A Survey of Blockchain and Artificial Intelligence for 6G Wireless Communications

Yiping Zuo, *Member, IEEE*, Jiajia Guo, *Member, IEEE*, Ning Gao, *Member, IEEE*, Yongxu Zhu, *Senior Member, IEEE*, Shi Jin, *Senior Member, IEEE*, and Xiao Li, *Member, IEEE*

***Abstract*—The research on the sixth-generation (6G) wireless communications for the development of future mobile communication networks has been officially launched around the world. 6G networks face multifarious challenges, such as resource-constrained mobile devices, difficult wireless resource management, high complexity of heterogeneous network architectures, explosive computing and storage requirements, privacy and security threats. To address these challenges, deploying blockchain and artificial intelligence (AI) in 6G networks may realize new breakthroughs in advancing network performances in terms of security, privacy, efficiency, cost, and more. In this paper, we provide a detailed survey of existing works on the application of blockchain and AI to 6G wireless communications. More specifically, we start with a brief overview of blockchain and AI. Then, we mainly review the recent advances in the fusion of blockchain and AI, and highlight the inevitable trend of deploying both blockchain and AI in wireless communications. Furthermore, we extensively explore integrating blockchain and AI for wireless communication systems, involving secure services and Internet of Things (IoT) smart applications. Particularly, some of the most talked-about key services based on blockchain and AI are introduced, such as spectrum management, computation allocation, content caching, and security and privacy. Moreover, we also focus on some important IoT smart applications supported by blockchain and AI, covering smart healthcare, smart transportation, smart grid, and unmanned aerial vehicles (UAVs). Moreover, we thoroughly discuss operating frequencies, visions, and requirements from the 6G perspective. We also analyze the open issues and research challenges for the joint deployment of blockchain and AI in 6G wireless communications. Lastly, based on lots of existing meaningful works, this paper aims to provide a comprehensive survey of blockchain and AI in 6G networks. We hope this survey can shed new light on the research of this newly emerging area and serve as a roadmap for future studies.**

***Index Terms*—Blockchain, AI, wireless communications, 6G networks, secure services, IoT smart applications, spectrum management, security and privacy, smart healthcare, UAVs**

I. Introduction

From 2020, the fifth-generation (5G) wireless networks achieve large-scale commercial deployment worldwide. Academia, industry, and governments are now engaged in research and development of the sixth-generation (6G) wireless communication technology to meet the demands of future networks in 2030 and beyond [1]. Compared with 5G networks, 6G networks will have ultra-high network speed, ultra-low communication delay, and wider coverage depth. 6G networks will fully share ultra-high frequency wireless spectrum resources such as millimeter waves, terahertz, and light waves. 6G networks will also integrate technologies such as terrestrial mobile communications, satellite Internet, and microwave networks to form an integrated green network with group collaboration of all things, intelligent data perception, real-time security assessment, and coordinated coverage of space and earth [2]–[4]. Facing the 6G era, the network will usher in new application scenarios and new performance requirements. In the 6G era, an air-space-ground integrated network communication system will be built to realize a ubiquitous network for full coverage and all scenarios [5]. However, diverse applications and communication scenarios, ultra-heterogeneous network connections, and service requirements for extreme performance all place higher requirements on the bandwidth, latency, security, connection density, and flexibility of 6G networks [6]–[8].

In the 6G era, artificial intelligence (AI) [9] is becoming more and more important. AI relies on mining big data for training and learning, continuously enhancing computing power to cope with higher transmission rates, and gaining more flexibility through continuous learning. In the future, 6G networks need to deal with explosive data traffic growth and massive device connections. Real-time management and control of these massive data will result in high complexity and latency overhead. Therefore, how to effectively perceive service characteristics, accurately monitor and control network resources, and dynamically allocate wireless resources has become an important issue for 6G networks. The use of AI at the application layer and network layer of 6G networks makes the network more intelligent and automated, which will be a necessary way to manage and control massive wireless big data [10], [11]. In addition, 6G network supports large-scale users, large-scale antennas, and multi-band hybrid transmission, so traditional physical layer transmission technologies will face multiple challenges in performance, complexity, and efficiency. This provides the possibility for AI technology to be applied to the wireless physical layer [12], [13]. Notably, a 6G white paper [14] released by the University of Oulu believed that AI will play an important role in 6G networks. The report of [15] also indicated that it is necessary to introduce AI technology into complex network architectures in the future.

Y. Zuo is with the College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210028, China, and also with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (Email: zuoyiping@njupt.edu.cn).

J. Guo, N. Gao, S. Jin, and X. Li are with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (Email: jiajiaguo@seu.edu.cn; ninggao@seu.edu.cn; jinshi@seu.edu.cn; li_xiao@seu.edu.cn).

Y. Zhu is with the School of Engineering, University of Warwick, Coventry, UK (Email: yongxu.zhu@warwick.ac.uk).

(*Corresponding author: Shi Jin)*

Blockchain is another highly anticipated emerging technology. In fact, blockchain is a technical system that integrates various technologies such as chain data structure, point-to-point transmission, distributed storage, consensus mechanism, and encryption algorithm [16]. The performance index requirements of 6G networks, such as ultra-high peak rate, ultra-low latency, ultra-high reliability, ultra-low energy consumption, and seamless connection, make system security, data privacy, sustainability, scalability, and other aspects subject to many risks and challenges [17], [18]. Blockchain technology is an important technical means to cope with these challenges, especially with the advantages of distributed network architecture, intelligent node consensus, and smart contracts. The integrated application of blockchain and 6G networks provide a safe, intelligent, and efficient underlying technical support for the realization of the 6G network vision [19], [20]. In particular, 6G white paper [14] pointed out that 6G network requires an endogenous trust network, and blockchain technology may play an important role in the 6G networks to deal with a variety of complex new privacy challenges. Blockchain is a potential solution for privacy protection of 6G networks [21]. Moreover, blockchain can provide a strong guarantee for 6G networks to build a distributed, secure, and trusted transaction environment.

Research institutions and operators worldwide are accelerating the development of the cross-integration between emerging technologies such as blockchain and AI with 6G networks. The IMT-2030 (6G) Promotion Group's white paper proposes various scenarios for the application of blockchain technology in 6G networks, including dynamic spectrum management, ubiquitous access management, edge computing, and so on. China has established several international standard projects of blockchain in ITU, such as the establishment of "Framework of blockchain of things as decentralized service platform" in ITU-T SG20 and the "Reference framework for distributed ledger technologies" in ITU-T SG16. Sprint, an American operator, has partnered with NXM Labs to launch a 5G connected vehicle platform powered by blockchain technology. China Mobile and Huobi China have created a "blockchain + Internet of Things (IoT)" identity authentication platform. Meanwhile, 3GPP specifically defines the network data analysis function, aiming to provide a standard interface for the development and application of AI models in wireless networks. The European Telecommunications Standards Institute has also established an industry standard working group to use AI for network management, expecting to achieve a high-level autonomous network with endogenous AI. The IMT-2030 (6G) Promotion Group puts forward the 6G vision of "Intelligent Internet of Everything, Digital Twin", pointing out that 6G will enable the efficient and intelligent interconnection of all things.

A. Previous Survey Works and Motivations

AI model or algorithm is based on the trained intelligence data. Meanwhile, blockchain is essentially a data storage method, or "hyper ledger", which embodies data intelligence [52]. Consequently, these two technologies, which are both closely related to data, can be effectively combined to complement each other and achieve technological improvement [37]–[39]. As a trusted platform, blockchain can improve the authenticity, relevance, and validity of the data used by AI. From the perspective of data, computing power, and algorithms, blockchain improves the level of AI technology, innovates AI collaboration models and computing paradigms, and constructs a new AI ecosystem. With intelligent and automatic characteristics, AI can promote the natural evolution and data sorting of blockchain through the optimization and simulation of AI algorithms. Additionally, AI can effectively prevent the occurrence of blockchain node forks, can handle the operation of the blockchain more effectively, and improve efficiency intelligently. Most importantly, the close combination of blockchain and AI can promote and optimize various services and applications and also can provide a reliable, secure, and ultra-low latency intelligent network environment for next-generation wireless communications. Accordingly, in the future 6G networks, the research on the simultaneous deployment of blockchain and AI is of positive significance.

Next, we briefly describe the existing survey on the adoption of blockchain and AI in wireless communication systems. Researchers integrated blockchain with wireless communications to form secure and trusted mobile networks and services. In [22]–[27], a large number of reviews on blockchain-supported wireless communications have been published, broadly elaborating the basic concepts, network architecture, enabling technologies, research challenges, and future research directions. Moreover, the mutual integration of blockchain and AI has also been investigated in detail by multiple studies [33]–[41]. Most importantly, the disruptive integration of blockchain and AI for wireless communications can greatly improve the network performance for a variety of services and applications. Many pieces of literature [42]–[51] have summarized and reviewed the topic of joint blockchain and AI for wireless communications. However, to the best of our knowledge, none of the existing surveys have comprehensively investigated this popular topic, especially few research emphasized the simultaneous deployment of blockchain and AI for next-generation wireless communications. For example, the research of [46] only briefly discussed the potential of the joint application of blockchain and machine learning (ML) in wireless communication systems. Similarly, the work in [47] briefly reviewed reinforcement learning (RL)-empowered blockchains applied in Industrial IoT (IIoT) networks. The authors of [51] simply investigated the benefits of adopting blockchain with ML under the secure in-vehicle network. TABLE I displays a straightforward comparison of our work with existing related surveys.

B. Novelty and Contributions

Compared with the existing aforementioned works, our survey provides a comprehensive analysis and outlook on the current research progress of blockchain and AI for 6G wireless communications. We hope that this survey has some reference significance for carrying out more innovative research in this promising field. The main contributions of this article can be summarized as follows:

1) We briefly outline the basic knowledge of blockchain and AI. First, the concept, characteristics, and categories of

TABLE I. Comparison of our work with existing related research.

Research Work	Year	Blockchain for 5G/6G	AI for 5G/6G	Blockchain for AI	AI for Blockchain	Blockchain and AI for 5G/6G	Key Technologies
Wang et al. [22]	2021	Yes	No	No	No	No	Blockchain, RAN
Wu et al. [23]	2019	Yes	No	No	No	Limited	Blockchain, IoT
Nguyen et al. [24]	2020	Yes	No	No	No	Limited	Blockchain, IoT, SDN, NFV
Yue et al. [25]	2021	Yes	No	No	No	No	Blockchain, DApps
Tahir et al. [26]	2020	Yes	No	No	No	No	Blockchain, RAN, D2D, SDN
Bhat et al. [27]	2020	Yes	No	No	No	Limited	Blockchain, IoT, MEC
Sharma et al. [28]	2021	Limited	Yes	No	No	No	ML, DL, IoT, Blockchain
Sun et al. [29]	2020	Limited	Yes	No	No	No	ML, FL, Blockchain
Rekkas et al. [30]	2021	No	Yes	No	No	No	ML
Liu et al. [31]	2020	No	Yes	No	No	No	ML, FL
Lin et al. [32]	2020	No	Yes	No	No	Limited	AI, Blockchain
Salah et al. [33]	2019	No	No	Yes	No	No	Blockchain, AI
Shafay et al. [34]	2022	No	No	Yes	No	No	Blockchain, DL, ML, FL
Wang et al. [35]	2021	No	No	Yes	No	No	Blockchain, AI
Xing et al. [36]	2018	No	No	No	Yes	No	Blockchain, AI
Pandl et al. [37]	2020	No	No	Yes	Yes	No	Blockchain, AI
Dinh et al. [38]	2018	No	No	Yes	Yes	No	Blockchain, AI
Singh et al. [39]	2020	No	No	Yes	Yes	Limited	Blockchain, AI, IoT
Hussain et al. [40]	2021	No	No	No	Yes	No	Blockchain, AI
Yang et al. [41]	2022	No	No	Limited	Limited	No	Blockchain, AI, Metaverse
Mohanta et al. [42]	2020	No	No	No	No	Limited	Blockchain, AI, ML, IoT
Tagde et al. [43]	2021	Limited	Limited	No	No	Limited	Blockchain, AI
Gill et al. [44]	2019	No	No	No	No	Limited	Blockchain, AI, IoT
Dhar et al. [45]	2021	Limited	No	No	No	Limited	Blockchain, AI, IoT
Liu et al. [46]	2020	Yes	Yes	Yes	Yes	Limited	Blockchain, ML
Jameel et al. [47]	2020	No	No	No	Limited	Limited	Blockchain, RL, IIoT
Wu et al. [48]	2021	No	No	No	Limited	Limited	Blockchain, DRL, IoT
Miglani et al. [49]	2021	No	No	Yes	Yes	Limited	Blockchain, ML, DL, RL, FL
El Azzaoui et al. [50]	2020	Yes	Yes	No	No	Limited	Blockchain, AI, IoT
Dibaei et al. [51]	2022	Limited	Limited	No	No	Limited	Blockchain, ML, DL
Our Work	2023	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	Blockchain, AI, IoT

blockchain and AI are introduced. Then, we separately discuss the classic applications of blockchain and AI for wireless communication systems.

2) We systematically summarize the integration of blockchain and AI from two directions: blockchain-assisted AI and AI-assisted blockchain. Furthermore, we also emphasize the advantages of integrating blockchain and AI for wireless communication systems.
3) We deeply elaborate on the latest developments of combining blockchain and AI in 6G secure services. We specifically focus on some of the most popular 6G secure services, such as spectrum management, computation allocation, content caching, and security and privacy.
4) We review the latest achievements of joint blockchain and AI in 6G IoT smart applications. We extensively discuss some important 6G IoT smart applications, including smart healthcare, smart transportation, smart grid, and unmanned aerial vehicle (UAV).
5) On the basis of the comprehensive survey, we thoroughly discuss operating frequencies, visions, and requirements from the 6G perspective. We also propose some open issues and research challenges that need to be resolved for the applications of blockchain and AI to 6G wireless communications, and summarize several future research directions.

C. Outline of the Survey

The outline of this article is presented in Fig. 1. The remainder of this survey is organized as follows. Section II-A provides an overview of blockchain, including the concept, characteristics, categories, and representative applications in wireless communications. In Section II-B, we describe an overview of AI, taking into account the concept, characteristics, categories, and typical applications in wireless communications. In Section II-C, we discuss the mutual fusion of blockchain and AI, and emphasize the abundant benefits of this fusion for wireless communication systems. Section III presents the integration of blockchain and AI for wireless communications, covering secure services and IoT smart applications. Some open issues and research challenges are discussed in Section IV, and the future work is also addressed. Finally, we conclude the main works of the survey in Section V. The major acronyms used in this paper are summarized in TABLE II.

II. Background of Blockchain and AI

A. An Overview of Blockchain

1) Concept of Blockchain: The concept of blockchain was first mentioned in the Bitcoin white paper written by S. Nakamoto [53], marking the birth of blockchain 1.0. Ethereum based on smart contracts means the arrival of the blockchain 2.0 era [54]. Blockchain 3.0 emphasizes its application to all aspects of society. Blockchain is essentially a distributed super-accounting ledger [55]. This digital ledger guarantees

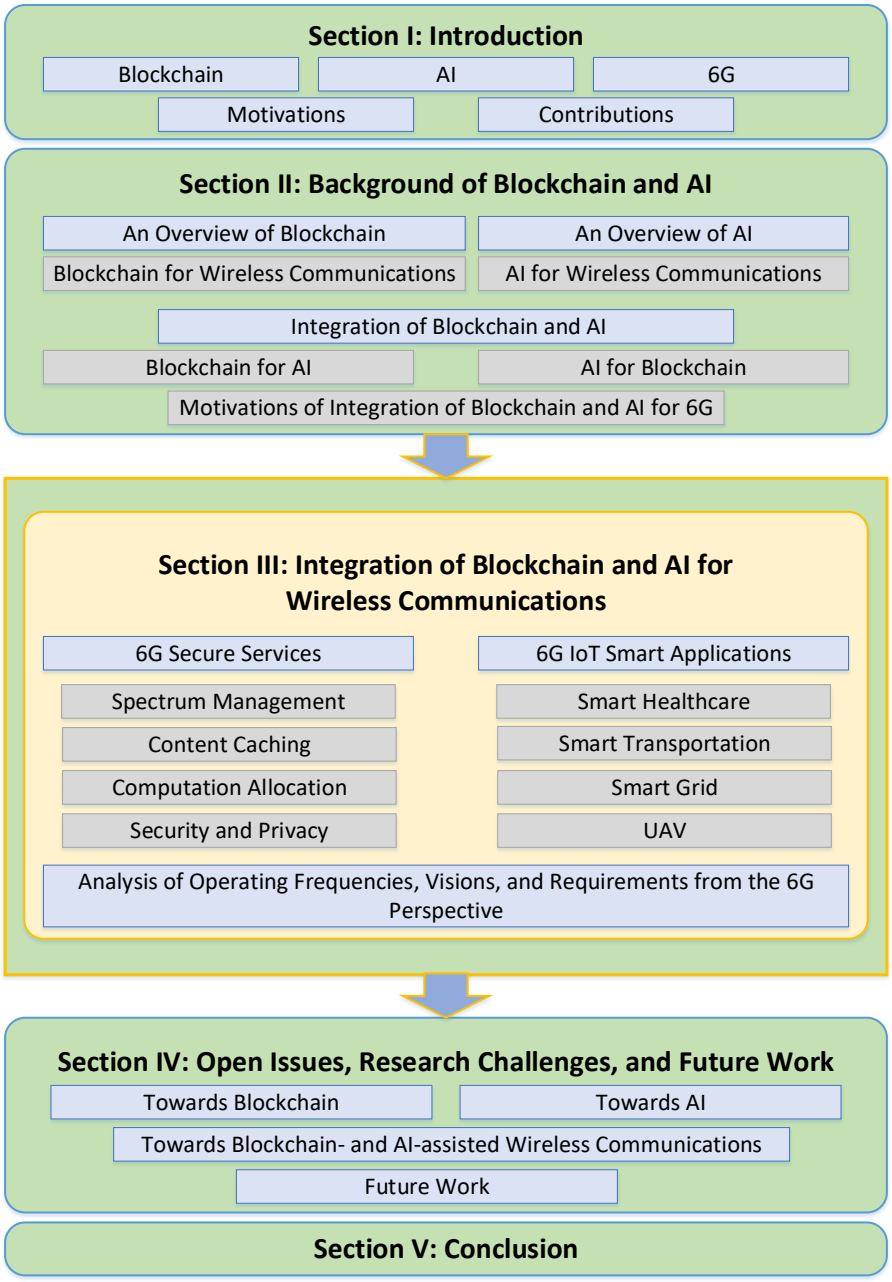

Fig. 1. Outline of the paper.

data security through encryption algorithms and consensus mechanisms. Over time, the past transaction records on the blockchain ledger will not be deleted and cannot be tampered with. The blockchain network consists of multiple peer nodes, and these nodes do not need to trust each other. Each node independently maintains a copy of the global ledger. The transaction data in the ledger is encapsulated by blocks. The new block will be added to the end of the previous block in the form of a linked list, so this accounting ledger is called "blockchain" [56]. Taking bitcoin as an example, the typical block structure is shown in Fig. 2. Each block is divided into two parts: block header and block body. The block body stores the verified transaction data. The block header contains the version, hash value of the previous block, hash value of the current block, timestamp, difficulty value, nonce, and Merkle root.

In the blockchain system, the consensus algorithm ensures that each node can maintain the same transaction content and sequence, which is the core component of the blockchain network [57]. Currently, the widely used and common consensus algorithms are as follows: Proof of Work (PoW) [53], Proof of Stake (PoS) [58], Delegated Proof of Stake (DPoS) [59], and Practical Byzantine Fault Tolerance (PBFT) [60]. PoW introduces distributed node computing power competition to maintain data consistency and consensus security. The core idea of PoS is that the node with the highest stake obtains the accounting right of the block. DPoS elects representatives through shareholder voting to get the right to keep accounts.

TABLE II. List of major acronyms.

Acronyms	Definitions
AI	Artificial Intelligence
6G	Sixth-Generation
IoT	Internet of Things
IIoT	Industrial Internet of Things
UAV	Unmanned Aerial Vehicle
PoW	Proof of Work
PoS	Proof of Stake
DPoS	Delegated Proof of Stake
PBFT	Practical Byzantine Fault Tolerance
P2P	Peer-to-Peer
MBS	Macro Base Station
MEC	Mobile Edge Computing
ML	Machine Learning
DL	Deep Learning
RL	Reinforcement Learning
FL	Federated Learning
DRL	Deep Reinforcement Learning
KNN	K-Nearest Neighbor
DNN	Deep Neural Network
CNN	Convolutional Neural Network
RNN	Recurrent Neural Network
GAN	Generative Adversarial Network
SGD	Stochastic Gradient Descent
CSI	Channel State Information
FDM	Frequency Division Multiplexing
LSTM	Long Short-Term Memory
MIMO	Multiple-Input Multiple-Output
RF	Radio Frequency
MMSE	Minimum Mean Square Error
AMP	Approximate Message Passing
SDN	Software-Defined Networking
RAN	Radio Access Network
NFV	Network Function Virtualization
DApps	Decentralized Applications
D2D	Device-to-Device
BP	Belief Propagation
RSU	Road Side Unit
HDPC	High Density Parity Check
LEO	Low Earth Orbit

PBFT sorts the request through the leader node, the follower node responds to the request, and the response result of most nodes is the final result. In addition, there is no perfect consensus protocol, because the adopted consensus protocol needs to be matched according to the type of blockchain system used. These algorithms have their own advantages but also have their own shortcomings, as presented in TABLE III.

Since blockchain systems run in the Peer-to-Peer (P2P) network where nodes do not trust each other, the initiated transaction needs to be completed under the witness of all nodes in the network. The transaction execution process of the blockchain is as follows. Specifically, the node first randomly generates its own private key and public key and constructs a transaction through a wallet or script tool, and then uses its own private key to sign the transaction. The signed transaction is propagated between neighbor nodes through the P2P network. Then, the node receiving the transaction verifies the legality of the transaction, and the miner digs out a new block according to the consensus algorithm. Next, the miners broadcast the new block to other nodes through the P2P network. Other miners verify the legitimacy of the new block to decide to discard or add to the local chain. After confirming the new block through the nodes of the whole network, this indicates that the new transaction is transferred successfully.

2) Characteristics of Blockchain: The development of blockchain technology has formed a relatively complete technology stack. Blockchain has been widely concerned and studied because of its important characteristics: decentralization, non-tampering, traceability, and anonymity [23].

Decentralization: Blockchain technology is to complete data interaction without relying on any third-party intermediaries or institutions. Compared with the centralized network, the bottom layer of blockchains adopts the P2P network architecture. In the blockchain network, there is no traditional central server to process data recording, storage, and updating. Every node is equal, and the data maintenance of the entire blockchain network is jointly participated by all nodes. In addition, the withdrawal of any node will not affect the operation of the entire system, and the blockchain network has strong robustness.

Non-Tampering: Once the transaction data is packaged on the chain by miner nodes and permanently stored in the blockchain to form an immutable historical ledger. By storing the hash value of the previous block in each block, the blocks are connected back and forth to form a chain structure. This special chained data structure enables all blocks storing transaction data to be added to the end of the blockchain in chronological order. The malicious node wants to tamper with the data, which inevitably causes the hash value of the current block and all subsequent blocks to change, leading to the collapse of the chain structure. Therefore, the cost of data tampering becomes extremely high, making it almost impossible to modify the blockchain.

Traceability: In blockchain networks, all transactions are public and any node can get a record of all transactions. Except for the encrypted private information of both parties to the transaction, all data on the blockchain can be queried through public interfaces. Blockchain uses the chain block structure with a timestamp to store data, resulting in adding a time dimension to data. Each transaction on the block is connected to two adjacent blocks through cryptographic methods, which guarantees that users can trace the source of any transaction.

Anonymity: Since the nodes in the blockchain network do not need to trust each other, there is no need to disclose the identity between the nodes. This ensures the anonymity of each participating node in the blockchain system and protects the privacy of the nodes. Nodes can conduct transactions without knowing the identity of the other party. Both nodes of the transaction only need to publish their own addresses to communicate with each other. In the blockchain network, nodes use asymmetric encryption technology to build trust between nodes in an anonymous environment.

3) Categories of Blockchain: According to different application scenarios, blockchains are classified into public blockchain, consortium blockchain, and private blockchain [46].

Public Blockchain: The public blockchain is a completely decentralized blockchain [61], and any user can join the blockchain network. There is no official organization, management agency, and no central server. Participating nodes can freely enter and exit the network without being controlled.

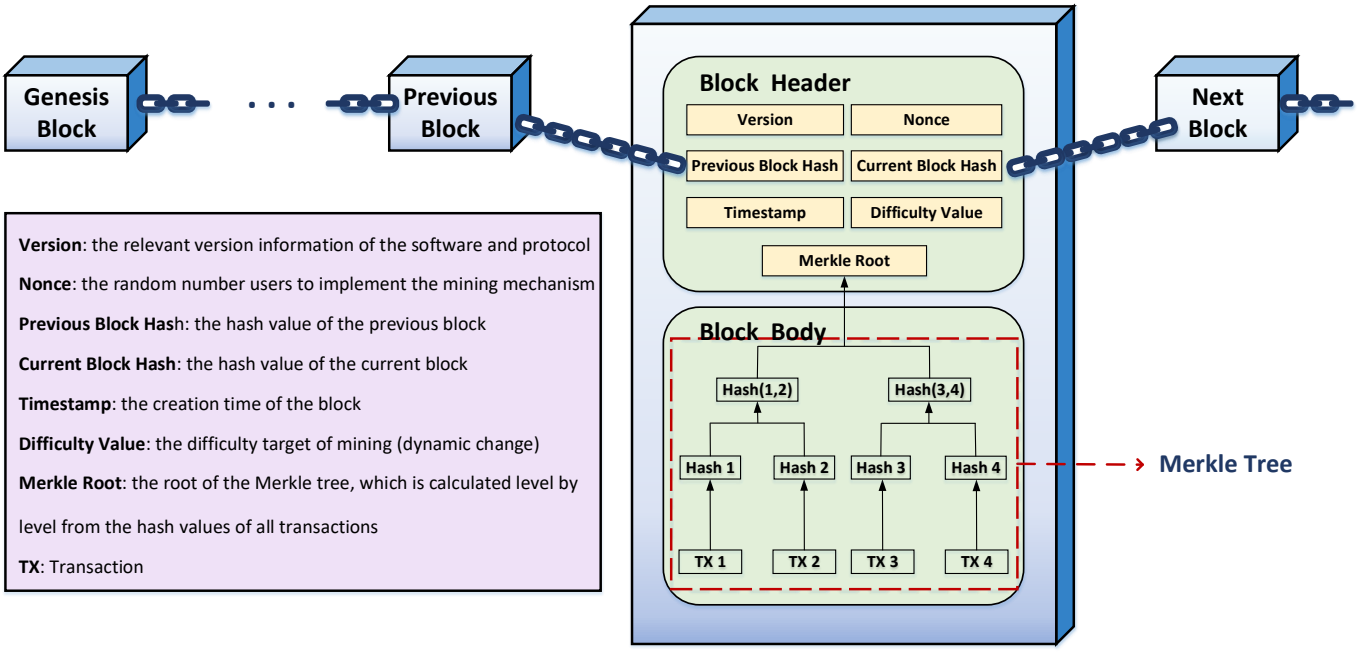

Fig. 2. The structure of blocks.

Private Blockchain: The private blockchain is fully centralized [23], and only authorized and trusted nodes can join the blockchain network. All nodes in the network are controlled by an organization. The operating rules and consensus mechanism of the system are determined by the organization itself.

Consortium Blockchain: The consortium blockchain is a partially decentralized blockchain [62] that is jointly maintained by multiple companies or organizations. This type of blockchain is between the public blockchain and the private blockchain and has the characteristics of multi-center or partial decentralization. Only members belonging to the alliance can generate transactions or view blockchain information.

According to the way of trust construction in different scenarios, the blockchain can also be divided into a permissionless blockchain and a permissioned blockchain [24]. The permissionless blockchain is also called the public blockchain, which is a completely open blockchain. That is, anyone can join the network and participate in the complete consensus accounting process. The permissioned blockchain is a semi-open blockchain. Only designated members can join the network, and each member has different rights to participate. The permission chain often establishes a trust relationship by issuing identity certificates. This blockchain has partial decentralization characteristics, which is more efficient than permissionless blockchains. Private blockchains and consortium blockchains belong to permission chains. The comparison of the characteristics of the above-mentioned different blockchains is shown in TABLE IV.

4) Blockchain for Wireless Communications: Blockchain technology naturally has many advantages such as decentralization, traceability, distribution, and tamper resistance. Therefore, researchers expect to apply the blockchain to all levels of the wireless communication system, which will achieve a substantial increase in system performance and a true sense of the connection of everything [24]. Blockchain can provide traceable communication for 6G networks, which not only facilitates network administrators to query historical resource conditions at any time, but also reduces malicious users' behavior of fabricating resource usage. In addition, the blockchain uses multi-party consensus mechanisms to record the interactions between users, so as to ensure the fairness and openness of all interactions. The integration of blockchain and 6G will provide a strong security guarantee for the construction of a safe and credible communication ecosystem. So far, the research on the integration of blockchain and 6G network mainly involves two main aspects [25]: blockchain-enabled 6G secure services [63]–[91] and blockchain-assisted 6G Internet of Things (IoT) smart applications [92]–[103].

Secure Services: The research on the blockchain-enabled 6G secure services mainly involves spectrum sharing [71]–[80], computing and storage [81]–[88], interference management [89]–[91], and so on. Take blockchain based spectrum sharing as an example, the authors of [71] and [72] proposed a blockchain-based verification and access control protocol to complete the spectrum sharing between primary and secondary users. The works in [73], [74] proposed a blockchain-based spectrum sensing as a service solution. Here, the smart contract is mainly responsible for the following functions: 1) Scheduling the spectrum allocation between users and the helper to maximize system revenue; 2) Identifying whether the helper is a malicious node, and ensuring the security of spectrum sharing. [75] discussed the application of blockchain in different spectrum access scenarios and analyzed the advantages and disadvantages of different spectrum sharing mechanisms. Based on the consortium blockchain, a secure spectrum trading and sharing scheme for drone-assisted communication systems was contrived in [76]. To solve the issue of privacy risk in spectrum sharing, [77] proposed a trusted framework found

TABLE III. Comparison of four typical consensus algorithms.

Consensus Algorithm	Security	Decentralization	Fork	Resource Consumption	Transaction Confir mation Time	Transaction Throughput	Network Scale	Typical Application System
PoW	High	Higher	Easy	Large	Long	Small	Large	Bitcoin
PoS	Higher	Higher	Easy	General	General	Small	Large	Peercoin
DPoS	General	Low	Hard	Small	Short	General	Large	Bitshares
PBFT	General	General	Hard	Small	Short	General	Small	Hyperleder

TABLE IV. Comparison of different blockchains.

Type of Blockchain	Public Blockchain (Permissionless Blockchain)	Private Blockchain (Permissioned Blockchain)	Consortium Blockchain (Permissioned Blockchain)
Degree of Centralization	Decentralization	Centralization	Multi-centralization
Participant	Anyone	Designated member	Alliance member
Bookkeeper	All participants	Self-determined	Participants decided after negotiation
Advantage	High credibility	High security & Low latency	Good scalability
Disadvantage	High latency & Low efficiency	Limited nodes & Centralization	Have a trust issue
Typical Application Scenarios	Bitcoin, Ethereum	Hyperledger	Centralized Exchange

on blockchain entitled TrustSAS for dynamic spectrum access. The work in [78] introduced a smart network architecture, which uses smart contracts to handle unlicensed spectrum sharing between operators and users. The authors of [79] proposed a blockchain-based radio service model, which can reduce the management cost of dynamic access systems. For wireless downlink communication systems with multiple mobile operators, the work in [80] delineated a blockchain-based dynamic spectrum acquisition scheme.

The computing and storage capabilities of edge computing are valuable network resources, which can be efficiently managed through the blockchain. To solve the problem of low efficiency of computing resource transactions, in the blockchain-based edge-assisted IoT network, the work in [81] considered using the credit-based payment for fast computing resource transactions. The work in [82] proposed a blockchain-based multi-layer computing offloading architecture, which enhances the collaboration between users in sharing computing resources. In the blockchain-empowered multi-task cross-server edge computing scenario, the authors of [83] proposed two double auction mechanisms to drive end users and edge servers to securely allocate and trade resources. The works of [84] and [85] applied the consortium blockchain and smart contracts to the vehicle edge computing network for resource trading, data storage, and data sharing, and to defend against malicious behaviors of vehicles. Blockchain was used to construct an attribute-based encryption scheme for secure storage and sharing of electronic medical records in [86]. The authors of [87] designed a blockchain-enabled arbitrable remote data auditing scheme to provide reliable network storage services. To deal with the privacy issues in content-centric mobile networks, the study in [88] proposed a secure and efficient blockchain-inspired encrypted cloud storage solution.

The dense deployment of 6G networks will cause serious interference problems, so the use of blockchain for interference management is also a very important topic. The work in [89] described a greedy distributed algorithm, using the blockchain currency mechanism and coordination protocol. This algorithm can realize the optimal information distribution achieved by the traditional central controller before, and eliminate the interference between users. The authors of [90] analyzed the interference problem between transaction nodes in the blockchain-based IoT network, and derived the probability density function of the signal to interference plus noise ratio between IoT nodes and full nodes. The blockchain-based full node deployment solution can ensure a high transaction success rate and overall communication throughput, and protect the IoT network from security threats. In the blockchain-based femtocell network, to avoid excessive interference from femtocell users to the macro base station (MBS), the MBS set a price for the interference generated by the femtocell user in [91]. Femtocell users determined their transmission power and payment fees according to the modeled Stackelberg game. Blockchain enabled the femtocell network to reliably make payments without the involvement of intermediaries.

IoT Smart Applications: Blockchain has also been introduced into many IoT smart application systems, such as smart healthcare [92]–[94], smart transportation [95]–[97], smart grid [98]–[100], UAV [101]–[103], and so on. For example, the authors of [92] described a blockchain-energized patient-centric electronic medical record management architecture, and completed the prototype implementation of this architecture on the Hyperledger platform. The work in [93] proposed a mobile edge computing (MEC)- and blockchain-based distributed healthcare architecture for medical data offloading and data sharing. In the hospital network, the traditional centralized patient identity authentication method may cause problems such as long time and high cost. To resolve these problems, the authors of [94] designed a distributed patient authentication method using blockchain. A blockchain-enabled electricity trading scheme between vehicles was proposed in [95]. To alleviate the problem of incomplete information sharing, the Bayesian game was also used to price electricity. The study of [96] delineated a blockchain storage system, which supports incremental data updates of vehicles. This system used multiple technologies such as data partitioning, smart contracts, and redundant backups. To deal with the security threats of the Internet of Vehicles, [97] considered a blockchain-assisted certificateless key agreement protocol, which has high security and low communication and computing costs.

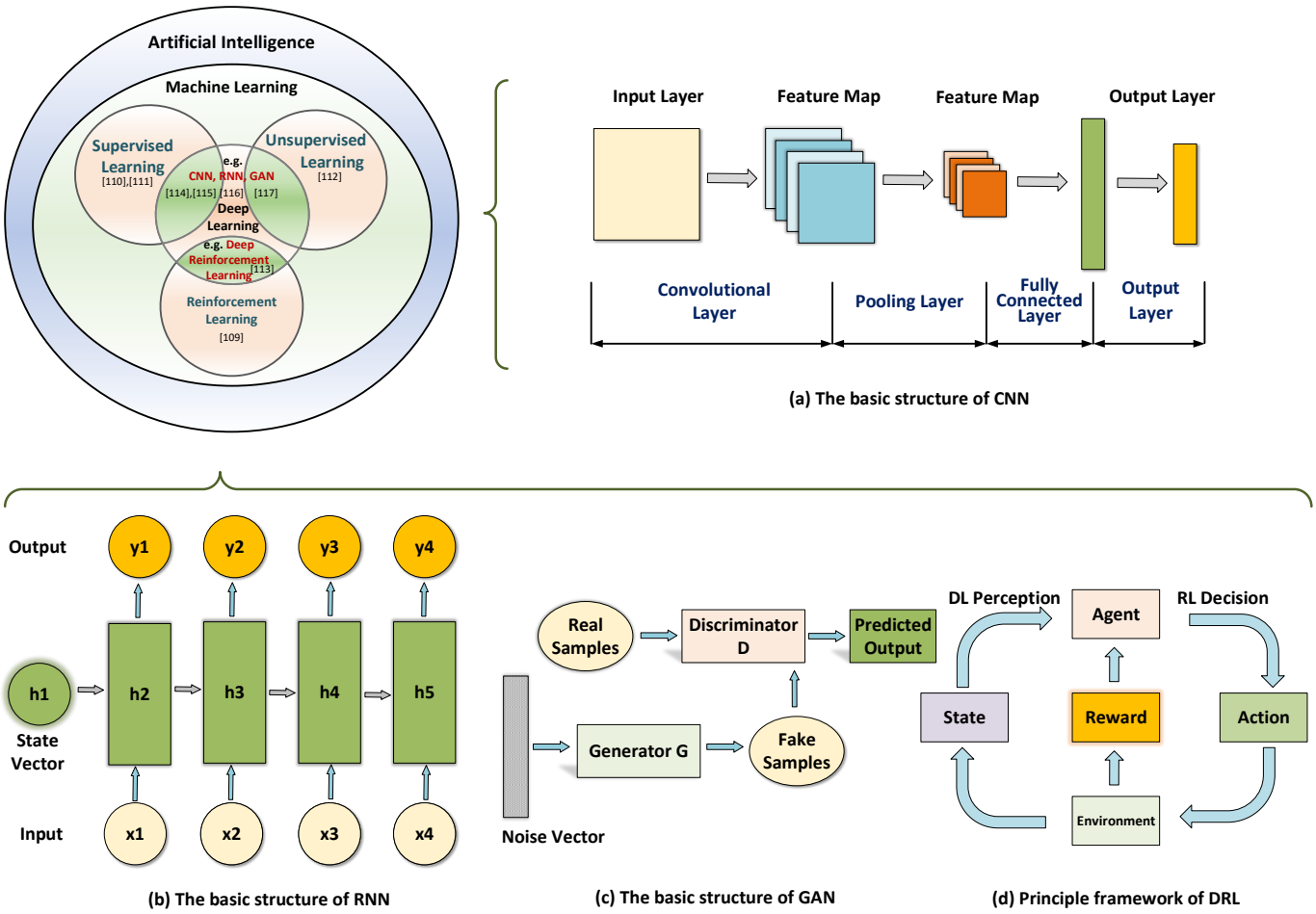

Fig. 3. Classification of AI.

The integration of blockchain into smart grid and UAV is also a hot topic. In the smart grid system based on edge computing, to realize the private and secure communication between grid terminals and edge servers, the work of [98] introduced a blockchain-enabled anonymous authentication and key agreement protocol. In the IoT-supported smart grid system, the data of smart meters can be safely transmitted to service providers through the private blockchain-based access control protocol proposed in [99]. The work in [100] introduced a blockchain-empowered security demand response management scheme, which processes energy transaction requests generated in the smart grid system. The authors of [101] proposed a blockchain-energized multi-party authentication scheme, which can provide secure point-to-point wireless communication and reliable group communication for UAV networks. Under the heterogeneous UAV flight ad hoc network, the study of [102] drew up a blockchain-based distributed key management scheme, which includes four modules: cluster key distribution, key updating, cluster UAV migration, and malicious UAV revocation. In order to solve the security and privacy issues faced by energy micro-transactions, [103] introduced a distributed and secure UAV-assisted radio transmission architecture, which utilizes the directed acyclic graph and consortium blockchain.

B. An Overview of AI

1) Concept of AI: Nowadays, AI has become a field with numerous practical applications and active research topics, and is booming [104]. It is difficult to give AI a scientific definition as rigorous as a mathematical one. Until now, "what is AI ?" is still a debated issue in academia, and there is no unanimously accepted statement. Professor N. J. Nisson of Stanford University's AI Research Center believes that "AI is the science of knowledge, that is, how to express knowledge, how to acquire knowledge, and how to use knowledge" [105]. Professor P. H. Winston of the Massachusetts Institute of Technology holds that "AI is the study of how to make computers do intelligent jobs that only humans could do in the past" [106]. From the perspective of knowledge engineering, Professor E. A. Feigenbaum of Stanford University considers that "AI is a knowledge information processing system" [107]. In a word, AI is a comprehensive discipline, which integrates many disciplines such as computer science, logic, biology, psychology, philosophy, etc. AI has achieved remarkable results in applications such as speech recognition, image processing, natural language processing, automatic theorem proving, and intelligent robots [108], [109].

In the early days of AI, problems that were very difficult for human intelligence but relatively simple for computers

were dealt with quickly. For example, some problems can be described by a series of formal mathematical rules. The real challenge for AI lies in solving tasks that are easy for humans to perform but difficult to describe formally, such as recognizing words spoken by people or faces in images. For these problems, human beings can often solve them easily and intuitively. In recent years, most of the major breakthroughs in the field of AI can be summarized as the development and application of ML technology. The relationship between AI and ML is depicted in Fig. 3. ML provides a solution for these relatively intuitive problems. This solution has its own ability to acquire knowledge, that is, the ability to extract patterns from raw data. Further, there is a key approach in ML, which can improve computer systems from experience and data. This approach allows computers to learn from experience and understand the world in terms of a hierarchical concept system, with each concept defined by its relationship to some relatively simple concepts. By allowing computers to acquire knowledge from experience, human beings can avoid formally specifying all the knowledge they need. Hierarchical concepts let computers construct simpler concepts to learn complex concepts. Drawing a diagram representing how these concepts build on top of each other, we obtain a 'deep' (many layers) diagram. For this reason, we call this approach as deep learning (DL) [109], [110]. ML can build AI systems running in complex real-world environments. DL is a specific type of ML with great power and flexibility. In DL, the big world can be described as a nested hierarchical concept system. This hierarchical concept system refers to the definition of complex concepts by the connection between simpler concepts, and the generalization from general abstraction to high-level abstraction.

2) Characteristics of AI: In this subsection, we will discuss some important characteristics of AI, including data driving, uncertainty, environmental perception, and scalability.

Data Driving: AI gradually completes the technology from artificial knowledge expression to big data-driven knowledge learning. AI rarely needs to rely on manual engineering, so it can easily take advantage of the increment in the amount of available computation and data [111]. For example, a data-driven ML network regards the function to be implemented as an unknown black box, replaces it with an ML network, and then relies on a large amount of training data to complete the training from input to output.

Uncertainty: There is a lot of uncertainty since AI has some similarities or differences compared with any other discipline such as mathematics, physics, cognitive, and behavioral psychology. Most areas of AI do not develop like traditional methods of mathematics, nor do they align with general models of physics. There will always be connections between AI and cognitive or behavioral psychology, but those connections ignore the mathematical and engineering themes. As a prescience, the framework of AI is not yet complete.

Environmental Perception: The AI system should be able to generate the ability to perceive the external environment with the help of sensors and other devices. AI can receive various information from the environment through hearing, vision, smell, and touch like humans, and generate necessary reactions to external input such as text, voice, expressions, and actions. These reactions even influence environmental or human decision-making. Ideally, an AI system should have certain adaptive characteristics and learning capabilities. That is, AI has a certain ability to adaptively adjust parameters or update optimization models with changes in the environment, data, or tasks.

Scalability: Over time, the computer hardware and software infrastructure for AI technology have improved, and the scale of AI models has grown accordingly. AI has been solving increasingly complex applications with increasing precision. With the development of new learning algorithms and architectures developed for deep neural networks (DNNs), AI is bound to have broader application prospects.

3) Categories of AI: As depicted in Fig. 3, we first introduce the classification of AI. Then, we focus on several important branches of ML in the AI field. According to the classification of learning methods, ML can be divided into: supervised learning, unsupervised learning, and RL. We also discuss some typical network architecture in DL.

Supervised Learning: Supervised learning refers to training on labeled data to predict the type or value of new data [111]. According to the different prediction results, supervised learning can be divided into two categories: classification and regression. In training, an objective function is usually given to measure the error (or distance) between the output and ground truth, and then its internal adjustable weights are modified to reduce the error via gradient descent. To improve the convergence speed and reduce the computational complexity, the stochastic gradient descent (SGD) [112] method is often used in practice. SGD randomly selects a sample to compute the loss and gradient each time. Compared with more complex optimization techniques, this simple process of SGD often finds a good set of weights quickly. The common methods of supervised learning are K-nearest neighbor (KNN), decision tree, and logistic/linear regression.

Unsupervised Learning: Unsupervised learning [113] is to do data mining without labels. One of the important functions of unsupervised learning reflects in clustering, which is simply to classify data according to different features without labels. Typical methods of unsupervised learning include K-means clustering and principal component analysis, etc. An important premise of K-means clustering is that the difference between data can be measured by Euclidean distance. If it cannot be measured, it needs to be converted into a usable Euclidean distance measure. Principal component analysis is a statistical method. By using orthogonal transformation, the variables with correlation are changed into variables without correlation. The transformed variables are called principal components. The basic idea is to replace the initially correlated indicators with a set of independent comprehensive indicators.

Reinforcement Learning: RL [109], [114] is about obtaining rewards by interacting with the environment. Moreover, RL judges the quality of actions by the level of rewards and then learns the optimal strategy. Agent perceives the state information in the environment, searches for strategies, and selects the optimal action. This causes a state change and a return value to update the evaluation function. After

TABLE V. Comparison of typical ML algorithms.

Learning Algorithms	Characteristics	Typical Methods
Supervised Learning	Predict the type or value of new data by training with labeled data.	KNN, Decision tree, Logistic/Linear regression
Unsupervised Learning	Do data mining when the data has no labels.	K-means clustering, Principal component analysis
Reinforcement Learning	A model consists of an Agent, which interacts with the environment. The optimal policy is learned through a trial-and-error mechanism to maximize long-term cumulative returns.	DRL

completing a learning process, enter the next round of learning and training. The learning process is repeated cyclically and iteratively, until the conditions of stop rule are met, and then the learning is terminated. For large-scale station-action pair, deep reinforcement learning (DRL) [115] is an end-to-end perception and control system with strong generality. The principle framework of DRL is represented in Fig. 3(d). The DRL learning process can be described as: (1) At each moment, the agent interacts with the environment to get a high-dimensional state, and uses DL to perceive the state to obtain a specific state feature representation; (2) The agent evaluates the value function of each action based on the expected return, and maps the current state to the corresponding action through a certain policy; (3) The environment reacts to this action and gets the next state. Through the continuous cycle of the above process, the optimal policy to achieve the goal can be finally obtained.

We summarize the characteristics and typical structures of several algorithms of ML discussed above as shown in the following TABLE V.

Basic Network Architecture of DL: The basic network structure is the convolutional neural network (CNN) [116], [117], which consists of an input layer, multiple convolutional layers, multiple pooling layers, a fully connected layer, and an output layer, as shown in Fig. 3(a). The convolutional layer and the pooling layer are set alternately. In the convolutional layer, each neuron of the convolutional kernel is locally connected to its input, and weighted and summed with the local input through the corresponding connection weight. Then, the bias value is added to get the output value of the neuron. Because this process is equivalent to the convolution process, it is called CNN. CNN is easier to train and popularize than the fully connected network between adjacent layers, and is widely adopted in the field of computer vision.

The recurrent neural network (RNN) [118] can process one element of the input sequence at a time. As shown in Fig. 3(b), the RNN maintains a "state vector" in its hidden units, which implicitly contains historical information for all past elements in the sequence. The output depends not only on the current input, but also on the information available in past moments or information available in future moments. With such special structure, RNNs are capable of providing memory for neural networks.

Additionally, the generative adversarial network (GAN) [119] is also a typical DL network that aims to learn a model capable of generating fake samples on real-distributed datasets. The basic structure of GAN is shown in Fig. 3(c), which includes a generator G and a discriminator D. Both the generator and the discriminator can be implemented by DL networks. The discriminator is used to distinguish the fake samples generated by the generator from the real samples of the actual dataset. The task of the generator is to generate sample data such that the discriminator cannot distinguish between real samples and fake samples. When the generator produces samples that the discriminator cannot distinguish from the real samples, training is balanced. The applications of GAN in basic fields such as image generation, image translation, and speech images are very rich.

4) AI for Wireless Communications: In this section, we mainly describe the latest research progress of AI applied to 6G wireless communications. The combination of AI and 6G networks mainly contains in physical layer and upper layer.

AI for Physical Layer: The main contents involve channel estimation [120]–[124], signal detection [125]–[129], channel state information (CSI) feedback and reconstruction [130]–[134], channel decoding [135]–[139], and end-to-end wireless communications [140]–[144]. In massive multiple-input multiple-output (MIMO) beam mmWave scenarios, channel estimation is extremely challenging, especially in scenarios where antenna arrays are dense and receivers are equipped with limited radio frequency (RF) links. The work of [120] pioneered channel estimation by using the DL-based method in wireless energy transfer systems. In [120], the authors developed an autoencoder-based channel estimation scheme, where the encoder is used to design pilots and the decoder is utilized to estimate the channel. The authors of [121] proposed a DL-based super-resolution channel estimation scheme in millimeter-wave massive MIMO systems. This scheme utilizes DNN for beam direction-of-arrival estimation. In contrast, there are some other DL-based channel estimation schemes that combine traditional algorithms with certain performance guarantees with DL algorithms. Reference [122] designed a learned denoising-based approximate message passing (LDAMP) network. The LDAMP network takes the channel matrix as a two-dimensional image as input, and integrates denoising CNN into the iterative signal reconstruction algorithm for channel estimation. To improve the performance of sparse signal recovery, the authors of [123] proposed a learned approximate message passing (LAMP) network. LAMP directly expands the iterations of the AMP algorithm into the corresponding hierarchical network structure, whose linear transformation coefficients and nonlinear shrinkage parameters are jointly optimized by DNN. Furthermore, starting from the basic structure of the minimum mean square error (MMSE) algorithm, the work of [124] developed a DL-based channel estimator, in which the estimated channel vector

consists of conditional Gaussian random variables with random covariance matrices. To reduce the complexity of channel estimation, an MMSE-based CNN network is proposed to compensate for the error in [124].

The authors in [125] applied DNN to tackle the problem of signal detection in orthogonal frequency division multiplexing (FDM) systems. Different from traditional wireless communication, [125] regarded channel estimation and signal detection as a whole, and directly uses DNN to realize the mapping from the received signal to the original signal bits. The work in [126] investigated the signal reconstruction problem of the MIMO system, and proposed a signal detection algorithm entitled Detection Network (DetNet). DetNet is based on the maximum likelihood method by adding the gradient descent algorithm to generate a DL network. Based on the orthogonal AMP (OAMP) iterative algorithm combined with the DL network, OAMP-Net was proposed in [127]. The purpose of OAMP-Net is to add adjustable training parameters on the basis of the original algorithm to further improve the signal detection performance of the existing algorithm. With the advantage of fewer trainable parameters, the model-driven detection network [128] was designed to improve detection performance by expanding a specific iterative detector and adding some trainable parameters. In addition, an adaptive signal detection method named JC-Net for massive MIMO systems was proposed in [129]. JC-Net has a foundation for the traditional Jacobi detector, adding trainable parameters to improve the convergence speed and perform corresponding soft projection. In FDM networks, the BS requires to attain downlink CSI feedback to perform precoding and achieve performance gains. However, there are many configured antennas in massive MIMO systems, so the feedback overhead of the complete CSI becomes extremely huge. The work of [130] presented a CNN-based CSI perception and recovery mechanism named CsiNet. Since then, DL-based CSI compression techniques have attracted a lot of attention [131]–[134]. On the basis of [130], the authors of [131] provided a real-time long short-term memory (LSTM)-based CSI feedback architecture entitled CsiNet-LSTM, which employs temporal correlation to improve the feedback accuracy of time-varying channels. CsiNet-LSTM can accomplish a trade-off between compression ratio, CSI reconstruction quality, and complexity. On the basis of the high correlation of amplitudes between bidirectional channels in the delay domain, DualNet was proposed in [132] to use uplink amplitude information to help reconstruct downlink channel amplitudes. The CSI feedback and reconstruction algorithms in [130]–[132] rely on a large amount of data for offline training, and the network complexity is high. The work of [133] focused on the complexity of the neural network. The experimental results in [134] demonstrated that the DL-based channel feedback framework can reduce the air time overhead by an average of 73% and improve the throughput by about 69% compared with the 802.11 feedback protocol.

The authors in [135] developed a DNN-based channel decoding method. This paper draws two conclusions about the application of DL to channel decoding: 1) Structured codes such as polar codes are easier to learn than random codes; 2) For structured codes, DL networks can decode untrained codewords. However, this proposed method is neither suitable for random codes nor codewords with long code lengths, and has great limitations. On the basis of the traditional polar code iterative decoding algorithm, the work of [136] presented a DL polar code decoding network that separates sub-blocks. The decoding algorithm in [136] is a highly parallel decoding algorithm. Compared with the decoding algorithm in [135], the algorithm of [136] significantly reduced the number of training times and the complexity of the network structure under the condition of comparable performance. Reference [137] conducted an iterative channel decoding algorithm: belief propagation (BP)-CNN. The algorithm concatenates the CNN with the standard BP decoder to estimate information bits in a noisy environment. For high density parity check (HDPC) codes, the performance of the BP algorithm is relatively poor. Nachmani et al. successively proposed the BP-DNN algorithm [138] and the BP-RNN algorithm [139], which combined the DNN and RNN networks with BP algorithms to improve the performance of BP algorithms applied to HDPC. Reference [140] put forward an end-to-end wireless communication system model, which explains the feasibility of replacing the processing module of the physical layer by DNN. The authors of [141] provided a differentiable channel computational model, which can be used for supervised autoencoder training. Since then, many non-modeled methods [142], [143] have been developed based on synchronization-around methods, none of which require any channel knowledge and can be directly executed on real hardware. In [144], the authors treated the communication system as an end-to-end DRL autoencoder. This technique does not require any information about the actual channel model.

AI for Upper Layer: In recent years, AI has been introduced into the upper layers of wireless communications to tackle various problems, thereby enabling near-optimal network performance. For example, since artificial neural networks have the approximation characteristics of universal functions, [145] and [146] adopted a data-driven approach to allow the training model to autonomously learn user access and power allocation strategies. Supervised learning requires predicting the labels of the training data, resulting in excessive data preprocessing burden. So, from the perspective of unsupervised learning, the authors of [147] leveraged a feed-forward neural network to autonomously learn the optimal power allocation. Bypassing channel estimation, the work in [148] efficiently scheduled interfering links based only on the geographic locations of transmitters and receivers via DL algorithms. In multi-cell systems, reference [149] approximated optimal link scheduling and power control through DNNs. Specifically, a matching link schedule was estimated using the deep Q-network, and then power was allocated to the corresponding link schedule.

As a data-driven ML method, DRL can directly learn dynamic environmental laws and obtain optimal decisions. Therefore, DRL can endow the network with the ability to self-optimize management according to the dynamic environment, making intelligent communication possible. Next, we focus on the application of DRL in the upper layer of wireless

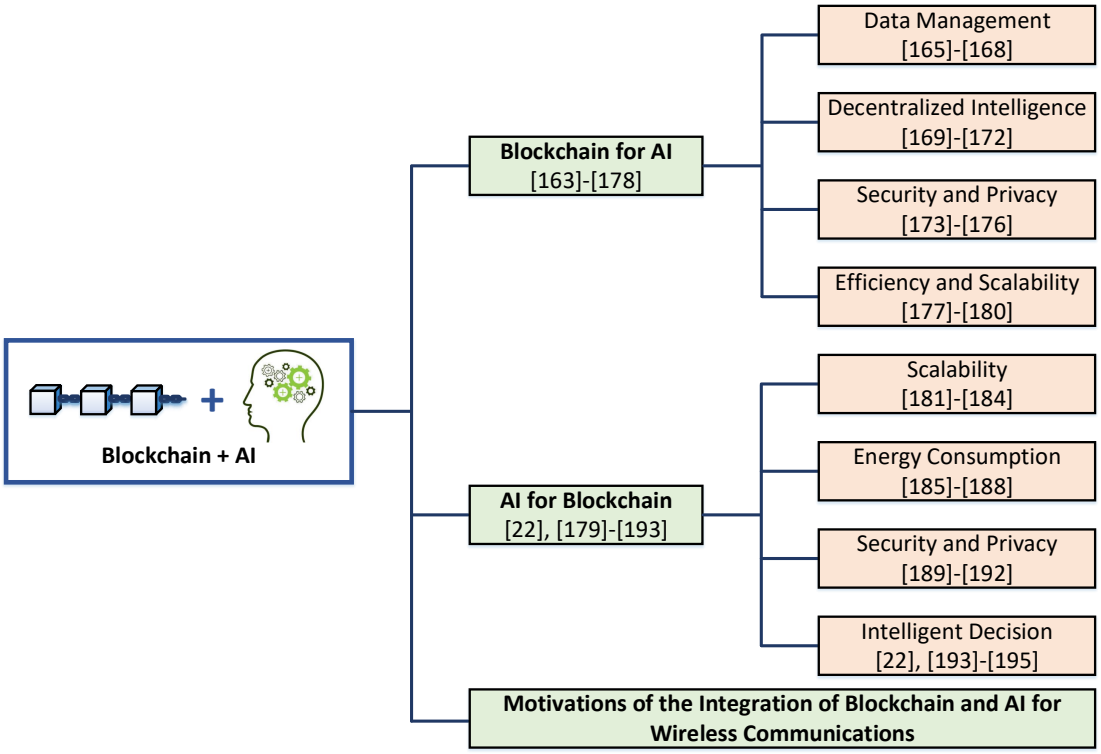

Fig. 4. Taxonomy of the integration of blockchain and AI.

communications. For example, reference [150] considered a power control problem in cognitive radio. Here, to improve the spectrum usage rate, secondary users performed communication by occupying the spectrum of primary users. To satisfy the service quality of primary and secondary users, the author of [150] proposed a DRL-enabled power control scheme. Reference [150] was aimed at the single-user power control problem, which cannot be applied to multi-user scenarios. To this end, the work of [151] discussed the problem of multi-user power resource allocation in cellular networks, where the goal was to maximize the weighted sum-rate of the entire network. Moreover, [152] extended [151] to multi-user device-to-device (D2D) communication scenarios. The authors of [153] used DRL to analyze the user's data request, and replaced the file in the cache as per the user's request rule. A DRL-empowered computing resource allocation scheme was presented in [154]. In this scheme, IoT devices adopted DRL algorithms to determine the power of each computing task to be executed locally, and a power of 0 meant that the computing task is executed in MEC servers. In addition, references [155]–[158] also successfully employed DRL algorithms in the joint optimization problem of caching and computing resources, indicating that DRL has a strong application prospect in managing network resources.

In [159], DRL was used to realize intelligent horizontal handover between BSs. The work of [160] further attempted to combine access control and resource allocation, and considered the DRL algorithm to solve the joint optimization problem of user access and channel allocation in multi-layer BS cellular networks. As the size of the network escalates, the probability of network failure also increases. The authors of [161] attempted to apply DRL to network fault self-healing. To enhance energy efficiency and reduce costs, wireless networks need to dynamically turn BSs on and off according to user traffic demands. In view of the dynamic randomness of traffic demands, [162] proposed to apply DL to analyze and predict the traffic of each BS, and then used DRL to control the switch of BSs according to the predicted traffic. In addition to [162], the work of [163] also introduced a DRL-supported intelligent sleep strategy for BSs to reduce network energy consumption. In sparsely populated areas, UAVs can be leveraged as air BSs to serve terrestrial communication terminals. Considering the coverage limitation of the UAV and the moving variation of the air-to-ground channel, the authors in [164] discussed to use DRL algorithms with deep Q-learning for deployment planning of air BSs.

C. Integration of Blockchain and AI

In recent years, the frontier technologies of blockchain and AI have aroused widespread attention and in-depth research in academia and industry. Blockchain technology has the characteristics of decentralization, anonymity, openness and transparency, and immutability. However, the blockchain needs to be improved urgently in terms of scalability, energy consumption, and security. As a powerful analysis and decision-making tool, AI can predict and analyze data in real-time scenarios and make optimal decisions. Nevertheless, the centralized structure of AI and its demand for security and credibility have greatly limited the wide application of AI. Therefore, there is complementary potential for the combination of blockchain

and AI. As shown in Fig. 4, we respectively elaborate and analyze from the two aspects of blockchain for AI and AI for blockchain.

1) Blockchain for AI: From the perspective of AI technology, blockchain as a trusted platform can create a secure, immutable, and distributed system for AI. In this secure system, no third-party participation and management are required, users trust each other and share data. Accordingly, based on the huge and reliable data set, the accuracy of the agent's decision-making is improved. We introduce blockchain-driven AI from some aspects below, including data management [165]–[168], decentralized intelligence [169]–[172], security and privacy [173]–[176], and efficiency and scalability [177]–[180].

Data Management: The massive amount of AI data lacks a consolidated and efficient sharing mechanism and management method. The poor maintainability of open-source data sets leads to uneven data quality, and the data is not centralized and unified. The distributed database of blockchain efficiently collects, shares, and stores the data of each node, so that every participant on the network can access the data. This can provide AI with broader data access and more efficient data monetization mechanisms. For instance, to make the updating of AI models more efficient, based on blockchain technology, the authors of [165] proposed the novel configurable distributed AI framework, where participants collaborated to construct datasets and used smart contracts to host continuously updated AI models. In order to break the data barriers between different mobile operators, [166] designed a blockchain-empowered data sharing framework and a Hyperledger-based prototype system. This system utilized smart contract-based monitoring and fine-grained data access control to create a safe and reliable environment for data sharing. Using blockchain to help AI manage trusted data, the work in [167] introduced a secure large-scale Internet architecture called SecNet. The SecNet can realize secure data storage, computing, and sharing, and enhance AI with a large number of data sources. The work in [168] demonstrated a blockchain-enabled joint framework for efficient data acquisition and secure sharing. This proposed framework used DRL to achieve the maximum amount of collected data, and leveraged the Ethereum blockchain technology to ensure the security and reliability of data sharing.

Decentralized Intelligence: Through AI algorithms, learning results and models can be obtained from massive data. Due to the distribution of IoT devices or edge computing devices and the data heterogeneity, the cooperation of multiple devices is required to complete complex model training tasks. That is, different devices need to share data for data analysis and prediction. Local learning models can also be shared across devices and then aggregated. Blockchain technology can guarantee that AI completes the interaction of data or models between devices in the decentralized environment. To realize asynchronous cooperative computing among untrusted nodes, the work in [169] developed a decentralized, privacy-preserving, and secure computing paradigm, which adopted various technical means such as blockchain, decentralized learning, and homomorphic encryption. A blockchain-assisted distributed secure multi-party learning architecture was proposed in [170]. Specifically, the authors formulated two types of Byzantine attacks, as well as elaborated "off-chain" and "on-chain" mining schemes. In response to the single point of failure problem of federated learning (FL), the work in [171] provided a decentralized FL scheme entitled ChainFL. The ChainFL utilized blockchain to delegate the responsibility of storing and aggregating models to nodes on the network without requiring any central server. In edge AI-supported IoT networks, to break knowledge silos, the authors of [172] proposed a P2P knowledge payment sharing architecture, which made use of the knowledge consortium blockchain to ensure that knowledge management and market transactions are safe and efficient. This knowledge consortium blockchain included the new encrypted currency knowledge currency, smart contracts, and new transaction consensus mechanism proof.

Security and Privacy: For AI technology, the greater amount of having data, the higher accuracy of its training model. However, if a small part of this data has security issues, the validity of the data will affect the system's decision-making accordingly and thus the overall performance of the system. Fortunately, blockchain has many technologies such as anonymity, immutability, interface access control, and signature authentication and authorization to ensure the security and privacy of transaction data, and to provide quality assurance for the data required for AI model training. The work in [173] proposed a blockchain-authorized edge intelligence system, which assured the security, privacy, latency, and efficiency of edge device data. Here, the public blockchain guaranteed the security and privacy of data of edge devices, while the private blockchain ensured secure communication between edge intelligent servers. The authors of [174] demonstrated a distributed DL architecture named DeepChain. DeepChain utilized the value-driven incentive mechanism of blockchain to encourage parties to collaborate in DL model training and share the obtained local gradients. Meanwhile, DeepChain guaranteed the privacy of local gradients for each participant and provided auditability for the entire training process. To prevent malicious attacks on AI models, the work in [175] introduced Biscotti, which was a fully decentralized P2P large-scale multi-party learning scheme. The Biscotti adopted blockchain and cryptographic primitives to coordinate the privacy-preserving ML process among peer nodes. The authors of [176] presented the blockchain-assisted asynchronous FL (BAFL) architecture, where the blockchain ensured that model data cannot be tampered with, and assured decentralized and secure data storage, and asynchronous learning accelerates global aggregation. The proposed BAFL guaranteed that each device uploaded the local model whenever the global aggregation can converge the global model faster.

Efficiency and Scalability: When using AI techniques, such as DL, it is difficult for people to understand what is in the black box and explain the decisions made by AI systems, so AI cannot be verified or trusted. Furthermore, without appropriate incentive mechanisms, various parties may be reluctant to participate in data training. The above-mentioned problems will reduce the efficiency and scalability of AI systems. Blockchain can track every link in the data processing and decision-making chain for explainable AI. Appropriate

incentive mechanisms can also be introduced from blockchain. The transparent and cost-effective incentive mechanism design can be implemented, which will greatly improve the enthusiasm of all parties in AI systems to take part in the training. A blockchain-based framework for more trustworthy and explainable AI was presented in [177]. This framework leveraged smart contracts to record and manage interactions, as well as provided consensus for trusted oracles. The proposed framework also addressed decentralized storage, registry, and reputation supporting services. To obtain better trusted AI, the authors of [178] designed a blockchain-enabled FL system, which used the blockchain to track the source information of the trained model. Aiming at the incentive mechanism problem of FL, the work in [179] presented a reputation-based miner selection scheme, and designed an efficient incentive mechanism by adopting a multi-weight subjective logic model to evaluate the user's credit. The proposed scheme also leveraged the consortium blockchain to achieve secure reputation management for miners in a decentralized manner. In [180], the authors described the FLChain framework based on trust and incentive. The FLChain saved miners' information and verifiable training details for public audits. The incentive mechanism of the FLChain encouraged honest and trustworthy miners. Otherwise, malicious nodes will be punished, so as to maintain a healthy and reliable public platform.

2) AI for Blockchain: From the perspective of blockchain technology, its scalability and system energy consumption can be optimized through AI algorithms. Using AI algorithms in blockchain networks, security vulnerabilities brought about by the implementation of smart contracts and consensus mechanisms can be identified and detected. We will represent AI-driven blockchain from four aspects below, including scalability [181]–[184], energy consumption [185]–[188], security and privacy [189]–[192], and intelligent decision [22], [193]–[195].

Scalability: Currently, as the number of transactions increasing significantly, scalability is the biggest barrier to the widespread application of blockchain technology. In blockchain systems, the core of scalability is to tackle the problems of transaction throughput and transaction speed. Due to the characteristics of decentralization and network-wide broadcasting, each node on the blockchain will record transactions generated by the entire network, leading to low efficiency. AI can introduce DRL or data sharding technology to propose new solutions to blockchain scalability issues and improve system efficiency. In [181], through the DRL algorithm, the agent dynamically selected different consensus algorithms and block production nodes, and adjusted the block size and time interval. The agent found optimal parameters to improve the scalability, while ensuring the decentralization, latency, and security of blockchain networks. To obtain better throughput, the authors of [182] adopted the deep Q network algorithm to dynamically adjust the block size, time interval, and the number of shards to seek the optimal related parameters, while meeting the security of the system. The work in [183] studied a DRL-enabled adaptive blockchain scheme, which improved scalability and met the needs of different users. Specifically, according to the service quality requirements of users, the DRL algorithm selected the most suitable consensus protocol for blockchain systems. To overcome the limitations of existing blockchain static sharding, [184] introduced a DRL-based dynamic sharding blockchain framework called SkyChain. In the dynamic environment of blockchain systems, this presented SkyChain can dynamically adjust the resharding interval, number of shards, and block size in order to maintain a long-term balance between performance and security.

Energy Consumption: Blockchain mining requires a large amount of computing power and electricity resources. At present, Bitcoin consumes about 2.55 billion watts of electricity every year, almost the same as the annual electricity consumption of some small countries. If the energy consumption problem cannot be solved well, the value of the blockchain itself will be diluted. To avoid excessive consumption of computing resources and energy resources in this mining process, AI algorithms can understand the blockchain network process and architecture, and explore a more effective consensus mechanism, which can make transactions on blockchain networks execute faster.

A Proof-of-Learning consensus protocol was formed by combining ML algorithms in [185]. This Proof-of-Learning protocol performed model training through ML of given tasks. Then, the ranking was based on the minimum loss function value. Finally, the optimal model parameters were selected and verified by other mining nodes to achieve distributed consensus. Through combining DL algorithms, the work of [186] proposed a Proof-of-Deep-Learning consensus protocol, which forced the agent to conduct DL model training, and proposed the training model as a proof of effectiveness. Only when an appropriate DL model was generated, can miners reach the consensus and generate new blocks. In response to the energy consumption problem in blockchain networks, the authors of [187] introduced a Proof-of-Useful-Work energy-saving consensus protocol. The proposed protocol required training a DL model during the mining process, and mining new blocks only when the performance of the training model exceeded a given threshold. The work in [188] demonstrated an AI-enabled node selection algorithm that exploited the nearly complementary information of each node and relied on a specially designed CNN to reach consensus. In order to ensure the decentralization and security of the network, dynamic thresholds were used to obtain super nodes and random nodes.

Security and Privacy: The decentralized power of blockchain may be at risk of abuse, especially since the smart contracts and consensus mechanisms in blockchain technology are vulnerable to malicious network attacks or tampering. As more and more personal data is stored in blockchain systems, data privacy protection becomes critical. We employ AI-assisted methods to identify and detect security vulnerabilities, greatly improving the security and privacy of blockchains. As an illustration, the work of [189] learned by extracting relevant features from user accounts and operation codes of a large number of smart contracts, and used the ML algorithm XGBoost to detect whether there is a potential Ponzi scheme in the smart contract. Ponzi scheme is a classic investment fraud, and it also has a blockchain-based form. The essence

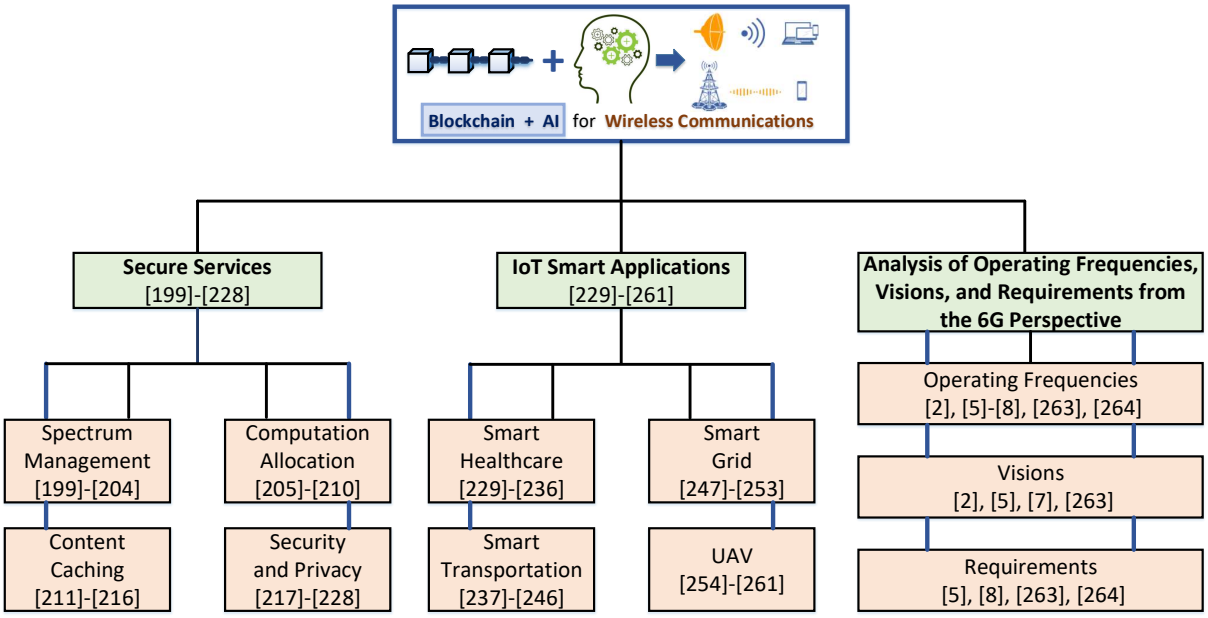

Fig. 5. Taxonomy of the integration of blockchain and AI for wireless communications.

of Ponzi is that the investment of new investors is the return of old investors. On the Hyperledger Fabric blockchain platform and with a relatively low tolerance for malicious activities, the authors of [190] designed an external detection algorithm based on supervised ML before the consensus protocol as the consensus of the previous step. This proposed detection algorithm verified the new data compatibility, and discarded suspicious data to improve the network's fault tolerance for the second-step consensus. In blockchain-based systems, a data fusion scheme based on collaborative clustering features was represented in [191]. The data fusion scheme applied AI algorithms to train and analyze data clusters to detect abnormal intrusion behaviors. To effectively detect abnormal behavior of blockchain systems, the work in [192] proposed an encoder-decoder-based DL model, which was an unsupervised model trained with aggregated information extracted by monitoring blockchain transactions.

Intelligent Decision: With the rise of blockchain technology, more people turn to study blockchain-empowered application projects. Investors want to predict some important behaviors of blockchain systems, such as cryptocurrency prices, transaction confirmation times, and blockchain forks. We consider embedding AI algorithms into blockchain systems and allowing AI to optimize or make decisions for the entire system, which is more conducive to investors making correct policies. In [22], without knowing the details of the blockchain network model, a multi-dimensional RL algorithm was proposed to solve the mining problem with the Markov decision process. The designed algorithm can obtain the near-optimal mining strategy solution in the time-varying blockchain network. In both short-term (1 day and 7 days) and medium-term (30 days and 90 days) time periods, the authors of [193] employed classification and regression models of ML to predict the trend of Bitcoin price. The results showed that the proposed four types of ML models predicted the actual Bitcoin price with a very low error rate. Applying ML, the work in [194] demonstrated an Ethereum prediction model, which can predict transaction execution times in Ethereum systems. The transaction execution time refers to the time frame within which a miner node accepts and includes a transaction in a block. To reduce the huge risk and cost brought by the fork, the work of [195] adopted an ML method to predict the blockchain fork, and compared the prediction accuracy of the fork by four well-known ML methods, namely K Near Neighbor, Naive Bayes, Decision Tree, and Multilayer Perceptron.

3) Motivations of the Integration of Blockchain and AI for Wireless Communications: Blockchain can establish a secure and decentralized resource sharing environment. AI can solve some problems with uncertain, time-varying, and complex characteristics. As shown in TABLE VI, we summarize and compare blockchain for 5G/6G, AI for 5G/6G, blockchain for AI, and AI for blockchain. We conduct a critical and original discussion of these existing solutions, highlighting the advantages, disadvantages, and main findings of various solutions. Although blockchain and AI are promising technologies to be applied in 6G networks, there are still many challenges and unresolved problems. Both blockchain and AI have attracted significant attention recently. The combination of these two technologies may further improve the performance of 6G networks. In the first place, to more systematically understand the integration and application of blockchain and AI technologies for 6G networks, we summarize the benefits of blockchain for AI and the benefits of AI for blockchain, respectively. For details, please refer to the above subsections: Section II-C1 and Section II-C2. Then, we briefly describe the benefits that fusing blockchain and AI can bring to 6G networks.

On the one hand, blockchain can improve AI in terms of data management, decentralized intelligence, security and privacy, and efficiency and scalability. Firstly, blockchain collects, shares, and stores data for AI, so that every participant

TABLE VI. Comparison of existing solutions.

Solution	Advantages	Disadvantages	Main Findings
Blockchain for 5G/6G [57]-[97]	The integration of blockchain and 6G will provide a strong security guarantee for the construction of a safe and credible communication ecosystem.	When there are massive blockchain applications and nodes communicating with each other, the 6G network may face uncertain local network congestion.	While blockchain poses challenges to the stability of 6G networks, it can also provide protection for the security of 6G networks and increase the value of data.
AI for 5G/6G [112]-[156]	AI enhances the performance of a specific module of 6G systems, including improving accuracy and reducing complexity, and also integrates multiple communication modules to break the existing modular communication architecture.	Inefficient data management schemes and high overhead of information exchange among communication participants are key bottlenecks. Data security and privacy issues are receiving increasing attention.	6G network realizes interconnected intelligence by supporting AI functions, and adopts a centralized network architecture, which is vulnerable to hacker attacks.
Blockchain for AI [157]-[172]	Blockchain can conduct a secure, immutable, and distributed system for AI. Users trust each other and share data. The performance of AI algorithms and decision-making are effectively upgraded.	The execution results of smart contracts in blockchains are often deterministic. While, the execution results of AI are usually uncertain, random, and unpredictable in most cases.	The contradiction between blockchain and AI poses certain challenges for AI embedded in blockchain to optimize the execution decisions.
AI for Blockchain [173]-[187]	AI can enhance the performance of blockchains in terms of scalability, energy consumption, security and privacy, and intelligent decision.	With the explosive growth of data in AI-assisted blockchain systems, the massive unlabeled and unclassified datasets are intractable for AI training.	Using AI algorithms, the scalability and energy consumption issues of blockchain can be mitigated, but AI training also faces challenges.

on the network can access the data. Blockchain-supported methods can provide AI with more efficient data management mechanisms and wider data access. Secondly, blockchain can ensure that AI can complete the collaborative interaction of data or models between devices in a decentralized environment. In addition, blockchain uses its own anonymity, immutability, interface access control, signature authentication and authorization, and other technologies to safeguard the security and privacy of transaction data in the AI system. Finally, blockchain can track every link in the data processing and decision-making chain for explainable AI. Transparent and cost-effective incentive mechanisms can also be designed, which will effectively upgrade the efficiency and scalability of AI systems.

On the other hand, AI can enhance the performance of blockchains in terms of scalability, energy consumption, security and privacy, and intelligent decision. First of all, AI can introduce DRL or data sharding technology, to propose new solutions for blockchain scalability issues and ameliorate system efficiency. Furthermore, in order to avoid the massive resource consumption of blockchain, AI algorithms can dissect the blockchain network process and architecture, as well as explore a more effective AI-based consensus mechanism based on AI, so that transactions on the blockchain can be executed faster. Next, AI-assisted methods are used to identify and detect security vulnerabilities, which remarkably augments the security and privacy of blockchains. Ultimately, we can consider embedding AI algorithms into blockchain systems and letting AI optimize or make decisions for the entire system, which is more conducive to investors making make correct decisions.

According to the above analysis, the amalgamation of blockchain and AI has complementary potential. Blockchain can conduct a secure, immutable, and distributed system for AI technologies. In this system, users trust each other and share data. Based on a huge and reliable data set, the performance of AI algorithms and decision-making can be effectively upgraded. Using AI algorithms, the scalability and energy consumption issues of blockchain can be mitigated, and its security vulnerabilities can also be identified and detected. The integration of AI and blockchain is not only to enhance each other, but also to push and optimize various services and applications for 6G scenarios in the process of mutual promotion. In this case, a reliable, secure, and ultra-low latency network environment can be provided for 6G wireless communications. Consequently, the research on the integration of blockchain and AI is extremely important and worth expecting in 6G networks.

In this section, we have provided a comprehensive overview of the fundamental concepts, characteristics, and categories of blockchain and AI. We have also discussed the classic applications of both technologies in wireless communication systems. Then, we systematically summarized the integration of blockchain and AI from two directions: blockchain-assisted AI and AI-assisted blockchain. Furthermore, we analyzed the advantages of integrating blockchain and AI for wireless communication systems. Through this section, we have gained valuable insights into the opportunities and challenges of leveraging blockchain and AI in wireless communication systems. We have also recognized the importance of considering different integration approaches and identifying suitable use cases to maximize the potential of these technologies. Overall, this section provides a solid foundation for further exploration and analysis of the integration of blockchain and AI in wireless communication systems.

III. Integration of Blockchain and AI for Wireless Communications

For the existing problems of blockchain and AI, the integration of these two technologies can complement each other. Facing the 6G era, the network will meet new application

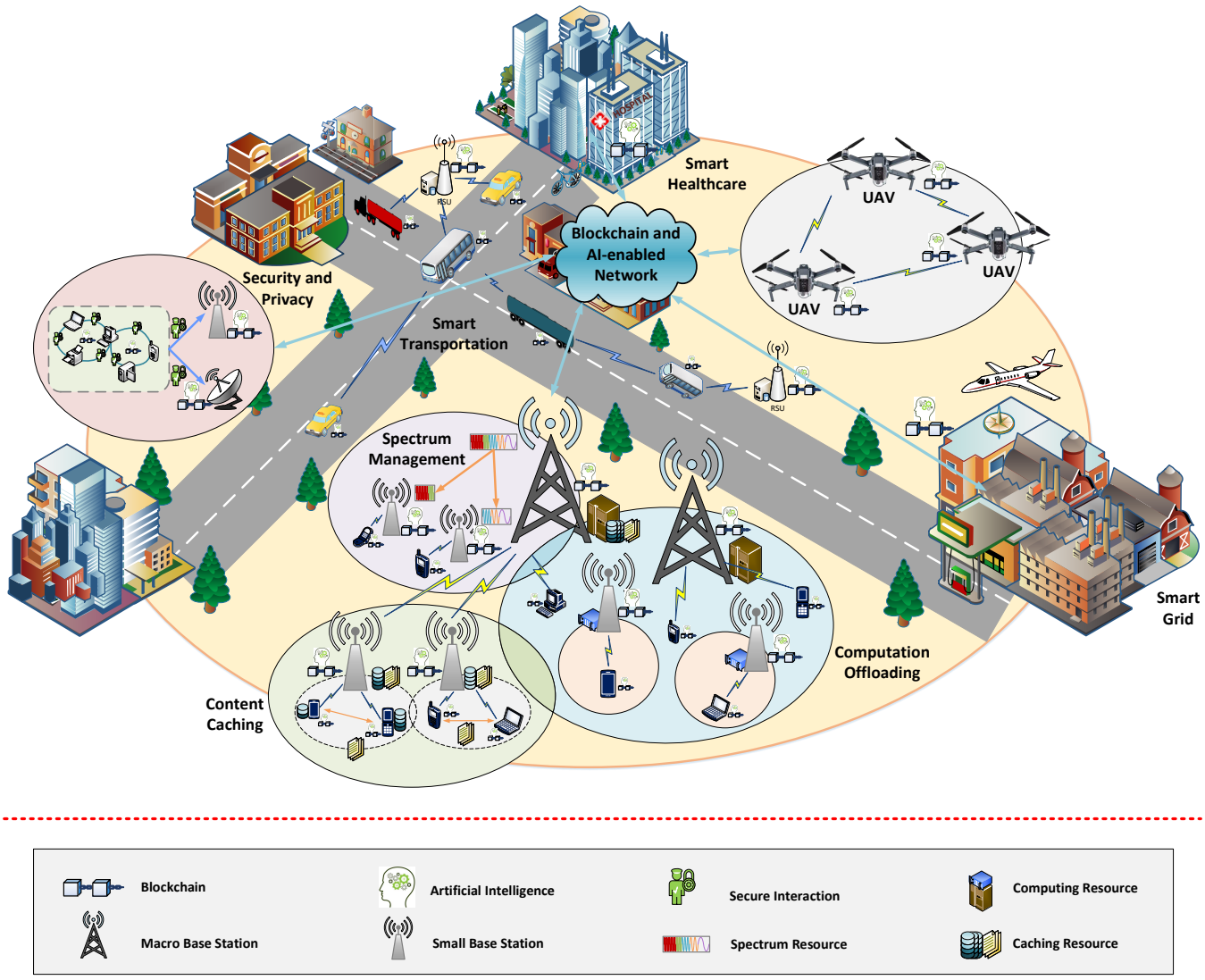

Fig. 6. The convergence of the integration of blockchain and AI for wireless communications.

scenarios and new performance requirements. Diverse applications, communication scenarios, ultra-heterogeneous network connections, and service requirements for extreme performance all put forward higher demands on mobile communication networks [46]. The merger of blockchain and AI can not only play to their respective advantages [196], [197], but also better bring optimization and improvement to various services and applications in 6G networks [47], [48], [198]. In this section, we will discuss broadly the applications of merging blockchain and AI in 6G networks, including 6G secure services [199]–[228] and 6G IoT smart applications [229]–[261] as depicted in Fig. 5. The convergence of the integration of blockchain and AI for wireless communications is illustrated in Fig. 6. Furthermore, we thoroughly discuss operating frequencies, visions, and requirements from the 6G perspective.

A. Secure Services

As mentioned in the previous section, the combination of blockchain and AI can not only promote each other, but also provide better services. In 6G networks, wireless resources such as spectrum, computing, and caching are some of the most concerned services. The development of 6G networks will bring explosive growth of user data, and security and privacy services are also the keys to improving the overall performance. In this subsection, we will focus on some key 6G secure services, where blockchain and AI are simultaneously applied, including spectrum management [199]–[204], computation allocation [205]–[210], content caching [211]–[216], and security and privacy [217]–[228]. TABLE VII presents an analysis of the integration of blockchain and AI for secure services.

1) Spectrum Management: Radio spectrum resources are scarce resources. Spectrum is widely used by various radio technologies and services, resulting in increasing demands for spectrum resources in various industries and fields. Facing ever-increasing demands for radio spectrum, spectrum management has never been more challenging. Given that traditional fixed spectrum allocation strategies lead to inefficient spectrum usage, dynamic spectrum management is

proposed as an encouraging approach to alleviate the spectrum scarcity problem [262]. Blockchain and AI are two promising enabling technologies for solving spectrum management issues. Blockchain can be applied to spectrum auctions, which improves security and decentralization, and reduces spectrum management costs. On the other hand, AI technologies represented by DL and DRL are very powerful and can automatically learn user behavior patterns or further make optimal decisions for users. Through the use of AI, behaviors such as users' mobility and data/computing traffic can be dynamically predicted, so as to optimize the allocation of wireless resources.

In 5G beyond and 6G wireless communications, the authors of [199] designed a blockchain- and AI-supported dynamic resource sharing architecture. The low-cost and low-complexity hierarchical blockchain is an enabling platform for dynamic resource sharing. AI is employed to optimize data management in the process of dynamic resource sharing. The proposed architecture in [199] can successfully implement dynamic spectrum sharing. Simulation results show that DRL can effectively maximize the user's profit margin compared to the traditional Q-Learning algorithm and stochastic decision-making. There is a competitive relationship between multiple operators. Therefore, the operator's spectrum utilization rate and infrastructure deployment efficiency are deeply low. 6G networks will enable more flexible mobile network deployments through spectrum and infrastructure sharing among operators. Under the 6G network of multiple mobile operators, the work in [200] developed a blockchain- and AI-empowered multi-plane framework for open spectrum and infrastructure sharing. The developed framework of [200] consists of user plane, infrastructure plane, operator plane, blockchain plane, and AI plane. As a case study of the developed multi-plane framework, the authors of [200] utilized deep RNN and blockchain technology to design a workflow for dynamic spectrum management among multiple operators. Simulation results indicate that the designed intelligent dynamic spectrum management workflow can provide more equitable bandwidth allocation for all users compared with static and semi-intelligent workflows. The authors in [201] proposed a general edge intelligent privacy-preserving framework, which is integrated blockchain with FL and can be specifically applied to spectrum resource sharing. Spectrum sharing information is recorded in the blockchain as a transaction, and consumers pay spectrum leasing fees to providers through the blockchain. FL can not only learn computational results from data, but also provide optimized spectrum sharing strategies. In the digital twin edge network, the work of [202] provided a permissioned blockchain-based FL architecture. To improve the communication efficiency, the authors of [202] also designed an efficient asynchronous aggregation model and DRL-based algorithm to optimize user scheduling and spectrum resource allocation. For the problem of adaptive resource allocation, reference [203] presented a blockchain-based MEC framework, where DRL method is utilized to tackle the joint optimization problem of spectrum resource allocation and block generation. In 6G networks, reference [204] discussed the possibility of distributed ledger technology and ML techniques to promote the coexistence of licensed and unlicensed spectrum.

2) Computation Allocation: Computing resource is one of the key resources in 6G wireless communications. Combining blockchain and AI can allocate and offload computing resources more efficiently. For instance, to facilitate the scalability and flexibility of resources, SDNIIoT, which integrates software-defined networking (SDN) into the IIoT, was proposed in [205]. In large-scale distributed SDNIIoT networks, the authors of [205] presented a novel permissioned blockchain-energized consensus mechanism. This mechanism synchronizes local views among different SDN controllers, and finally achieves a consensus on the global view. To further improve the throughput of the blockchain system, a joint optimization problem of view change, access selection, and computational resource allocation was constructed in [205]. To this end, a dueling deep Q-learning method was proposed to deal with the joint problem. In the network environment with more and more IoT devices, reference [206] introduced a general system framework for blockchain-assisted edge computing. In this framework, the complete procedure of transactions between IoT side and edge nodes is specified step by step. Furthermore, the authors of [206] provided a smart contract for resource allocation in the private blockchain network. The problem of allocating edge computing resources to data service users was described as a continuous-time Markov decision process. In [206], the designed smart contract adopted the RL algorithm and asynchronous advantage actor-critic algorithm to tackle the problem of edge computing resource allocation. Compared with some traditional algorithms, the proposed algorithm can distinguish multiple service quality requirements of different service users, thereby ameliorating the allocation efficiency of computing resources.

To enhance security resource management for edge users in a distributed manner, the work of [207] demonstrated a blockchain-guided offloading mode, which maximizes data availability. This mode alleviates the non-probabilistic hardness problem of data availability due to cooperative and probabilistic data offloading. The data offloading process occurs in the edge network assisted by blockchain. In this data offloading mode, Naive Bayes' learning was employed to linearly classify offloaded and non-offloaded instances to obstruct service delays and unnecessary backlogs. Aiming at the security and offloading requirements in mobile edge-cloud IoT networks, the work in [208] developed a secure computation offloading scheme by combining blockchain and DRL. In this scheme, the computing tasks of mobile IoT devices can be offloaded to the cloud or edge servers. To upgrade the security of data offloading, a trusted smart contract-empowered access control mechanism was presented in [208]. This mechanism prevents cloud resources from being accessed by illegal offloading devices. Again, for example, the authors of [208] formulated the computation offloading, edge resource allocation, bandwidth allocation, and smart contract cost as a joint optimization problem. This joint problem can be solved using an advanced DRL algorithm with a double-duling Q-network and a optimal offloading strategy for all IoT devices can be obtained. Under the vehicular fog computing network, reference [209] introduced a blockchain- and ML-assisted task

TABLE VII. Analysis of integration of blockchain and AI for secure services.

Taxonomy	Representative References	Year	Key Technologies	Main Contributions
Spectrum Management	Hu et al. [199]	2021	Hierarchical blockchain, DRL	Proposing a blockchain- and AI-supported dynamic resource sharing architecture in 6G and beyond networks, and DRL maximizes the user's profit margin.
	Maksymyuk et al. [200]	2022	Blockchain, AI, Deep RNN	A multi-plane framework based on blockchain and AI for open spectrum and infrastructure sharing in the 6G network with multiple mobile operators.
	Lu et al. [202]	2020	Permissioned blockchain, Digital twin, FL, DRL	Presenting a permissioned blockchain-based FL architecture in the digital twin edge network for user scheduling and spectrum resource allocation.
	Guo et al. [203]	2020	Blockchain, MEC, DRL	Building a blockchain-based MEC framework for adaptive resource allocation, and DRL is utilized to tackle the joint optimization problem of spectrum resource allocation and block generation.
Computation Allocation	He et al. [206]	2021	Private blockchain, RL, Edge computing	Providing a general system framework for blockchain-assisted edge computing and a smart contract for computing resource allocation in the private blockchain network.
	Manogaran et al. [207]	2021	Blockchain, Edge computing, Naïve Bayes' learning	Demonstrating a blockchain-guided offloading mode for distributed resource management of edge users, and Nave Bayes' learning was employed to linearly classify offloaded and non-offloaded instances.
	Nguyen et al. [208]	2021	Blockchain, DRL, Edge/cloud computing	Developing a secure computation offloading scheme by combining blockchain and DRL for meeting the security and offloading requirements in mobile edge-cloud IoT networks.
	Liao et al. [209]	2020	Blockchain, ML, Fog computing	Utilizing smart contracts and Merkle hash trees to introduce a blockchain- and ML-assisted task offloading framework under the vehicular fog computing network.
Content Caching	Qiu et al. [211]	2020	Blockchain, DL	Building a blockchain- and DL-guided edge intelligence framework entitled AI-Chain, which can handle the joint resource allocation problem of networking, edge computing and content caching.
	Dai et al. [213]	2020	Permissioned blockchain, DRL, Edge computing	Combining permissioned blockchain and DRL to design a secure and intelligent content caching scheme in vehicle edge computing networks.
	Cui et al. [215]	2020	Blockchain, FL	Discussing a compression algorithm named CREAT applied to the caching, and this algorithm integrates FL and blockchain.
	Zhang et al. [216]	2020	Blockchain, DRL, D2D, MEC	Introducing a blockchain- and smart contract-guided distributed cache sharing incentive mechanism to upgrade user sharing-depended caching performance.
Security and Privacy	Dhieb wt al. [218]	2020	Permissioned blockchain, ML	Integrating permissioned blockchain and AI to develop a distributed heterogeneous IoT network architecture to add additional security performance.
	Wang et al. [219]	2021	Hierarchical blockchain, Transfer learning	A secure user authentication mechanism called ATLB with the help of transfer learning and blockchain.
	Kumar et al. [222]	2021	Blockchain, DL, Smart contract	Leveraging blockchain and DL to provide two levels of security and privacy for collaborative intelligent transportation systems.
	Otoum et al. [225]	2022	Blockchain, FL	Constructing an adaptive trust model by combining FL and blockchain, and this model treated personal trust as a probability.

offloading framework. The framework utilizes smart contracts and Merkle hash trees to facilitate fair task offloading and mitigate various security attacks. Then, to tackle the task offloading optimization problem, an intelligent task offloading algorithm based on online learning was delineated in [209]. Without requiring the information and CSI of the vehicle fog computing server, this algorithm can learn the long-term optimal unloading strategy and effectively reduce the unloading delay, queuing delay, and switching cost. In an air-to-ground integrated power system, the work of [210] formulated a joint optimization problem of device-side task offloading and server-side resource allocation. Then, it demonstrated an electromagnetic interference-aware computational offloading algorithm by combining blockchain and semi-distributed learning.

3) Content Caching: Caching is introduced into the 6G communication architecture. Specifically, by deploying caching in terminals, BSs, and core network gateways, popular content is cached to the location closer to the user. Content caching can realize the local response of some user requests, reduce the transmission delay of the requested content, improve the user experience, and balance the network load. However, the current content caching strategy is relatively static. Therefore, the caching performance depends heavily on the popularity of the content and lacks the perception of users' personalized demands. At the same time, the caching

deployment in the mobile environment brings great security risks to the user's data privacy. Blockchain and AI are key enabling technologies to address these challenges. For example, in [211], a blockchain-guided edge intelligence framework entitled AI-Chain for 6G wireless networks was pioneered, which integrates DL and blockchain. The framework benefits from the transferability of DL. Specifically, each lightweight edge node trains neural network components, and then shares local learning results on the blockchain. To demonstrate the effectiveness of the proposed framework, the work in [211] applied AI-Chain to handle the joint resource allocation problem of networking, edge computing, and content caching. Aiming at the privacy leakage problem in cognitive vehicle networks, reference [212] provided a blockchain-inspired content caching architecture. Under this framework, road side units (RSUs) and vehicles that provide content cache the content in advance and broadcast it to surrounding vehicles. Vehicles with content requirements can selectively download the related content. Once the content transaction is completed, the transaction record is written to the blockchain and broadcast to all RSUs and vehicles. To enhance the cache hit ratio, the cognitive engine can sense the content demands of the underlying vehicles. Then, in [212], the perception data is analyzed by ML and DL algorithms, and predictive cached results are presented to RSUs and vehicles that provide content. In vehicle edge computing networks, a secure and intelligent content caching scheme by combining permissioned blockchain and DRL was demonstrated [213]. In this scheme, vehicles accomplish content caching and BSs sustain the permissioned blockchain. Furthermore, considering vehicle mobility, the work of [213] constructed a vehicle-to-vehicle content caching optimization problem, and applied the advanced DRL algorithm to obtain the optimal caching strategies.

In machine-to-machine communication networks, a blockchain- and edge computing-enabled network framework was proposed in [214]. In this architecture, edge computing improves data caching and computing capabilities, and blockchain ensures data security and efficiency. To reduce latency, the authors of [214] framed the joint optimization problem of content caching, computation offloading, and blockchain scheduling as a discrete Markov decision process. Then, a dueling optimization algorithm inspired by a dueling deep Q-network was adopted to solve this joint optimization problem. To polish up the file caching hit ratio, a compression algorithm named CREAT applied to the caching was provided in [215]. CREAT integrates FL and blockchain, which can cache files by predicting the popularity of different files through the FL algorithm and speed up the response to file requests from IoT devices. In the meantime, blockchain technology ensures the security of data transmitted by IoT devices and gradients uploaded by edge nodes. Additionally, an advanced compression algorithm is adopted in [215] to compress the uploaded gradients, so as to speed up the training process of FL. The most critical reason for the hindered development of user sharing-depended caching solutions is the lack of incentive mechanism. To upgrade user sharing-depended caching performance, the work of [216] provided a blockchain- and smart contract-guided distributed cache sharing incentive mechanism. In this mechanism, D2D and MEC caching nodes incentivize their cache sharing willingness by receiving expected rewards. Then, to depress consensus latency and undertake confidence, a partially PBFT consensus protocol was suggested. Furthermore, both the cache placement problem and the scene selection problem can be described as Markov decision processes [216]. Then, the DRL algorithm with deep Q-Network was presented to deal with these problems.

4) Security and Privacy: Security and privacy vulnerabilities increase with the scale of wireless communication systems. Accordingly, the security and privacy of communication participants have become an important issue. The combination of blockchain and AI can provide more effective solutions to security and privacy challenges 6G in wireless communication systems [217]. As an illustration, a distributed heterogeneous IoT network architecture by integrating permissioned blockchain and AI was designed in [218], so as to add additional security performance. Here, blockchain is applied to share and store data of IoT devices. On the hand, ML algorithms can detect Malware and cyberattacks of distributed IoT networks and can classify these anomalous behaviors in real time. On the other hand, the existing identity authentication mechanisms have the problems of singleness and poor adaptability. Based on this consideration, the authors of [219] introduced a secure user authentication mechanism called ATLB with the help of transfer learning and blockchain. ATLB described layered blockchain to implement the privacy protection of the authentication mechanism with collusion attack and Sybil attack. In addition, to reduce the model training time, reference [219] added transfer learning to optimize the authentication mechanism and build a trustworthy and intelligent blockchain. In the edge service network of IIoT, a distributed ML scheme guided by blockchain can guarantee the security and privacy of data processing of multiple resource-constrained devices [220]. To reduce the response delay of edge services, the proposed scheme of [220] employed blockchain to replace cloud servers as trusted third-party institutions. Moreover, a smart contract-based incentive mechanism was applied to encourage multiple devices to participate in computing tasks. Furthermore, a size-weighted aggregation strategy was discussed to validate and integrate model parameters, thereby improving model accuracy. The SM2 public key cryptosystem was applied in [220] to complete the privacy protection of model parameters in edge services. There are also security and privacy challenges for data in the software-defined Internet of Vehicles. To address these challenges, the work in [221] developed a spatial crowdsourcing framework guided by multiple blockchains and DRL together. In [222], blockchain and DL provided two levels of security and privacy for collaborative intelligent transportation systems. For the first level, smart contracts were employed for secure and intelligent data communication. For the second level, to prevent cyber attacks, LSTM auto-encoders in DL encoded data into new formats. To mitigate the precipitately growing security challenges of in-vehicle networks, a novel blockchain- and AI-empowered trust management architecture was developed in [223].

More interesting, many works [224]–[228] have proved that the combination of blockchain and FL can greatly enhance data security and privacy. For example, to defeat the privacy leakage problem in traditional device failure detection, the blockchain-authorized FL scheme of [224] can verify the integrity of the data. Then, an innovative centroid distance-weighted joint averaging algorithm can alleviate the data heterogeneity problem in device fault detection. In [225], an adaptive trust model was constructed by combining blockchain and FL, which treated personal trust as a probability. Moreover, under the constraints of certain security standards, the trust value of the terminal devices in different networks was evaluated. The study in [226] took advantage of blockchain and FL to design a distributed multi-party collaborative data sharing scheme. This scheme built and shared data models through FL without directly displaying the original data, thus realizing data privacy protection. Furthermore, permissioned blockchains supported secure data retrieval, thereby further controlling access to shared data and depressing the hazard of data disclosure. Similarly, integrating blockchain and FL can also be applied to enhance the security and privacy of data during data transmission [227] and vehicle intrusion detection [228].

B. IoT Smart Applications

IoT has become a fundamental component of future wireless communication networks. Various smart IoT applications have great potential to provide exciting services, which is receiving more and more attention from academia and industry. IoT is a huge network formed by combining various information sensing devices with the Internet, realizing the interconnection of people, machines, and things at any time and any place. In this subsection, we will extensively discuss some important 6G IoT smart applications supported by both blockchain and AI, including smart healthcare [229]–[236], smart transportation [237]–[246], smart grid [247]–[253], and UAV [254]–[261]. The analysis of integration of blockchain and AI for IoT smart applications is shown in TABLE VIII.

1) Smart Healthcare: At present, due to the impact of the new crown pneumonia epidemic, the integration of emerging technologies and medical scenarios is accelerating. New models such as telemedicine and intelligent pre-diagnosis have become rigid needs. Thus, the smart medical industry has ushered in a new round of outbreaks. The fusion of two emerging technologies, blockchain and AI, achieves leap-forward development of smart healthcare in areas including electronic health records, health insurance, biomedical research, drug supply, procurement process management, and medical education. For instance, a multi-party electronic health record sharing framework entitled BinDaas was proposed in [229]. This framework integrates two technologies, blockchain and DL. Here, the blockchain stores the patient's electronic health record data in a secure manner. DL provides future disease risk predictions for patients based on past repositories. Also, a lattice-based key and signature verification method was developed in [229] to fight against quantum and collusion attacks. The authors of [230] designed a distributed secure e-health architecture named Healthchain-RL by combining blockchain and DRL. The blockchain in the designed architecture assembled heterogeneous healthcare institutions with dissimilar demands. At the same time, the configuration of the blockchain network was optimized in real time through the online enlightened policy-making DRL algorithms, so as to accomplish a balance between security, delay, and cost. The work in [231] investigated a blockchain- and DL-enabled secure and intelligent healthcare diagnosis scheme. This healthcare diagnosis scheme mainly involves three main steps: 1) sharing medical images based on orthogonal particle swarm optimization (OPSO) algorithm; 2) running hash value encryption through neighborhood indexing sequence algorithm; 3) performing medical diagnosis by using OPSO-DNN algorithms.

The study of [232] leveraged the advantages of blockchain and FL to constitute a detection model for computed tomography (CT) scans of COVID-19 patients. The constituted model identified COVID-19 patients from lung CT images by applying the capsule network-supported segmentation and classification method. Therein, a global DL model was trained from data collected from different hospitals and facilities using FL algorithms and blockchain was used to authenticate data from different sources. Likewise, for screening and monitoring the COVID-19 epidemic, the authors in [233] developed a distributed collaborative healthcare architecture guided by blockchain and FL. Different from the detection of CT images in [232], reference [234] integrated blockchain and DNN to extract feature data from existing datasets, thereby helping to diagnose severe diseases such as COVID-19 and blood cancer. Detecting infectious diseases is difficult in remote and resource-poor rural areas. Meanwhile, smartphones are predicted to be one of the main tools driving improvements in healthcare delivery. Therefore, an end-to-end DeoxyriboNucleic Acid (DNA) diagnostic platform based on smartphones was proposed in [235]. In this platform, DL provided automatic detection of infectious disease DNA molecular test results and their analysis. Blockchain was used for secure data connection and management, thereby increasing the credibility of the entire diagnostic platform. Most critically, the authors of [235] also verified the feasibility of the proposed platform through field tests in rural areas. AI algorithms can predict the type of disease and surgery based on the patient's basic symptoms and historical health records. For example, the extreme gradient boosting algorithm was applied in [236] to classify diseases. In this reference, it described a blockchain- and AI-enabled drone-aided smart telesurgery architecture called BATS, which introduced smart contracts to maintain the integrity and reliability of data stored on the blockchain. During emergencies in traffic jams, UAVs can transport some light healthcare items, such as medicines and surgical tools.

2) Smart Transportation: With the rapid development of information technology, smart transportation has also ushered in more development opportunities. Smart transportation refers to the full use of big data, IoT, cloud computing, blockchain, AI, and other technologies in the field of transportation. Smart transportation can fully guarantee traffic safety, give full play to the efficiency of transportation infrastructure, and improve the operational efficiency and management level of

TABLE VIII. Analysis of integration of blockchain and AI for IoT smart applications.

Taxonomy	Representative References	Year	Key Technologies	Main Contributions
Smart Healthcare	Bhattacharya et al. [229]	2021	Blockchain, DL	Using blockchain and DL to propose a multi-party electronic health record sharing framework entitled BinDaas.
	Al-Marridi et al. [230]	2021	Blockchain, DRL	Designing a distributed secure e-health architecture named Healthchain-RL by combining blockchain and DRL.
	Otoum et al. [233]	2021	Blockchain, FL	A distributed collaborative healthcare architecture guided by blockchain and FL for screening and monitoring COVID-19.
	Mallikarjuna et al. [234]	2021	Blockchain, DNN	Integrating blockchain and DNN to extract feature data from existing datasets, thereby helping to diagnose severe diseases such as COVID-19 and blood cancer.
	Guo et al. [235]	2021	Blockchain, DL	An end-to-end DNA diagnostic platform based on smartphones for driving improvements in healthcare delivery.
	Gupta et al. [236]	2021	Blockchain, AI, Smart contract	Describing a blockchain- and AI-enabled drone-aided smart telesurgery architecture called BATS.
Smart Transportation	Al Ridhawi et al. [237]	2021	Blockchain, RL	A collaborative service composition approach by combining blockchain and RL to improve the quality of service for vehicles.
	Song et al. [240]	2020	Blockchain, DNN	Providing a blockchain- and DNN-assisted smart vehicle co-localization scheme.
	Jiang et al. [242]	2020	Blockchain, DRL, Edge computing	Combining blockchain and multi-access edge computing to build a video analytics architecture in autonomous driving systems.
	Pokhrel et al. [244]	2020	Blockchain, FL, Consensus mechanism	Using blockchain-enhanced FL to propose a fully decentralized communication system for autonomous vehicles.
Smart Grid	Keshk et al. [248]	2020	Blockchain, DL, LSTM	Demonstrating an advanced privacy-preserving scheme by integrating blockchain and DL in the environment of smart power.
	Wang et al. [249]	2020	Blockchain, FL	A power management system for electric vehicles merging blockchain and AI on the platform of smart grid.
	Ferrag et al. [250]	2020	Blockchain, DL, RNN	Designing a blockchain- and DL-guided reliable energy exchange architecture called DeepCoin to protect the smart grid from malicious attacks.
	Jamil et al. [251]	2021	Blockchain, ML, RNN, LSTM	Providing a blockchain- and ML-assisted scheme for forecasting P2P energy transactions to effectuate real-time scheduling of energy in microgrids.
	Gao et al. [252]	2021	Blockchain, Edge-AI	Adopting blockchain and edge-AI to formulate distributed energy trading and management system for smart microgrids named FogChain.
UAV	Singh et al. [254]	2021	Blockchain, DL	Introducing a security scheme for information transmission between UAVs, which integrated blockchain and DL.
	Feng et al. [255]	2022	Blockchain, FL	A novel secure identity authentication approach by leveraging blockchain-backed FL to overcome the security challenges of cross-domain UAVs' authentication.
	Pokhrel et al. [257]	2021	Blockchain, FL	A blockchain- and FL-assisted knowledge sharing and collaborative learning scheme for UAV swarms or LEO satellites.
	Gumaei et al. [259]	2021	Blockchain, DNN, Edge computing	Presenting a UAV recognition and detection architecture by combining blockchain, deep DNN, and edge computing.

the transportation system. In this part, we focus on the role of blockchain and AI in promoting smart transportation. To improve the quality of service for vehicles in 6G networks, the study in [237] discussed a collaborative service composition approach by combining blockchain and RL. Here, the blockchain was applied to announce combined tasks under certain constraints of service requests, ensuring that adjacent nodes interact securely and record transactions. To quicken the procedure of service composition path choice, the authors of [237] employed an RL algorithm to pick the optimal solution closest to the node request. To ward off traffic congestion, reference [238] described a blockchain-guided secure crowdsourcing scheme. This scheme encouraged users to voluntarily take part in traffic forecasting by sharing traffic information to earn tokens. Meanwhile, users can also spend these tokens to acquire the required traffic information from the network. Then, with the help of an LSTM neural network, the study of [238] fused the results of a feed-forward artificial neural network trained on historical data to prognosticate traffic congestion probabilities on real-time data. Similarly, the work in [239] considered integrating blockchain, RL, and edge computing to alleviate the traffic congestion problem.

Currently, vehicle positioning has challenges of low accuracy and network congestion in data sharing. To address these challenges, a blockchain- and DNN-assisted smart vehicle co-localization scheme was provided in [240]. This scheme was benchmarked with multiple traffic signs, and the DNN algorithm was applied to correct position of vehicles. For the localization errors of multiple vehicles, the work of [240] demonstrated a DL-inspired method for distance computation and prognostication to turn down localization errors for common vehicles on the unchanged road segment. Additionally, to actualize the safety information sharing between vehicles, the corresponding mechanisms of message asking, message selecting, message sharing, and punishment mechanism were presented based on smart contracts. In the in-vehicle self-organizing environment, an advanced blockchain-authorized distributed software-defined security architecture was delineated [241]. Then, the dueling deep Q-learning algorithm with prior experience playback was adopted in [241] to procure

the optimal strategy while satisfying the requirement of maximizing the system throughput. In autonomous driving vehicle networks, the sharing and storage of massive video data is terribly difficult. To cope with these difficulties, reference [242] combined blockchain and multi-access edge computing to build a video analytics architecture in autonomous driving systems. This architecture completed the secure storage and sharing of video data with the help of smart contract. Then, the study of [242] formulated the joint optimization problem of video offloading and resource allocation as a Markov decision process. Moreover, a high-level DRL algorithm with asynchronous advantage actor-critic was proposed to tackle this joint problem. Improper lanes for self-driving cars can cause tragic accidents, and thus, the authors of [243] demonstrated an autonomous lane changing system assisted by blockchain and collective learning. Blockchain ensured data security for autonomous vehicles while encouraging vehicle resources to join in collective learning. Then, an advanced algorithm based on the deep deterministic policy gradient was used in [243] to address the lane changing problem, so as to achieve optimal autonomous driving policies.

Interestingly, the fusion of blockchain and FL powerfully polishes up the performance of intelligent transportation systems [244]–[246]. For instance, on the basis of blockchain-enhanced FL, the study in [244] proposed a fully decentralized communication system for autonomous vehicles. In the proposed system, the local on-vehicle ML model updates are interchanged and validated with other vehicles in the distributed manner. At the same time, the proposed system made full use of the consensus mechanism of the blockchain and can complete the update of local vehicle ML models without any third-party server. To enhance the reliability of edge data sharing between vehicles, a hybrid blockchain- and FL-assisted secure data sharing framework was designed in [245]. In this framework, the hybrid blockchain was composed of the permissioned blockchain and the local directed acyclic graph of vehicle operation, which can further upgrade the security of in-vehicle data. Furthermore, to further polish up the training efficiency, the authors of [245] introduced an asynchronous FL scheme for model learning from edge data, and preferred the better participating node through the DRL algorithm. The work of [246] demonstrated a layered blockchain- and FL-embedded vehicle knowledge sharing system. This system adopted a hierarchical blockchain to record the FL model. Then, integrating a proof-of-learning-based consensus protocol with high-precision hierarchical FL effectively prevent the waste of a large amount of computing resources. Also, the knowledge sharing process among vehicles was constructed as a multi-leader and multi-follower non-cooperative game problem in [246].

3) Smart Grid: The construction of a smart grid provides a strong guarantee for improving the related functions of smart cities, thus further accelerating the pace of urban intelligence. As a network with extensive coverage, the smart grid should realize the interaction with users, the intelligentization of power grid equipment, the full automation of power production, and the greening of energy, so as to comprehensively improve the level of informatization and intelligence of the power grid. Modern communication technology is fully utilized to build a safe, reliable, green, and efficient smart grid. The application of blockchain and AI to the smart grid can improve the quality and efficiency of grid engineering, thereby enhancing the stability of the smart grid system. For example, the work of [247] systematically discussed the enabling role of blockchain, AI and IoT in improving smart grid performance. In the environment of smart power, reference [248] demonstrated an advanced privacy-preserving scheme by integrating two emerging technologies, blockchain and DL, which consisted of a two-level privacy mechanism and an anomaly detection mechanism. Specifically, the first-level privacy mechanism applied a blockchain found on an enhanced PoW consensus protocol to validate data integrity and diminish data poisoning attacks. To avoid inference attacks, the second-level privacy mechanism converted the raw data into an encoded form with the assistance of a variational autoencoder. Then, in [248], an LSTM-inspired anomaly detection mechanism employed two public datasets to train and validate the output of the two-level privacy mechanism. On the platform of smart grid, a power management system for electric vehicles merging blockchain and AI was creatively demonstrated in [249]. The system applied artificial neural networks and FL to prophesy the electricity consumption of electric vehicles. At the same time, the blockchain can incorporate all distributed electric vehicles to form a smart energy storage framework. The blockchain traded memory and time for the security and transparency performance of the proposed power management system. To protect the smart grid from malicious attacks, the study of [250] designed a blockchain- and DL-guided reliable energy exchange architecture called DeepCoin. In DeepCoin, the blockchain adopted the PBFT algorithm to accomplish the consensus in the P2P energy system, thereby promoting users to voluntarily trade redundant energy to other adjacent users. In [250], the blockchain also applied bilinear pairing, short signature, and hash function to complete the privacy protection of smart grid users. Then, DeepCoin tracked down cyber-attacks and deceitful transactions in smart grids through the RNN-based DL algorithm.

Recently, microgrids are small-scale power systems that utilize renewable energy sources to distribute electricity near users. To effectuate the real-time scheduling of energy in microgrids, the authors of [251] provided a blockchain- and ML-assisted scheme for forecasting P2P energy transactions. This energy transaction scheme was modeled and completed on the permissioned blockchain network entitled Hyperledger Fabric. At the same time, smart contracts performed real-time scheduling of distributed energy and controllable loads. In addition, RNN, LSTM, and bidirectional LSTM-powered ML algorithms are employed to forecast energy requirements in microgrids while downgrading electricity transportation expenses. In [252], a distributed energy trading and management system for smart microgrids named FogChain was presented. FogChain adopted blockchain to formulate a decentralized energy trading platform and applied edge-based AI methods to draw distributed controllers for microgrids. In the same direction, the work in [253] combined blockchain and ML to address data sharing, processing, and forecasting problems

in microgrid systems.

4) UAV: In recent years, with the development of information technology, UAV has formed an intelligent aircraft that combines multiple technologies such as flight control, network communication, and electric power. UAVs can be regarded as flying IoT devices, and have been widely applied in military, agriculture, forestry, transportation, meteorology, and other fields. UAV has the advantages of low cost, high dynamics, and deployment flexibility. However, UAV communication faces many threats such as being susceptible to interference, inability to cover large areas, and unstable communication. The combination of blockchain and AI provides new research ideas for alleviating these threats. For example, under the UAV Internet system, reference [254] introduced a security scheme for information transmission between UAVs, which integrated blockchain and DL. This scheme applied a zero-knowledge-proof-based blockchain to maintain the security and privacy of data dissemination between UAVs. Moreover, the DL-inspired miner selection algorithm in [254] can obtain the optimal miner node strategy, thereby shortening the block generation time and transaction submission time. To overcome the security challenges of cross-domain UAVs' authentication, a novel secure identity authentication approach by leveraging blockchain-backed FL was provided in [255]. In this approach, FL only shared the data model uploaded by the authenticated UAV instead of directly sharing the original data. The authors of [255] made full use of multi-signature smart contracts to practice distributed cross-domain UAVs' identity authentication. And, to surmount the single point failure, these multi-signature smart contracts were also employed to perform aggregations of global model updates. In the IoT environment, the work of [256] proposed a distributed dynamic resource management and pricing system that integrated blockchain-as-a-service (BaaS) and UAV-authorized MEC. Specifically, MEC servers are installed on both the ground BSs and the UAVs acting as the air BSs to process some blockchain tasks. BaaS combined blockchain and cloud computing so that resource management and pricing can be handled on BSs with MEC servers in [256]. Then, in the case of incomplete information, the interaction process of resource management and pricing between BSs and peers of the proposed system was expressed as a stochastic Stackelberg game with multiple leaders.

Additionally, UAV swarms or low earth orbit (LEO) satellites are extremely vulnerable to security threats. Therefore, reference [257] elucidated a blockchain- and FL-assisted knowledge sharing and collaborative learning scheme. Specifically, this scheme considered the influence of the number of miners, block transfer, and the mobility of UAVs/LEOs, the authors of [257] derived the probability of regular forks and optimized the energy consumption of PoW computation for blocks. More importantly, in [257], an advanced FL-enabled algorithm was used to complete the resource allocation of mobile mining. And, the coordination gains of blockchain and FL for UAV swarms was illustrated. The work of [258] integrated blockchain, AI, and UAV swarms to design an autonomous detection framework for infectious diseases. Here, UAV swarms can expand coverage and lessen human participation. This detection framework applied a lightweight blockchain and two-stage security authentication mechanism to remote areas where the network is scarce to degrade the burden of UAVs. Then, a DL-inspired algorithm was provided to autonomously detect disease prevalence in [258]. The security of RF signal transmission between UAVs and the accuracy of identification and detection are challenged. Consequently, a UAV recognition and detection architecture by combining blockchain, deep DNN, and edge computing was elucidated in [259]. This architecture applied blockchain to protect the security of data transmission. Moreover, the deep DNN was adopted for training by using the collected RF signal data from UAVs in different flight modes. Then, the trained model was downloaded to edge devices to identify UAVs and detect their flight modes. There are trade-off problems in terms of quantity, energy consumption, coverage area, and height when installing BSs on the UAV side (UAV-BS). To address this deployment problem of UAV-BS, the study of [260] demonstrated a blockchain- and ML-guided smart placement scheme for UAV-BS. More interestingly, in 6G networks, the work in [261] combined blockchain and FL can provide a new idea for UAV-assisted construction of disaster response systems.

C. Analysis of Operating Frequencies, Visions, and Requirements from the 6G Perspective

1) Operating Frequencies from the 6G Perspective: Considering the operating frequencies of AI and blockchain for 6G is crucial from 6G perspective, as 6G networks have higher requirements for high-speed data transmission and processing. However, there are currently no established standards or fixed ranges for the operating frequencies of AI and blockchain in 6G. Since 6G technology is still in the research and standardization phase, there is limited discussion and research on this specific topic in the existing literature. Current works [2], [5]–[8], [263], [264] primarily focus on the communication characteristics, spectrum range, and key technologies of 6G. The operating frequencies in 6G are expected to encompass a wide range of spectrum, including low-frequency, mid-frequency, high-frequency, as well as millimeter-wave and terahertz bands. However, the current work does not specifically address the operating frequencies of AI and blockchain in 6G. Until further research and standardization developments, specific discussions and research on the operating frequencies of AI and blockchain for 6G may remain limited.

Although specific references may be limited, we can provide a general discussion on the operating frequencies of AI and blockchain in 6G networks. **Millimeter-wave and Terahertz Bands:** 6G networks will utilize high-frequency millimeter-wave and terahertz bands to achieve higher data transmission rates and lower latency. The use of these frequency bands will impact the operating frequencies of AI and blockchain, requiring consideration of their performance and adaptability in these bands. **Power Consumption and Resource Management:** 6G networks demand high performance while minimizing power consumption. When determining the operating frequencies of AI and blockchain, a comprehensive consideration of power consumption and resource management is

necessary to achieve efficient computation and communication. **Adaptive Adjustment Strategies:** Given the dynamic nature and diverse application requirements of 6G networks, adaptive adjustment strategies are crucial for the operating frequencies of AI and blockchain. By continuously monitoring and analyzing network conditions, application demands, and resource availability, it is possible to dynamically adjust the operating frequencies of AI and blockchain to meet real-time requirements and optimize network performance.

The operating frequencies of AI and blockchain for 6G will be determined based on specific application scenarios and requirements. For example, in the fields of IoT, UAV or smart cities, different frequency bands may be used to support the 6G secure services and 6G IoT smart applications by integrating of AI and blockchain. The specific operating frequencies will depend on communication requirements, device characteristics, as well as the needed bandwidth and capacity. Therefore, from the 6G perspective, determining the operating frequencies of AI and blockchain requires considering multiple factors and referencing the development of future 6G standards and the demand of practical application. Notably, the discussion provided above only offers general perspectives on operating frequencies and does not establish specific frequency band ranges. As 6G technology continues to be researched and developed, future studies and standardization efforts will provide more specific and detailed guidance.

2) Visions from the 6G Perspective: The vision of 6G is to build a highly intelligent, highly connected, and highly adaptive network to meet the needs of future society and industries. From the 6G perspective, the visions include several key aspects. **Ultra-high rates and ultra-low latency:** The vision of 6G is to achieve higher data transmission rates and lower communication latency to support a wide range of applications, including enhanced mobile broadband, virtual and augmented reality, high-definition video, etc. Through high-speed and low-latency network transmission, the data processing and interaction capabilities of AI and blockchain will be enhanced, supporting more complex and real-time application scenarios. This will provide a stronger foundation for integrated AI and blockchain applications. **Super connectivity:** The vision of 6G is to establish a super-connected network that enables highly interconnected devices. The super-connected network includes D2D, device-to-infrastructure, and device-to-cloud connections. This will provide more connectivity options and broader coverage for AI and blockchain services and applications. **Powerful intelligence and adaptability:** The vision of 6G is to build an intelligent network with edge computing and distributed intelligence capabilities. This will enable real-time processing and decision-making of AI and blockchain technologies at the network edge, reducing latency and improving performance. Moreover, the intelligent network will be able to adaptively optimize based on application requirements, providing more efficient support for AI and blockchain services and applications. **Security and privacy protection:** The vision of 6G is to ensure network security and privacy protection to address the growing security threats. In the services and applications of AI and blockchain, security and privacy protection are crucial. 6G will provide stronger security mechanisms, including encryption, identity authentication, and access control, to ensure the secure and reliable operation of AI and blockchain services and applications.

In summary, the vision of 6G is an evolving and developing concept, and there is no unified definition or standard yet. Therefore, our discussion is primarily based on current research and academic discussions [2], [5], [7], [263] provide a general 6G vision for blockchain and AI services and applications.

3) Requirements from the 6G Perspective: To achieve the 6G vision discussed above, it naturally leads to the demand for higher bandwidth, lower latency, super connectivity, high security, and high reliability in 6G. Specifically, in the topic of blockchain and AI for 6G, the requirements of 6G include the following key aspects. **High bandwidth demand:** With the increasing adoption of AI and blockchain services and applications, there is a growing need for higher bandwidth to support large-scale data transmission, real-time decision-making, and complex computations. **Low latency requirement:** AI and blockchain services and applications require real-time responsiveness. To support these services and applications, 6G needs to provide lower communication latency to ensure fast data transmission and processing capabilities. **Large-scale connectivity capability:** With the proliferation of IoT devices and AI applications, 6G needs to have the ability to connect a massive number of devices to facilitate interconnection and data exchange. **High security and privacy protection:** Security and privacy are crucial in AI and blockchain services and applications. 6G needs to provide robust security mechanisms, including identity authentication, encryption, and secure transmission, to ensure the confidentiality and integrity of data. **High reliability and robustness:** 6G should exhibit high reliability and robustness to handle various network environments and cope with interferences and failures. This will ensure the stability and reliability of AI and blockchain services and applications.

In summary, the aforementioned requirements [5], [8], [263], [264] are based on the 6G perspective of integrating AI and blockchain services and applications. As 6G technology continues to evolve and standardization efforts progress, these requirements may be further refined and supplemented.

In this section, we have broadly discussed the services and applications of merging blockchain and AI for 6G networks. This includes the integration of blockchain and AI for 6G secure services, such as spectrum management, content caching, computation allocation, and security and privacy. We have also examined the 6G IoT smart applications of merging blockchain and AI, covering areas such as smart healthcare, smart transportation, smart grid, and UAV. Furthermore, we have thoroughly discussed the operating frequencies, visions, and requirements from the 6G perspective. In summary, this section highlights the complementary nature of blockchain and AI in addressing existing challenges and meeting the evolving requirements of the 6G era. The integration of blockchain and AI in 6G networks demonstrates the potential to enhance secure services and enable advanced IoT applications. Additionally, the analysis of operating frequencies, visions, and requirements provides valuable insights for shaping the future

of 6G networks. By studying the integration of blockchain and AI for 6G networks, we have gained a deeper understanding of their synergistic capabilities and the opportunities they present for transforming wireless communications.

IV. Open Issues, Research Challenges, and Future Work

Integrating blockchain and AI in 6G wireless communications is currently a hot research topic. In the previous sections, we focused on investigating the possibilities of combining blockchain and AI. Moreover, we extensively discussed the integration of blockchain and AI for wireless communications, involving secure services and IoT smart applications. Research on integrating blockchain and AI for wireless communications is still emerging, but future works need to address some questions and challenges. In this section, based on extensive research works in current literatures, we summarize the possible open issues and research challenges for integrating blockchain and AI in 6G wireless communications. The purpose is to provide beneficial inspirations and references for future innovation research. We also explore potential research directions in the future.

A. Towards Blockchain

In recent years, the research and application of blockchain has begun to grow explosively. Blockchain is considered to be the key technology leading the current information internet to the value internet. Although blockchain has great potential for 6G networks, there are still some challenges that limit its widespread application in 6G networks.

As the number of transactions increases significantly, scalability is the biggest hurdle limiting the widespread adoption of blockchain technology in 6G networks. For example, the Bitcoin and Ethereum systems process an average of 7 to 20 transactions per second, far behind the Visa system that handles tens of thousands of transactions per second. Moreover, the multi-copy feature of the blockchain requires a large amount of additional storage space, which increases storage costs. This will result in limited space utilization, making it difficult to support large-scale applications. There have been many researchers improving the scalability of blockchains by using techniques such as sidechains, lightning networks, sharding, pruning, and directed acyclic graphs. However, these methods still have their own problems, such as how to properly divide the tiles, and which transactions to prune. In addition, the blockchain is a high-energy-consumption industry. As an illustration, the blockchain system based on the PoW consensus mechanism relies on the computing power contributed by the blockchain nodes. However, only part of the computing power has been rewarded, and other computing power is doing useless work, which wastes a lot of resources. This problem of high energy consumption problem affects the popularization and application of blockchain in 6G.

Security attack is the most important problem faced by the blockchain so far, such as Bitcoin's 51% attack and botnet attack. The asymmetric encryption mechanism of the blockchain will become more and more fragile with the development of mathematics, cryptography, and computing technology. Security issues are also a great threat to the further application of blockchain to 6G networks. The data transactions recorded on the blockchain are open and transparent, which is beneficial for data sharing and verification, but not conducive to the privacy protection of user information. As more and more personal data is stored in blockchain-powered 6G networks, privacy leakage becomes another key issue.

B. Towards AI

In recent years, AI, especially DL, has achieved great success in computer vision, natural language processing, speech recognition, and other fields. The researchers expect to apply AI to all levels of the 6G system, thereby generating an intelligent communication system, realizing the true interconnection of everything, and meeting people's ever-changing demands for data transmission rates. However, there are still many challenges and unsolved issues in implementing and managing complex intelligent communication systems.

Inefficient data management schemes and high overhead of information exchange among communication participants are key bottlenecks in the development of AI technology. The AI-based solutions, such as ML methods, usually require large amounts of training data, which need to be collected and implemented on a centralized server with sufficient storage and computing resources. Nevertheless, current wireless communication systems do not have access to massive amounts of data to train models. In heterogeneous networks, aggregating data from different sources to train models is also an open problem. In 6G networks, users may have different service quality requirements in different scenarios. For example, in video streaming applications, users demand high throughput and low latency at the cost of security. However, in payment softwares, users require high security, even at the expense of throughput. In this direction, designing a cross-layer, action-based AI protocol for different applications is a key issue to satisfy various service demands while balancing the network resources of 6G networks.

Notably, in the current era of rapid development of AI, data security and privacy issues are receiving increasing attention. 6G network realizes interconnected intelligence by supporting AI functions, and adopts a centralized network architecture, which is vulnerable to hacker attacks. Moreover, 6G network needs to collect a large amount of user data for training through billions of devices. The training data involves a large amount of personal information, so AI can easily lead to privacy leakage of user data. Using distributed technology to design AI-enabled 6G network architectures can actualize a decentralized security and trustworthy mechanism. Without sending all data to the cloud computing center, the distributed technology processes data where it is generated, which can alleviate the problem of privacy leakage to a certain extent. Nevertheless, communication needs to exchange the knowledge information perceived by both parties and update the knowledge bases of both parties collaboratively, which also leads to the risk of privacy leakage of local data. How to develop an efficient coordination mechanism among

communication participants without causing any private data leakage remains an urgent problem to be solved.

C. Towards Blockchain- and AI-assisted Wireless Communications

Integrating blockchain and AI brings new opportunities to 6G networks, as well as some open issues and research challenges. For example, the natural conflict between blockchain and AI, the processing of a large amounts of data, and the collaborative optimization of multiple systems and multiple indicators. Furthermore, the effectiveness and feasibility of blockchain- and AI-assisted wireless communications still need to be verified by large-scale practice of wireless communication networks.

There are some conflicts with the combination of blockchain and AI. For example, the execution results of smart contracts in blockchains are often deterministic. While, the execution results of AI algorithms are usually uncertain, random, and unpredictable in most cases. The contradiction between blockchain and AI poses certain challenges for AI embedded in blockchain to optimize the execution decisions of 6G networks. Therefore, in future research, a new solution is required to deal with the contradiction between the certainty of smart contracts and the randomness of AI algorithms. The new solution can handle approximate calculations for smart contracts and design consensus protocols for each participating node of blockchain. The purpose of the new solution is to output the decision results under the 6G network with specific certainty, high accuracy, and high precision. With the explosive growth of data in 6G networks, the processing of large amounts of data in blockchain- and AI-assisted wireless communication systems is a terribly large challenge. Typically, blockchain is applied to securely collect and store large amounts of data, and AI uses these data for model training processing. The massive unlabeled and unclassified datasets are intractable for AI training. At the same time, the blockchain also presents a potential bottlenecks in storing these large-scale distributed data. For example, the data recorded on the blockchain is open and transparent. The blockchain-based storage method is beneficial for data sharing and verification, but not conducive to data privacy protection. Furthermore, at present, most works in related kinds of literature often only optimize a single performance index in a single wireless communication system. The collaborative optimization of multiple performance indexes of multiple wireless communication systems is ignored. However, with the maturity and in-depth research of blockchain and AI technologies in the future, the solutions proposed for the performance of different wireless communication systems can be combined with each other. Thereby, the goal of co-optimizing multiple performances of multiple systems can be achieved.

Observing the existing literature, blockchain- and AI-assisted wireless communications are still in the infant stage. Many works apply blockchain to create a trusted environment for wireless communications, and provide prediction, optimization, identification, detection, and decision-making for wireless communication systems through AI algorithms. Few works have really deeply integrated blockchain and AI into wireless communications. Whether we look at the current technical indicators of blockchains or the actual implementation of AI and 6G networks, there are still many uncertainties to truly realize the integration and implementation of blockchain and AI technologies for 6G networks. The potential outcomes of the fusion of blockchain and AI for 6G networks are also difficult to assess. Therefore, while actively investigating the integration of blockchain and AI for 6G networks, we must also look at it rationally and focus on practical implementation. In the future, we will continue to take an organic combination and flexible and innovative approach to truly realize the practice and exploration of the integration of blockchain and AI in 6G wireless communications.

D. Future Work

In future work, we still need to tackle the technical barriers of blockchain and AI. We can deeply investigate the matching and joint optimization of blockchain- and AI-powered 6G networks in terms of performance indicators, security, stability, etc. We can also further research and ensure the healthy and sustainable development of blockchain and AI technologies in 6G networks. In addition, the Federal Communications Commission, at the 2018 US Mobile World Congress, emphasized that 6G can introduce blockchain technology into spectrum sharing [265]. Research institutions such as the Institute of Electrical and Electronics Engineers and the France's Spectrum Regulator have also begun to explore the application of blockchain to manage spectrum [266]. Thus, we will focus on the fusion of blockchain and AI to obtain smarter and more distributed dynamic wireless resource allocation. 6G can combine emerging advanced technologies such as cloud computing, edge computing, and big data to promote the development of blockchain and AI technologies. Accordingly, the mutual promotion and integration of blockchain, AI, and 6G is also one of the key research directions in the future. With the further improvement of blockchain and AI, academia and industry will continue to transform theory into technology and put it into practice. We believe that future integration of blockchain and AI will be more in-depth, and the scenarios applied to 6G networks will be more abundant. Deploying Blockchain and AI in 6G networks will bring more surprises and possibilities to our lives.

In this section, we have outlined the open issues and research challenges associated with integrating blockchain and AI in 6G wireless communications. Future work should focus on innovative solutions for scalability and energy efficiency in blockchain, as well as exploring techniques for security and privacy protection. Additionally, efficient data management schemes and cross-layer AI protocols need to be developed to address AI-related challenges. The integration of blockchain and AI for 6G networks is still in its early stages, and future research should aim to overcome technical barriers and uncertainties, promote mutual promotion and integration, and explore practical applications. Overall, addressing these challenges and furthering the integration of blockchain and AI in 6G networks will bring significant advancements to wireless communications.

V. Conclusion

This survey reviewed the latest progress of blockchain and AI for 6G wireless communications. We began our comprehensive survey with a basic overview of blockchain and AI. Specifically, we briefly described the concepts, characteristics, and categories of blockchain and AI. The recent developments in applying blockchain and AI to wireless communications, respectively, were also showcased. To thoroughly explore the possibility of combining blockchain and AI, we started with two aspects of blockchain-assisted AI and AI-aided blockchain. We also highlighted the motivations for integrating blockchain with AI for 6G wireless communications. Next, we then extensively discussed the simultaneous deployment of blockchain and AI in 6G wireless communication systems, involving secure services and IoT smart applications. In particular, a comprehensive exploration of the widely popular secure services supported by blockchain and AI was conducted, spotlighting spectrum management, computation allocation, content caching, and security and privacy services. In addition, we also covered the latest achievements of blockchain and AI empowerment in various IoT smart applications. We made an exhaustive analysis from four scenarios: smart healthcare, smart transportation, smart grid, and UAV. Furthermore, we have thoroughly discussed operating frequencies, visions, and requirements from the 6G perspective. Finally, we have pointed out several open issues, research challenges, and potential research directions toward blockchain and AI for 6G networks.

In summary, this survey attempts to comprehensively explore the technologies related to blockchain and AI for wireless communications. Although the research on integrating blockchain and AI for 6G networks is still in its infancy, it is obvious that blockchain and AI will significantly uplift the performance of various services and applications in 6G networks. We believe our study will shed valuable insights into the research challenges associated with blockchain- and AI-assisted 6G networks as well as motivate interested researchers and practitioners to devote more research efforts to this promising area.

References

[1] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?" *Nat. Electron.*, vol. 3, no. 1, pp. 20–29, Jan. 2020.

[2] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6G wireless communications: Vision and potential techniques," *IEEE Netw.*, vol. 33, no. 4, pp. 70–75, Jul. 2019.

[3] F. Tariq, M. R. Khandaker, K.-K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A speculative study on 6G," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 118–125, Aug. 2020.

[4] W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, "The road towards 6G: A comprehensive survey," *IEEE Open J. Comm. Soc.*, vol. 2, pp. 334–366, Feb. 2021.

[5] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, "6G wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 28–41, Sept. 2019.

[6] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, D. Niyato, O. Dobre, and H. V. Poor, "6G internet of things: A comprehensive survey," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 359–383, Jan. 2022.

[7] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May 2019.

[8] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Open J. Comm. Soc.*, vol. 1, pp. 957–975, Jul. 2020.

[9] N. Kato, B. Mao, F. Tang, Y. Kawamoto, and J. Liu, "Ten challenges in advancing machine learning technologies toward 6G," *IEEE Wireless Commun.*, vol. 27, no. 3, pp. 96–103, Jun. 2020.

[10] H. Yang, A. Alphones, Z. Xiong, D. Niyato, J. Zhao, and K. Wu, "Artificial-intelligence-enabled intelligent 6G networks," *IEEE Netw.*, vol. 34, no. 6, pp. 272–280, Nov. 2020.

[11] S. Khan, A. Hussain, S. Nazir, F. Khan, A. Oad, and M. D. Alshehri, "Efficient and reliable hybrid deep learning-enabled model for congestion control in 5G/6G networks," *Comput. Commun.*, vol. 182, pp. 31–40, Jan. 2022.

[12] J. Guo, Y. Zuo, C.-K. Wen, and S. Jin, "User-centric online gossip training for autoencoder-based CSI feedback," *IEEE J. Sel. Topics Signal Process.*, vol. 16, no. 3, pp. 559–572, Apr. 2022.

[13] J. Guo, C.-K. Wen, and S. Jin, "CAnet: Uplink-aided downlink channel acquisition in FDD massive MIMO using deep learning," *IEEE Trans. Commun.*, vol. 70, no. 1, pp. 199–214, Jan. 2022.

[14] M. Latva-aho, K. Leppänen, F. Clazzer, and A. Munari, "Key drivers and research challenges for 6G ubiquitous wireless intelligence (White Paper)," 6G Flagship, University of Oulu, Oulu, 2019. [Online]. Available: http://urn.fi/urn:isbn:9789526223544.

[15] ITU-T, "Framework for evaluating intelligence levels of future networks including IMT-2020," Y.3173, Feb. 2020. [Online]. Available: https://www.itu.int/rec/T-REC-Y.3173/en.

[16] J. Leng, M. Zhou, J. L. Zhao, Y. Huang, and Y. Bian, "Blockchain security: A survey of techniques and research directions," *IEEE Trans. Serv. Comput.*, vol. 15, no. 4, pp. 2490–2510, Jul.-Aug. 2022.

[17] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: New areas and new challenges," *Digit. Commun. Netw.*, vol. 6, no. 3, pp. 281–291, Aug. 2020.

[18] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 4, pp. 3416–3452, May 2018.

[19] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6G: Challenges, opportunities and research directions," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*. Levi, Finland: IEEE, Mar. 2020, pp. 1–5.

[20] Y. Zhu, G. Zheng, and K.-K. Wong, "Blockchain-empowered decentralized storage in air-to-ground industrial networks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3593–3601, Jun. 2019.

[21] M. Ylianttila, R. Kantola, A. Gurtov, L. Mucchi, I. Oppermann, Z. Yan, T. H. Nguyen, F. Liu, T. Hewa, M. Liyanage *et al.*, "6G white paper: Research challenges for trust, security and privacy," *arXiv preprint arXiv:2004.11665*, 2020.

[22] J. Wang, X. Ling, Y. Le, Y. Huang, and X. You, "Blockchain-enabled wireless communications: a new paradigm towards 6G," *Natl. Sci. Rev.*, vol. 8, no. 9, p. nwab069, Sept. 2021.

[23] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A comprehensive survey of blockchain: From theory to IoT applications and beyond," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8114–8154, Oct. 2019.

[24] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and beyond networks: A state of the art survey," *J. Netw. and Comput. Appl.*, vol. 166, p. 102693, 2020.

[25] K. Yue, Y. Zhang, Y. Chen, Y. Li, L. Zhao, C. Rong, and L. Chen, "A survey of decentralizing applications via blockchain: The 5G and beyond perspective," *IEEE Commun. Surv. Tutor.*, vol. 23, no. 4, pp. 2191–2217, Sept. 2021.

[26] M. Tahir, M. H. Habaebi, M. Dabbagh, A. Mughees, A. Ahad, and K. I. Ahmed, "A review on application of blockchain in 5G and beyond networks: Taxonomy, field-trials, challenges and opportunities," *IEEE Access*, vol. 8, pp. 115 876–115 904, Jun. 2020.

[27] S. A. Bhat, I. B. Sofi, and C.-Y. Chi, "Edge computing and its convergence with blockchain in 5G and beyond: security, challenges, and opportunities," *IEEE Access*, vol. 8, pp. 205 340–205 373, Nov. 2020.

[28] P. Sharma, S. Jain, S. Gupta, and V. Chamola, "Role of machine learning and deep learning in securing 5G-driven industrial IoT applications," *Ad Hoc Netw.*, vol. 123, p. 102685, Dec. 2021.

[29] Y. Sun, J. Liu, J. Wang, Y. Cao, and N. Kato, "When machine learning meets privacy in 6G: A survey," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 4, pp. 2694–2724, Jul. 2020.

[30] V. P. Rekkas, S. Sotiroudis, P. Sarigiannidis, S. Wan, G. K. Karagiannidis, and S. K. Goudos, "Machine learning in beyond 5G/6G

networks—state-of-the-art and future trends," *Electronics*, vol. 10, no. 22, p. 2786, Nov. 2021.

[31] Y. Liu, X. Yuan, Z. Xiong, J. Kang, X. Wang, and D. Niyato, "Federated learning for 6G communications: Challenges, methods, and future directions," *China Commun.*, vol. 17, no. 9, pp. 105–118, Sept. 2020.

[32] M. Lin and Y. Zhao, "Artificial intelligence-empowered resource management for future wireless communications: A survey," *China Commun.*, vol. 17, no. 3, pp. 58–77, Mar. 2020.

[33] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10 127–10 149, Jan. 2019.

[34] M. Shafay, R. W. Ahmad, K. Salah, I. Yaqoob, R. Jayaraman, and M. Omar, "Blockchain for deep learning: review and open challenges," *Cluster Computing*, pp. 1–25, Mar. 2022.

[35] R. Wang, M. Luo, Y. Wen, L. Wang, K.-K. Raymond Choo, and D. He, "The applications of blockchain in artificial intelligence," *Secur. Commun. Netw.*, vol. 2021, Sept. 2021.

[36] B. Xing and T. Marwala, "The synergy of blockchain and artificial intelligence," *Available at SSRN 3225357*, Aug. 2018.

[37] K. D. Pandl, S. Thiebes, M. Schmidt-Kraepelin, and A. Sunyaev, "On the convergence of artificial intelligence and distributed ledger technology: A scoping review and future research agenda," *IEEE Access*, vol. 8, pp. 57 075–57 095, Mar. 2020.

[38] T. N. Dinh and M. T. Thai, "AI and blockchain: A disruptive integration," *Computer*, vol. 51, no. 9, pp. 48–53, Sept. 2018.

[39] S. K. Singh, S. Rathore, and J. H. Park, "BlockIoTIntelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence," *Future Gener. Comput. Syst.*, vol. 110, pp. 721–743, Sept. 2020.

[40] A. A. Hussain and F. Al-Turjman, "Artificial intelligence and blockchain: A review," *T. Emerg. Telecommun. T.*, vol. 32, no. 9, p. e4268, Apr. 2021.

[41] Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng, "Fusing blockchain and AI with metaverse: A survey," *IEEE Open J. Comp. Soc.*, vol. 3, pp. 122–136, Jul. 2022.

[42] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on iot security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet of Things*, vol. 11, p. 100227, Sept. 2020.

[43] P. Tagde, S. Tagde, T. Bhattacharya, P. Tagde, H. Chopra, R. Akter, D. Kaushik, and M. H. Rahman, "Blockchain and artificial intelligence technology in e-health," *Environ. Sci. Pollut. Res.*, vol. 28, pp. 52 810–52 831, Sept. 2021.

[44] S. S. Gill, S. Tuli, M. Xu, I. Singh, K. V. Singh, D. Lindsay, S. Tuli, D. Smirnova, M. Singh, U. Jain *et al.*, "Transformative effects of iot, blockchain and artificial intelligence on cloud computing: Evolution, vision, trends and open challenges," *Internet of Things*, vol. 8, p. 100118, Dec. 2019.

[45] A. Dhar Dwivedi, R. Singh, K. Kaushik, R. Rao Mukkamala, and W. S. Alnumay, "Blockchain and artificial intelligence for 5g-enabled internet of things: Challenges, opportunities, and solutions," *T. Emerg. Telecommun. T.*, p. e4329, Jul. 2021.

[46] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, "Blockchain and machine learning for communications and networking systems," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 2, pp. 1392–1431, Feb. 2020.

[47] F. Jameel, U. Javaid, W. U. Khan, M. N. Aman, H. Pervaiz, and R. Jäntti, "Reinforcement learning in blockchain-enabled IIoT networks: A survey of recent advances and open challenges," *Sustainability*, vol. 12, no. 12, p. 5161, Jun. 2020.

[48] Y. Wu, Z. Wang, Y. Ma, and V. C. Leung, "Deep reinforcement learning for blockchain in industrial IoT: A survey," *Comput. Netw.*, vol. 191, p. 108004, May 2021.

[49] A. Miglani and N. Kumar, "Blockchain management and machine learning adaptation for IoT environment in 5G and beyond networks: A systematic review," *Comput. Commun.*, vol. 178, pp. 37–63, Oct. 2021.

[50] A. El Azzaoui, S. K. Singh, Y. Pan, and J. H. Park, "Block5GIntell: Blockchain for AI-enabled 5G networks," *IEEE Access*, vol. 8, pp. 145 918–145 935, Aug. 2020.

[51] M. Dibaei, X. Zheng, Y. Xia, X. Xu, A. Jolfaei, A. K. Bashir, U. Tariq, D. Yu, and A. V. Vasilakos, "Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: A survey," *IEEE Trans. Intell. Transp. Syst.*, Feb. 2022.

[52] Y. Yuan, T. Zhou, A. Zhou, Y. Duan, and F. Wang, "Blockchain technology: from data intelligence to knowledge automation," *Acta Autom. Sin.*, vol. 43, no. 9, pp. 1485–1490, Sept. 2017.

[53] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *White Paper*, May 2008. [Online]. Available: http://nakamotoinstitute.org/bitcoin/.

[54] S. Aggarwal and N. Kumar, "Blockchain 2.0: smart contracts," in *Advances in Computers*. Elsevier, 2021, vol. 121, pp. 301–322.

[55] D. D. F. Maesa and P. Mori, "Blockchain 3.0 applications survey," *J. Parallel Distrib. Comput.*, vol. 138, pp. 99–114, Apr. 2020.

[56] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surv. Tutor.*, vol. 18, no. 3, pp. 2084–2123, Mar. 2016.

[57] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22 328–22 370, Jan. 2019.

[58] 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 (CRYPTO)*. Santa Barbara, CA, USA, Aug. 2017, pp. 357–388.

[59] D. Larimer, "Delegated proof-of-stake (DPoS)." Blacksburg, VA, USA, 2014.

[60] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst. (TOCS)*, vol. 20, no. 4, pp. 398–461, Nov. 2002.

[61] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[62] O. Dib, K.-L. Brousmiche, A. Durand, E. Thea, and E. B. Hamida, "Consortium blockchains: Overview, applications and challenges," *Int. J. Adv. Telecommun.*, vol. 11, no. 1&2, pp. 51–64, 2018.

[63] 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, Jun. 2021.

[64] X. Ling, Y. Le, J. Wang, Z. Ding, and X. Gao, "Practical modeling and analysis of blockchain radio access network," *IEEE Trans. Commun.*, vol. 69, no. 2, pp. 1021–1037, Feb. 2021.

[65] Y. Zuo, S. Jin, and S. Zhang, "Computation offloading in untrusted MEC-aided mobile blockchain IoT systems," *IEEE Trans. Wireless Commun.*, vol. 20, no. 12, pp. 8333–8347, Dec. 2021.

[66] Y. Zuo, S. Jin, S. Zhang, Y. Han, and K.-K. Wong, "Delay-limited computation offloading for MEC-assisted mobile blockchain networks," *IEEE Trans. Commun.*, vol. 69, no. 12, pp. 8569–8584, Dec. 2021.

[67] X. Ling, P. Chen, J. Wang, and Z. Ding, "Data broker: Dynamic multi-hop routing protocol in blockchain radio access network," *IEEE Commun. Lett.*, vol. 25, no. 12, pp. 4000–4004, Dec. 2021.

[68] Y. Zuo, S. Jin, and S. Zhang, "Blockchain storage, computation offloading, and user association for heterogeneous cellular networks," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8191–8204, Jun. 2022.

[69] Y. Zuo, S. Zhang, Y. Han, and S. Jin, "Computation resource allocation in mobile blockchain-enabled edge computing networks," in *2020 IEEE/CIC International Conference on Communications in China (ICCC)*. Chongqing, China, Aug. 2020, pp. 617–622.

[70] Y. Zuo, S. Jin, and S. Zhang, "Computation offloading and user association for blockchain-enabled heterogeneous cellular networks," in *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*. Norman, OK, USA, Sept. 2021, pp. 01–06.

[71] K. Kotobi and S. G. Bilén, "Blockchain-enabled spectrum access in cognitive radio networks," in *2017 Wireless Telecommunications Symposium (WTS)*, Apr. 2017, pp. 1–6.

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

[73] S. Bayhan, A. Zubow, and A. Wolisz, "Spass: Spectrum sensing as a service via smart contracts," in *2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, Oct. 2018, pp. 1–10.

[74] S. Bayhan, A. Zubow, P. Gawłowicz, and A. Wolisz, "Smart contracts for spectrum sensing as a service," *IEEE Trans. on Cogn. Commun. Netw.*, vol. 5, no. 3, pp. 648–660, Sept. 2019.

[75] M. B. H. Weiss, K. Werbach, D. C. Sicker, and C. E. C. Bastidas, "On the application of blockchains to spectrum management," *IEEE Trans. on Cogn. Commun. Netw.*, vol. 5, no. 2, pp. 193–205, Jun. 2019.

[76] J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator's perspective," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 451–466, Jan. 2020.

[77] M. Grissa, A. A. Yavuz, and B. Hamdaoui, "TrustSAS: A trustworthy spectrum access system for the 3.5 GHz CBRS band," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, Apr. 2019, pp. 1495–1503.

[78] T. Maksymyuk, J. Gazda, L. Han, and M. Jo, "Blockchain-based intelligent network management for 5G and beyond," in *2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)*, Jul. 2019, pp. 36–39.

[79] H. Zhang, S. Leng, and H. Chai, "A blockchain enhanced dynamic spectrum sharing model based on proof-of-strategy," in *2020 IEEE International Conference on Communications (ICC)*, Jun. 2020, pp. 1–6.

[80] M. Jiang, Y. Li, Q. Zhang, G. Zhang, and J. Qin, "Decentralized blockchain-based dynamic spectrum acquisition for wireless downlink communications," *IEEE Trans. Signal Process.*, vol. 69, pp. 986–997, Jan. 2021.

[81] Z. Li, Z. Yang, S. Xie, W. Chen, and K. Liu, "Credit-based payments for fast computing resource trading in edge-assisted internet of things," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6606–6617, Aug. 2019.

[82] D. Chatzopoulos, M. Ahmadi, S. Kosta, and P. Hui, "FlopCoin: A cryptocurrency for computation offloading," *IEEE Trans. Mobile Comput.*, vol. 17, no. 5, pp. 1062–1075, May 2018.

[83] W. Sun, J. Liu, Y. Yue, and P. Wang, "Joint resource allocation and incentive design for blockchain-based mobile edge computing," *IEEE Trans. Wireless Commun.*, vol. 19, no. 9, pp. 6050–6064, Sept. 2020.

[84] S. Wang, D. Ye, X. Huang, R. Yu, Y. Wang, and Y. Zhang, "Consortium blockchain for secure resource sharing in vehicular edge computing: A contract-based approach," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1189–1201, Jun. 2021.

[85] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019.

[86] J. Sun, X. Yao, S. Wang, and Y. Wu, "Blockchain-based secure storage and access scheme for electronic medical records in IPFS," *IEEE Access*, vol. 8, pp. 59 389–59 401, Mar. 2020.

[87] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, "Blockchain empowered arbitrable data auditing scheme for network storage as a service," *IEEE Trans. Serv. Comput.*, vol. 13, no. 2, pp. 289–300, Apr. 2020.

[88] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," *IET Commun.*, vol. 12, pp. 527–532, Feb. 2018.

[89] A. El Gamal and H. El Gamal, "A single coin monetary mechanism for distributed cooperative interference management," *IEEE Wireless Commun. Lett.*, vol. 8, no. 3, pp. 757–760, Jun. 2019.

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

[91] Z. Liu, L. Gao, Y. Liu, X. Guan, K. Ma, and Y. Wang, "Efficient QoS support for robust resource allocation in blockchain-based femtocell networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 11, pp. 7070–7080, Nov. 2020.

[92] A. P. Singh, N. R. Pradhan, A. K. Luhach, S. Agnihotri, N. Z. Jhanjhi, S. Verma, Kavita, U. Ghosh, and D. S. Roy, "A novel patient-centric architectural framework for blockchain-enabled healthcare applications," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5779–5789, Aug. 2021.

[93] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "BEdge-Health: A decentralized architecture for edge-based IoMT networks using blockchain," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11 743–11 757, Jul. 2021.

[94] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and M. Aledhari, "Decentralized authentication of distributed patients in hospital networks using blockchain," *IEEE J. Biomed. Health Inform.*, vol. 24, no. 8, pp. 2146–2156, Aug. 2020.

[95] S. Xia, F. Lin, Z. Chen, C. Tang, Y. Ma, and X. Yu, "A bayesian game based vehicle-to-vehicle electricity trading scheme for blockchain-enabled internet of vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 6856–6868, Jul. 2020.

[96] Y. Yin, Y. Li, B. Ye, T. Liang, and Y. Li, "A blockchain-based incremental update supported data storage system for intelligent vehicles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4880–4893, May 2021.

[97] D. Chattaraj, B. Bera, A. K. Das, S. Saha, P. Lorenz, and Y. Park, "Block-CLAP: Blockchain-assisted certificateless key agreement protocol for internet of vehicles in smart transportation," *IEEE Trans. Veh. Technol.*, vol. 70, no. 8, pp. 8092–8107, Aug. 2021.

[98] J. Wang, L. Wu, K.-K. R. Choo, and D. He, "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1984–1992, Mar. 2020.

[99] B. Bera, S. Saha, A. K. Das, and A. V. Vasilakos, "Designing blockchain-based access control protocol in IoT-enabled smart-grid system," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5744–5761, Apr. 2021.

[100] A. Jindal, G. S. Aujla, N. Kumar, and M. Villari, "GUARDIAN: Blockchain-based secure demand response management in smart grid system," *IEEE Trans. Serv. Comput.*, vol. 13, no. 4, pp. 613–624, Jul.-Aug. 2020.

[101] K. Gai, Y. Wu, L. Zhu, K.-K. R. Choo, and B. Xiao, "Blockchain-enabled trustworthy group communications in UAV networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4118–4130, Jul. 2021.

[102] Y. Tan, J. Liu, and N. Kato, "Blockchain-based key management for heterogeneous flying ad hoc network," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7629–7638, Nov. 2021.

[103] L. Jiang, B. Chen, S. Xie, S. Maharjan, and Y. Zhang, "Incentivizing resource cooperation for blockchain empowered wireless power transfer in UAV networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15 828–15 841, Dec. 2020.

[104] J. Guo, C.-K. Wen, S. Jin, and G. Y. Li, "Overview of deep learning-based CSI feedback in massive MIMO systems," *IEEE Trans. Commun.*, vol. 70, no. 12, pp. 8017–8045, Dec. 2022.

[105] N. J. Nilsson, *The quest for artificial intelligence*. Cambridge University Press, 2009.

[106] P. H. Winston, *Artificial intelligence*. Addison-Wesley Longman Publishing Co., Inc., 1992.

[107] A. Barr, E. A. Feigenbaum, and P. R. Cohen, *The handbook of artificial intelligence*. William Kaufmann, 1981, vol. 1.

[108] Q. Mao, F. Hu, and Q. Hao, "Deep learning for intelligent wireless networks: A comprehensive survey," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 4, pp. 2595–2621, Jun. 2018.

[109] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015.

[110] J. Zhou, T. Han, F. Xiao, G. Gui, B. Adebisi, H. Gacanin, and H. Sari, "Multiscale network traffic prediction method based on deep echo-state network for internet of things," *IEEE Internet Things J.*, vol. 9, no. 21, pp. 21 862–21 874, Nov. 2022.

[111] I. Goodfellow, Y. Bengio, and A. Courville, *Deep learning*. MIT press, 2016.

[112] L. Bottou and O. Bousquet, "The tradeoffs of large scale learning," *In Proc. Advances in Neural Information Processing Systems*, vol. 20, pp. 161–168, 2007.

[113] G. E. Hinton, S. Osindero, and Y.-W. Teh, "A fast learning algorithm for deep belief nets," *Neural Comput.*, vol. 18, no. 7, pp. 1527–1554, Jul. 2006.

[114] Q. Xue, Y.-J. Liu, Y. Sun, J. Wang, L. Yan, G. Feng, and S. Ma, "Beam management in ultra-dense mmwave network via federated reinforcement learning: An intelligent and secure approach," *IEEE Trans. on Cogn. Commun. Netw.*, vol. 9, no. 1, pp. 185–197, Feb. 2023.

[115] K. Arulkumaran, M. P. Deisenroth, M. Brundage, and A. A. Bharath, "Deep reinforcement learning: A brief survey," *IEEE Signal Process. Mag.*, vol. 34, no. 6, pp. 26–38, Nov. 2017.

[116] Y. LeCun, B. Boser, J. Denker, D. Henderson, R. Howard, W. Hubbard, and L. Jackel, "Handwritten digit recognition with a back-propagation network," *In Proc. Advances in Neural Information Processing Systems*, vol. 2, pp. 396–404, 1989.

[117] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proceedings of the IEEE*, vol. 86, no. 11, pp. 2278–2324, Nov. 1998.

[118] Z. C. Lipton, J. Berkowitz, and C. Elkan, "A critical review of recurrent neural networks for sequence learning," *arXiv preprint arXiv:1506.00019*, 2015.

[119] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial nets," *In Proc. Advances in Neural Information Processing Systems*, vol. 27, 2014.

[120] J.-M. Kang, C.-J. Chun, and I.-M. Kim, "Deep-learning-based channel estimation for wireless energy transfer," *IEEE Commun. Lett.*, vol. 22, no. 11, pp. 2310–2313, Nov. 2018.

[121] H. Huang, J. Yang, H. Huang, Y. Song, and G. Gui, "Deep learning for super-resolution channel estimation and DOA estimation based massive MIMO system," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8549–8560, Sept. 2018.

[122] H. He, C.-K. Wen, S. Jin, and G. Y. Li, "Deep learning-based channel estimation for beamspace mmWave massive MIMO systems," *IEEE Wireless Commun. Lett.*, vol. 7, no. 5, pp. 852–855, Oct. 2018.

[123] M. Borgerding, P. Schniter, and S. Rangan, "AMP-inspired deep networks for sparse linear inverse problems," *IEEE Trans. Signal Process.*, vol. 65, no. 16, pp. 4293–4308, Aug. 2017.

[124] D. Neumann, T. Wiese, and W. Utschick, "Learning the MMSE channel estimator," *IEEE Trans. Signal Process.*, vol. 66, no. 11, pp. 2905–2917, Jun. 2018.

[125] H. Ye, G. Y. Li, and B.-H. Juang, "Power of deep learning for channel estimation and signal detection in OFDM systems," *IEEE Wireless Commun. Lett.*, vol. 7, no. 1, pp. 114–117, Feb. 2018.

[126] N. Samuel, T. Diskin, and A. Wiesel, "Deep MIMO detection," in *2017 IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. Sapporo, Japan: IEEE, Jul. 2017, pp. 1–5.

[127] H. He, C.-K. Wen, S. Jin, and G. Y. Li, "A model-driven deep learning network for MIMO detection," in *2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*. Anaheim, CA, USA: IEEE, Nov. 2018, pp. 584–588.

[128] J. Liao, J. Zhao, F. Gao, and G. Y. Li, "A model-driven deep learning method for massive MIMO detection," *IEEE Commun. Lett.*, vol. 24, no. 8, pp. 1724–1728, Aug. 2020.

[129] Q. Cao, F. Li, T. Li, W. Ji, and Y. Liang, "Adaptive signal detection method based on model-driven for massive MIMO systems," in *2021 13th International Conference on Wireless Communications and Signal Processing (WCSP)*. Changsha, China: IEEE, Oct. 2021, pp. 1–5.

[130] C.-K. Wen, W.-T. Shih, and S. Jin, "Deep learning for massive MIMO CSI feedback," *IEEE Wireless Commun. Lett.*, vol. 7, no. 5, pp. 748–751, Oct. 2018.

[131] T. Wang, C.-K. Wen, S. Jin, and G. Y. Li, "Deep learning-based CSI feedback approach for time-varying massive MIMO channels," *IEEE Wireless Commun. Lett.*, vol. 8, no. 2, pp. 416–419, Apr. 2019.

[132] Z. Liu, L. Zhang, and Z. Ding, "Exploiting bi-directional channel reciprocity in deep learning for low rate massive MIMO CSI feedback," *IEEE Wireless Commun. Lett.*, vol. 8, no. 3, pp. 889–892, Jun. 2019.

[133] J. Guo, J. Wang, C.-K. Wen, S. Jin, and G. Y. Li, "Compression and acceleration of neural networks for communications," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 110–117, Aug. 2020.

[134] P. K. Sangdeh, H. Pirayesh, A. Mobiny, and H. Zeng, "LB-SciFi: Online learning-based channel feedback for MU-MIMO in wireless LANs," in *2020 IEEE 28th International Conference on Network Protocols (ICNP)*. Madrid, Spain: IEEE, Oct. 2020, pp. 1–11.

[135] T. Gruber, S. Cammerer, J. Hoydis, and S. ten Brink, "On deep learning-based channel decoding," in *2017 51st Annual Conference on Information Sciences and Systems (CISS)*. Baltimore, MD, USA: IEEE, Mar. 2017, pp. 1–6.

[136] S. Cammerer, T. Gruber, J. Hoydis, and S. Ten Brink, "Scaling deep learning-based decoding of polar codes via partitioning," in *2017 IEEE global communications conference (GLOBECOM)*. Singapore: IEEE, Dec. 2017, pp. 1–6.

[137] F. Liang, C. Shen, and F. Wu, "An iterative BP-CNN architecture for channel decoding," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 1, pp. 144–159, Feb. 2018.

[138] E. Nachmani, Y. Be'ery, and D. Burshtein, "Learning to decode linear codes using deep learning," in *2016 54th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. Monticello, IL, USA: IEEE, Sept. 2016, pp. 341–346.

[139] E. Nachmani, E. Marciano, L. Lugosch, W. J. Gross, D. Burshtein, and Y. Be'ery, "Deep learning methods for improved decoding of linear codes," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 1, pp. 119–131, Feb. 2018.

[140] S. Dörner, S. Cammerer, J. Hoydis, and S. Ten Brink, "Deep learning based communication over the air," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 1, pp. 132–143, Feb. 2017.

[141] H. Ye, G. Y. Li, B.-H. F. Juang, and K. Sivanesan, "Channel agnostic end-to-end learning based communication systems with conditional GAN," in *2018 IEEE Globecom Workshops (GC Wkshps)*. Abu Dhabi, United: IEEE, Dec. 2018, pp. 1–5.

[142] M. Damrath and P. A. Hoeher, "Low-complexity adaptive threshold detection for molecular communication," *IEEE Trans. Nanobiosci.*, vol. 15, no. 3, pp. 200–208, Apr. 2016.

[143] N. Farsad and A. Goldsmith, "Sliding bidirectional recurrent neural networks for sequence detection in communication systems," in *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. Calgary, AB, Canada: IEEE, Apr. 2018, pp. 2331–2335.

[144] S. Mohamed, J. Dong, A. Junejo *et al.*, "Model-based: End-to-end molecular communication system through deep reinforcement learning auto encoder," *IEEE Access*, vol. 7, pp. 70 279–70 286, May 2019.

[145] Y. Zhao, I. G. Niemegeers, and S. H. De Groot, "Power allocation in cell-free massive MIMO: A deep learning method," *IEEE Access*, vol. 8, pp. 87 185–87 200, May 2020.

[146] C. D'Andrea, A. Zappone, S. Buzzi, and M. Debbah, "Uplink power control in cell-free massive MIMO via deep learning," in *2019 IEEE 8th International Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP)*. Le gosier, Guadeloupe: IEEE, Dec. 2019, pp. 554–558.

[147] N. Rajapaksha, K. S. Manosha, N. Rajatheva, and M. Latva-Aho, "Deep learning-based power control for cell-free massive MIMO networks," in *ICC 2021-IEEE International Conference on Communications*. Montreal, QC, Canada: IEEE, Jun. 2021, pp. 1–7.

[148] W. Cui, K. Shen, and W. Yu, "Spatial deep learning for wireless scheduling," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 6, pp. 1248–1261, Jun. 2019.

[149] S. Xu, P. Liu, R. Wang, and S. S. Panwar, "Realtime scheduling and power allocation using deep neural networks," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*. Marrakesh, Morocco: IEEE, Apr. 2019, pp. 1–5.

[150] X. Li, J. Fang, W. Cheng, H. Duan, Z. Chen, and H. Li, "Intelligent power control for spectrum sharing in cognitive radios: A deep reinforcement learning approach," *IEEE Access*, vol. 6, pp. 25 463–25 473, Apr. 2018.

[151] Y. S. Nasir and D. Guo, "Multi-agent deep reinforcement learning for dynamic power allocation in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 10, pp. 2239–2250, Oct. 2019.

[152] J. Tan, Y.-C. Liang, L. Zhang, and G. Feng, "Deep reinforcement learning for joint channel selection and power control in D2D networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 2, pp. 1363–1378, Feb. 2021.

[153] A. Sadeghi, G. Wang, and G. B. Giannakis, "Deep reinforcement learning for adaptive caching in hierarchical content delivery networks," *IEEE Trans. on Cogn. Commun. Netw.*, vol. 5, no. 4, pp. 1024–1033, Dec. 2019.

[154] J. Ren, H. Wang, T. Hou, S. Zheng, and C. Tang, "Federated learning-based computation offloading optimization in edge computing-supported internet of things," *IEEE Access*, vol. 7, pp. 69 194–69 201, Jun. 2019.

[155] X. Wang, Y. Han, C. Wang, Q. Zhao, X. Chen, and M. Chen, "In-edge AI: Intelligentizing mobile edge computing, caching and communication by federated learning," *IEEE Netw.*, vol. 33, no. 5, pp. 156–165, Sept. 2019.

[156] Y. He, C. Liang, F. R. Yu, and Z. Han, "Trust-based social networks with computing, caching and communications: A deep reinforcement learning approach," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 1, pp. 66–79, Jan. 2020.

[157] Y. He, N. Zhao, and H. Yin, "Integrated networking, caching, and computing for connected vehicles: A deep reinforcement learning approach," *IEEE Trans. Veh. Technol.*, vol. 67, no. 1, pp. 44–55, Jan. 2018.

[158] A. Ndikumana, N. H. Tran, T. M. Ho, Z. Han, W. Saad, D. Niyato, and C. S. Hong, "Joint communication, computation, caching, and control in big data multi-access edge computing," *IEEE Trans. Mobile Comput.*, vol. 19, no. 6, pp. 1359–1374, Jun. 2020.

[159] Y. Xu, W. Xu, Z. Wang, J. Lin, and S. Cui, "Load balancing for ultradense networks: A deep reinforcement learning-based approach," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9399–9412, Dec. 2019.

[160] N. Zhao, Y.-C. Liang, D. Niyato, Y. Pei, M. Wu, and Y. Jiang, "Deep reinforcement learning for user association and resource allocation in heterogeneous cellular networks," *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5141–5152, Nov. 2019.

[161] F. B. Mismar and B. L. Evans, "Deep Q-learning for self-organizing networks fault management and radio performance improvement," in *2018 52nd Asilomar Conference on Signals, Systems, and Computers*. Pacific Grove, CA, USA: IEEE, Oct. 2018, pp. 1457–1461.

[162] J. Ye and Y.-J. A. Zhang, "DRAG: Deep reinforcement learning based base station activation in heterogeneous networks," *IEEE Trans. Mobile Comput.*, vol. 19, no. 9, pp. 2076–2087, Sept. 2020.

[163] J. Liu, B. Krishnamachari, S. Zhou, and Z. Niu, "DeepNap: Data-driven base station sleeping operations through deep reinforcement learning," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4273–4282, Dec. 2018.

[164] J. Wu, P. Yu, L. Feng, F. Zhou, W. Li, and X. Qiu, "3D aerial base station position planning based on deep Q-network for capacity enhancement," in *2019 IFIP/IEEE Symposium on Integrated Network*

and Service Management (IM). Arlington, VA, USA: IEEE, Apr. 2019, pp. 482–487.

[165] J. D. Harris and B. Waggoner, "Decentralized and collaborative AI on blockchain," in *2019 IEEE International Conference on Blockchain (Blockchain)*. Atlanta, GA, USA, Jul. 2019, pp. 368–375.

[166] G. Zhang, T. Li, Y. Li, P. Hui, and D. Jin, "Blockchain-based data sharing system for AI-powered network operations," *J. Commun. Inf. Netw.*, vol. 3, no. 3, pp. 1–8, Sept. 2018.

[167] K. Wang, J. Dong, Y. Wang, and H. Yin, "Securing data with blockchain and AI," *IEEE Access*, vol. 7, pp. 77 981–77 989, Jun. 2019.

[168] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3516–3526, Jun 2019.

[169] G. J. Mendis, Y. Wu, J. Wei, M. Sabounchi, and R. Roche, "A blockchain-powered decentralized and secure computing paradigm," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 4, pp. 2201–2222, Oct.-Dec. 2021.

[170] Q. Wang, Y. Guo, X. Wang, T. Ji, L. Yu, and P. Li, "AI at the edge: Blockchain-empowered secure multiparty learning with heterogeneous models," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9600–9610, Oct. 2020.

[171] C. Korkmaz, H. E. Kocas, A. Uysal, A. Masry, O. Ozkasap, and B. Akgun, "Chain FL: Decentralized federated machine learning via blockchain," in *2020 Second International Conference on Blockchain Computing and Applications (BCCA)*. Antalya, Turkey, Nov. 2020, pp. 140–146.

[172] X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, "Making knowledge tradable in edge-AI enabled IoT: A consortium blockchain-based efficient and incentive approach," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6367–6378, Dec. 2019.

[173] R. Gupta, D. Reebadiya, S. Tanwar, N. Kumar, and M. Guizani, "When blockchain meets edge intelligence: Trusted and security solutions for consumers," *IEEE Netw.*, vol. 35, no. 5, pp. 272–278, Sept. 2021.

[174] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, "DeepChain: Auditable and privacy-preserving deep learning with blockchain-based incentive," *IEEE Trans. Depend. Sec. Comput.*, vol. 18, no. 5, pp. 2438–2455, Sept.-Oct. 2021.

[175] M. Shayan, C. Fung, C. J. M. Yoon, and I. Beschastnikh, "Biscotti: A blockchain system for private and secure federated learning," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 7, pp. 1513–1525, Jul. 2021.

[176] L. Feng, Y. Zhao, S. Guo, X. Qiu, W. Li, and P. Yu, "Blockchain-based asynchronous federated learning for internet of things," *IEEE Trans. Comput.*, vol. 99, pp. 1–9, Apr. 2021.

[177] M. Nassar, K. Salah, M. H. ur Rehman, and D. Svetinovic, "Blockchain for explainable and trustworthy artificial intelligence," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 10, no. 1, p. e1340, Oct. 2020.

[178] K. Sarpatwar, R. Vaculin, H. Min, G. Su, T. Heath, G. Ganapavarapu, and D. Dillenberger, "Towards enabling trusted artificial intelligence via blockchain," in *Policy-based autonomic data governance*. Springer, Apr. 2019, pp. 137–153.

[179] J. Kang, Z. Xiong, D. Niyato, S. Xie, and J. Zhang, "Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10 700–10 714, Dec. 2019.

[180] X. Bao, C. Su, Y. Xiong, W. Huang, and Y. Hu, "FLChain: A blockchain for auditable federated learning with trust and incentive," in *2019 5th International Conference on Big Data Computing and Communications (BIGCOM)*. QingDao, China, Aug. 2019, pp. 151–159.

[181] 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. Informat.*, vol. 15, no. 6, pp. 3559–3570, Jun. 2019.

[182] J. Yun, Y. Goh, and J.-M. Chung, "DQN-based optimization framework for secure sharded blockchain systems," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 708–722, Jan. 2021.

[183] C. Qiu, X. Ren, Y. Cao, and T. Mai, "Deep reinforcement learning empowered adaptivity for future blockchain networks," *IEEE Open J. Comm. Soc.*, vol. 2, pp. 99–105, Jul. 2021.

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

[185] F. Bravo-Marquez, S. Reeves, and M. Ugarte, "Proof-of-learning: a blockchain consensus mechanism based on machine learning competitions," in *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)*. Newark, CA, USA, Apr. 2019, pp. 119–124.

[186] C. Chenli, B. Li, Y. Shi, and T. Jung, "Energy-recycling blockchain with proof-of-deep-learning," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. Seoul, Korea (South), May 2019, pp. 19–23.

[187] A. Baldominos and Y. Saez, "Coin.AI: A proof-of-useful-work scheme for blockchain-based distributed deep learning," *Entropy*, vol. 21, no. 8, p. 723, Jul. 2019.

[188] J. Chen, K. Duan, R. Zhang, L. Zeng, and W. Wang, "An AI based super nodes selection algorithm in blockchain networks," *arXiv preprint arXiv:1808.00216*, Aug. 2018.

[189] W. Chen, Z. Zheng, J. Cui, E. Ngai, P. Zheng, and Y. Zhou, "Detecting ponzi schemes on ethereum: Towards healthier blockchain technology," in *2018 world wide web conference*, Apr. 2018, pp. 1409–1418.

[190] M. Salimitari, M. Joneidi, and M. Chatterjee, "AI-enabled blockchain: An outlier-aware consensus protocol for blockchain-based IoT networks," in *2019 IEEE Global Communications Conference (GLOBECOM)*. Waikoloa, HI, USA, Dec. 2019, pp. 1–6.

[191] W. Liang, L. Xiao, K. Zhang, M. Tang, D. He, and K.-C. Li, "Data fusion approach for collaborative anomaly intrusion detection in blockchain-based systems," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14 741–14 751, Aug. 2022.

[192] F. Scicchitano, A. Liguori, M. Guarascio, E. Ritacco, and G. Manco, "A deep learning approach for detecting security attacks on blockchain." in *ITASEC*, 2020, pp. 212–222.

[193] M. Mudassir, S. Bennbaia, D. Unal, and M. Hammoudeh, "Time-series forecasting of bitcoin prices using high-dimensional features: a machine learning approach," *Neural Comput. Appl.*, pp. 1–15, Jul. 2020.

[194] H. J. Singh and A. S. Hafid, "Prediction of transaction confirmation time in ethereum blockchain using machine learning," in *International Congress on Blockchain and Applications*. Springer, Jun. 2019, pp. 126–133.

[195] S. Mohammadi and E. Rabieinejad, *Prediction forks in the blockchain using machine learning*, Dec. 2020.

[196] Q. Pan, J. Wu, J. Li, W. Yang, and Z. Guan, "Blockchain and AI empowered trust-information-centric network for beyond 5G," *IEEE Netw.*, vol. 34, no. 6, pp. 38–45, Nov. 2020.

[197] K. Zhang, Y. Zhu, S. Maharjan, and Y. Zhang, "Edge intelligence and blockchain empowered 5G beyond for the industrial internet of things," *IEEE Netw.*, vol. 33, no. 5, pp. 12–19, Sept. 2019.

[198] S. Rathore, J. H. Park, and H. Chang, "Deep learning and blockchain-empowered security framework for intelligent 5G-enabled IoT," *IEEE Access*, vol. 9, pp. 90 075–90 083, Jun. 2021.

[199] S. Hu, Y.-C. Liang, Z. Xiong, and D. Niyato, "Blockchain and artificial intelligence for dynamic resource sharing in 6G and beyond," *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 145–151, Aug. 2021.

[200] T. Maksymyuk, J. Gazda, M. Liyanage, L. Han, B. Shubyn, B. Strykhaliuk, O. Yaremko, M. Jo, and M. Dohler, "AI-enabled blockchain framework for dynamic spectrum management in multi-operator 6G networks," in *Future Intent-Based Networking*. Springer, 2022, pp. 322–338.

[201] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for 5G beyond," *IEEE Netw.*, vol. 35, no. 1, pp. 219–225, Jan. 2020.

[202] ——, "Communication-efficient federated learning and permissioned blockchain for digital twin edge networks," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2276–2288, Feb. 2020.

[203] F. Guo, F. R. Yu, H. Zhang, H. Ji, M. Liu, and V. C. Leung, "Adaptive resource allocation in future wireless networks with blockchain and mobile edge computing," *IEEE Trans. Wireless Commun.*, vol. 19, no. 3, pp. 1689–1703, Mar. 2020.

[204] G. Gür, "Expansive networks: Exploiting spectrum sharing for capacity boost and 6G vision," *J. Commun. Networks*, vol. 22, no. 6, pp. 444–454, Dec. 2020.

[205] C. Qiu, F. R. Yu, H. Yao, C. Jiang, F. Xu, and C. Zhao, "Blockchain-based software-defined industrial internet of things: A dueling deep Q-learning approach," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4627–4639, Jun. 2019.

[206] Y. He, Y. Wang, C. Qiu, Q. Lin, J. Li, and Z. Ming, "Blockchain-based edge computing resource allocation in IoT: a deep reinforcement learning approach," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2226–2237, Feb. 2021.

[207] G. Manogaran, S. Mumtaz, C. X. Mavromoustakis, E. Pallis, and G. Mastorakis, "Artificial intelligence and blockchain-assisted offload-

ing approach for data availability maximization in edge nodes," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2404–2412, Mar. 2021.

[208] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Secure computation offloading in blockchain based IoT networks with deep reinforcement learning," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 4, pp. 3192–3208, Oct. 2021.

[209] H. Liao, Y. Mu, Z. Zhou, M. Sun, Z. Wang, and C. Pan, "Blockchain and learning-based secure and intelligent task offloading for vehicular fog computing," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4051–4063, Jul. 2020.

[210] H. Liao, Z. Wang, Z. Zhou, Y. Wang, H. Zhang, S. Mumtaz, and M. Guizani, "Blockchain and semi-distributed learning-based secure and low-latency computation offloading in space-air-ground-integrated power IoT," *IEEE J. Sel. Topics Signal Process.*, vol. 16, no. 3, pp. 381–394, Apr. 2022.

[211] C. Qiu, H. Yao, X. Wang, N. Zhang, F. R. Yu, and D. Niyato, "AI-Chain: blockchain energized edge intelligence for beyond 5G networks," *IEEE Netw.*, vol. 34, no. 6, pp. 62–69, Nov. 2020.

[212] Y. Qian, Y. Jiang, L. Hu, M. S. Hossain, M. Alrashoud, and M. Al-Hammadi, "Blockchain-based privacy-aware content caching in cognitive internet of vehicles," *IEEE Netw.*, vol. 34, no. 2, pp. 46–51, Mar. 2020.

[213] Y. Dai, D. Xu, K. Zhang, S. Maharjan, and Y. Zhang, "Deep reinforcement learning and permissioned blockchain for content caching in vehicular edge computing and networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4312–4324, Apr. 2020.

[214] 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, Oct. 2020.

[215] L. Cui, X. Su, Z. Ming, Z. Chen, S. Yang, Y. Zhou, and W. Xiao, "CREAT: Blockchain-assisted compression algorithm of federated learning for content caching in edge computing," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14 151–14 161, Aug. 2022.

[216] R. Zhang, F. R. Yu, J. Liu, T. Huang, and Y. Liu, "Deep reinforcement learning (DRL)-based device-to-device (D2D) caching with blockchain and mobile edge computing," *IEEE Trans. Wireless Commun.*, vol. 19, no. 10, pp. 6469–6485, Oct. 2020.

[217] N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi, and M. Usman, "Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures," *ACM Computing Surveys (CSUR)*, vol. 53, no. 6, pp. 1–37, Nov. 2021.

[218] N. Dhieb, H. Ghazzai, H. Besbes, and Y. Massoud, "Scalable and secure architecture for distributed IoT systems," in *2020 IEEE Technology & Engineering Management Conference (TEMSCON)*, Novi, MI, USA, Jun. 2020, pp. 1–6.

[219] X. Wang, S. Garg, H. Lin, M. J. Piran, J. Hu, and M. S. Hossain, "Enabling secure authentication in industrial IoT with transfer learning empowered blockchain," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7725–7733, Nov. 2021.

[220] Y. Tian, T. Li, J. Xiong, M. Z. A. Bhuiyan, J. Ma, and C. Peng, "A blockchain-based machine learning framework for edge services in IIoT," *IEEE Trans. Ind. Informat.*, vol. 18, no. 3, pp. 1918–1929, Mar. 2022.

[221] H. Lin, S. Garg, J. Hu, G. Kaddoum, M. Peng, and M. S. Hossain, "Blockchain and deep reinforcement learning empowered spatial crowdsourcing in software-defined internet of vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3755–3764, Jun. 2021.

[222] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, N. Kumar, and M. M. Hassan, "A privacy-preserving-based secure framework using blockchain-enabled deep-learning in cooperative intelligent transport system," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 16 492–16 503, Sept. 2022.

[223] C. Zhang, W. Li, Y. Luo, and Y. Hu, "AIT: An AI-enabled trust management system for vehicular networks using blockchain technology," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3157–3169, Mar. 2021.

[224] W. Zhang, Q. Lu, Q. Yu, Z. Li, Y. Liu, S. K. Lo, S. Chen, X. Xu, and L. Zhu, "Blockchain-based federated learning for device failure detection in industrial IoT," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5926–5937, Apr. 2021.

[225] S. Otoum, I. Al Ridhawi, and H. Mouftah, "Securing critical IoT infrastructures with blockchain-supported federated learning," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2592–2601, Feb. 2022.

[226] 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. Informat.*, vol. 16, no. 6, pp. 4177–4186, Jun. 2020.

[227] P. Zhang, Y. Hong, N. Kumar, M. Alazab, M. D. Alshehri, and C. Jiang, "BC-EdgeFL: Defensive transmission model based on blockchain assisted reinforced federated learning in IIoT environment," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3551–3561, May 2022.

[228] H. Liu, S. Zhang, P. Zhang, X. Zhou, X. Shao, G. Pu, and Y. Zhang, "Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 6073–6084, Jun. 2021.

[229] 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, Apr. 2021.

[230] A. Z. Al-Marridi, A. Mohamed, and A. Erbad, "Reinforcement learning approaches for efficient and secure blockchain-powered smart health systems," *Comput. Netw.*, vol. 197, p. 108279, Oct. 2021.

[231] T. Veeramakali, R. Siva, B. Sivakumar, P. Senthil Mahesh, and N. Krishnaraj, "An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model," *J. Supercomput.*, vol. 77, no. 9, pp. 9576–9596, Feb. 2021.

[232] R. Kumar, A. A. Khan, J. Kumar, N. A. Golilarz, S. Zhang, Y. Ting, C. Zheng, W. Wang *et al.*, "Blockchain-federated-learning and deep learning models for COVID-19 detection using CT imaging," *IEEE Sensors J.*, vol. 21, no. 14, pp. 16 301–16 314, Jul. 2021.

[233] S. Otoum, I. Al Ridhawi, and H. T. Mouftah, "Preventing and controlling epidemics through blockchain-assisted AI-enabled networks," *IEEE Netw.*, vol. 35, no. 3, pp. 34–41, May 2021.

[234] B. Mallikarjuna, G. Shrivastava, and M. Sharma, "Blockchain technology: A DNN token-based approach in healthcare and COVID-19 to generate extracted data," *Expert Syst.*, p. e12778, Jul. 2021.

[235] X. Guo, M. A. Khalid, I. Domingos, A. L. Michala, M. Adriko, C. Rowel, D. Ajambo, A. Garrett, S. Kar, X. Yan *et al.*, "Smartphone-based DNA diagnostics for malaria detection using deep learning for local decision support and blockchain technology for security," *Nat. Electron.*, vol. 4, no. 8, pp. 615–624, Aug. 2021.

[236] R. Gupta, A. Shukla, and S. Tanwar, "BATS: A blockchain and AI-empowered drone-assisted telesurgery system towards 6G," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 4, pp. 2958–2967, Oct. 2021.

[237] I. Al Ridhawi, M. Aloqaily, A. Boukerche, and Y. Jararweh, "Enabling intelligent IoCV services at the edge for 5G networks and beyond," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5190–5200, Aug. 2021.

[238] V. Hassija, V. Gupta, S. Garg, and V. Chamola, "Traffic jam probability estimation based on blockchain and deep neural networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 3919–3928, Jul. 2021.

[239] K. Tiba, R. M. Parizi, Q. Zhang, A. Dehghantanha, H. Karimipour, and K.-K. R. Choo, "Secure blockchain-based traffic load balancing using edge computing and reinforcement learning," in *Blockchain Cybersecurity, Trust and Privacy*. Springer, Mar. 2020, pp. 99–128.

[240] Y. Song, Y. Fu, F. R. Yu, and L. Zhou, "Blockchain-enabled internet of vehicles with cooperative positioning: A deep neural network approach," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3485–3498, Apr. 2020.

[241] D. Zhang, F. R. Yu, and R. Yang, "Blockchain-based distributed software-defined vehicular networks: A dueling deep Q-learning approach," *IEEE Trans. on Cogn. Commun. Netw.*, vol. 5, no. 4, pp. 1086–1100, Dec. 2019.

[242] X. Jiang, F. R. Yu, T. Song, and V. C. Leung, "Intelligent resource allocation for video analytics in blockchain-enabled internet of autonomous vehicles with edge computing," *IEEE Internet Things J*, vol. 9, no. 16, pp. 14 260–14 272, Aug. 2022.

[243] Y. Fu, C. Li, F. R. Yu, T. H. Luan, and Y. Zhang, "An autonomous lane-changing system with knowledge accumulation and transfer assisted by vehicular blockchain," *IEEE Internet Things J.*, vol. 7, no. 11, pp. 11 123–11 136, Nov. 2020.

[244] S. R. Pokhrel and J. Choi, "Federated learning with blockchain for autonomous vehicles: Analysis and design challenges," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 4734–4746, Aug. 2020.

[245] 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, Apr. 2020.

[246] H. Chai, S. Leng, Y. Chen, and K. Zhang, "A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 3975–3986, Jul. 2021.

[247] N. M. Kumar, A. A. Chand, M. Malvoni, K. A. Prasad, K. A. Mamun, F. Islam, and S. S. Chopra, "Distributed energy resources and the

application of AI, IoT, and blockchain in smart grids," *Energies*, vol. 13, no. 21, p. 5739, Nov. 2020.

[248] M. Keshk, B. Turnbull, N. Moustafa, D. Vatsalan, and K.-K. R. Choo, "A privacy-preserving-framework-based blockchain and deep learning for protecting smart power networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 8, pp. 5110–5118, Aug. 2020.

[249] Z. Wang, M. Ogbodo, H. Huang, C. Qiu, M. Hisada, and A. B. Abdallah, "AEBIS: AI-enabled blockchain-based electric vehicle integration system for power management in smart grid platform," *IEEE Access*, vol. 8, pp. 226 409–226 421, Dec. 2020.

[250] M. A. Ferrag and L. Maglaras, "DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1285–1297, Nov. 2020.

[251] F. Jamil, N. Iqbal, S. Ahmad, D. Kim *et al.*, "Peer-to-peer energy trading mechanism based on blockchain and machine learning for sustainable electrical power supply in smart grid," *IEEE Access*, vol. 9, pp. 39 193–39 217, Feb. 2021.

[252] G. Gao, C. Song, A. Bandara, M. Shen, F. Yang, W. Posdorfer, D. Tao, and Y. Wen, "FogChain: a blockchain-based peer-to-peer solar power trading system powered by fog AI," *IEEE Internet Things J.*, vol. 9, no. 7, pp. 5200–5215, Apr. 2022.

[253] Z. Li, J. Xu, Y. Xie, J. Jiang, Y. Zhu, and X. Yang, "Integration of blockchain and machine learning for microgrids," in *2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS)*, Chengdu, China, Apr. 2021, pp. 211–216.

[254] M. Singh, G. S. Aujla, and R. S. Bali, "A deep learning-based blockchain mechanism for secure internet of drones environment," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4404–4413, Jul. 2021.

[255] C. Feng, B. Liu, K. Yu, S. K. Goudos, and S. Wan, "Blockchain-empowered decentralized horizontal federated learning for 5G-enabled UAVs," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, May 2022.

[256] A. Asheralieva and D. Niyato, "Distributed dynamic resource management and pricing in the IoT systems with blockchain-as-a-service and UAV-enabled mobile edge computing," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1974–1993, Mar. 2020.

[257] S. R. Pokhrel, "Blockchain brings trust to collaborative drones and LEO satellites: an intelligent decentralized learning in the space," *IEEE Sensors J.*, vol. 21, no. 22, pp. 25 331–25 339, Nov. 2021.

[258] A. Islam, T. Rahim, M. Masuduzzaman, and S. Y. Shin, "A blockchain-based artificial intelligence-empowered contagious pandemic situation supervision scheme using internet of drone things," *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 166–173, Aug. 2021.

[259] A. Gumaei, M. Al-Rakhami, M. M. Hassan, P. Pace, G. Alai, K. Lin, and G. Fortino, "Deep learning and blockchain with edge computing for 5G-enabled drone identification and flight mode detection," *IEEE Netw.*, vol. 35, no. 1, pp. 94–100, Jan. 2021.

[260] A. Aftab, N. Ashraf, H. K. Qureshi, S. A. Hassan, and S. Jangsher, "BLOCK-ML: blockchain and machine learning for UAV-BSs deployment," in *2020 IEEE 92nd Vehicular Technology Conference (VTC-Fall)*, Victoria, BC, Canada, Nov. 2020, pp. 1–5.

[261] S. R. Pokhrel, "Federated learning meets blockchain at 6G edge: A drone-assisted networking for disaster response," in *Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond*, Sept. 2020, pp. 49–54.

[262] Y.-C. Liang, *Dynamic spectrum management: From cognitive radio to blockchain and artificial intelligence*. Springer Nature, 2020.

[263] C.-X. Wang, X. You, X. Gao, X. Zhu, Z. Li, C. Zhang, H. Wang, Y. Huang, Y. Chen, H. Haas *et al.*, "On the road to 6G: Visions, requirements, key technologies and testbeds," *IEEE Commun. Surv. Tutor.*, vol. 25, no. 2, pp. 905–974, Feb. 2023.

[264] C. De Alwis, A. Kalla, Q.-V. Pham, P. Kumar, K. Dev, W.-J. Hwang, and M. Liyanage, "Survey on 6G frontiers: Trends, applications, requirements, technologies and future research," *IEEE Open J. Comm. Soc.*, vol. 2, pp. 836–886, Apr. 2021.

[265] J. Rosenworcel, "The FCC should use blockchain to manage wireless spectrum (2018-03-20)," May 2020, [Online]. Available: https://www.wired.com/story/the-fcc-should-use-blockchain-to-manage-wireless-spectrum.

[266] M. B. Weiss, K. Werbach, D. C. Sicker, and C. E. C. Bastidas, "On the application of blockchains to spectrum management," *IEEE Trans. Cognit. Commun. Netw.*, vol. 5, no. 2, pp. 193–205, Jun. 2019.