et al.[100] brought node credit into PoW consensus mechanism. The higher the credit, the lower the mining difficulty assigned to the node. They considered the credit from both positive behaviors that obey the system rules to send transactions and negative behaviors that cause extra delay or failure transactions. Comparing to Eq. (5), the mining difficulty in Ref. [100] is defined as Eq. (6).

$$\begin{aligned} &D' \propto \mathrm{Cr}_i, \\ &\mathrm{Cr}_i = \lambda_1 \times \mathrm{Cr}_i^P + \lambda_2 \times \mathrm{Cr}_i^N \end{aligned} \tag{6}$$

where $\lambda_1$ and $\lambda_2$ are trade-off factors. PoBT[101], i.e., Proof of Block & Trade, is a two-stage consensus. At the first stage, if the transaction is within IoT devices that are connected to one local blockchain node, the local consensus is quickly made. At the second stage,

the transaction is sent to global orders who are delegated to form final global consensus. The core idea of Proof of Transactions[103] is that the node that collects the most valid transactions in the same time period should be recognized as winner and create the new block for the cluster, which can effectively increase the throughput. Dorri et al.[104] proposed a Lightweight Scalable Blockchain (LSB) for industrial IoT, where nodes are divided into clusters and managed by cluster heads. A Distributed Throughput Management (DTM) algorithm is proposed to dynamically adjust number of clusters and consensus period for maintaining high transaction throughput. Biswas et al.[105] separated the workers in IoT network from the peers in blockchain network. The workers in IoT networks are defined as local peers who are connected to designated anchor peer representing one organization in blockchain network. Transaction commitment can be made within organization without global consensus, hence the transaction throughput is improved.

Incentive mechanisms are also studied for IoT. Ding et al.[106] designed an incentive mechanism to motivate devices to devote more power in mining. A two-stage Stackelberg game is formulated to find reasonable reward pricing strategy to maximize blockchain utility.

#### 4.1.2 Blockchain systems for IoT

Instead of proposing consensus mechanism, some works specified more details and designed comprehensive blockchain systems for IoT applications, such as AEChain[107], BPAF[108], BET[109], and B-MET[110]. AEChain[107] divides IoT devices into groups and assigns a blockchain node for each group as a worker to communicate with IoT devices as well as maintaining blockchain. In BET[109], the PoW is also associated with IoT device credit which is similar to Ref. [103]. Li et al.[111] were the first to study the problem of extra cost caused by frequent smart contract updates in blockchain-enabled IoT system. A new smart contract architecture is proposed, namely ATOM, that can construct the bytecode of smart contract from application by directly assembling templates pre-built upon the designed Application-oriented Instruction (AoI) set rather than by compilation. Zhou et al.[112] aimed to improve the storage efficiency of blockchain-enabled wireless communication by proposing Dynamic Adjusted Block-assignment (DAB) contract which dynamically assigns blockchain portions to different devices.

#### 4.1.3 Machine learning in blockchain-enabled IoT

Reinforcement learning methods are developed to optimize resource allocation in IoT networks to achieve better scalability[113, 114] and resource allocation[115]. Liu et al.[116] proposed a deep reinforcement learning approach that can help maximize on-chain transaction throughput of the blockchain system by selecting the block producers and consensus algorithms as well as adjusting the block size and block interval. Yun et al.[117] proposed Deep Q Network Shard based Blockchain (DQNSB) scheme that dynamically finds the optimal throughput by selecting transaction sharding methods, also the block size and block interval. Ding et al.[118] introduced edge server into IoT networks, where IoT devices are able to purchase computational power from edge servers. They derived a Stackelberg equilibrium to optimize the pricing and budget allocation.

### 4.2 Internet of Vehicles

Internet of Vehicles (IoV) or vehicular network is a special IoT application where the IoT nodes are the mobile devices installed on vehicles. In IoV system, vehicles can share information such as road condition, traffic conjunction, and accident information with other vehicles, so that vehicles are able to decide best routes or collaborating with each other on some emergency issues.

Blockchain technology brings decentralized architecture to IoV as it does to IoT. IoV usually has more strict requirements on applied blockchain system[119]. Vehicles are moving, making them can only connect to roadsides or other vehicles periodically. Vehicles also have limited battery and computation power, making them reluctant to participating in low-profit or computation-expensive tasks.

#### 4.2.1 Consensus mechanisms for IoV

Despite some classic consensus mechanisms are adopted in IoV, such as PoS[120, 121], PoET[122], and PBFT[123, 124], researchers are developing more scenario-specific consensus mechanisms in order to achieve better security, latency, and throughput in IoV. Kang et al.[120] designed a reputation-based voting scheme to improve the security of blockchain-enabled IoV. This scheme evaluates candidates' reputation using both past interactions and recommended opinions from other vehicles. Proof of Quality Factor[65] is proposed to bridge vehicles and edge computing servers, which allows mobile edge nodes to

serve as mining nodes. As the number of Electric Vehicles (EVs) increases, Luo et al.[125] studied the energy trading in the internet of electric vehicles. They proposed to deploy blockchain server in Local Energy Aggregators (LEAG) to store all the trading transaction records and specify smart contacts as agents for optimal energy pricing and allocation. Abishu et al.[126] jointly considered PBFT and Proof of Reputation (PoR) and proposed PBFT-based PoR (PPoR). Electric vehicles are grouped in clusters according to the roadside units they connect to. PPoR will select miners (validators) in the cluster based on their reputation value that is calculated based on evidence and opinion spaces collected from EVs in each cluster.

#### 4.2.2 Blockchain systems for IoV

Cho et al.[127] proposed iCarChain for managing vehicle related businesses in decentralized manner. iCarChain is an initial attempt for benefiting consumers and vehicle business industry with fewer technological restrictions and more affordable expenses by decentralizing the business system. Blockchain serves as distributed storage system for IoV in Ref. [121] where roadside units are selected based on both PoS and PoW as miners to pack data and messages generated by vehicles. Wang et al.[128] proposed TrafficChain which is a two-layer blockchain-enabled secure and privacy-preserving decentralized traffic information collection system. Wang et al.[128] specially studied Byzantine attack and Sybil attack on TrafficChain and proposed novel LSTM based methods to defend against them. Yin et al.[129] studied a special case in IoV that multi-vehicles to collaboration can be performed when a single vehicle is not able to accomplish a task. They carefully designed an incentive mechanism and a task assignment algorithm to motivate vehicles to participate the tasks as well as shorten the collaborative tasks' finishing time. Hui et al.[130] studied similar collaborative crowd sensing problem that aims to motivate vehicles to collaborate each other by formulating and solving a Coalition Game.

#### 4.2.3 Machine learning in blockchain-enabled IoV

Similar to IoT, reinforcement learning also plays important roles in many works of blockchain-enabled IoV[131]. Kim and Ibrahim[132] designed a reinforcement learning model to decide the optimal number of peers participating in consensus making to improve the latency and throughput without compromising the Byzantine fault tolerance. They connected peers in different groups through channels, and formulated the problem of choosing channels as Multi-Arm Bandit problem which is solved by the proposed reinforcement learning algorithm. Liu et al.[133] first proposed a methodology to quantify the performance of blockchain systems in IoV from the aspects of scalability, decentralization, latency, and security, then applied deep reinforcement learning technique to select block producers and adjust block size and block interval, in order to maximize the transaction throughput without sacrificing other properties.

## 5 Advances in Blockchain-Enabled Edge Computing

Edge computing is a technology to allow devices at the edge of network, such as smart devices, mobile micro computers, bases stations, and network access points, to generate, collect, transmit, and process data. Edge computing is an extension of IoT and overlaps with IoT in many applications. For example, the sensors or smart objects in IoT might need to connect to some edge servers to complete data sharing and computing. Some devices in IoT such as electric vehicles can also be considered as edge nodes in edge computing. In this section, we first investigate the blockchain development in general edge computing, then specially discuss an emerging topic in edge computing, namely federated learning.

### 5.1 General edge computing

#### 5.1.1 Blockchain for off-loading in edge computing

Like the deficiencies of blockchain system in many other application fields, blockchain system brings extra computation cost and communication cost to edge nodes. Off-loading as a popular methodology to alleviate the stress of edge nodes is to move computation task to external machines, such as Edge Computing Service Provider (ESP) or Cloud Computing Service Provider (CSP)[134]. Those service providers that are qualified to conduct the off-loaded tasks may earn some profit or reward for providing computation service. In the process of computation offloading in edge computing, it is critical to dynamically make optimal offloading decisions minimize the communication delay, energy consumption spent on the devices, and the throughput of data storage on blockchain[135].

Jiang et al.[134] designed a multi-leader multi-follower Stackelberg game to address computing resource management and maximized profits of service providers and the rewards of miners in the network. Hu et al.[136] detailed a blockchain-enabled edge computing system, and proposed a deep reinforcement learning algorithm to jointly optimize the computation offloading policy and block generation strategy to maximize the scalability. Though abundant off-loading optimization methods have been developed, it is hard to evaluate how good the outcome as well as to compare these methods. To address this issue, Qu et al.[135] proposed ChainFL, that is a lightweight simulation platform for building a test edge computing environment which also supports federated learning and blockchain technology.

#### 5.1.2 Blockchain for collaborative edge computing

Cooperative or collaborative offloading in edge computing is an extended problem over off-loading. Instead of handing over the task to edge servers, collaborative learning is to share a task among edge nodes. Feng et al.[137] utilized deep reinforcement learning algorithm to jointly optimize the cooperative offloading decision and blockchain parameters in blockchain-enabled mobile edge computing systems. Zuo et al.[138] also studied cooperative mobile edge computing and formulated the offloading optimization problem with a three-stage Stackelberg game. Cheng et al.[139] used blockchain to form an authentication system for collaborative edge computing systems that achieve anonymity while avoiding malicious attacks from fake IoT devices.

Xiao et al.[140] addressed selfish attack problem in edge computing that attackers use less computation resources than promised to process offloading tasks or provide faked computation results. They proposed a trust mechanism to assign reputations to edge nodes, then the CPU computation resources are allocated based on the reputation. Liu et al.[141] addressed the problem of the existence of low-quality data such as missing values, inconsistent values, and incorrect values due to the data heterogeneity in edge computing. These low-quality data may not support or even slow down the computation tasks. To tackle this issue, a consortium blockchain was designed in Ref. [141] where the data quality will first be evaluated and repaired before being off-loaded.

#### 5.1.3 Blockchain systems for miscellaneous edge computing

More works incorporated blockchain system deeper with edge computing network to allow blockchain to provide more reliable functions by proposing specific consensus mechanisms and comprehensive blockchain-enabled edge computing systems. Baranwal and Kumar[142] proposed PoSP consensus mechanism that replaces the hash puzzle in PoW with a service placement problem whose result can meanwhile help the resource allocation in edge computing. Maskey et al.[143] used neural networks to decide the miner's reputation instead of a heuristic computation in a blockchain-enabled vehicular edge computing environment. Balistri et al.[144] embedded blockchain into edge computing network in order to promote the cyber-resiliency, where edge nodes and service providers work as peers in a blockchain system. Li et al.[145] designed a typical multi-layer blockchain enabled system, where the blockchain layer is incorporated into edge-computing layer. Similar to Ref. [144], the edge computing nodes in Ref. [145] are also the blockchain peers (nodes) to conduct consensus mechanism and create new blocks. Yuan et al.[146] were the first to extend the collaborative task offloading to collaborative edge storage. They proposed a blockchain system called CSEdge where a reputation based consensus mechanism called ER-BFT is designed to select edge servers based on their reputation, and an incentive mechanism is proposed to motivate edge servers to help complete data offloading.

### 5.2 Federated learning

Federated Learning (FL), first proposed by Google[147] is an emerging distributed machine learning schema. Instead of collecting all the data first from data providers, then training a complicated machine learning model on a central computing device, federated learning allows each data provider to train a local model first and then upload the parameters to the central computing device. In federated learning schema, since data providers keep their data locally, the communication cost is saved and the privacy of data provider can be preserved.

Before federated learning is proposed, blockchain had been adopted to secure the data or model parameters in machine learning. Goel et al.[148] proposed DeepRing which is a blockchain secured

Convolution Neural Network (CNN) model and shows more significant resistance to tampering attack than ordinary models. Fu et al.[149] used blockchain system to secure the collective learning in IoV environment which is similar to federated learning schema. The adoption of blockchain technology in federated learning further promotes the security of machine learning to next level[25, 75, 150, 151]. Based on literature review, we create a generalized blockchain-enabled federated learning architecture, and compare it with conventional federated learning in Fig. 8.

Lu et al.[152] designed a data sharing platform for IoT with blockchain-enabled federated learning, and proposed Proof of Training Quality (PoQ) as a light weight consensus mechanism. Lu et al.[153] proposed a blockchain-enabled federated learning scheme to strengthen communication security and data privacy for communication between digital twins of IoT devices and edge network. The digital twins get the trained parameters from IoT devices instead of tedious device state information. Peng et al.[154] proposed to use blockchain to achieve verifiable and auditable federated learning framework where committee-based aggregation model and an authenticated data structure are developed over blockchain system.

Li et al.[155] proposed a committee consensus to improve the consensus efficiency for a blockchain-enabled federated learning framework, called BFLC. In BFLC, the local updated model gradients and model parameters are stored on blockchain. A committee is formed to evaluate the updates, and only the qualified updates will be stored in blockchain. Qu et al.[156] creatively combined the PoW with federated learning and proposed Proof of Federated Learning (PoFL) that instead of solving the meaningless puzzles in PoW, solving the actual tasks in the federated learning will make much less computation power waste. Nodes are gathered in pools where the PoFL is making for aggregating the desired model.

#### 5.2.1 Incentive mechanisms in blockchain-enabled FL

In federated learning, it is important to define suitable rewards for the worker clients who spend local computation and communication resources training local models. Otherwise, workers may be reluctant to do the training and report useless or even harmful parameters to global model aggregators. In order to jointly satisfy the privacy, integrity, and fair incentives of blockchain-enabled federated learning, Rückel et al.[157] proposed a federated learning framework that incentivizes each client based on their individual contribution to the global model, uses zero-knowledge proofs to ensure data integrity, and adopts local differential privacy to perturb each clients' model update with Laplacian noise to ensure the data privacy. Gao et al.[158] proposed FGFL model that assesses workers based on both contribution and reputation. They also concluded that it is crucial to design both an effective incentive mechanism and a reliable incentive management system to insure the fairness of incentives.

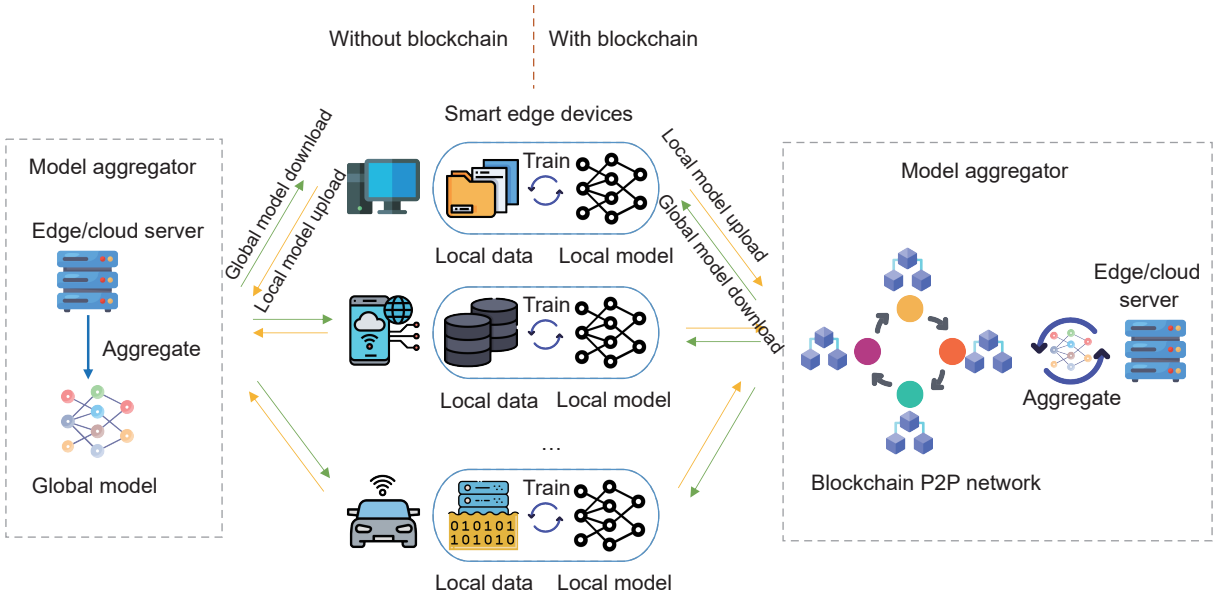


**Fig. 8 Comparison between federated learning architecture with and without blockchain.**

#### 5.2.2 Model synchronization in blockchain-enabled FL

Since federated learning requires each device to upload the trained models to the aggregator, the global model may need to wait the slowest device to finally get updated. Asynchronous federated learning is then studied to deal with the delay of communication from multiple devices. Lu et al.[159] attempted to solve the asynchronous problem in IoV by optimally selecting the participating nodes through deep reinforcement learning. The models will first be aggregated within local range of vehicles asynchronously, then globally aggregated by roadside units synchronously. Feng et al.[160] proposed BAFL, which is a blockchain-based asynchronous federated learning framework. In BAFL, each device is communicating with one miner, for local model uploading and global model updating. The global model can be aggregated by each device once the device decides to update it with local models. Then the consensus of global model will be reached in blockchain layer, hence avoid waiting for all devices. Wang and Tsai[161] proposed to compose a blockchain-enabled asynchronous federated learning system with multiple blockchains, where Sub-Blockchains are responsible for the model local training in multiple devices, and those Sub-Blockchains will communicate with a Main-Blockchain which is for the global model aggregation.

#### 5.2.3 Blockchain systems for joint FL with IoT

The distributed nature of federated learning schema makes it easy to be integrated into IoT networks or edge computing networks, where sensing nodes in IoT and mobile devices can be the clients to train local models[162, 163]. Otoum et al.[164] proposed a blockchain-enabled FL model to decentralize the learning process to ensure privacy and security for critical IoT infrastructure systems. Feng et al.[165] proposed a two-layer blockchain system to enable federated learning in mobile edge computing network where the first layer blockchain is for local model updates and the second layer blockchain helps update global model. Ayaz et al.[166] proposed a blockchain-enabled federated learning in vehicular networks to improve the quality and efficiency of message dissemination.

## 6 Advances in Emerging Applications of Blockchain

In this section, we investigate four emerging research fields where blockchain is increasingly playing important roles to bring decentrality, system robustness, and security to related applications.

### 6.1 Healthcare

The potential of blockchain technology in healthcare has shown and been discussed as a revolution for over 5 years[10, 167, 168]. Traditional healthcare systems are suffering from single-point failures and information leakage by cyber attacks[169], as well as lacking transparency, trustful traceability, immutability, audit, privacy, and security[170]. Blockchain technology provides promising solutions to tackle above issues that can decentralize the storage and permission management, and keep data traceable, verifiable, and immutable[171, 172].

#### 6.1.1 Blockchain for heath information management

Person Health Information (PHI) nowadays is usually digitized into Electrical Health/Medical Record (EHR/EMR) and stored in healthcare authorities' databases, such as hospitals, health insurance companies, or medical laboratories. People may have their PHI in multiple healthcare authorities. Though the information is private, people are not able to manage the abuse of their own information[173]. Blockchain-enabled decentralized healthcare information management systems are proposed to tackle this issue[173−175]. Soni and Singh[176] provided a general mapping from blockchain technology to medical processes and discussed the ability of blockchain to enable access control, secure devices, identity protection, and cost reduction. Zaabar et al.[177] proposed HealthBlock which is a six-layer blockchain-enabled health information management system. Blockchain works in a layer in HealthBlock to manage the access from multiple parties in other layers. Bhattacharya et al.[178] proposeed Blockchain-Based Deep Learning as-a-Service (BinDaaS) system that first adopts blockchain to securely store the collected information using lattice-based signature generation and verifying operations, then applies deep learning technology to produce valuable prediction service, such as patient future disease prediction. Zhang et al.[179] used pairing-based cryptography to generate temper-proof EHR which is further packaged into transactions in blocks. They also designed secure payment protocols between patients and healthcare providers through smart contracts in

blockchain. Chelladurai and Pandian[180] focused on improving the data access speed among multiple parties with proposed Modified Merkle Tree data structure in blockchain. Wu et al.[181] proposed multi-level smart contracts to achieve dynamic access control that allows different access rights for different scenarios. They proposed a Privacy Attribute Classification algorithm to classify medical records into different privacy levels, then the access right can be matched.

Some miscellaneous topics in healthcare information management are studied with blockchain. Liu et al.[182] and Mendoza-Tello et al.[183] proposed to use blockchain to avoid healthcare insurance fraud. Blockchain can also be used to secure the channel of remote patient monitoring[184]. Pighini et al.[185] implemented SynCare ecosystem with blockchain and cloud service that allows patients to directly send data to healthcare professionals without concern of data leakage so that the patient can be securely remotely monitored. Many other patient monitoring systems require participation of IoT devices, such as smart sensors, meters, or network access points, which will be discussed later. Blockchain is also introduced into clinical trails which are usually with a larger flow of information and more confidential data from more parties[186]. Wong et al.[186] and Albanese et al.[187] implemented prototype of blockchain system for clinical trail data management.

#### 6.1.2 Blockchain for medication tracing and medical supply chain

Another helpful blockchain use case in healthcare is medication tracing. Counterfeit medications have brought unneglectable public health concern and severe impact on treatment outcomes due to insufficient, incorrect, and erroneous ingredients, falsified information, or wrong labeling[188]. Blockchain as a powerful distributed data storage method that can manage accessibility, and ensure data transparency and immutability is hence a proactive approach to track, detect, and manage counterfeits in healthcare supply chain[189, 190]. Musamih et al.[189] implemented a blockchain-enabled healthcare supply chain system with Ethereum. They designed on-chain and off-chain structure where the actual healthcare data are stored in off-chain low-cost decentralized storage system, and blockchain is responsible for storing the logs and interact with off-chain resources. Abbas et al.[191] designed Couch-DB where a machine-learning model is built upon the blockchain system to provide drug recommendation to customers.

#### 6.1.3 Blockchain for IoT-enabled healthcare and AI-based healthcare

Blockchain bridges healthcare with various other research fields. As mentioned above, IoT devices are widely used in healthcare, such as monitoring the status of patients and sensing important parameters for treatment or surgery[192]. Ali et al.[193] proposed an efficient blockchain system for IoT-incorporated healthcare applications where a secure search algorithm is designed to encrypt and anonymously search the data stored in blockchain. Hossein et al.[194] proposed two-chain structured blockchain system, namely BCHealth for IoT healthcare applications that allows data owners to personalize the access policies over their healthcare data. In BCHealth, one chain stores access policies and the other chain stores data transactions.

In healthcare, artificial intelligence models provide valuable predictions and analysis for diagnosis. However, due to privacy, healthcare providers are reluctant to share their data for a common Artificial Intelligence (AI) task. Federated learning is hence introduced into healthcare with blockchain to protect the data and AI models in healthcare. Aich et al.[195] proposed a general framework to incorporate federated learning with multiple healthcare providers, where blockchain works as the intermediate platform for transmitting data from healthcare providers to federated learning AI task.

### 6.2 Special healthcare case study: COVID-19 pandemic

COVID-19 pandemic has lasted for over 3 years. Researchers have developed abundant approaches contributing to the prevention of virus spread. In this section, we review the literature of this special use case in healthcare, and discuss how blockchain can benefit the recovery from pandemics.

#### 6.2.1 Blockchain for heath information management in COVID-19

As special use case of healthcare, there are blockchain-enabled EHR management systems specially designed for COVID-19 pandemic[196, 197]. Tan et al.[198] proposed a traceable COVID-19 record sharing system powered by blockchain where a security game (IND-CPA) is built in the system to achieve attack resistance.

Aslan and Atasen[199] evaluated the possibility of world-wide COVID-19 information sharing among countries with Decentralized Applications (DApps) on blockchain system, but the idea is initial and of high level, no implementation is provided. Abid et al.[200] proposed NovidChain which is a blockchain system to replace the central server that stores test/vaccine certificates of users. NovidChain works as a bridge for certificate issuer, holder, and verifier, and is evaluated to be secure, scalable, and low-cost extensively in the paper. However, NovidChain is set to be private and managed by governments or healthcare institutions, which brings centralization and privacy concerns to NovidChain.

#### 6.2.2 Blockchain-enabled contact tracing

Contact tracing as one of the most effective ways to defeat pandemic has been developed in many countries[201]. Contact tracing requires people to share their private contact history, sometimes even including sensitive information such as GPS coordinates or medical history[202, 203]. Most initial attempts of blockchain-powered contact tracing approaches are of high level and treat blockchain naively as external storage or with no simulation provided to illustrate the effectiveness, such as BeepTrace[204], Arifeen et al.[205], and Choudhury et al.[206] Hasan et al.[207] proposed to use blockchain to record participants' GPS coordinates and trigger proof of location to conduct contact tracing and risk alert. In their proposed system, external oracles are adopted to conduct contact tracing algorithm, and blockchain works as a bridge from external oracles to involved parties, including testing center and patients. Torky et al.[208] also used blockchain to securely bridge contact tracing-concerned parties and proposed to use specific code patterns to encode peoples' locations, so that only people who have been to the same place can be identified as contact cases while protecting privacy. However, this method is not able to reflect accurate contact history but only possibilities of contacting. Peng et al.[209] focused on contact data verification to ensure data integrity and proposed a Privacy-Preserving Blockchain-based Contact Tracing system ($P^2B$).

Most of above contact tracing approaches assume people are willing to join the contact tracing system and share their contact history. However, in practice, people may be reluctant to use such system or act reluctantly after joining the contact tracing system, which will reduce the effectiveness of contact tracing. Incentive mechanisms play important roles in blockchain systems that motivate people or participants to perform contact tracing function honestly and actively. Naren et al.[210] analyzed importance of incentive mechanisms, but no specific method is proposed to solve the mechanism. Lv et al.[211] considered large-scale contact tracing with the help of IoT and proposed ByChain where an artificial potential field based incentive allocation mechanism is proposed to motivate IoT witnesses to maximize monitoring coverage.

Alansari et al.[212] extended contact tracing with two other subsystems to perform public places access control and safe-places recommendation, respectively. All three subsystems are incorporated with consortium blockchain to manage the data access and storage.

#### 6.2.3 Blockchain for COVID-19 vaccine control

Blockchain technology also helps COVID-19 vaccine control and management[202]. Considering fragile biological substances, which should be taken special care during transmission and distribution, Rotbi et al.[213] discussed a concept of blockchain-enabled automatic vaccine lots management to promote the transparency and immutability of management data. Musamih et al.[214] implemented a prototype of blockchain system on Ethereum to help track the vaccine during delivery from raw material supplier to the beneficiary. The blockchain is responsible for storing logs and events generated by smart contracts and recording delivery events of the COVID-19 vaccine. The management of vaccine is a special case of supply chain management, we will investigate more blockchain works on supply chain in Section 6.4.

### 6.3 Social network

Social network has became an indispensable part of our daily lives. Users of social media, such as Facebook, Twitter, and Weibo set up their profiles and make posts. The huge amount of data generated by users are managed by the social media providers which are sometimes not reliable. For instance, Facebook has several data leakage incidents recent years. Users have no control of their data, even some data are of high privacy concern. To solve the single-point failure problem, ensure data security, and preserve necessary privacy in public social network, blockchain

technology is discovered to be one possible solution[215, 216].

#### 6.3.1 Decentralized social networks

Jiang and Zhang[217] designed a blockchain-based decentralized social network, where blockchain serves as a replacement of centralized server to allow user registration, user posting, adding friends or, commenting with the help of smart contracts. In the evaluation, the authors showed each post users made will cost around 1.137 US dollar, which makes the system not a budget solution. The data stored on blockchain are not modifiable, therefore how users update their registration information and posts is a remaining problem. Zhang et al.[218] proposed another blockchain-based social network, namely BPP. They also proposed a privacy preserving searching algorithm in BPP. However, BPP is not fully decentralized, and blockchain works as external storage system to assist social network providers.

Fully decentralized storage also brings extraordinary cost for maintaining the decentralized social network. Chen et al.[219] proposed DEPLEST, a blockchain-based distributed database system. They focused on solving the storage cost if all users of social network store whole copies of database in blockchain-based social network. They proposed each user only needs to store a part whole data, and the size of storage on each device is fixed. To save the storage cost of synchronized blockchain, only sensitive data will be encrypted and secured through blockchain, non-sensitive data will be stored in traditional external database. Proof-of-Communication is also proposed to save the time for appending a new block. Nguyen et al.[220] proposed SoChainDB, which is a general database framework to facilitate blockchain-based social networks for collecting data generated in the network. SoChainDB provides an efficient pipeline to crawl and formalize distributed data storage in blockchain-based social network, and fills in the gap between conventional social network engineers and blockchain developers.

Most current designs or implementations of blockchain in social network systems are still at very early stage that blockchain only takes a minor part of the system and has many deficiencies such as scalabity and throughput problems. With the development of blockchain system, a handful of fully decentralized social networks are able to come to surface, such as Steemit‡ and FORESTING※ which are both implemented with Steem Blockchain[221]. The diagram of social network without a central server requires all peers to maintain the whole network, which gives much more rights to peers than centralized diagram. With no proper user behavior control mechanism, malicious users might make the blockchain-enabled social network more vulnerable than traditional ones.

#### 6.3.2 Blockchain for authentication control in social network

Gu et al.[222] studied privacy concern during resource sharing, such as movies, songs, or pictures within social network communities. Access control of the resource is achieved by blockchain, and peers within the communities are motivated by a smart contract to help disseminate the resources. Rahman et al.[223] also studied access control problem in social network with blockchain. They designed four smart contracts, namely, Access Control Contract for controlling the access to the resources in the network, Reputation Contract for calculating reputation score of users, Inspector Contract for monitoring user behavior, and Registrar Contract for verifying user identities. Zhang et al.[224] extended the resource sharing within one community to the sharing across multiple social networks. Their proposed framework achieves consistent consensus on photo dissemination control across independent and disparate social network platforms.

Yan et al.[225] proposed Social-Chain to solve the trust issue in Pervasive Social Networking (PSN) which is usually lacking a centralized party to perform information collection, social data aggregation, and trust evaluation. Social-Chain is able to efficiently store the trust evaluation of users into blockchain with the proposed Proof-of-Trust. Guo et al.[226] studied user reputation evaluation task in social network where existing methods are facing the issue caused by fake comments posted by adversaries. They proposed a consortium blockchain based method that users are the peers in the blockchain and a behavior game model mechanism is developed to motivate peers to work honestly. Ochoa et al.[227] proposed FakeChain to detect fake news in social network. They assumed each node in social network is also a node in blockchain,

‡ https://steemit.com

※ https://foresting.io/

and when each node publishes some news, the news will be stored in blockchain. Then, with the tractability of blockchain, the source of fake news can be easily detected.

#### 6.3.3 Blockchain for social network in IoV

Vehicular Social Network (VSN) is an emerging concept that enables resource sharing among vehicles[228, 229]. Zhang et al.[228] used blockchain to realize access control among vehicular social network. Shen et al.[229] developed a location-based blockchain to enable transactions between certificate authorities. The vehicular social network is a special term for IoV where the functions are limited to information sharing and most blockchain use cases are similar to Section 4.2.

### 6.4 Supply chain

Supply chain management is a vital component of industry. Good traceability of products allows manufactures and retailers to identify the sources of parts and raw materials, as well as avoid business fraud with transparent product information. With the increasing complexity of global supply chain networks, traditional supply chain management approaches are facing challenges to match the requirements of efficiency, accessibility, transparency, and security[230, 231].

Blockchain can be a revolutionary technique in supply chain to provide effective product tracing, transparent information sharing, and reliable attack resistance. Many companies have announced blockchain projects in their supply chain for better tractability, such as Walmart*, Toyota, and Alibaba[232]. Queiroz et al.[233] systematically analyzed the barrier for the adoption of blockchain in supply chain with a real-world empirical study in the Brazilian Operations and Supply Chain Management (OSCM) context. Through questionnaire, they found out that the performance expectancy may also constitute an impediment to adoption of blockchain. In Ref. [234], blockchain technology is able to elevate the profit of supply chain, though the profit may differ when different parties lead the construction of the blockchain system.

#### 6.4.1 Enhance the traceability of supply chain with blockchain

One of the most fundamental properties that supply chains ought to have is traceability. Abundant blockchain-enabled supply chains have been investigated and designed for many specific use cases to improve traceability, including fresh produces and foods[234−236], animal products[237], agriculture[238], and healthcare[214, 239]. Yakubu et al.[240] proposed RiceChain to provide traceable rice supply chain, achieving at most 25% lower tracing latency than existing work. Caro et al.[241] proposed AgriBlockIoT and implemented with Ethereum and Hyperledger Sawtooth, which is a fully-decentralized traceable supply chain for agriculture and food with blockchain and IoT. In AgriBlockIoT, IoT devices deployed in the supply chain processes are working nodes of blockchain, and the whole blockchain is maintained on cloud. To evaluate the traceability level of blockchain-enabled supply chain, Dasaklis et al.[242] defined the granularity levels of traceability. They designed a smart contract to collect necessary information for conducting traceability classification based on the existing traceability granularity standard¤.

Kouhizadeh et al.[243] and Saberi et al.[244] analyzed that blockchain could help verify audit and certificate sustainability in supply chain which is emphasized of great importance recent years, yet hardly can be achieved in most supply chain systems. The key idea of sustainability of supply chain is to save energy and build environmental-friendly products in sustainable manner. However, in addition to the benefits brought by blockchain for supporting sustainability, blockchain itself may introduce extra overhead and energy consumption for maintaining functionality of smart contracts and miners. Some other problems such as scalability, communication deficiency, and unprecedented security issues may also be presented[245].

#### 6.4.2 Blockchain for trust management in supply chain

The interactions between multiple partners in the supply chain rely on the trust among them. Therefore, trust management plays the crucial role to build and maintain a supply chain. Except that the above blockchain-based tamper-proof and audible supply chain is proposed, Malik et al.[246] considered the trust evaluation problem for parties in the supply chain. In the proposed TrustChain, a reputation evaluation algorithm is developed for calculating the ratings of

* https://one.walmart.com/content/globaltechindia/en_in/Tech-insights/blog/Blockchain-in-the-food-supply-chain.html

¤ https://www.gs1.org/docs/tl/T_L_Keys_Implementation_Guideline.pdf

product sellers in the blockchain-based supply chain. Al-Rakhami and AI-Mashari[247] brought both blockchain and IoT into trust management in supply chain. In their work, IoT devices work as data collector and relayor to transmit cryptographically edited essential data to blockchain. However, incorporating IoT devices may introduce potential security threats into supply chain that unauthorized or uncontrolled IoT devices from malicious parties may access and tamper the sensitive data. Song et al.[248] proposed a robust blockchain based IoT enabled supply chain management framework, where a registration module is designed for enforcing registration policies on all participants and inspection module is designed for monitoring, analyzing, and judging misbehaviour of participants.

Circular supply chain extends the one-way supply from manufacture to products with three extra process, namely recycle, remanufacture, and redistribute. Different from the simple forward manner in common supply chains, circular supply chains usually have more complicated product information flow among multiple parties that may be back and forth when redistributing and recycling. Figure 9 illustrates the information flow and material flow in regular supply chain and circular supply chain. Centobelli et al.[249] designed a Triple Retry blockchain framework with multiple smart contracts for executing different processes.

Raj et al.[250] proposed to use blockchain to solve the payment delay issue in supply chain especially when the participants locate at different places of the globe. With smart contracts enforced on participants as well as the authenticity and tamper-proof nature, blockchain is able to achieve trustable information and payment confirming which alleviates the transaction delays in supply chain.

### 6.4.3 Cost of blockchain in supply chain

Despite abundant blockchain-based supply chains are designed and implemented, the profiting outcome with the adoption of blockchain technology is still a question to be answered. Blockchain technology usually can not work independently, but also other related technologies are required to acquire and preprocess necessary data for blockchain system[251]. Therefore, a company may face additional cost for investing in extra technology devices, such as RFID, code reader, and sensors[252].

Zhou et al.[253] and Sun et al.[254] conducted detailed analysis and proof on the cost of blockchain in two-echelon supply chain where only one supplier and one retailer exist. Zhou et al.[253] pointed out that, blockchain-enabled supply chains are not necessarily superior than non-blockchain ones, which is closely related to the reliability of information and the transparency cost of products. Based on full equilibrium results through the Stackelberg game between the supplier and the retailer designed in the paper, the authors concluded that the retailer can tolerate higher blockchain adopting cost than supplier in most cases especially when the product

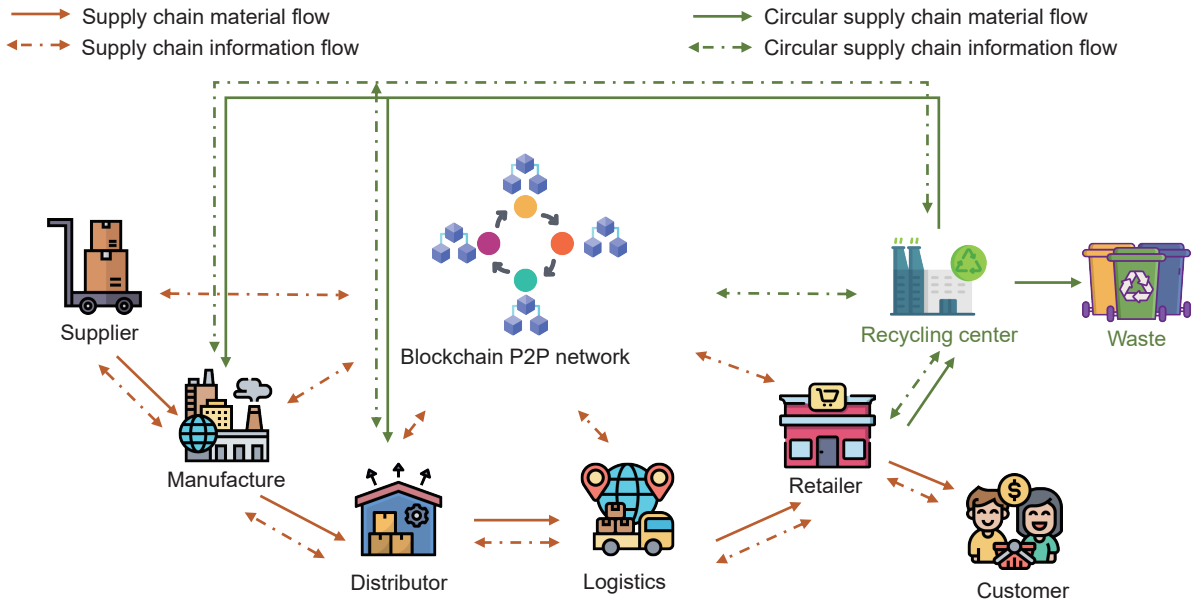


**Fig. 9 Blockchain-enabled (circular) supply chain.**

cost is high, while supplier can tolerate a higher adopting cost only when both the product cost and consumers' willing to pay are low. Sun et al.[254] introduced a consumer suspicion coefficient to denote how much consumers trust blockchain from retailer. They produced equilibrium result for retailer pricing and profit under three different setting: (1) no blockchain and no information sharing in supply chain, (2) no blockchain but use traditional method to share information, and (3) use blockchain to share information. They found that when the consumer suspicion coefficient increases, consumers will have limited faith in the authenticity of the product, which will negatively affect the retailer's optimal decision and profit.

Researchers may result in opposite conclusions when modeling and scenario settings differ. Zhou et al.[253] thought both supplier and retailer will benefit from blockchain technology when the adopting cost is low enough, while Sun et al.[254] concluded blockchain technology can always improve the supply chain profit no matter what the status of market demand.

## 7 Discussion

In above extensive literature review, we have investigated and discussed recent advances of blockchain and its applications as well as provided some suggestions for some specific research topics. In this section, we make further conclusions and more suggestions on future academic or industry work on blockchain.

Blockchain systems are constructed upon peer-to-peer networks, where smart contracts and consensus mechanisms are enforced on every participant to achieve transparency. Some consensus mechanisms, especially Proof of Work and its variants, will consume notable computation resources. Though many other consensus mechanisms are proposed, such as Proof of Stake or PBFT which significantly reduces computation cost, they also bring extra communication resource consumption. The communication or communication consumption is not affordable to many lightweight applications. On the other hand, applications with resource-limited devices are often not able to consistently perform stable communications or computation tasks. For example, in an IoT network, the out-door smart meters or smart sensors not only have limited computation resources, but also may face challenges to collect data or lose network connection due to bad weather, which will interrupt effective communications. Though many works have succeeded to simultaneously optimize blockchain consensus mechanism and communication schema, more research is still desired to advance the current solutions and make blockchain effective in above use cases.

Another obstacle to the adoption of blockchain technology is the scalability issue. In other words, the transaction throughput, the transaction processing latency, and the storage cost of blockchain can not all satisfy the demands of many use cases. We have mentioned many remarkable works above that improve the scalability. Efficient consensus mechanisms, such as PoS, DPoS, and community-wise consensus mechanisms are developed to package transactions into blocks in much shorter time than PoW. In order to mitigate the total storage consumption meanwhile to keep the robustness and tamper-proof ability, literature proposes blockchain sharding methods and storing actual data at external databases while only keeping the data index on blockchain. However, it is hard to achieve the perfect balance among three key properties: decentralization, security, and scalability[14]. Most above-mentioned works are able to optimize one or two of them under given particular application scenarios, and only a handful of works are trying to optimize all three properties at the same time[116], which are still initial attempts under many constraints, for example, only limited number of consensus mechanisms are considered and the block size is assumed to be only discrete numbers. New consensus mechanisms are highly demanded by optimizing all three properties under much more general settings and use cases.

The industry is no doubt a critical role in the adoption of blockchain technology from theory to practice. The main concern of companies to adopt blockchain in IoT services, healthcare systems, or supply chain systems is if blockchain will bring more profit than the cost to build it. The cost of blockchain technology is seldom analyzed in existing literature. We have mentioned several works that theoretically analyze the potential benefits and cost of blockchain in supply chain[234, 253, 254]. Further extensive research can be done in many other applications such as IoT, edge computing, and healthcare. In addition, blockchain simulation tools are highly desired for helping evaluate

the performance of blockchain systems, which provides intuitive results for industry to understand the performance and cost of blockchain systems.

Apparently, lowering the cost of blockchain will promote the adoption of blockchain in industry. The cost to build a blockchain generally comes from the development of blockchain client for each working node, the computation resource to perform consensus mechanism, the storage resource to store the blocks, and the cost of incentive mechanism to reward working nodes if necessary. The cost for developing blockchain client is mostly decided by software engineering market price. Therefore, better consensus mechanisms and corresponding incentive mechanisms take great weights in reducing the cost for blockchain industry.

Blockchain is a third-party free, non-trust built, and distributed data management approach. The adoption of blockchain technology brings not only benefits, but also potential risks and security weakness due to anonymity. Though most popular consensus mechanisms are proved to resist dishonest users when the ratio is under 51% or 1/3, the resistance to cyber-security attacks such as registration attack, data leakage, and encryption break-through is still a question. Different from the most famous successful blockchain system such as Bitcoin and Ethereum which run on high-end computers, the blockchain applications in IoT, edge computing, healthcare, and supply chain usually involve tremendous edge devices, such as mobile smart phones, IoT smart devices, or network access points, which can be easily compromised. Future academy and industry may work together to study those external cyber-security attacks in blockchain systems.

In many existing blockchain-enabled applications, we found that blockchain serves as an external distributed storage approach to simply replace the traditional storage instead of being specially designed to be integrated into application logistics. In this architecture, blockchain assists computation server by providing authentication control, data indexing, system logging without defining specific consensus mechanisms, and incentive mechanisms. In other words, the participants or peers in the blockchain can not actively compute and generate data, while only passively take the data given by the computation server. Some works take on-chain/off-chain architecture for their applications as illustrated in Fig. 10, that uses blockchain for making important consensus and storing important system logs or transaction, while still keeping the logistics and massive data on off-chain devices. Though this architecture is good for alleviating consumption of blockchain system in term of computation and storage resources, the blockchain does not directly participate in system logistics. We believe the blockchain-enabled applications can put more functions on blockchain through smart contracts to decentralize the computation power and take full advantages of blockchain technology.

It is also worth mentioning that the advantages of blockchain are not necessarily the benefits for applications sometimes. For example, blockchain is tamper-proof, that everything stored on blockchain can never be modified or deleted in anyway, otherwise the chain rule will be broken due to the uniqueness of block hash. For the application of social network, it is common that people can leave the social network and

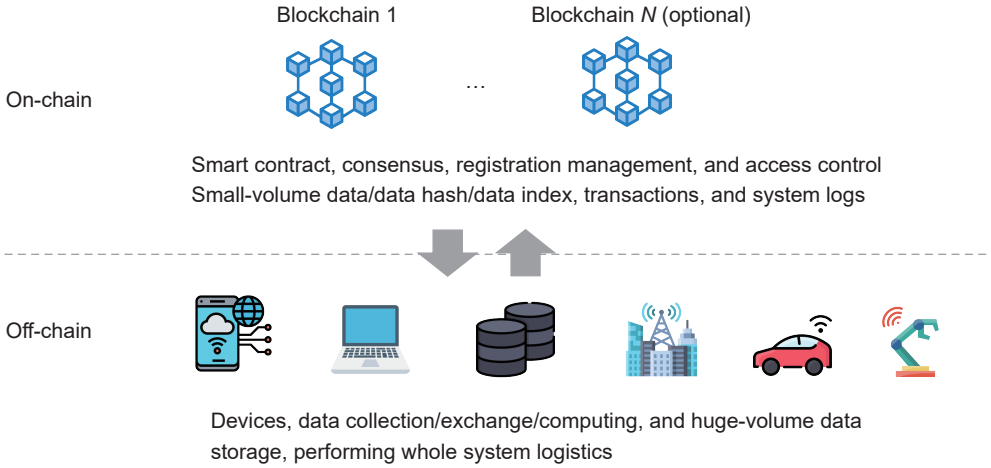


**Fig. 10 On-chain/off-chain architecture of blockchain applications.**

need to erase all the social records. However, blockchain-enabled social networks are hard to achieve this as long as there is any data of users stored on blockchain. Another example is that blockchain is decentralized that ideally requires every participants to store the full copy of blockchain. However, in real world, many use cases mentioned above can not satisfy the ideal situation that the storage cost will soon become unaffordable if the blockchain stores all data. In addition, in some use cases, such as healthcare, it is not always secure to allow everyone to hold full copy of data, since some sensitive information of patients may not be supposed to be accessible to some particular parties. We suggest future work may develop variants of current popular blockchain systems to meet the demands of particular use cases.

## 8 Conclusion

In this paper, we created an overview picture of blockchain ecosystem by reviewing the recent advances of blockchain technology as well as the most active blockchain applications connected with each other. With the steep expanding of the whole blockchain ecosystem, it is of great meaning to review the development in the most noticeable parts in the ecosystem. We first reviewed the recent studies on general blockchain technology, then the blockchain-enabled applications, including IoT, IoV, edge computing, federated learning, healthcare, COVID-19, social network, and supply chain. With the extensive review, we suggested several future developments of blockchain ecosystem, including developing more solutions to the dilemma to achieve balance among scalability, security, dencentrality, and cost, the external security risks outside blockchain from cyber-attack in industry, the ignorance of blockchain smart contracts, and the unexpected disadvantages caused by blockchain inevitable properties. This paper is formulated towards weaving the core part of current blockchain ecosystem from academic research to frontier industry applications. Therefore, we expect this survey to be helpful for future researchers developing more and better blockchain-enabled applications.

## Acknowledgment

This work was supported in part by the US National Science Foundation (NSF) (No. 1822985).

## References

[1] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, *Decentralized Business Review*, p. 21260, 2008.

[2] G. Wood, Ethereum: A secure decentralised generalized transaction ledger, *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014.

[3] S. King and S. Nadal, Ppcoin: Peer-to-peer crypto-currency with proof-of-stake, https://peercoin.net/assets/paper/peercoin-paper.pdf, 2012.

[4] F. Schär, Decentralized finance: On blockchain- and smart contract-based financial markets, *Federal Reserve Bank of St. Louis Review*, vol. 103, no. 2, pp. 153–174, 2021.

[5] L. D. Xu, Y. Lu, and L. Li, Embedding blockchain technology into IoT for security: A survey, *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10452–10473, 2021.

[6] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, A survey on the adoption of blockchain in IoT: Challenges and solutions, *Blockchain: Research and Applications*, vol. 2, no. 2, p. 100006, 2021.

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

[8] R. Belchior, M. Correia, and A. Vasconcelos, Justicechain: Using blockchain to protect justice logs, in *Proc. Confederated International Conferences: CoopIS, ODBASE, C&TC 2019*, Rhodes, Greece, 2019, pp. 318–325.

[9] R. Belchior, A. Vasconcelos, and M. Correia, Towards secure, decentralized, and automatic audits with blockchain, presented at 28th European Conference on Information Systems, Marrakech, Morocco, 2020.

[10] H. M. Hussien, S. M. Yasin, N. I. Udzir, A. A. Zaidan, and B. B. Zaidan, A systematic review for enabling of develop a blockchain technology in healthcare application: Taxonomy, substantially analysis, motivations, challenges, recommendations and future direction, *J. Medical Syst.*, vol. 43, p. 320, 2019.

[11] S. Jabbar, H. Lloyd, M. Hammoudeh, B. Adebisi, and U. Raza, Blockchain-enabled supply chain: Analysis, challenges, and future directions, *Multim. Syst.*, vol. 27, pp. 787–806, 2021.

[12] S. Wan, M. Li, G. Liu, and C. Wang, Recent advances in consensus protocols for blockchain: A survey, *Wirel. Networks*, vol. 26, pp. 5579–5593, 2020.

[13] A. Singh, G. Kumar, R. Saha, M. Conti, M. Alazab, and R. Thomas, A survey and taxonomy of consensus protocols for blockchains, *J. Syst. Archit.*, vol. 127, p. 102503, 2022.

[14] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, Solutions to scalability of blockchain: A survey, *IEEE Access*, vol. 8, pp. 16440–16455, 2020.

[15] R. Zhang, R. Xue, and L. Liu, Security and privacy on blockchain, *ACM Comput. Surv.*, vol. 52, no. 3, pp. 1–34, 2019.

[16] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar,

A survey on privacy protection in blockchain system, *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, 2019.

[17] H. T. M. Gamage, H. D. Weerasinghe, and N. G. J. Dias, A survey on blockchain technology concepts, applications, and issues, *SN Comput. Sci.*, vol. 1, p. 114, 2020.

[18] R. Huo, S. Zeng, Z. Wang, J. Shang, W. Chen, T. Huang, S. Wang, F. R. Yu, and Y. Liu, A comprehensive survey on blockchain in industrial internet of things: Motivations, research progresses, and future challenges, *IEEE Commun. Surv. Tutorials*, vol. 24, no. 1, pp. 88–122, 2022.

[19] C. Wang, X. Cheng, J. Li, Y. He, and K. Xiao, A survey: Applications of blockchain in the internet of vehicles, *EURASIP J. Wirel. Commun. Netw.*, vol. 2021, p. 77, 2021.

[20] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, C. Yuen, S. Sun, K. Lam, and L. H. Koh, Blockchain for the internet of vehicles towards intelligent transportation systems: A survey, *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4157–4185, 2021.

[21] T. Alladi, V. Chamola, N. Sahu, V. Venkatesh, A. Goyal, and M. Guizani, A comprehensive survey on the applications of blockchain for securing vehicular networks, *IEEE Commun. Surv. Tutorials*, vol. 24, no. 2, pp. 1212–1239, 2022.

[22] J. Zou, D. He, S. Zeadally, N. Kumar, H. Wang, and K. R. Choo, Integrated blockchain and cloud computing systems: A systematic survey, solutions, and challenges, *ACM Comput. Surv.*, vol. 54, no. 8, pp. 1–36, 2022.

[23] Z. Liao, X. Pang, J. Zhang, B. Xiong, and J. Wang, Blockchain on security and forensics management in edge computing for IoT: A comprehensive survey, *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 2, pp. 1159–1175, 2022.

[24] D. Li, D. Han, T. Weng, Z. Zheng, H. Li, H. Liu, A. Castiglione, and K. Li, Blockchain for federated learning toward secure distributed machine learning systems: A systemic survey, *Soft Comput.*, vol. 26, pp. 4423–4440, 2022.

[25] D. C. Nguyen, M. Ding, Q. Pham, P. N. Pathirana, L. B. Le, A. Seneviratne, J. Li, D. Niyato, and H. V. Poor, Federated learning meets blockchain in edge computing: Opportunities and challenges, *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12806–12825, 2021.

[26] V. Sreerakhi, N. Balagopal, and A. Mohan, Transforming supply chain network and logistics using blockchain—A survey, *Int. J. Bus. Inf. Syst.*, vol. 39, no. 2, pp. 193–218, 2022.

[27] M. S. Rahman, M. A. Islam, M. A. Uddin, and G. Stea, A survey of blockchain-based IoT ehealthcare: Applications, research issues, and challenges, *Internet of Things*, vol. 19, p. 100551, 2022.

[28] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K. R. Choo, Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey, *Comput. Secur.*, vol. 97, p. 101966, 2020.

[29] T. M. Hewa, M. Ylianttila, and M. Liyanage, Survey on blockchain based smart contracts: Applications, opportunities and challenges, *J. Netw. Comput. Appl.*, vol. 177, p. 102857, 2021.

[30] P. Sharma, R. Jindal, and D. B. Malaya, A review of blockchain-based applications and challenges, *Wirel. Pers. Commun.*, vol. 123, no. 2, pp. 1201–1243, 2022.

[31] A. G. Gad, D. T. Mosa, L. Abualigah, and A. A. Abohany, Emerging trends in blockchain technology and applications: A review and outlook, *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6719–6742, 2022.

[32] L. Lamport. Constructing digital signatures from a one-way function. Tech. rep. CSL-98, SRI International, Palo Alto, CA, USA, 1979.

[33] R. C. Merkle, A digital signature based on a conventional encryption function, in *Proc. Conference on the Theory and Application of Cryptographic Techniques*, Santa Barbara, CA, USA, 1987, pp. 369–378.

[34] D. D. F. Maesa, A. Marino, and L. Ricci, Uncovering the bitcoin blockchain: An analysis of the full users graph, in *Proc. 2016 IEEE International Conference on Data Science and Advanced Analytics*, Montreal, Canada, 2016, pp. 537–546.

[35] D. D. F. Maesa, A. Marino, and L. Ricci, The bow tie structure of the bitcoin users graph, *Appl. Netw. Sci.*, vol. 4, p. 56, 2019.

[36] Y. Chen and J. Liu, Distributed community detection over blockchain networks based on structural entropy, in *Proc. 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure*, Auckland, New Zealand, 2019, pp. 3–12.

[37] B. B. F. Pontiveros, M. Steichen, and R. State, Mint centrality: A centrality measure for the bitcoin transaction graph, in *Proc. 2019 IEEE International Conference on Blockchain and Cryptocurrency*, Seoul, Republic of Korea, 2019, pp. 159–162.

[38] Y. Li, U. Islambekov, C. G. Akcora, E. Smirnova, Y. R. Gel, and M. Kantarcioglu, Dissecting ethereum blockchain analytics: What we learn from topology and geometry of ethereum graph? in *Proc. 2020 SIAM Conference on Data Mining* (*SDM*), Cincinnati, OH, USA, 2020, pp. 523–531.

[39] R. Banno and K. Shudo, Simulating a blockchain network with simblock, in *Proc. 2019 IEEE International Conference on Blockchain and Cryptocurrency* (*ICBC*), Seoul, Republic of Korea, 2019, pp. 3–4.

[40] L. Liu, W. Tsai, M. Z. A. Bhuiyan, and D. Yang, Automatic blockchain whitepapers analysis via heterogeneous graph neural network, *J. Parallel Distributed Comput.*, vol. 145, pp. 1–12, 2020.

[41] C. Feng and J. Niu, Selfish mining in ethereum, in *Proc. 2019 IEEE 39th International Conference on Distributed Computing Systems* (*ICDCS*), Dallas, TX, USA, 2019, pp. 1306–1316.

[42] F. Ritz and A. Zugenmaier, The impact of uncle rewards on selfish mining in ethereum, in *Proc. 2018 IEEE European Symposium on Security and Privacy Workshops* (*EuroS&PW*), London, UK, 2018, pp. 50–57.

[43] H. Kang, X. Chang, R. Yang, J. V. Mišić, and V. B. Mišić, Understanding selfish mining in imperfect bitcoin and ethereum networks with extended forks, *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 3, pp. 3079–3091, 2021.

[44] W. Chen, X. Guo, Z. Chen, Z. Zheng, and Y. Lu, Phishing scam detection on ethereum: Towards financial security for blockchain ecosystem, in *Proc. 29th International Joint Conference on Artificial Intelligence* (*IJCAI*), Yokohama, Japan, 2020, pp. 4506–4512.

[45] C. Hou, M. Zhou, Y. Ji, P. Daian, F. Tramèr, G. Fanti, and A. Juels, SquirRL: Automating attack analysis on blockchain incentive mechanisms with deep reinforcement learning, presented at 28th Annual Network and Distributed System Security Symposium (NDSS), Virtual, 2021.

[46] A. Kiayias, A. Russell, B. David, and R. Oliynykov, Ouroboros: A provably secure proof-of-stake blockchain protocol, in *Proc. 37th Annual International Cryptology Conference*, Santa Barbara, CA, USA, 2017, pp. 357–388.

[47] D. Larimer, Delegated proof-of-stake (dpos), *Bitshare Whitepaper*, vol. 81, p. 85, 2014.

[48] F. Schuh and D. Larimer, Bitshares 2.0: General overview, http://docs.bitshares.org/downloads/bitshares-general.pdf, 2017.

[49] Y. Huang, H. Wang, L. Wu, G. Tyson, X. Luo, R. Zhang, X. Liu, G. Huang, and X. Jiang, Understanding (mis)behavior on the EOSIO blockchain, *Proc. ACM Meas. Anal. Comput. Syst.*, vol. 4, no. 2, pp. 1–28, 2020.

[50] B. Xu, D. Luthra, Z. Cole, and N. Blakely, EOS: An architectural, performance, and economic analysis, *Retrieved June*, vol. 11, p. 2019, 2018.

[51] B. Guidi, A. Michienzi, and L. Ricci, Steem blockchain: Mining the inner structure of the graph, *IEEE Access*, vol. 8, pp. 210251–210266, 2020.

[52] Y. Sun, B. Yan, Y. Yao, and J. Yu, Dt-dpos: A delegated proof of stake consensus algorithm with dynamic trust, *Procedia Computer Science*, vol. 187, pp. 371–376, 2021.

[53] J. Liu, M. Xie, S. Chen, C. Ma, and Q. Gong, An improved dpos consensus mechanism in blockchain based on PLTS for the smart autonomous multi-robot system, *Inf. Sci.*, vol. 575, pp. 528–541, 2021.

[54] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism, *IEEE Access*, vol. 7, pp. 118541–118555, 2019.

[55] X. Fan and Q. Chai, Roll-DPoS: A randomized delegated proof of stake scheme for scalable blockchain-based internet of things systems, in *Proc. 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, New York, NY, USA, 2018, pp. 482–484.

[56] Y. Luo, Y. Chen, Q. Chen, and Q. Liang, A new election algorithm for dpos consensus mechanism in blockchain, in *Proc. 2018 7th International Conference on Digital Home* (*ICDH*), Guilin, China, 2018, pp. 116–120.

[57] G. Xu, Y. Liu, and P. W. Khan, Improvement of the dpos consensus mechanism in blockchain based on vague sets, *IEEE Trans. Ind. Informatics*, vol. 16, no. 6, pp. 4252–4259, 2020.

[58] M. Castro and B. Liskov, Practical byzantine fault tolerance, in *Proc. Third Symposium on Operating Systems Design and Implementation*, New Orleans, LA, USA, 1999, pp. 173–186.

[59] Y. Li, L. Qiao, and Z. Lv, An optimized byzantine fault tolerance algorithm for consortium blockchain, *Peer-to-Peer Netw. Appl.*, vol. 14, no. 5, pp. 2826–2839, 2021.

[60] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, A scalable multi-layer PBFT consensus for blockchain, *IEEE Trans. Parallel Distributed Syst.*, vol. 32, no. 5, pp. 1146–1160, 2021.

[61] L. Luu, V. Narayanan, K. Baweja, C. Zheng, S. Gilbert, and P. Saxena, SCP: A computationally-scalable byzantine consensus protocol for blockchains, http://eprint.iacr.org/2015/1168, 2015.

[62] Z. Li, J. Huang, D. Gao, Y. Jiang, and L. Fan, ISCP: An improved blockchain consensus protocol, *Int. J. Netw. Secur.*, vol. 21, no. 3, pp. 359–367, 2019.

[63] M. J. Amiri, D. Agrawal, and A. E. Abbadi, Parblockchain: Leveraging transaction parallelism in permissioned blockchain systems, in *Proc. 2019 IEEE 39th International Conference on Distributed Computing Systems* (*ICDCS*), Dallas, TX, USA, 2019, pp. 1337–1347.

[64] F. Gai, B. Wang, W. Deng, and W. Peng, Proof of reputation: A reputation-based consensus protocol for peer-to-peer network, in *Proc. 23rd International Conference on Database Systems for Advanced Application*, Gold Coast, Australia, 2018, pp. 666–681.

[65] F. Ayaz, Z. Sheng, D. Tian, and Y. L. Guan, A proof-of-quality-factor (PoQF)-based blockchain and edge computing for vehicular message dissemination, *IEEE Access*, vol. 8, no. 4, pp. 2468–2482, 2021.

[66] H. Guo, W. Li, M. M. Nejad, and C. Shen, Proof-of-event recording system for autonomous vehicles: A blockchain-based solution, *IEEE Access*, vol. 8, pp. 182776–182786, 2020.

[67] L. Bahri and S. Girdzijauskas, Trust mends blockchains: Living up to expectations, in *Proc. 2019 IEEE 39th International Conference on Distributed Computing Systems* (*ICDCS*), Dallas, TX, USA, 2019, pp. 1358–1368.

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

[69] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, A secure sharding protocol for open blockchains, in *Proc. 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, 2016, pp. 17–30.

[70] R. Han, J. Yu, H. Lin, S. Chen, and P. J. Esteves-Veríssimo, On the security and performance of blockchain sharding, https://eprint.iacr.org/2021/1276, 2021.

[71] M. Zamani, M. Movahedi, and M. Raykova, Rapidchain: Scaling blockchain via full sharding, in *Proc. 2018 ACM SIGSAC Conference on Computer and Communications Security*, Toronto, Canada, 2018, pp. 931–948.

[72] Y. Xu and Y. Huang, An n/2 byzantine node tolerate blockchain sharding approach, in *Proc. 35th ACM*

*Symposium on Applied Computing*, Brno, Czech Republic, 2020, pp. 349–352.

[73] J. Zhang, Z. Hong, X. Qiu, Y. Zhan, S. Guo, and W. Chen, Skychain: A deep reinforcement learning-empowered dynamic blockchain sharding system, in *Proc. 49th International Conference on Parallel Processing*, Edmonton, Canada, 2020, pp. 1–11.

[74] E. Bandara, S. Shetty, A. Rahman, R. Mukkamala, and X. Liang, Moose: A scalable blockchain architecture for 5G enabled IoT with sharding and network slicing, in *Proc. 2022 IEEE Wireless Communications and Networking Conference* (*WCNC*), Austin, TX, USA, 2022, pp. 1194–1199.

[75] E. Madill, B. Nguyen, C. K. Leung, and S. Rouhani, ScaleSFL: A sharding solution for blockchain-based federated learning, in *Proc. 4th ACM International Symposium on Blockchain and Secure Critical Infrastructure*, Nagasaki, Japan, 2022, pp. 95–106.

[76] Y. Xu and Y. Huang, Segment blockchain: A size reduced storage mechanism for blockchain, *IEEE Access*, vol. 8, pp. 17434–17441, 2020.

[77] X. Qi, Z. Zhang, C. Jin, and A. Zhou, A reliable storage partition for permissioned blockchain, *IEEE Trans. Knowl. Data Eng.*, vol. 33, no. 1, pp. 14–27, 2021.

[78] X. Wang, X. Jiang, Y. Liu, J. Wang, and Y. Sun, Data propagation for low latency blockchain systems, *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 12, pp. 3631–3644, 2022.

[79] C. Decker and R. Wattenhofer, Information propagation in the bitcoin network, in *Proc. 13th IEEE International Conference on Peer-to-Peer Computing*, Trento, Italy, 2013, pp. 1–10.

[80] K. Ayinala, B. Choi, and S. Song, Pichu: Accelerating block broadcasting in blockchain networks with pipelining and chunking, arXiv preprint arXiv: 2101.08212, 2021.

[81] D. Ding, X. Jiang, J. Wang, H. Wang, X. Zhang, and Y. Sun, Txilm: Lossy block compression with salted short hashing, arXiv preprint arXiv: 1906.06500, 2019.

[82] B. Yu, X. Li, and H. Zhao, PoW-BC: A pow consensus protocol based on block compression, *KSII Transactions on Internet and Information Systems*, vol. 15, no. 4, pp. 1389–1408, 2021.

[83] P. Deutsch, DEFLATE compressed data format specification version 1.3, *RFC 1951*, doi: 10.17487/RFC1951.

[84] I. Stoica, R. T. Morris, D. R. Karger, M. F. Kaashoek, and H. Balakrishnan, Chord: A scalable peer-to-peer lookup service for internet applications, *ACM SIGCOMM Computer Communication Review*, vol. 31, no. 4, pp. 149–160, 2001.

[85] S. Ratnasamy, P. Francis, M. Handley, R. M. Karp, and S. Shenker, A scalable content-addressable network, *ACM SIGCOMM Computer Communication Review*, vol. 31, no. 4, pp. 161–172, 2001.

[86] B. Y. Zhao, L. Huang, J. Stribling, S. C. Rhea, A. D. Joseph, and J. D. Kubiatowicz, Tapestry: A resilient global-scale overlay for service deployment, *IEEE J. Sel. Areas Commun.*, vol. 22, no. 1, pp. 41–53, 2004.

[87] A. P. Ozisik, G. Andresen, B. N. Levine, D. Tapp, G. Bissias, and S. Katkuri, Graphene: Efficient interactive set reconciliation applied to blockchain propagation, in *Proc. ACM Special Interest Group on Data Communication*, Beijing, China, 2019, pp. 303–317.

[88] E. Rohrer and F. Tschorsch, Kadcast: A structured approach to broadcast in blockchain networks, in *Proc. 1st ACM Conference on Advances in Financial Technologies*, Zurich, Switzerland, 2019, pp. 199–213.

[89] P. Maymounkov and D. Mazières, Kademlia: A peer-to-peer information system based on the XOR metric, in *Proc. First International Workshop on Peer-to-Peer Systems*, Cambridge, MA, USA, 2002, pp. 53–65.

[90] Y. Mao, S. Deb, S. B. Venkatakrishnan, S. Kannan, and K. Srinivasan, Perigee: Efficient peer-to-peer network design for blockchains, in *Proc. 39th Symposium on Principles of Distributed Computing*, Virtual event, Italy, 2020, pp. 428–437.

[91] L. Eckey, S. Faust, and J. Loss, Efficient algorithms for broadcast and consensus based on proofs of work, http://eprint.iacr.org/2017/915, 2017.

[92] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, Algorand: Scaling byzantine agreements for cryptocurrencies, in *Proc. 26th Symposium on Operating Systems Principles*, Shanghai, China, 2017, pp. 51–68.

[93] V. K. Bagaria, S. Kannan, D. Tse, G. Fanti, and P. Viswanath, Prism: Deconstructing the blockchain to approach physical limits, in *Proc. 2019 ACM SIGSAC Conference on Computer and Communications Security*, London, UK, 2019, pp. 585–602.

[94] A. J. Al-Musharaf, S. M. Al-Alak, and H. M. Al-Mashhadi, Improving blockchain consensus mechanism via network clusters, in *Proc. 2021 1st Babylon International Conference on Information Technology and Science* (*BICITS*), Babil, Iraq, 2021, pp. 293–298.

[95] H. Tran-Dang, N. Krommenacker, P. Charpentier, and D. S. Kim, The internet of things for logistics: Perspectives, application review, and challenges, *IETE Technical Review*, vol. 39, no. 1, pp. 93–121, 2022.

[96] A. Alkhateeb, C. Catal, G. Kar, and A. Mishra, Hybrid blockchain platforms for the internet of things (IoT): A systematic literature review, *Sensors*, vol. 22, no. 4, p. 1304, 2022.

[97] O. Novo, Blockchain meets IoT: An architecture for scalable access management in IoT, *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, 2018.

[98] J. Marchang, G. Ibbotson, and P. Wheway, Will blockchain technology become a reality in sensor networks? in *Proc. 2019 Wireless Days,* Manchester, UK, 2019, pp. 1–4.

[99] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K. R. Choo, and A. Y. Zomaya, Blockchain for smart communities: Applications, challenges and opportunities, *J. Netw. Comput. Appl.*, vol. 144, pp. 13–48, 2019.

[100] J. Huang, L. Kong, G. Chen, L. Cheng, K. Wu, and X. Liu, B-IoT: Blockchain driven internet of things with credit-based consensus mechanism, in *Proc. 2019 IEEE 39th International Conference on Distributed Computing Systems* (*ICDCS*), Dallas, TX, USA, 2019, pp. 1348–1357.

[101] S. Biswas, K. Sharif, F. Li, S. Maharjan, S. P. Mohanty,

and Y. Wang, PoBT: A lightweight consensus algorithm for scalable IoT business blockchain, *IEEE Internet Things J.*, vol. 7, no. 3, pp. 2343–2355, 2020.
[102] E. K. Wang, Z. Liang, C. Chen, S. Kumari, and M. K. Khan, PoRX: A reputation incentive scheme for blockchain consensus of IIoT, *Future Gener. Comput. Syst.*, vol. 102, pp. 140–151, 2020.
[103] Z. Ai and W. Cui, A proof-of-transactions blockchain consensus protocol for large-scale IoT, *IEEE Internet Things J.*, vol. 9, no. 11, pp. 7931–7943, 2022.
[104] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, LSB: A lightweight scalable blockchain for IoT security and anonymity, *J. Parallel Distributed Comput.*, vol. 134, pp. 180–197, 2019.
[105] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, An incentive mechanism for building a secure blockchain-based internet of things, *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4650–4659, 2019.
[106] X. Ding, J. Guo, D. Li, and W. Wu, An incentive mechanism for building a secure blockchain-based internet of things, *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 1, pp. 477–487, 2021.
[107] S. Khan, W. Lee, and S. O. Hwang, Aechain: A lightweight blockchain for IoT applications, *IEEE Consumer Electron. Mag.*, vol. 11, no. 2, pp. 64–76, 2022.
[108] C. Zhang, L. Zhu, and C. Xu, BPAF: Blockchain-enabled reliable and privacy-preserving authentication for fog-based IoT devices, *IEEE Internet Things J.*, vol. 11, no. 2, pp. 88–96, 2022.
[109] J. Guo, X. Ding, and W. Wu, A blockchain-enabled ecosystem for distributed electricity trading in smart city, *IEEE Internet Things J.*, vol. 8, no. 3, pp. 2040–2050, 2021.
[110] J. Guo, X. Ding, and W. Wu, An architecture for distributed energies trading in byzantine-based blockchains, *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 2, pp. 1216–1230, 2022.
[111] T. Li, Y. Fang, Z. Jian, X. Xie, Y. Lu, and G. Wang, ATOM: Architectural support and optimization mechanism for smart contract fast update and execution in blockchain-based IoT, *IEEE Internet Things J.*, vol. 9, no. 11, pp. 7959–7971, 2022.
[112] J. Zhou, G. Feng, and Y. Wang, Optimal deployment mechanism of blockchain in resource-constrained IoT systems, *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8168–8177, 2022.
[113] L. Yang, M. Li, P. Si, R. Yang, E. Sun, and Y. Zhang, Energy-efficient resource allocation for blockchain-enabled industrial internet of things with deep reinforcement learning, *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2318–2329, 2021.
[114] Y. Wu, Z. Wang, Y. Ma, and V. C. M. Leung, Deep reinforcement learning for blockchain in industrial IoT: A survey, *Comput. Networks*, vol. 191, p. 108004, 2021.
[115] M. Li, F. R. Yu, P. Si, W. Wu, and Y. Zhang, Resource optimization for delay-tolerant data in blockchain-enabled IoT with edge computing: A deep reinforcement learning approach, *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9399–9412, 2020.
[116] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, Performance optimization for blockchain-enabled industrial internet of things (IIoT) systems: A deep reinforcement learning approach, *IEEE Trans. Ind. Informatics*, vol. 15, no. 6, pp. 3559–3570, 2019.
[117] J. Yun, Y. Goh, and J. Chung, DQN-based optimization framework for secure sharded blockchain systems, *IEEE Trans. Ind. Informatics*, vol. 8, no. 2, pp. 708–722, 2021.
[118] X. Ding, J. Guo, D. Li, and W. Wu, Pricing and budget allocation for IoT blockchain with edge computing, *IEEE Transactions on Cloud Computing*, doi: 10.1109/TCC.2022.3150766.
[119] A. K. V, A. K. Tyagi, and S. P. Kumar, Blockchain technology for securing internet of vehicle: Issues and challenges, in *Proc. 2022 International Conference on Computer Communication and Informatics* (*ICCCI*), Coimbatore, India, 2022, pp. 1–6.
[120] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory, *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2906–2920, 2019.
[121] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, Blockchain-based decentralized trust management in vehicular networks, *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, 2019.
[122] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, On security analysis of proof-of-elapsed-time (PoET), in *Proc. 19th International Symposium on Stabilization, Safety, and Security of Distributed Systems*, Boston, MA, USA, 2017, pp. 282–297.
[123] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles, *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 50–57, 2018.
[124] L. Zhang, M. Luo, J. Li, M. H. Au, K. R. Choo, T. Chen, and S. Tian, Blockchain based secure data sharing system for internet of vehicles: A position paper, *Veh. Commun.*, vol. 16, pp. 85–93, 2019.
[125] L. Luo, J. Feng, H. Yu, and G. Sun, Blockchain-enabled two-way auction mechanism for electricity trading in internet of electric vehicles, *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8105–8118, 2022.
[126] H. N. Abishu, A. M. Seid, Y. H. Yacob, T. Ayall, G. Sun, and G. Liu, Consensus mechanism for blockchain-enabled vehicle-to-vehicle energy trading in the internet of electric vehicles, *IEEE Trans. Veh. Technol.*, vol. 71, no. 1, pp. 946–960, 2022.
[127] S. Cho, N. Chen, and X. Hua, Developing a vehicle networking platform based on blockchain technology, in *Proc. Second International Conference on Blockchain*, San Diego, CA, USA, 2019, pp. 186–201.
[128] Q. Wang, T. Ji, Y. Guo, L. Yu, X. Chen, and P. Li, Trafficchain: A blockchain-based secure and privacy-preserving traffic map, *IEEE Access*, vol. 8, pp. 60598–60612, 2020.
[129] B. Yin, Y. Wu, T. Hu, J. Dong, and Z. Jiang, An efficient collaboration and incentive mechanism for internet of

vehicles (IoV) with secured information exchange based on blockchains, *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1582–1593, 2020.

[130] Y. Hui, Y. Huang, Z. Su, T. H. Luan, N. Cheng, X. Xiao, and G. Ding, BCC: Blockchain-based collaborative rowdsensing in autonomous vehicular networks, *IEEE Internet Things J.*, vol. 9, no. 6, pp. 4518–4532, 2022.

[131] S. Wang, S. Sun, X. Wang, Z. Ning, and J. J. P. C. Rodrigues, Secure crowdsensing in 5G internet of vehicles: When deep reinforcement learning meets blockchain, *IEEE Consumer Electron. Mag.*, vol. 10, no. 5, pp. 72–81, 2021.

[132] S. Kim and A. S. Ibrahim, Byzantine-fault-tolerant consensus via reinforcement learning for permissioned blockchain-empowered V2X network, *IEEE Transactions on Intelligent Vehicles*, doi: 10.1109/TIV.2022.3168575.

[133] M. Liu, Y. Teng, F. R. Yu, V. C. M. Leung, and M. Song, Deep reinforcement learning based performance optimization in blockchain-enabled internet of vehicle, in *Proc. 2019 IEEE International Conference on Communications* (*ICC*), Shanghai, China, 2019, pp. 1–6.

[134] S. Jiang, X. Li, and J. Wu, Hierarchical edge-cloud computing for mobile blockchain mining game, in *Proc.* 2019 *IEEE 39th International Conference on Distributed Computing Systems* (*ICDCS*), Dallas, TX, USA, 2019, pp. 1327–1336.

[135] G. Qu, N. Cui, H. Wu, R. Li, and Y. Ding, ChainFL: A simulation platform for joint federated learning and blockchain in edge/cloud computing environments, *IEEE Trans. Ind. Informatics*, vol. 18, no. 5, pp. 3572–3581, 2022.

[136] Z. Hu, H. Gao, T. Wang, D. Han, and Y. Lu, Joint optimization for mobile edge computing-enabled blockchain systems: A deep reinforcement learning approach, *Sensors*, vol. 22, no. 9, p. 3217, 2022.

[137] J. Feng, F. R. Yu, Q. Pei, X. Chu, J. Du, and L. Zhu, Cooperative computation offloading and resource allocation for blockchain-enabled mobile-edge computing: A deep reinforcement learning approach, *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6214–6228, 2020.

[138] Y. Zuo, S. Jin, S. Zhang, and Y. Zhang, Blockchain storage and computation offloading for cooperative mobile-edge computing, *IEEE Internet Things J.*, vol. 8, no. 11, pp. 9084–9098, 2021.

[139] G. Cheng, Y. Chen, S. Deng, H. Gao, and J. Yin, A blockchain-based mutual authentication scheme for collaborative edge computing, *IEEE Trans. Comput. Soc. Syst.*, vol. 9, no. 1, pp. 146–158, 2022.

[140] L. Xiao, Y. Ding, D. Jiang, J. Huang, D. Wang, J. Li, and H. V. Poor, A reinforcement learning and blockchain-based trust mechanism for edge networks, *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5460–5470, 2020.

[141] Y. Liu, X. Guan, Y. Peng, H. Chen, T. Ohtsuki, and Z. Han, Blockchain-based task offloading for edge computing on low-quality data via distributed learning in the internet of energy, *IEEE J. Sel. Areas Commun.*, vol. 40, no. 2, pp. 657–676, 2022.

[142] G. Baranwal and D. Kumar, PoSP: A novel proof of service placement in blockchain-based edge computing, in *Proc. 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events* (*PerCom Workshops*), Pisa, Italy, 2022, pp. 18–21.

[143] S. R. Maskey, S. Badsha, S. Sengupta, and I. Khalil, Reputation-based miner node selection in blockchain-based vehicular edge computing, *IEEE Consumer Electron. Mag.*, vol. 10, no. 5, pp. 14–22, 2021.

[144] E. Balistri, F. Casellato, S. Collura, C. Giannelli, G. Riberto, and C. Stefanelli, Design guidelines and a prototype implementation for cyber-resiliency in IT/OT scenarios based on blockchain and edge computing, *IEEE Internet Things J.*, vol. 9, no. 7, pp. 4816–4832, 2022.

[145] C. Li, S. Liang, J. Zhang, Q. Wang, and Y. Luo, Blockchain-based data trading in edge-cloud computing environment, *Inf. Process. Manag.*, vol. 59, no. 1, p. 102786, 2022.

[146] L. Yuan, Q. He, F. Chen, J. Zhang, L. Qi, X. Xu, Y. Xiang, and Y. Yang, CSEdge: Enabling collaborative edge storage for multi-access edge computing based on blockchain, *IEEE Trans. Parallel Distributed Syst.*, vol. 33, no. 8, pp. 1873–1887, 2022.

[147] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, Federated learning: Strategies for improving communication efficiency, arXiv preprint arXiv: 1610.05492, 2016.

[148] A. Goel, A. Agarwal, M. Vatsa, R. Singh, and N. Ratha, Deepring: Protecting deep neural network with blockchain, in *Proc. 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops* (*CVPRW*), Long Beach, CA, USA, 2019, pp. 2821–2828.

[149] Y. Fu, F. R. Yu, C. Li, T. H. Luan, and Y. Zhang, Vehicular blockchain-based collective learning for connected and autonomous vehicles, *IEEE Wirel. Commun.*, vol. 27, no. 2, pp. 197–203, 2020.

[150] J. Sun, Y. Wu, S. Wang, Y. Fu, and X. Chang, Permissioned blockchain frame for secure federated learning, *IEEE Commun. Lett.*, vol. 26, no. 1, pp. 13–17, 2022.

[151] P. Ramanan and K. Nakayama, BAFFLE: Blockchain based aggregator free federated learning, in *Proc. 2020 IEEE International Conference on Blockchain*, Rhodes, Greece, 2020, pp. 72–81.

[152] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, Blockchain and federated learning for privacy-preserved data sharing in industrial IoT, *IEEE Trans. Ind. Informatics*, vol. 16, no. 6, pp. 4177–4186, 2020.

[153] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, Communication-efficient federated learning and permissioned blockchain for digital twin edge networks, *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2276–2288, 2021.

[154] Z. Peng, J. Xu, X. Chu, S. Gao, Y. Yao, R. Gu, and Y. Tang, VFChain: Enabling verifiable and auditable federated learning via blockchain systems, *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 1, pp. 173–186, 2022.

[155] Y. Li, C. Chen, N. Liu, H. Huang, Z. Zheng, and Q. Yan,

A blockchain-based decentralized federated learning framework with committee consensus, *IEEE Netw.*, vol. 35, no. 1, pp. 234–241, 2021.
[156] X. Qu, S. Wang, Q. Hu, and X. Cheng, Proof of federated learning: A novel energy-recycling consensus algorithm, *IEEE Trans. Parallel Distributed Syst.*, vol. 32, no. 8, pp. 2074–2085, 2021.
[157] T. Rückel, J. Sedlmeir, and P. Hofmann, Fairness, integrity, and privacy in a scalable blockchain-based federated learning system, *Comput. Networks*, vol. 202, p. 108621, 2022.
[158] L. Gao, L. Li, Y. Chen, C. Xu, and M. Xu, FGFL: A blockchain-based fair incentive governor for federated learning, *J. Parallel Distributed Comput.*, vol. 163, pp. 283–299, 2022.
[159] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles, *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4298–4311, 2020.
[160] L. Feng, Y. Zhao, S. Guo, X. Qiu, W. Li, and P. Yu, BAFL: A blockchain-based asynchronous federated learning framework, *IEEE Trans. Computers*, vol. 71, no. 5, pp. 1092–1103, 2022.
[161] R. Wang and W. Tsai, Asynchronous federated learning system based on permissioned blockchains, *Sensors*, vol. 22, no. 4, p. 1672, 2022.
[162] B. Jia, X. Zhang, J. Liu, Y. Zhang, K. Huang, and Y. Liang, Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT, *IEEE Trans. Ind. Informatics*, vol. 18, no. 6, pp. 4049–4058, 2022.
[163] Y. Zhao, J. Zhao, L. Jiang, R. Tan, D. Niyato, Z. Li, L. Lyu, and Y. Liu, Privacy-preserving blockchain-based federated learning for IoT devices, *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1817–1829, 2021.
[164] S. Otoum, I. A. Ridhawi, and H. T. Mouftah, Securing critical IoT infrastructures with blockchain-supported federated learning, *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2592–2601, 2022.
[165] L. Feng, Z. Yang, S. Guo, X. Qiu, W. Li, and P. Yu, Two-layered blockchain architecture for federated learning over the mobile edge network, *IEEE Netw.*, vol. 36, no. 1, pp. 45–51, 2022.
[166] F. Ayaz, Z. Sheng, D. Tian, and Y. L. Guan, A blockchain based federated learning for message dissemination in vehicular networks, *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 1927–1940, 2022.
[167] M. Mettler, Blockchain technology in healthcare: The revolution starts here, in *Proc. 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services*, Munich, Germany, 2016, pp. 1–3.
[168] T. McGhin, K. -K. R. Choo, C. Z. Liu, and D. He, Blockchain in healthcare applications: Research challenges and opportunities, *J. Netw. Comput. Appl.*, vol. 135, pp. 62–75, 2019.
[169] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, Blockchain for healthcare data management: Opportunities, challenges, and future recommendations, *Neural Computing and Applications*, vol. 34, pp. 11475–11490, 2022.
[170] 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. Medical Syst.*, vol. 40, no. 10, p. 218, 2016.
[171] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, Blockchain technology in healthcare: A systematic review, *Healthcare*, vol. 7, no. 2, p. 56, 2019.
[172] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, Blockchain technology applications in healthcare: An overview, *International Journal of Intelligent Networks*, vol. 2, pp. 130–139, 2021.
[173] S. Rahmadika and K. -H. Rhee, Blockchain technology for providing an architecture model of decentralized personal health information, *International Journal of Engineering Business Management*, doi: 10.1177/1847979018790589.
[174] V. Jaiman and V. Urovi, A consent model for blockchain-based health data sharing platforms, *IEEE Access*, vol. 8, pp. 143734–143745, 2020.
[175] L. Liu, X. Li, M. H. Au, Z. Fan, and X. Meng, Metadata privacy preservation for blockchain-based healthcare systems, in *Proc. 27th International Conference on Database Systems for Advanced Applications*, Virtual event, 2022, pp. 404–412.
[176] M. Soni and D. K. Singh, Withdrawn: Blockchain-based security & privacy for biomedical and healthcare information exchange systems, *Materials Today: Proceedings*, doi: 10.1016/j.matpr.2021.02.094.
[177] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, Healthblock: A secure blockchain-based healthcare data management system, *Comput. Networks*, vol. 200, p. 108500, 2021.
[178] P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi, and N. Kumar, Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications, *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1242–1255, 2021.
[179] G. Zhang, Z. Yang, and W. Liu, Blockchain-based privacy preserving e-health system for healthcare data in cloud, *Comput. Networks*, vol. 203, p. 108586, 2022.
[180] U. Chelladurai and S. Pandian, A novel blockchain based electronic health record automation system for healthcare, *J. Ambient Intell. Humaniz. Comput.*, vol. 13, no. 1, pp. 693–703, 2022.
[181] G. Wu, S. Wang, Z. Ning, and B. Zhu, Privacy-preserved electronic medical record exchanging and sharing: A blockchain-based smart healthcare system, *IEEE J. Biomed. Health Informatics*, vol. 26, no. 5, pp. 1917–1927, 2022.
[182] W. Liu, Q. Yu, Z. Li, Z. Li, Y. Su, and J. Zhou, A blockchain-based system for anti-fraud of healthcare insurance, in *Proc. 2019 IEEE 5th International Conference on Computer and Communications* (*ICCC*), Chengdu, China, 2019, pp. 1264–1268.
[183] J. C. Mendoza-Tello, T. Mendoza-Tello, and H. Mora, Blockchain as a healthcare insurance fraud detection tool, in *Proc. Research and Innovation Forum 2020—Disruptive Technologies in Times of Change*, Athens, Greece, 2020, pp. 545–552.

[184] M. J. H. Faruk, H. Shahriar, M. Valero, S. Sneha, S. I. Ahamed, and M. Rahman, Towards blockchain-based secure data management for remote patient monitoring, in *Proc. 2021 IEEE International Conference on Digital Health* (*ICDH*), Chicago, IL, USA, 2021, pp. 299–308.

[185] C. Pighini, A. Vezzoni, S. Mainini, A. G. Migliavacca, A. Montanari, M. R. Guarneri, E. G. Caiani, and A. Cesareo, Syncare: An innovative remote patient monitoring system secured by cryptography and blockchain, in *Proc. 16th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School on Privacy and Identity 2021*, Virtual event, 2021, pp. 73–89.

[186] D. R. Wong, S. Bhattacharya, and A. J. Butte, Prototype of running clinical trials in an untrustworthy environment using blockchain, *Nature Communications*, vol. 10, no. 1, p. 917, 2019.

[187] G. Albanese, J. -P. Calbimonte, M. Schumacher, and D. Calvaresi, Dynamic consent management for clinical trials via private blockchain technology, *J. Ambient Intell. Humaniz. Comput.*, vol. 11, no. 11, pp. 4909–4926, 2020.

[188] M. Uddin, K. Salah, R. Jayaraman, S. Pesic, and S. Ellahham, Blockchain for drug traceability: Architectures and open challenges, *Health Informatics J.*, doi: 10.1177/14604582211011228.

[189] A. Musamih, K. Salah, R. Jayaraman, J. Arshad, M. Debe, Y. Al-Hammadi, and S. Ellahham, A blockchain-based approach for drug traceability in healthcare supply chain, *IEEE Access*, vol. 9, pp. 9728–9743, 2021.

[190] E. K. Kambilo, H. B. Zghal, C. G. Guegan, V. Stankovski, P. Kochovski, and D. Vodislav, A blockchain-based framework for drug traceability: Chaindrugtrac, in *Proc. 37th ACM/SIGAPP Symposium on Applied Computing,* Virtual event, 2022, pp. 1900–1907.

[191] K. Abbas, M. Afaq, T. Ahmed Khan, and W. Song, A blockchain and machine learning-based drug supply chain management and recommendation system for smart pharmaceutical industry, *Electronics*, vol. 9, no. 5, p. 852, 2020.

[192] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, and B. Yoon, A framework for privacy-preservation of IoT healthcare data using federated learning and blockchain technology, *Future Gener. Comput. Syst.*, vol. 129, pp. 380–388, 2022.

[193] A. Ali, M. A. Almaiah, F. Hajjej, M. F. Pasha, O. H. Fang, R. Khan, J. Teo, and M. Zakarya, An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network, *Sensors*, vol. 22, no. 2, p. 572, 2022.

[194] K. M. Hossein, M. E. Esmaeili, T. Dargahi, A. Khonsari, and M. Conti, Bchealth: A novel blockchain-based privacypreserving architecture for IoT healthcare applications, *Comput. Commun.*, vol. 180, pp. 31–47, 2021.

[195] S. Aich, N. K. Sinai, S. Kumar, M. Ali, Y. R. Choi, M. -I. Joo, and H. -C. Kim, Protecting personal healthcare record using blockchain & federated learning technologies, in *Proc. 24th International Conference on Advanced Communication Technology* (*ICACT*), PyeongChang, Republic of Korea, 2022, pp. 109–112.

[196] M. Torky, A. Darwish, and A. E. Hassanien, Blockchain use cases for COVID-19: Management, surveillance, tracking and security, in *Digital Transformation and Emerging Technologies for Fighting COVID-19 Pandemic: Innovative Approaches*, A. E. Hassanien and A. Darwish, eds. Cham, Switzerland: Springer, 2021, pp. 261–274.

[197] S. Yao, P. Jing, P. Li, and J. Chen, A multi-dimension traceable privacy-preserving prevention and control scheme of the COVID-19 epidemic based on blockchain, *Connect. Sci.*, vol. 34, no. 1, pp. 1654–1677, 2022.

[198] L. Tan, K. Yu, N. Shi, C. Yang, W. Wei, and H. Lu, Towards secure and privacy-preserving data sharing for COVID-19 medical records: A blockchain-empowered approach, *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 1, pp. 271–281, 2022.

[199] B. Aslan and K. Atasen, COVID-19 information sharing with blockchain, *Inf. Technol. Control.*, vol. 50, no. 4, pp. 674–685, 2021.

[200] A. Abid, S. Cheikhrouhou, S. Kallel, and M. Jmaiel, Novidchain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates, *Softw. Pract. Exp.*, vol. 52, no. 4, pp. 841–867, 2022.

[201] S. Tahir, H. Tahir, A. Sajjad, M. Rajarajan, and F. Khan, Privacy-preserving COVID-19 contact tracing using blockchain, *J. Commun. Networks*, vol. 23, no. 5, pp. 360–373, 2021.

[202] L. Ricci, D. D. F. Maesa, A. Favenza, and E. Ferro, Blockchains for COVID-19 contact tracing and vaccine support: A systematic review, *IEEE Access*, vol. 9, pp. 37936–37950, 2021.

[203] M. Kassab and G. Destefanis, Blockchain and contact tracing applications for COVID-19: The opportunity and the challenges, in *Proc. 2021 IEEE International Conference on Software Analysis, Evolution and Reengineering* (*SANER*), Honolulu, HI, USA, 2021, pp. 723–730.

[204] H. Xu, L. Zhang, O. Onireti, Y. Fang, W. J. Buchanan, and M. A. Imran, Beeptrace: Blockchain-enabled privacy-preserving contact tracing for COVID-19 pandemic and beyond, *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3915–3929, 2021.

[205] M. M. Arifeen, A. A. Mamun, M. S. Kaiser, and M. Mahmud, Blockchain-enable contact tracing for preserving user privacy during COVID-19 outbreak, *Preprints*, doi: 10.20944/preprints202007.0502.v1.

[206] H. Choudhury, B. Goswami, and S. K. Gurung, COVIDchain: An anonymity preserving blockchain based framework for protection against COVID-19, *Inf. Secur. J. A Glob. Perspect.*, vol. 30, no. 5, pp. 257–280, 2021.

[207] H. R. Hasan, K. Salah, R. Jayaraman, I. Yaqoob, M. A. Omar, and S. Ellahham, COVID-19 contact tracing using blockchain, *IEEE Access*, vol. 9, pp. 62956–62971, 2021.

[208] M. Torky, E. Goda, V. Snasel, and A. E. Hassanien, COVID-19 contact tracing and detection-based on blockchain technology, *Informatics*, vol. 8, no. 4, p. 72, 2021.

[209] Z. Peng, C. Xu, H. Wang, J. Huang, J. Xu, and X. Chu, P$^2$B-trace: Privacy-preserving blockchain-based contact tracing to combat pandemics, in *Proc. 2021 International*

*Conference on Management of Data*, Virtual event, China, 2021, pp. 2389–2393.
[210] Naren, A. Tahiliani, V. Hassija, V. Chamola, S. S. Kanhere, and M. Guizani, Privacy-preserving and incentivized contact tracing for COVID-19 using blockchain, *IEEE Internet Things Mag.*, vol. 4, no. 3, pp. 72–79, 2021.
[211] W. Lv, S. Wu, C. Jiang, Y. Cui, X. Qiu, and Y. Zhang, Towards large-scale and privacy-preserving contact tracing in COVID-19 pandemic: A blockchain perspective, *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 1, pp. 282–298, 2022.
[212] S. A. Alansari, M. M. Badr, M. M. E. A. Mahmoud, W. Alasmary, F. Alsolami, and A. M. Ali, Efficient and privacy-preserving infection control system for COVID-19-like pandemics using blockchain, *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2744–2760, 2022.
[213] M. F. Rotbi, S. Motahhir, and A. E. Ghzizal, Blockchain technology for a safe and transparent COVID-19 vaccination, *J. ICT Stand.*, vol. 10, no. 2, pp. 125–144, 2022.
[214] A. Musamih, R. Jayaraman, K. Salah, H. R. Hasan, I. Yaqoob, and Y. Al-Hammadi, Blockchain-based solution for distribution and delivery of COVID-19 vaccines, *IEEE Access*, vol. 9, pp. 71372–71387, 2021.
[215] G. Lax, A. Russo, and L. S. Fascì, A blockchain-based approach for matching desired and real privacy settings of social network users, *Inf. Sci.*, vol. 557, pp. 220–235, 2021.
[216] B. Guidi, When blockchain meets online social networks, *Pervasive Mob. Comput.*, vol. 62, p. 101131, 2020.
[217] L. Jiang and X. Zhang, BCOSN: A blockchain-based decentralized online social network, *IEEE Trans. Comput. Soc. Syst.*, vol. 6, no. 6, pp. 1454–1466, 2019.
[218] S. Zhang, T. Yao, V. K. A. Sandor, T. Weng, W. Liang, and J. Su, A novel blockchain-based privacy-preserving framework for online social networks, *Connect. Sci.*, vol. 33, no. 3, pp. 555–575, 2021.
[219] Y. Chen, H. Xie, K. Lv, S. Wei, and C. Hu, DEPLEST: A blockchain-based privacy-preserving distributed database toward user behaviors in social networks, *Inf. Sci.*, vol. 501, pp. 100–117, 2019.
[220] H. H. Nguyen, D. Bozhkov, Z. Ahmadi, N. Nguyen, and T. Doan, SoChainDB: A database for storing and retrieving blockchain-powered social network data, in *Proc. 45th International ACM SIGIR Conference on Research and Development in Information Retrieval*, Madrid, Spain, 2022, pp. 3036–3045.
[221] A. Kiayias, B. Livshits, A. M. Mosteiro, and O. S. T. Litos, A puff of steem: Security analysis of decentralized content curation, arXiv preprint arXiv: 1810.01719, 2018.
[222] K. Gu, L. Wang, and W. Jia, Autonomous resource request transaction framework based on blockchain in social network, *IEEE Access*, vol. 7, pp. 43666–43678, 2019.
[223] M. U. Rahman, B. Guidi, and F. Baiardi, Blockchain-based access control management for decentralized online social networks, *J. Parallel Distributed Comput.*, vol. 144, pp. 41–54, 2020.
[224] M. Zhang, Z. Sun, H. Li, B. Niu, F. Li, Y. Xie, and C. Zheng, A blockchain-based privacy-preserving framework for cross-social network photo sharing, in *Proc. IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops*, New York, NY, USA, 2022, pp. 1–6.
[225] Z. Yan, L. Peng, W. Feng, and L. T. Yang, Socialchain: Decentralized trust evaluation based on blockchain in pervasive social networking, *ACM Trans. Internet Techn.*, vol. 21, no. 1, pp. 1–28, 2021.
[226] W. Guo, J. Xue, Y. Wang, and Z. Zhou, Blockchain-based reputation evaluation using game theory in social networking, in *Proc. 4th ACM International Symposium on Blockchain and Secure Critical Infrastructure*, Nagasaki, Japan, 2022, pp. 107–114.
[227] I. S. Ochoa, G. D. Mello, L. A. Silva, A. J. P. Gomes, A. M. R. Fernandes, and V. R. Q. Leithardt, Fakechain: A blockchain architecture to ensure trust in social media networks, in *Proc. 12th International Conference on Quality of Information and Communications Technology*, Ciudad Real, Spain, 2019, pp. 105–118.
[228] L. Zhang, Y. Zhang, Q. Wu, Y. Mu, and F. Rezaeibagha, A secure and efficient decentralized access control scheme based on blockchain for vehicular social networks, *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17938–17952, 2022.
[229] H. Shen, J. Zhou, Z. Cao, X. Dong, and K. R. Choo, Blockchain-based lightweight certificate authority for efficient privacy-preserving location-based service in vehicular social networks, *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6610–6622, 2020.
[230] D. M. Lambert and M. G. Enz, Issues in supply chain management: Progress and potential, *Industrial Marketing Management*, vol. 62, pp. 1–16, 2017.
[231] D. Ivanov, A. Dolgui, and B. Sokolov, The impact of digital technology and industry 4.0 on the ripple effect and supply chain risk analytics, *International Journal of Production Research*, vol. 57, no. 3, pp. 829–846, 2019.
[232] N. Kshetri and E. Loukoianova, Blockchain adoption in supply chain networks in Asia, *IT Prof.*, vol. 21, no. 1, pp. 11–15, 2019.
[233] M. M. Queiroz, S. F. Wamba, M. D. Bourmont, and R. Telles, Blockchain adoption in operations and supply chain management: Empirical evidence from an emerging economy, *International Journal of Production Research*, vol. 59, no. 20, pp. 6087–6103, 2021.
[234] X. Wu, Z. -P. Fan, and B. Cao, An analysis of strategies for adopting blockchain technology in the fresh product supply chain, *International Journal of Production Research*, doi: 10.1080/00207543.2021.1894497.
[235] F. Casino, V. Kanakaris, T. K. Dasaklis, S. J. Moschuris, S. Stachtiaris, M. Pagoni, and N. P. Rachaniotis, Blockchain-based food supply chain traceability: A case study in the dairy sector, *International Journal of Production Research*, vol. 59, no. 19, pp. 5758–5770, 2021.
[236] J. D. Sekuloska and A. Erceg, Blockchain technology toward creating a smart local food supply chain, *Comput.*, vol. 11, no. 6, p. 95, 2022.

[237] F. Marinello, M. Atzori, L. Lisi, D. Boscaro, and A. Pezzuolo, Development of a traceability system for the animal product supply chain based on blockchain technology, in *Proc. 8th European Conference on Precision Livestock Farming* (*ECPLF*), Nantes, France, 2017, pp. 258–268.
[238] S. S. Kamble, A. Gunasekaran, and R. Sharma, Modeling the blockchain enabled traceability in agriculture supply chain, *International Journal of Information Management*, vol. 52, p. 101967, 2020.
[239] I. A. Omar, M. Debe, R. Jayaraman, K. Salah, M. A. Omar, and J. Arshad, Blockchain-based supply chain traceability for COVID-19 personal protective equipment, *Comput. Ind. Eng.*, vol. 167, p. 107995, 2022.
[240] B. M. Yakubu, R. Latif, A. Yakubu, M. I. Khan, and A. I. Magashi, Ricechain: Secure and traceable rice supply chain framework using blockchain technology, *PeerJ Comput. Sci.*, vol. 8, p. e801, 2022.
[241] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, Blockchain-based traceability in agri-food supply chain management: A practical implementation, in *Proc. 2018 IoT Vertical and Topical Summit on Agriculture*, Tuscany, Italy, 2018, pp. 1–4.
[242] T. K. Dasaklis, F. Casino, and C. Patsakis, Defining granularity levels for supply chain traceability based on IoT and blockchain, in *Proc. International Conference on Omni-Layer Intelligent Systems*, Crete, Greece, 2019, pp. 184–190.
[243] M. Kouhizadeh, S. Saberi, and J. Sarkis, Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers, *International Journal of Production Economics*, vol. 231, p. 107831, 2021.
[244] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, Blockchain technology and its relationships to sustainable supply chain management, *International Journal of Production Research*, vol. 57, no. 7, pp. 2117–2135, 2019.
[245] R. L. Rana, C. Tricase, and L. D. Cesare, Blockchain technology for a sustainable agri-food supply chain, *British Food Journal*, vol. 123, no. 11, pp. 3471–3485, 2021.
[246] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, Trustchain: Trust management in blockchain and IoT supported supply chains, in *Proc. 2019 IEEE International Conference on Blockchain*, Atlanta, GA, USA, 2019, pp. 184–193.
[247] M. S. Al-Rakhami and M. Al-Mashari, A blockchain-based trust model for the internet of things supply chain management, *Sensors*, vol. 21, no. 5, p. 1759, 2021.
[248] Q. Song, Y. Chen, Y. Zhong, K. Lan, S. J. Fong, and R. Tang, A supply-chain system framework based on internet of things using blockchain technology, *ACM Transactions on Internet Technology*, vol. 21, no. 1, pp. 1–24, 2021.
[249] P. Centobelli, R. Cerchione, P. D. Vecchio, E. Oropallo, and G. Secundo, Blockchain technology for bridging trust, traceability and transparency in circular supply chain, *Information & Management*, vol. 59, no. 7, p. 103508, 2021.
[250] P. V. R. P. Raj, S. K. Jauhar, M. Ramkumar, and S. Pratap, Procurement, traceability and advance cash credit payment transactions in supply chain using blockchain smart contracts, *Comput. Ind. Eng.*, vol. 167, p. 108038, 2022.
[251] R. Azzi, R. K. Chamoun, and M. Sokhn, The power of a blockchain-based supply chain, *Computers & Industrial Engineering*, vol. 135, pp. 582–592, 2019.
[252] A. Bateman and L. Bonanni, What supply chain transparency really means, *Harvard Business Review*, vol. 20, pp. 2–8, 2019.
[253] Z. Zhou, X. Liu, F. Zhong, and J. Shi, Improving the reliability of the information disclosure in supply chain based on blockchain technology, *Electron. Commer. Res. Appl.*, vol. 52, p. 101121, 2022.
[254] Z. Sun, Q. Xu, and B. Shi, Price and product quality decisions for a two-echelon supply chain in the blockchain era, *Asia Pac. J. Oper. Res.*, vol. 39, no. 1, p. 2140016, 2022.

**Weili Wu** received the MS and PhD degrees from University of Minnesota, Minneapolis, MN, USA in 1998 and 2002, respectively. She is currently a full professor with the Department of Computer Science, University of Texas at Dallas, Richardson, TX, USA. She is a senior member of IEEE. Her research mainly deals in the general research area of data communication and data management. Her research focuses on the design and analysis of algorithms for optimization problems that occur in wireless networking environments and various database systems.

**Xiao Li** received the BS and MS degrees in software engineering from Dalian University of Technology, China in 2016 and 2019, respectively. He is currently pursuing the PhD degree with the Department of Computer Science, University of Texas at Dallas, Richardson, TX, USA. His current research interests include data mining and blockchain.