Hindawi
Security and Communication Networks
Volume 2021, Article ID 9991535, 15 pages
https://doi.org/10.1155/2021/9991535

Review Article

Recent Advances in Blockchain and Artificial Intelligence Integration: Feasibility Analysis, Research Issues, Applications, Challenges, and Future Work

Zhonghua Zhang,[1] Xifei Song,[2] Lei Liu,[2] Jie Yin,[2] Yu Wang,[3] and Dapeng Lan[4]

[1]*Shenzhen HTI Group Co., Ltd., Shenzhen 518040, China*
[2]*State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China*
[3]*Institute of Artificial Intelligence and Blockchain, Guangzhou University, Guangzhou 510006, Guangdong, China*
[4]*Department for Informatics, University of Oslo, Postboks 1080 Blindern 0316, Oslo, Norway*

Correspondence should be addressed to Xifei Song; cifer.sxf@foxmail.com

Received 19 March 2021; Revised 22 May 2021; Accepted 9 June 2021; Published 25 June 2021

Academic Editor: Neeraj Kumar

Blockchain constructs a distributed point-to-point system, which is a secure and verifiable mechanism for decentralized transaction validation and is widely used in financial economy, Internet of Things, large data, cloud computing, and edge computing. On the other hand, artificial intelligence technology is gradually promoting the intelligent development of various industries. As two promising technologies today, there is a natural advantage in the convergence between blockchain and artificial intelligence technologies. Blockchain makes artificial intelligence more autonomous and credible, and artificial intelligence can prompt blockchain toward intelligence. In this paper, we analyze the combination of blockchain and artificial intelligence from a more comprehensive and three-dimensional point of view. We first introduce the background of artificial intelligence and the concept, characteristics, and key technologies of blockchain and subsequently analyze the feasibility of combining blockchain with artificial intelligence. Next, we summarize the research work on the convergence of blockchain and artificial intelligence in home and overseas within this category. After that, we list some related application scenarios about the convergence of both technologies and also point out existing problems and challenges. Finally, we discuss the future work.

1. Introduction

As the cutting-edge technologies nowadays, blockchain and artificial intelligence have attracted increasing attention due to the irreplaceable role that they play in technological innovation and industrial transformation [1–3]. The concept of artificial intelligence technology originated from the Dartmouth Society in 1956. As an essential branch of computer science, artificial intelligence technology is dedicated to the research and development of technical sciences used to simulate, extend, and expand human intelligence. In recent years, thanks to the tremendous breakthroughs made in machine learning (especially deep learning) [4] and the exponential growth of data, artificial intelligence has ushered in an explosive period. Due to its advantages in analysis, prediction, judgment, and decision-making, artificial intelligence can fundamentally empower industries such as security, finance, retail, transportation, and education [5–8]. Blockchain technology started relatively late, firstly starting with Bitcoin proposed by Satoshi Nakamoto in 2008. The blockchain is essentially a distributed ledger [9, 10]. It can use a decentralized consensus mechanism in an environment where different entities participate, without the intervention of a third trusted party. Blockchain also realizes the generation and verification of transactions in an untrusted distributed system, building trust at a lower cost [11]. It is precisely because of this that more and more researchers have concentrated on blockchain technology [12, 13].

Artificial intelligence and blockchain have their own advantages, but each one of them also has corresponding drawbacks. Blockchain has problems regarding energy consumption, scalability, security, privacy, and efficiency, while artificial intelligence faces issues such as interpretability and effectiveness. As two different research directions, they can be related to each other and have the advantages of natural integration. These two technologies have common demands for data analysis, security, and trust, and they can empower each other. For instance, artificial intelligence depends on three key elements: algorithms, computing power, and data, and the blockchain can break the island of data and realize the flow of algorithms, computing power, and data resources, based on its inherent characteristics, including decentralization, immutability, and anonymization. In addition, blockchain can guarantee the credibility of the original data as well as the audit credibility and traceability of artificial intelligence. Moreover, blockchain can record the decision-making of artificial intelligence, which helps to analyze and understand the behavior of artificial intelligence and ultimately promotes the decision-making of artificial intelligence, making it more transparent, explainable, and trustworthy. Artificial intelligence can optimize the construction of the blockchain to make it more secure, energy-saving, and efficient.

To date, there has been a certain amount of literature to review the research of artificial intelligence and blockchain. However, there is still a lack of generalization and summarization of the work on their integration, and the correlation between the two is not yet reflected. Existing literature shows that researchers pay attention to the combination of blockchain and artificial intelligence for application in a variety of vertical fields and business [14–18]. In contrast, this paper analyzes the feasibility of the combination of blockchain and artificial intelligence from a more comprehensive and three-dimensional perspective, and extensively collect and demonstrate the combination points of the two in various research fields. The primary contributions of this paper can be summarized as follows:

(1) We analyze the relationship between blockchain and artificial intelligence, as well as the feasibility of their integration.

(2) We make a comprehensive summary from different classifications, according to the current domestic and foreign research on the integration of blockchain and artificial intelligence.

(3) We select various application scenarios and practical use cases in various fields to discuss how to integrate the blockchain and artificial intelligence.

(4) We point out the problems and challenges in the integration of blockchain and artificial intelligence, and look forward to the research work in the future.

The rest of the paper is organized as follows. Section 2 and Section 3 introduce the necessary foundation and background knowledge of artificial intelligence and blockchain technology respectively. Section 4 analyzes the feasibility of the combination of blockchain and artificial intelligence. Section 5 discusses the current research issues at home and abroad in detail. Application scenarios in various fields are categorized in Section 6. Section 7 describes the existing difficulties and challenges, and Section 8 presents the future research progress. Section 9 concludes the paper. Table 1 contains a detailed list of all acronyms used in this paper.

2. Artificial Intelligence Technology

Artificial intelligence technology started in 1956 and has experienced three peaks of development from 1956 to 1970, 1980 to 1990, and 2000 to the present. The proposal for machine learning in 1959 promoted the peak of the first development. The United States and Japan were dedicated to artificial intelligence research in the 1980s and 1990s which promoted the peak of the second development. Benefiting from the breakthrough of deep learning and reinforcement learning algorithms, the exponential growth of network data and the qualitative leap in computing power, artificial intelligence has entered the third period of rapid development [19, 20]. Artificial intelligence includes the following key technologies: computational vision technology, natural language processing technology, cross-media reasoning technology, intelligent adaptive learning technology, swarm intelligence technology, autonomous drone system technology, smart chip technology, and brain-computer interface technology, which can be widely used in various industries, such as healthcare, driverless cars [21], education development, games, entertainment, Internet of Things [22, 23], maritime Internet of Things [24, 25], and communication networks [26, 27].

3. Blockchain Technology

3.1. Concept of Blockchain. Blockchain technology is a kind of distributed ledger technology that stores data in a chain data structure. It is a new distributed infrastructure and computing paradigm, which employs the distributed node consensus algorithm to verify the transaction data and further synchronize the entire network, as well as uses cryptography to ensure data security and credibility [28].

3.2. Characteristics of Blockchain

3.2.1. Multicenter. The blockchain adopts distributed decentralized storage, so the distributed recording, storage, and update of data can be realized without a single central point. Since there is no centralized hardware or management organization, any node can operate on the data on the blockchain according to the established rules.

3.2.2. Transparency. The system data of the blockchain is open and transparent, and any node can have a general ledger of the entire network. Except for the private information of the directly related parties of the data being encrypted through asymmetric encryption technology, the

Table 1: Abbreviations and their corresponding meaning.

Acronym	Meaning
AI	Artificial intelligence
ML	Machine learning
DRL	Deep reinforcement learning
DNN	Deep neural networks
PoW	Proof of work
PoS	Proof of stack
DPos	Delegated proof of stake
D2D	Device-to-device
BaaS	Blockchain as a service
MEC	Mobile edge computing
DApp	Decentralized application

blockchain data are open to all nodes, so the entire system information is highly open and transparent.

3.2.3. Autonomy. The blockchain system has multiple participants, and they have formulated automatically negotiated specifications and protocols based on open rules and algorithms. Each node in the system always follows these specifications and protocols during operation. This ensures that every transaction in a trustless environment can guarantee its correctness and authenticity. The nodes can securely exchange, record, and update data, and operations that do not follow the specifications and protocols will not take effect.

3.2.4. Immutability. After the transaction information of the blockchain passes the consensus of all nodes and is recorded in the block, there is a complete backup locally on each node. At the same time, the correlation between blocks is carried out by the hash algorithm. If you want to tamper with a piece of data, you need to modify all subsequent blocks, which is very costly.

3.2.5. Traceability. Each node in the blockchain saves all the records in the history. Any piece of data can be found by traversing the local blockchain data, which makes all the data on the blockchain chain traceable.

3.2.6. Programmability. The nature of the blockchain provides a trusted application environment for the execution of smart contracts, so the blockchain can provide users with programmable data manipulation capabilities. Users can customize smart contract rules that meet their needs. At the same time, due to its open and automatic execution characteristics, it also guarantees the security of assets and data on the chain.

3.3. Concept of Blockchain. The rich application scenarios of blockchain are basically based on the four core technologies of blockchain, namely, consensus mechanism, data structure, cryptography, and distributed storage. As the key future research direction of blockchain technology, cross-training technology has gradually become one of the core technologies of blockchain.

3.3.1. Consensus Mechanism. To ensure that nodes are willing to take the initiative to keep accounts, the blockchain has formed an important consensus mechanism. Common consensus mechanisms are as follows: (1) The proof of work mechanism (PoW) is the original consensus mechanism, and all participating nodes compete for bookkeeping rights by comparing computing power. Since everyone participates, but only one node can be selected, many resources and time costs will be wasted. (2) For the proof-of-stake (PoS) mechanism, the longer you hold the digital currency and the more assets you hold, the more likely this mechanism is to obtain the right to bookkeeping and rewards, which saves time but easily causes the Matthew effect. (3) The delegated proof-of-stake mechanism (DPoS) selects representative nodes for proxy verification and accounting, which is simpler and more efficient, but it also sacrifices some decentralization to a certain extent.

3.3.2. Data Structure. The blockchain is similar to an iron chain in form, consisting of one block after another to form a complete chain. Each block includes a block header and a block body. The blocks are linked back and forth through the hash pointer in the block header. The hash value contained in each block header is similar to a digital fingerprint of all the data in the previous block, so there is an interlocking connection between each block. This relationship forms a chain. When any data in the block are modified, all subsequent hash values will change. Such a structure and content constitute the entire blockchain.

3.3.3. Cryptography. Blockchain uses killer feature-cryptography. The symmetric encryption is equivalent to using the same key to open and lock the door. Asymmetric encryption is equivalent to using a pair of different keys to open and lock the door, namely, public key and private key. If you use the public-key encryption, you can use the private key to decrypt; if you use private-key encryption, you can use the public key to decrypt. These two keys are generally stored in the user's personal wallet. Once the private key is lost, the assets are gone. It is relatively safe in the blockchain in which the public key and private key are formed through multiple transformations, and the characters are relatively long and complex [29].

3.3.4. Distributed Storage. The most attractive thing about blockchain is its distributed storage mechanism. The information record on each block in the blockchain is recorded by each node participating in the bookkeeping competition. To prevent some malicious nodes from doing damage, the new data in the blockchain that adopts the PoW consensus mechanism need to be unanimously confirmed and agreed upon by most nodes, and at least 51% of the nodes must agree. Therefore, it is difficult to tamper with data.

3.3.5. Cross-Chain Technology. Cross-chain technology is an important technical means for blockchain to realize interconnection and improve scalability. In terms of network morphology, blockchain is different from the Internet. The latter supports one network to connect to global nodes, while the former forms multiple isolated parallel networks. In addition to the extensive coexistence of public chains, private chains and consortium chains allow different organizations to have their own blockchains and even allow multiple blockchains to run simultaneously within the same organization. The number of global blockchains is increasing, and the isolation of different blockchain networks makes it impossible to effectively carry out operations, such as digital asset transfer and cross-chain communication between chains. In the cross-chain process, the two most important things are: The first is to recognize atomicity, that is, cross-chain transactions either happen or do not happen, so that honest nodes will not be damaged; the second is to ensure that the total assets on each chain will not decrease.

4. Feasibility Analysis of the Integration of Blockchain and Artificial Intelligence

The combination of artificial intelligence and blockchain is complementary. Blockchain provides a trustworthy foundation for artificial intelligence, and artificial intelligence provides the landing conditions for blockchain.

4.1. Blockchain Empowers Artificial Intelligence

4.1.1. Transparent and Reliable Data Sources. To more securely share data among multiple organizations, it is particularly important to ensure the transparency and reliability of data sources. Smart blockchain technology ensures the transparency of data on the chain through the synchronization of the full ledger of the nodes and ensures the traceability of data through transaction signatures and time stamps and so on after certificate authentication. A transparent and reliable information-sharing channel has been constructed among multiple participants.

4.1.2. Strong Fairness Guarantee. The traditional blockchain system rewards miners who work hard for the normal operation of the system through tokens and promotes the good operation of the system by ensuring fairness. The party who misbehaves in multiple parties will be punished economically, and the honest party will be compensated accordingly. Smart blockchain technology ensures that system participants can obtain corresponding rewards as long as they honestly abide by the agreement through automatically executed preset smart contract codes. At the same time, the condition-triggered automatic transfer mechanism is used to distribute the rewards to the corresponding participants, which provides a strong fairness guarantee for the intelligent scene of multiparty participation.

4.1.3. Efficient Autonomy. As a distributed ledger technology, the main feature of blockchain is decentralization. Decentralization means that there is no authoritative center or server to manage the entire system, so the blockchain system will not be controlled by a single organization. Using the automatic execution characteristics of smart contracts, predefining management rules in smart contracts can reduce the uncertainty and possible attacks brought about by the human operation process [30, 31].

4.1.4. Privacy Protection. As increasingly more data content is shared on the chain, the privacy of users may be directly or indirectly leaked [32]. Traditional blockchain systems use pseudonyms, shuffling, and other methods to protect users' privacy, but malicious attackers can nevertheless steal users' private information through data mining and analysis. In the new smart blockchain system, some cryptographic technologies with excellent security performance are used to protect users' data privacy. Li et al. [33] proposed a privacy protection scheme based on ring signatures using an anonymous signature method based on an elliptic curve encryption algorithm to protect privacy. Cai et al. [34] provided a privacy protection scheme based on Pedersen's commitment for the deletable blockchain system, which can hold users accountable when necessary while protecting privacy. The Prada-Delgado team [35] used zero-knowledge proof technology to identify the Internet of things devices in the smart blockchain system, which can protect the data privacy of lightweight devices efficiently and at low cost.

4.1.5. Distributed Computing Power. Artificial intelligence is usually provided by a single unit of computing capacity or computing platform. With the rapid increase in the amount of data and the obvious increase in computational complexity, it is difficult for traditional computing platforms to independently provide the computing capacity required for artificial intelligence, and the hardware costs and maintenance costs of enterprises are also rising [36]. Blockchain realizes the decentralization of computing capacity with its distributed nature, which is helpful to realize the operation of artificial intelligence models on global mass decentralized nodes and realize decentralized computing. Lin et al. [37] propose a new wireless edge intelligence framework to achieve stable and robust edge intelligence through energy collection methods on a permissioned edge blockchain, and design the optimal edge learning strategy to maximize the efficiency of edge intelligence.

4.2. Artificial Intelligence Empowers Blockchain.

The design and operation of blockchain involves thousands of parameters, as well as the trade-off of security, throughput, decentralization, and other parameters. Artificial intelligence technology can simplify these decisions and optimize the blockchain to achieve higher performance and better governance. Moreover, artificial intelligence can also improve the intelligence of blockchain applications and reduce errors caused by human influence.

4.2.1. Security. As we all know, unless the adversary owns the majority of mining rights, blockchain is almost impossible to hack. Unfortunately, the programs and functions of decentralized applications built on the blockchain platform are not so secure. For example, in the DAO incident [38], hackers took advantage of loopholes in smart contracts to repeatedly withdraw funds, resulting in a loss of $50 million. Artificial intelligence technology provides new development opportunities for the intelligentization of blockchain system security protection and can provide security and technical support for the entire life-cycle of blockchain transactions. As far as the security of smart contracts is concerned, some work has been done. Raja et al. [39] have used artificial intelligence technology to automatically generate smart contracts, so as to reduce the vulnerability of smart contracts as much as possible. Furthermore, data mining and other technologies are used to analyze the vulnerabilities of the smart contract, and big data analysis is used to check malicious vulnerabilities to avoid economic losses caused by hackers. The involvement of artificial intelligence in the blockchain can make smart contracts more intelligent and efficient, allowing them to form a more complete code through continuous learning and practice and reshape the capabilities of blockchain smart contracts.

4.2.2. Efficiency. In the industrial sector, a large number of mature blockchain systems have been put into practical application, and more enterprises are increasing investment in the application of blockchain. However, due to the limitation of data storage mode, the blockchain system generally faces serious problems of simple query function and low query performance. The reason is that the underlying data storage systems of most blockchain systems use levelDB, a data storage system designed for write-intensive applications. At the cost of data reading performance, writing performance has improved. With the increase of data and the expansion of applications in blockchain systems, it is often necessary to deal with frequent queries. The underlying storage system has excessive writing performance but insufficient reading performance, which has become the main bottleneck limiting the query performance. The data-storing methods of blockchain can likewise be enhanced with the assistance of AI algorithms. Gawas et al. [40] propose an AI-based novel TTA-CB protocol to establish a secure and distributed blockchain for data management in VECONs and utilize a PSO algorithm to solve the optimal data provider selection problem. Artificial intelligence technology has brought new opportunities for the development of blockchain. Through continuous learning and practice, it has significantly improved the speed of data query and the efficiency of blockchain applications.

5. Research Issues of Blockchain and Artificial Intelligence Integration

In this section, we classify and summarize the applications of blockchain and artificial intelligence integration.

5.1. Sharing Applications. The information age has ushered in an explosive growth of data, and the value of data lies in circulation. However, the existing data trust system is not perfect, which restricts the secure circulation of data and affects the development of the industry. Blockchain technology can provide new technical means for data sharing due to its inherent characteristics, such as immutability, decentralization, and traceability. However, in general data-sharing applications, blockchain is often only used as a secure and reliable distributed database. Because of missing data analysis capability, the practicality of blockchain is greatly reduced. For this reason, artificial intelligence technology can be used to compensate for the deficiencies of blockchain and enhance the value of its applications.

In the industrial IoT driven by mobile crowd sensing, Liu et al. [41] combined Ethereum and deep reinforcement learning to propose a joint framework to ensure effective data collection and secure data sharing. To achieve maximum data collection, minimum energy expenditure, and regional fairness, the authors used a distributed deep reinforcement learning mechanism to help smart mobile terminals perceive nearby points of interest and then used blockchain technology to ensure the security and reliability of data sharing.

To ensure flexible and secure resource sharing, Dai et al. [42] made full use of the advantages of blockchain and artificial intelligence to construct a secure and intelligent network architecture for the next generation of wireless networks, as shown in Figure 1. Blockchain technology was used to establish a secure and distributed resource-sharing environment, while artificial intelligence technology was used to solve the problems of uncertainty, time variation, and complexity in wireless systems. In particular, the authors used the consortium blockchain to establish a secure content-caching environment and used deep-reinforcement learning to design a caching mechanism to maximize the use of cache resources.

To reduce the burden of transmission and address privacy issues, Lu et al. [43] established a network architecture based on federated learning. The authors ensured the security and stability of model parameters through a hybrid blockchain architecture that integrated consortium blockchains and local directed acyclic graphs and then designed an asynchronous federated learning mechanism empowered by deep-reinforcement learning to improve model-learning efficiency. The model was integrated into the blockchain, and two-phase verification was performed to ensure the reliability of the shared data.

Using video analysis technology based on artificial intelligence, the current intelligent surveillance system can provide more diversified services. However, there are still security and privacy issues caused by malicious attackers and untrusted third parties. To solve this problem, the blockchain technology developed by Lee et al. [44] was used to ensure the integrity and security of cloud-based intelligent monitoring systems. The proposed Merkle-Tree method can promote the effective transmission of video data, help reduce the bandwidth required for transmission and the overhead of redundant data storage, and realize the secure

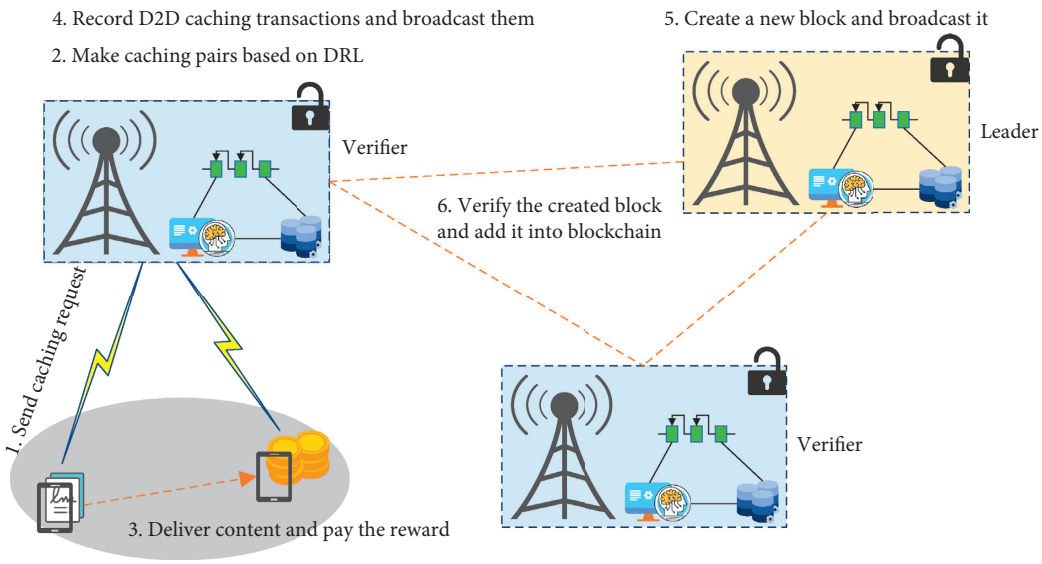

Figure 1: Secure content storage based on consortium blockchain.

synchronization of video data without exposing the privacy of the target.

At present, the wearable device market is growing, storing a large amount of personal health data, which can be used to implement various health-related applications. Blockchain technology transparently records these massive amounts of health data, which can provide support to some researchers and commercial companies while also protecting the privacy of data providers. Bagchi et al. used neural networks to process different types of cardiovascular clinical data and integrated them into the main cardiovascular output [45]. These outputs were shared with patients and doctors through the designed blockchain mechanism. To deal with low data quality in data sharing, Zheng et al. proposed a data quality check module based on machine learning. When integrated into the system, the module can analyze the high-quality data required by related applications [46].

5.2. Security Applications. With the continuous development of the blockchain system, the perfection of smart contracts and incentive mechanisms will depend on the occurrence of malicious behavior in the system. On the one hand, these malicious behaviors pose huge challenges to the security of the blockchain system. On the other hand, the large amount of data generated by the blockchain will increase the difficulty of reviewing and detecting malicious behavior. The integration of blockchain and artificial intelligence is conducive to enhancing the existing blockchain system.

Smart contracts may contain wrong codes and loopholes, which can easily cause huge financial losses. The current smart contract vulnerability detection methods mainly focus on symbolic execution and dynamic execution methods with low accuracy. Liao et al. proposed a smart contract vulnerability detection method [47], namely, SoliAudit. This method used both static and dynamic testing technologies and enhanced smart contract vulnerability detection capabilities through machine learning and dynamic fuzzers. The SoliAudit method achieved up to 90% vulnerability identification accuracy on 17,979 samples and can still quickly adapt to new unknown weaknesses without expert knowledge and predefined features. Zhuang et al. also proposed a vulnerability detection method fused with machine learning, using a graph neural network method to detect smart contracts from another perspective [48]. Aiming at the syntactic and semantic structure of the smart contract function, the authors constructed a contract graph and designed an elimination phase to normalize the graph and highlight the main nodes. Furthermore, a nondegree graph convolutional neural network and a novel time information dissemination network were proposed to learn from the normalized graph and detect smart contract vulnerabilities.

The incentive mechanism is the core of the public chain. It encourages participants to run and ensure the security of the underlying consensus protocol. However, it is very difficult to design an incentive mechanism compatible with incentives. Hou et al. proposed a framework based on deep learning to detect vulnerabilities in the blockchain incentive mechanism-SquirRL [49], as shown in Figure 2. Developers of the protocol can use SquirRL as a general method to test the deficiencies of the incentive mechanism. SquirRL does not provide theoretical guarantees, but its instantiation is very effective in checking adversarial strategies, which can be used to show that an incentive mechanism is insecure.

The blockchain system will generate a large amount of transaction data, which brings certain challenges to the review and detection of malicious behavior. The authors in [50] proposed a method of using data mining and machine learning to detect and capture Ponzi schemes that occurred in Ethereum. This method first extracted features from user accounts and operating codes of smart contracts and then built a classification model to detect potential Ponzi

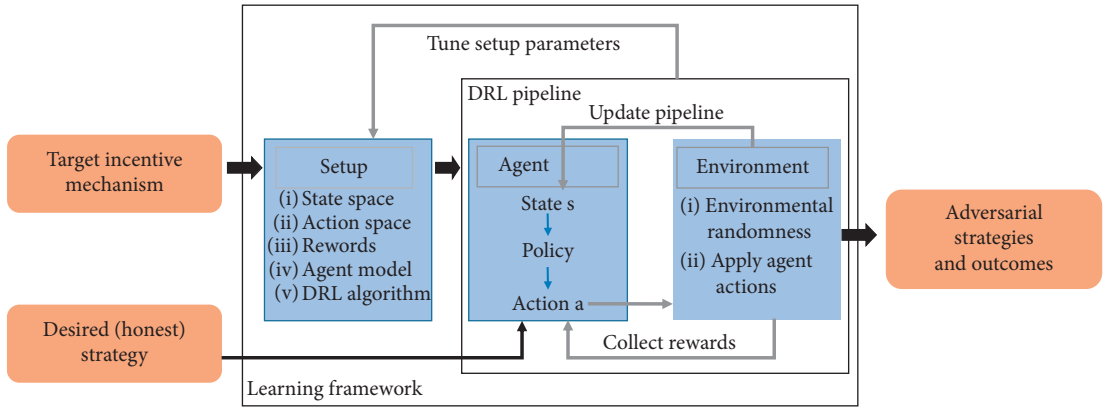

Figure 2: Schematic diagram of the SquirRL learning framework.

schemes. DOORChain was proposed in [51] for the malicious behavior of blockchain. It combined three powerful intrusion and malicious detection methods, namely, deep learning, ontology, and operations research. This method utilized the constraints of operations research to formalize and detect malicious behaviors on the network, especially using ontology to detect behavioral malicious behavior, and then used feedback from this formalization of deep learning to check whether transactions in the blockchain were malicious.

5.3. Transaction Applications. Blockchain has great advantages in protecting data, while artificial intelligence is good at analysis, prediction, and judgment. The combination of the two can be used for related research, such as price prediction and transaction analysis.

McNally et al. applied machine learning technology to predict the price trend of Bitcoin and completed this task by Bayesian optimization of recurrent neural networks and long short-term memory networks [52]. McNally et al. also compared the experimental results with the results predicted by the popular ARIMA model and found that the effect of nonlinear deep learning methods was better than that of ARIMA prediction. Users in the Bitcoin system used pseudonymous Bitcoin addresses as transaction accounts, making Bitcoin address correlation analysis a challenging task. In this case, a new Bitcoin address association scheme was proposed in [53], making it possible to track addresses in the Bitcoin system. After extracting the Bitcoin addresses, the authors converted the address clustering problem into a binary classification problem to reduce the computational complexity. Then, the system analyzed whether the two Bitcoin addresses belong to the same user by constructing a two-layer model. Finally, the system clustered addresses belonging to the same user. Shao et al. proposed a deep learning method to implement address-user mapping [54], which makes it possible to realize user identification in the Bitcoin system. Shao et al. mapped the representation of the address to the Euclidean space and used a deep neural network to embed transaction behavior, thereby obtaining the feature vector of each address. Finally, the owner of the address is identified through address verification, identification, and clustering.

5.4. Deposit Applications. Blockchain can guarantee the authenticity, integrity, and credibility of stored digital information due to its inherent characteristics. Artificial intelligence can assist in data analysis and processing as well as the natural evolution and dynamic adjustment of smart contracts. Combining blockchain and artificial intelligence technology can provide a wide range of application scenarios for data storage, retrieval, and inspection services.

Immunization is an indispensable mechanism for preventing infectious diseases in modern society. Vaccine safety is closely related to public health and national security. However, issues such as vaccine expiration and vaccine record fraud are still common in the vaccine supply chain. Therefore, there is an urgent need to establish an effective vaccine regulatory system. To this end, Yong et al. developed a vaccine blockchain system based on blockchain and machine learning technology [55]. Blockchain technology aims to change the current information management method and establish a new trust mechanism, while machine learning technology provides an additional method for data analysis in the information management system. The vaccine blockchain system was designed with a smart contract based on Ethereum to query personal vaccination records and vaccine circulation for consumers and to track vaccine operation records for vaccine institutions and governments. If the vaccine has liability issues, it can be solved through the vaccine blockchain system.

For environmental protection considerations, electric cars are regarded as an important tool for green city projects. As the demand for electric cars increases, it is not easy for users to find suitable charging facilities. On the other hand, energy companies operate their own charging stations for their own purposes, and their charging information is not transparent to the outside world. To solve these problems, Fu et al. [56] proposed a charging system for electric cars, which provided users with convenient charging services by realizing collaboration between energy companies, as shown in Figure 3. The author used the consortium blockchain to

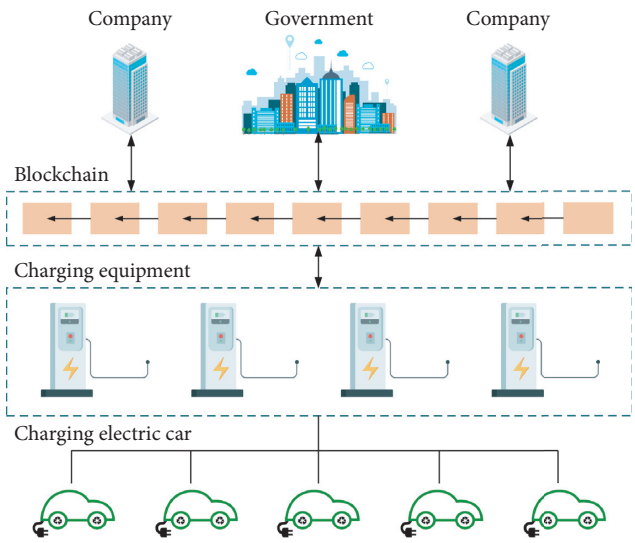

Figure 3: Tram charging strategy.

realize the management and recording of charging information between energy companies. In particular, smart contracts were designed to balance the company's charging-user-scheduling problem to ensure the fairness of the benefits of different energy companies.

The food supply chain is a complex system involving many stakeholders, such as farmers, production plants, distributors, retailers, and consumers. Information asymmetry between different stakeholders is an important reason for fraud, and the application of blockchain helps ensure food safety. However, there are some studies that are more inclined to study the traceability of food than supervision. In this regard, Mao et al. designed a blockchain-based credit evaluation system to strengthen the effectiveness of supervision and management of the food supply chain [57]. The system collected credit evaluation texts from traders through smart contracts, analyzed the texts collected by a network called long- and short-term memory, and used the credit results of traders as a reference for supervision and management.

The voting system is a powerful means to ensure fairness. Because of this, various complex security measures are used to ensure the security of the voting system. In view of the transparency and auditability issues of the current voting system, Pawlak et al. used smart methods to improve the electronic voting system based on blockchain [58]. The system aimed to provide a secure electronic voting solution that can resist voting tampering and fraud, and can be audited and verified by public voters.

5.5. Resource Management Applications. Both blockchain technology and artificial intelligence technology need the support of network resources, so their integration in resource management applications involves many scenarios. Considering that large computing and energy resources are consumed in the process of blockchain mining, Loung et al. proposed an optimal auction mechanism based on deep learning to allocate edge computing resources [59]. In this mechanism, the provider of edge computing services can support the offloading of mining tasks from mobile devices (i.e., miners) in a mobile blockchain environment. Based on the analytical solution of the optimal auction, the authors constructed a multilayer neural network structure. The network first implemented the monotonic transformation of absenteeism bids and then provided rules for the allocation and conditional payment for absenteeism. The estimate of absenteeism was used as training data to adjust the parameters of the neural network to maximize the loss function. Similarly, Asheralieva et al. [60] conducted research on resource management and pricing in IoT systems and discussed resource management solutions in blockchain as a service (BaaS) and mobile edge computing (MEC) scenarios [61, 62].

Feng et al. [63] aimed to optimize the blockchain system more comprehensively, improve the security and privacy of MEC as much as possible, and solve the problem of task offloading of MEC. The authors took the computing speed of the edge computing system and the throughput of the blockchain system as the joint optimization goal. To meet the performance requirements of the system, the collaborative offloading decision-making, energy allocation, block size, and block interval were jointly optimized. Aiming at the dynamic characteristics of wireless channels and available resources, the optimization problem was modeled as a Markov decision process problem, and a deep reinforcement learning algorithm that can stably train neural networks was proposed.

Liao et al. constructed a secure and intelligent task offloading architecture using blockchain and smart contracts to promote fair scheduling of tasks and alleviate various security attacks [64]. The authors quantified the success probability of task offloading through a trust index based on subjective logic and then proposed a trust evaluation mechanism. In addition, an online intelligent algorithm was designed to learn the long-term optimal offloading strategy, and a good balance was achieved between task offloading delay, queuing delay, and switching overhead. Federated learning that supports blockchain is usually limited by energy and CPU when performing collaborative training on mobile devices, which will increase the training delay due to the blockchain mining process. Hieu et al. [65] proposed a resource management scheme based on deep reinforcement learning. The author modeled the blockchain network in the federated learning system as an M/M/1 queue, proposed a random optimization model for the resource management of the machine learning model owner, and used deep reinforcement learning to provide an optimal solution for the model.

The architecture and data sources of the energy Internet are becoming increasingly complex. It is a good opportunity and trend to use blockchain technology to combine energy equipment and data information. Applying blockchain technology and broad learning technology based on the Energy Internet platform, Zhai et al. [66] conducted multisource data fusion calculations. The authors introduced in detail a novel combination model that comprehensively processes energy equipment data, blockchain data, and user

feedback data, using convolutional neural network modules to deal with prediction accuracy and computational complexity and using long- and short-term memory network modules to enhance the system's advantages in long-term memory.

With the development of the Internet of Things, data centers will generate massive amounts of data. On the one hand, these data can give rise to different data-driven services; on the other hand, they will bring about further energy expenditures. Xu et al. [67] used grid and green energy to solve the problem of how to reduce the overall energy expenditure. To this end, the authors proposed a distributed resource management architecture based on blockchain. The architecture can record all transaction activities without any scheduling. In addition, the authors used the reinforcement-learning-based demand migration method with embedded smart contracts to save costs.

5.6. Scalability Optimization Applications. With the increase in the number of transactions, the scalability of the blockchain has gradually become a key bottleneck, restricting the development of the blockchain. The choice of consensus algorithm plays an important role in the actual solution of the scalability problem. The method, based on Byzantine fault tolerance, is most preferred to solve the scalability problem of the blockchain network. Bugday et al. [68] proposed a new model to replace the proof of work to form a consensus group. This consensus group allowed the use of Byzantine fault tolerance methods in public blockchain networks. The model used an online learning algorithm of decision theory to calculate the reputation value for the nodes that wish to participate in the consensus committee and selected nodes with a higher reputation value for the consensus committee to reduce the chance of harm to the nodes in the consensus committee.

Another way to expand the blockchain is slicing technology. It can divide the network into fragments for concurrent transaction processing. Most of the existing blockchain systems use proof-of-work consensus protocols to create fragments. Ruparel et al. [69] proposed a network sharing algorithm based on machine learning. This algorithm can quickly and accurately create fragments, map the IP addresses of nodes to geographic coordinates, and then use the k-means clustering algorithm to divide these coordinates into fragments. The nodes in the shard were geographically closer, thereby reducing the propagation delay in the network during intrashard communication. Compared with the PoW-based slicing algorithm, GeoSharding is significantly faster, bringing scalability to a new level.

To solve the scalability and increase the throughput of the Industrial Internet of Things, Liu et al. [70] proposed a system performance optimization framework based on deep reinforcement learning and blockchain, which quantitatively evaluated the new blockchain system from four aspects, namely, scalability, decentralization, security, and delay. Then, Liu et al. designed an algorithm based on deep reinforcement learning to dynamically adjust the block producers, consensus algorithm, block size, and block interval, which improve the performance of the system and promote the wide application of the system.

The emerging federated edge learning technology can not only ensure good machine learning performance but also solve the "data island" problem caused by data privacy issues. However, large-scale federated edge learning technology lacks a secure and effective communication model training program, and there is no updateable and flexible framework to update local models and global model sharing (transaction) management. Kang et al. [71] proposed a blockchain-based federated edge learning system, which has a hierarchical blockchain framework composed of a main chain and subchains. It can separately manage local model updates or model sharing to achieve performance isolation. This framework can also realize scalable and flexible distributed federated edge learning.

Table 2 summarizes the applications of blockchain and artificial intelligence integration based on the above classification.

6. Application Scenarios

In this section, we select application scenarios and practical use cases in various fields.

6.1. Smart Grid. A smart grid is part of the energy Internet, where everyone contributes to the energy supply [12, 72, 73]. Distributed energy trading is the current mainstream development trend of smart grids, but traditional centralized grid systems cannot be organically combined with distributed energy trading. Therefore, the decentralized characteristics of smart blockchains can effectively help smart grids realize the transformation from centralization to distribution [12]. The decentralization of smart blockchain breaks information barriers and realizes secure data sharing among multiple participants. In addition, smart blockchain technology can reduce the operation and maintenance costs of smart grids and improve the participation of market players.

6.2. Internet of Vehicles. With the development of communication technologies, Internet of Vehicles is playing an increasingly important role in smart transportation [74–76]. The Internet of Vehicles can help solve existing traffic and road safety problems through vehicular communication, but there may be a crisis of trust and safety hazards in the process of information exchange [77, 78]. Smart blockchain can provide trust guarantees, reliable data security, and effective incentive mechanisms, and can also escort the development of Internet of Vehicles technology. Blockchain introduces elements, such as cars, people, and service providers, into the chain. Through its transparency, anonymity, and immutability characteristics, it can ensure mutual trust between different elements, strengthen data information security, and promote data information sharing.

Table 2: Summary of integrated applications of blockchain and artificial intelligence.

Subject	Literature	Time	Contribution	Goal
Sharing applications	[41]	2018	Proposed a data collection scheme based on deep reinforcement learning	Smart mobile terminal data collection and sharing
	[42]	2019	Used deep reinforcement learning to optimize the system's cache resource utilization	Realize secure resource sharing in wireless network
	[43]	2020	Selected nodes through deep reinforcement learning to improve the efficiency of federated learning	Solve the problem of collaborative training in the Internet of Vehicles
	[44]	2020	Provides blockchain-based privacy preserving multimedia intelligent video surveillance	Ensure the integrity and security of cloud-based intelligent monitoring systems
	[45]	2019	Integrated machine learning and natural language processing, which can detect different types of cardiovascular clinical data	Predict the type of illness and simplify the diagnosis process
	[46]	2018	Proposed a data inspection module based on machine learning	Securely sharing personal information
Security applications	[47]	2019	Combined machine learning and fuzzing to detect contract vulnerabilities	Detect smart contract vulnerabilities
	[48]	2020	Proposed a vulnerability detection model based on GNN	Detect smart contract vulnerabilities
	[49]	2019	Proposed a detection framework based on deep reinforcement learning	Detect loopholes in the blockchain incentive mechanism
	[50]	2018	Proposed a classification model combining data mining and machine learning	Detect Ponzi schemes in Ethereum
	[51]	2019	Proposed a DOORChain model that integrates deep learning, ontology, and operations research	Detect malicious transactions in the blockchain
Transaction application	[52]	2018	Proposed two prediction models based on cyclic convolutional network and long short-term memory algorithm, respectively	Predict bitcoin price
	[53]	2019	Proposed an association scheme based on binary classification	Bitcoin address correlation analysis
	[54]	2018	Proposed a recognition scheme based on DNN	Bitcoin address-user identification
Deposit application	[55]	2020	Proposed a vaccine blockchain system integrated with machine learning	Vaccine supervision and recommendation
	[56]	2020	Proposed a smart tram charging system based on consortium blockchain	Solve the problem of independent operation of energy companies and opaque charging information
	[57]	2018	Designed a blockchain-based credit evaluation system	Strengthen the effectiveness of supervision and management of the food supply chain
	[58]	2019	Designed an electronic voting system based on blockchain using intelligent agents	Guarantee the security of voting
Resource applications management	[59]	2018	Proposed an optimal auction mechanism based on deep learning	Edge computing resource allocation
	[60]	2019	Proposed a new type of hierarchical reinforcement learning algorithm	Dynamic resource management of the IoT system
	[63]	2019	Proposed an actor-critic algorithm with asynchronous advantages of stable training	Solve the computing offload problem of mobile edge computing
	[64]	2020	Proposed a secure and intelligent vehicle task offloading strategy based on blockchain and learning algorithms	Reduce task delay and switching overhead under the premise of ensuring security, privacy, and fairness
	[65]	2020	Proposed a resource management scheme based on deep reinforcement learning	System resource management
	[66]	2020	Proposed a fusion model of blockchain and width learning	Forecast user energy demand
	[67]	2017	Researched the smart resource management strategy of cloud data center based on blockchain	Save the energy cost
Scalability optimization applications	[68]	2019	Utilized machine learning to build a consensus committee	Improve blockchain scalability
	[69]	2020	Addressed clustering and fragmentation based on k-means algorithm	Efficient fragmentation
	[70]	2019	Designed a deep reinforcement learning algorithm to improve the scalability of the blockchain	Solve the scalability problem of the Industrial Internet of Things and improve throughput
	[71]	2020	Combined federated learning to improve blockchain scalability	Design a secure federal edge learning system

6.3. Supply Chain. Blockchain technology has become an important technical means to break through the development constraints of traditional supply chains because of its decentralization, high reliability, and immutability. Using the blockchain network to publish the information data stored in the database can leverage the accurate and rapid sharing and collaboration of logistics data as well as effectively solve the problem of information asymmetry between upstream and downstream enterprises in the supply chain system. The application of artificial intelligence technology in the blockchain system can redefine the supply chain by automating the entire workflow. When integrated with the blockchain, the artificial intelligence platform can discover useful information from point-of-sale sales data, historical purchase data, etc., so that data characteristics can be identified, and predictive analysis can be implemented, including future demand forecasts, sales model forecasts, path planning, and network management.

6.4. Health Care. With the development of the social economy, health care has entered a stage of rapid development. However, there are certain problems that need to be resolved. On the one hand, users have extremely high requirements for the security of personal information and health data; on the other hand, data sharing between medical institutions can achieve an accurate and effective diagnosis and medical treatment. Blockchain can solve the above problems. Through its immutability, the blockchain is conducive to data tracking and anti-counterfeiting while using a reliable trust mechanism. The blockchain can realize secure data sharing. The use of artificial intelligence technology can then mine the hidden value behind the data, thereby allowing more comprehensive data analysis.

7. Problems and Challenges

In this section, we point out the problems and challenges in the integration of blockchain and artificial intelligence.

7.1. Scalability. The scalability issue is the key to the smooth implementation of smart blockchain applications. Blockchain decentralized application (DApp) must run on the underlying platform of the existing blockchain. If the performance and scalability of the system are insufficient, it cannot be implemented as a large-scale application. On the premise of ensuring data security and decentralization, the scalability challenges of blockchain mainly include three aspects, namely, consistency issues, network delays, and performance limitations. To ensure the security of the blockchain, most nodes need to reach a consensus on the transaction data. One-sided pursuit of scalability reduces the consistency requirement of the distributed network, which will cause the blockchain to bifurcate. Since the blockchain is a peer-to-peer distributed network, the network delay between nodes will limit the scalability of the entire system, especially those with longer delays. The third point is the limitation of transaction performance on the scalability of the blockchain, which is also the core reason that restricts the implementation of blockchain applications. To ensure security and eventual consistency, blockchain transactions cannot be performed in parallel, which makes it difficult to increase transaction throughput.

7.2. Security and Privacy. Among the challenges of blockchain application, landing, security, and privacy protection are important issues. As the infrastructure of the Internet of Value, the information between the nodes of the blockchain system is open and transparent, and it may contain private information that users do not want to disclose. Therefore, how to protect user privacy is the key to whether blockchain applications can be implemented on a large scale. Common blockchain privacy protection methods include information hiding and identity confusion. Identity obfuscation technology partially anonymizes the user's identity on the blockchain and uses privacy protection signature technologies, such as group signatures and ring signatures, to confuse the identity information of both parties to the transaction, making it impossible to correspond to the real user. When necessary, the supervisor can use the supervisor's private key to view user information to ensure identity security.

Information hiding uses technologies, such as zero-knowledge proof and secure multiparty computing, to conduct transactions without revealing any private information and to ensure the credibility of the results, which effectively protects the user's transaction privacy. However, the increase in the calculation process leads to a system with reduced efficiency, and further improvement is needed in actual applications. How to make rational use of artificial intelligence algorithm to improve the low efficiency is a difficult problem. In addition, the application of artificial intelligence algorithm to distributed environment obviously needs to redesign the existing algorithm.

7.3. Data Collaboration between On-Chain and Off-Chain Storage. Traditional information systems and blockchain systems are two ways of storing data, and each has limitations. On the one hand, blockchain needs to improve performance through off-chain storage and computing systems; on the other hand, traditional information systems need blockchain technology to ensure the safe sharing and credibility of data. This requires an effective combination of blockchain technology and traditional information systems, and the most critical point is to ensure the relevance and consistency of the data on the chain and the data off the chain. Moreover, the development of artificial intelligence cannot be separated from data. Artificial intelligence technology is still facing many problems, such as poor data quality, data monopoly, data abuse, and so on. The intervention of blockchain gives these problems new development opportunities. Only by correctly combining the data on the chain with the data off the chain, can the combination

of blockchain and artificial intelligence be truly applied to the real economy.

8. Future Work

In this section, we look forward to the possible research work on the integration of blockchain and artificial intelligence in the future.

8.1. Hybrid Architecture Combining On-Chain and Off-Chain Storage. In view of different distributed scenarios, the transaction and data storage modes of smart blockchain in the future may become a hybrid architecture, combining on-chain and off-chain storage. Off-chain storage has the advantages of faster efficiency, lower cost, and higher privacy, but it is difficult for off-chain data to take advantage of the blockchain trust. A key research direction in the future is to closely integrate the on-chain and off-chain data so that the trust on the chain can be mapped to the off-chain data.

8.2. Balance between Performance Improvement and Security Guarantees. Although blockchain has many advantages in various aspects, its own performance bottleneck still limits its practical application. Most of the technical challenges of the blockchain itself focus on performance issues, especially transaction throughput, transaction confirmation delay, and block capacity. Different solutions such as directed acyclic graphs, transaction sharing, off-chain transactions, and block expansion have been proposed to solve the performance problems of the blockchain, but they will inevitably reduce the credibility and security of the blockchain. However, in scenarios with stronger privacy protection requirements, some cryptographic schemes with higher security are applied to the blockchain system, which improves the degree of privacy protection and reduces the transaction efficiency of the blockchain system. An important concern for further breakthroughs in blockchain technology is determining how to directly balance performance improvement and privacy protection.

8.3. Distributed Trust Construction. In the application scenarios enabled by blockchain, there is more cooperation and intercommunication between devices. The basis of cooperation is the existence of trust between the partners; that is, they all believe that the identity of the other party and the provided information are true and reliable. Blockchain technology naturally guarantees the authenticity and reliability of data due to its consensus mechanism and immutability modification, which can better build trust in an open network. In a scenario in which a node has a specific identity and role, the identity of the node where the device is located needs to be authenticated. This requires the construction of distributed trust in the blockchain scenario. A key research direction in the future is to authenticate the identities of other nodes without a central authority.

8.4. Improve User Awareness and Enhance Legal Regulations. The development of blockchain is fast, and the introduction of relevant industry regulations is relatively lagging, so chaos and bubbles inevitably exist. Deleveraging, strong supervision, and the ups and downs of the capital market have made people always wait and see the blockchain, and some illegal behaviors under the guise of blockchain have been repeatedly prohibited. Therefore, people's understanding of blockchain technology is not uniform, and the dividing line between coin and chain is also very blurred. Therefore, it is necessary to strengthen the popularization of blockchain knowledge for the public.

9. Conclusion

As two most cutting-edge technologies, blockchain and artificial intelligence have the corresponding integration opportunities in addition to their own advantages, which can completely revolutionize the information technology in the future. In this paper, we introduce the background knowledge of artificial intelligence and blockchain in detail, conduct an in-depth analysis of the feasibility of the integration of blockchain and artificial intelligence, and comprehensively summarize the research work on the integration of blockchain and artificial intelligence in the domestic market and overseas. Finally, we point out the promising application scenarios and future work.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Key Research and Development Program of China under Grant No. 2020YFB1807500, the National Natural Science Foundation of China under Grant Nos. 62001357 and 61802080, the Guangdong Basic and Applied Basic Research Foundation under Grant Nos. 2020A1515110496 and 2020A1515110079, the Education Bureau of Guangzhou Municipality Higher Education Research Project under Grant No. 201831827, the Key Research and Development Programs of Shaanxi under Grant Nos. 2019ZDLGY13-07 and 2019ZDLGY13-04, and the Guangzhou University Research Project under Grant Nos. RQ2020085 and RD2020076.

References

[1] A. Barredo Arrieta, N. Díaz-Rodríguez, J. Del Ser et al., "Explainable Artificial Intelligence (XAI): concepts, taxonomies, opportunities and challenges toward responsible AI," *Information Fusion*, vol. 58, pp. 82–115, 2020.

[2] Y. Song, Y. Fu, F. R. Yu et al., "Blockchain-enabled internet of vehicles with cooperative positioning: a deep neural network approach," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3485–3498, 2020.

[3] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M. Obaidat, and B. Sadoun, "Habits: blockchain-based telesurgery framework

for healthcare 4.0," in *Proceedings of the 2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp. 1–5, IEEE, Beijing China, August 2019.

[4] J. Wang, C. Jiang, H. Zhang, Y. Ren, and K-C. Cheng, "Thirty years of machine learning: the road to Pareto-optimal wireless networks," *IEEE Communications Surveys & Tutorials*, vol. 22, pp. 1472–1514, 2020.

[5] W. Sun, N. Xu, L. Wang, H. Zhang, and Y. Zhang, "Dynamic digital twin and federated learning with incentives for air-ground networks," *IEEE Transactions on Network Science and Engineering*, p. 1, 2020.

[6] X. Hou, Z. Ren, J. Wang et al., "Reliable computation offloading for edge computing-enabled software-defined IoV," *IEEE Internet of Things Journal*, vol. 7, pp. 7097–7111, 2020.

[7] J. Wang, C. Jiang, Z. Han, Y. Ren, and L. Hanzo, "Internet of vehicles: sensing-aided transportation information collection and diffusion," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 3813–3825, 2018.

[8] J. Guo, Y. Zhou, P. Zhang, B. Song, and C. Chen, "Trust-aware recommendation based on heterogeneous multi-relational graphs fusion," *Information Fusion*, vol. 74, pp. 87–95, 2021.

[9] M. B. Mollah, J. Zhao, D. Niyato et al., "Blockchain for the internet of vehicles towards intelligent transportation systems: a survey," *IEEE Internet of Things Journal*, vol. 8, pp. 4157–4185, 2020.

[10] J. Feng, F. R. Yu, Q. Pei, J. Du, and L. Zhu, "Joint optimization of radio and computational resources allocation in blockchain-enabled mobile edge computing systems," *IEEE Transactions on Wireless Communications*, vol. 19, no. 6, pp. 4321–4334, 2020.

[11] Z. Zheng, S. Xie, H. N. Dai, X. Cheng, and H. Wang, "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[12] M. B. Mollah, J. Zhao, D. Niyato et al., "Blockchain for future smart grid: a comprehensive survey," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 18–43, 2021.

[13] P. K. Sharma, N. Kumar, and J. H. Park, "Blockchain-based distributed framework for automotive industry in a smart city," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4197–4205, 2018.

[14] T. Baltrušaitis, C. Ahuja, and L. P. Morency, "Multimodal machine learning: a survey and taxonomy," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 41, no. 2, pp. 423–443, 2018.

[15] 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, Article ID 100227, 2020.

[16] D. Nguyen, M. Ding, P. N. Pathirana, and A. Seneviratne, "Blockchain and ai-based solutions to combat coronavirus (COVID-19)-like epidemics: a survey," *Preprints*, 2020.

[17] R. Gupta, A. Kumari, and S. Tanwar, "Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, Article ID e4176, 2021.

[18] S. Hu, Y. C. Liang, Z. Xiong, and D. Niyato, "Blockchain and artificial intelligence for dynamic resource sharing in 6G and beyond," *IEEE Wireless Communications*, vol. 99, pp. 1–7, 2021.

[19] J. Du, F. R. Yu, G. Lu, J. Wang, J. Jiang, and X. Chu, "MEC-assisted immersive VR video streaming over terahertz wireless networks: a deep reinforcement learning approach," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9517–9529, 2020.

[20] Y. Xiao, Q. Pei, T. Xiao, L. Yao, and H. Liu, "MutualRec: joint friend and item recommendations with mutualistic attentional graph neural networks," *Journal of Network and Computer Applications*, vol. 177, Article ID 102954, 2020.

[21] J. Wang, C. Jiang, K. Zhang, T. Q. S. Quek, Y. Ren, and L. Hanzo, "Vehicular sensing networks in a smart city: principles, technologies and applications," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 122–132, 2017.

[22] Y. Song, F. R. Yu, L. Zhou, X. Yang, and Z. He, "Applications of the internet of things (IoT) in smart logistics: a comprehensive survey," *IEEE Internet of Things Journal*, vol. 99, p. 1, 2020.

[23] H. Cao, L. Yang, and H. Zhu, "Novel node-ranking approach and multiple topology attributes-based embedding algorithm for single-domain virtual network embedding," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 108–120, 2017.

[24] T. Yang, Z. Jiang, R. Sun, N. Cheng, and H. Feng, "Maritime search and rescue based on group mobile computing for UAVs and USVs," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 12, pp. 7700–7708, 2020.

[25] T. Yang, H. Feng, S. Gao et al., "Two-stage offloading optimization for energy-latency tradeoff with mobile edge computing in maritime Internet of Things," *IEEE Internet of Things Journal*, vol. 7, pp. 5954–5963, 2019.

[26] P. Guo, W. Hou, L. Guo, Z. Cao, and Z. Ning, "Potential threats and possible countermeasures for photonic network-on-chip," *IEEE Communications Magazine*, vol. 58, no. 9, pp. 48–53, 2020.

[27] X. Li, M. Zhao, Y. Liu, L. Li, Z. Ding, and A. Nallanathan, "Secrecy analysis of ambient backscatter NOMA systems under I/Q imbalance," 2020, https://arxiv.org/abs/2004.14563.

[28] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthu, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proceedings of the IEEE Symposium on Security & Privacy*, IEEE, San Jose,CA,USA, August 2016.

[29] D. He, M. Ma, S. Zeadally, N. Kumar, and K. Liang, "Certificateless public key authenticated encryption with keyword search for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3618–3627, 2017.

[30] N. Diallo, W. Shi, L. Xu et al., "eGov-DAO: a better government using blockchain based decentralized autonomous organization," in *Proceedings of the International Conference on Edemocracy Egovernment*, pp. 166–171, Quito Equador, June 2018.

[31] L. Liu, J. Feng, Q. Pei et al., "Blockchain-enabled secure data sharing scheme in mobile edge computing: an asynchronous advantage actor-critic learning approach," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2342–2353, 2020.

[32] W. Zhang, M. Li, R. Tandon, and H. Li, "Online location trace privacy: an information theoretic approach," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 235–250, 2018.

[33] X. Li, Y. Mei, J. Gong, F. Xiang, and Z. Sun, "A blockchain privacy protection scheme based on ring signature," *IEEE Access*, vol. 8, pp. 76765–76772, 2020.

[34] X. Cai, Y. Ren, and X. Zhang, "Privacy-protected deletable blockchain," *IEEE Access*, vol. 8, pp. 6060–6070, 2019.

[35] M. Á. Prada-Delgado, I. Baturone, G. Dittmann, J. Jelitto, and A. Kind, "PUF-derived IoT identities in a zero-knowledge protocol for blockchain," *Internet of Things*, vol. 9, Article ID 100057, 2020.

[36] W. Sun, S. Lei, L. Wang, Z. Liu, and Y. Zhang, "Adaptive federated learning and digital twin for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5605–5614, 2020.

[37] X. Lin, J. Wu, A. K. Bashir, J. Li, W. Yang, and J. Piran, "Blockchain-based incentive energy-knowledge trading in IoT: joint power transfer and AI design," *IEEE Internet of Things Journal*, vol. 99, p. 1, 2020.

[38] M. I. Mehar, C. L. Shier, A. Giambattista et al., "Understanding a revolutionary and flawed grand experiment in blockchain: the DAO attack," *Journal of Cases on Information Technology*, vol. 21, no. 1, pp. 19–32, 2019.

[39] G. Raja, Y. Manaswini, G. D. Vivekanandan et al., "AI-powered blockchain-a decentralized secure multiparty computation protocol for IoV," in *Proceedings of the conference IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 865–870, IEEE, Toronto, ON, Canada, August 2020.

[40] M. Gawas, H. Patil, and S. S. Govekar, "An integrative approach for secure data sharing in vehicular edge computing using Blockchain," *Peer-to-Peer Networking and Applications*, pp. 1–9, 2021.

[41] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3516–3526, 2018.

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

[43] 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 Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4298–4311, 2020.

[44] D. Lee and N. Park, "Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree," *Multimedia Tools and Applications*, pp. 1–18, 2020.

[45] S. Bagchi, M. Chakraborty, and A. K. Chattopadhyay, "APDRChain: ANN based predictive analysis of diseases and report sharing through blockchain," in *Proceedings of the International Ethical Hacking Conference*, pp. 105–115, Springer, Kolkata, India, November 2019.

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

[47] J. W. Liao, T. Tsai, C. He, and C. Tien, "Soliaudit: smart contract vulnerability assessment based on machine learning and fuzz testing," in *Proceedings of the 2019 sixth international conference on internet of things: systems, management and security (IOTSMS)*, pp. 458–465, IEEE, Granada,Spain, October-2019.

[48] Y. Zhuang, Z. Liu, P. Qian et al., "Smart contract vulnerability detection using graph neural networks," in *Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence and Seventeenth Pacific Rim International Conference on Artificial Intelligence (IJCAI-PRICAI-20)*, Yokohomo, Japan, July 2020.

[49] C. Hou, M. Zhou, Y. Ji et al., "SquirRL: automating attack discovery on blockchain incentive mechanisms with deep reinforcement learning," 2019, https://arxiv.org/abs/1912.01798.

[50] W. Chen, Z. Zheng, J. Cui et al., "Detecting ponzi schemes on ethereum: towards healthier blockchain technology," in *Proceedings of the 2018 World Wide Web Conference*, pp. 1409–1418, Lyon, France, April 2018.

[51] M. A. El-Dosuky and G. H. Eladl, "DOORchain: deep ontology-based operation research to detect malicious smart contracts," in *Proceedings of the World Conference on Information Systems and Technologies*, pp. 538–545, Springer, Galicia, Spain, September 2019.

[52] S. McNally, J. Roche, and S. Caton, "Predicting the price of bitcoin using machine learning," in *Proceedings of the 2018 26th euromicro international conference on parallel, distributed and network-based processing (PDP)*, pp. 339–343, IEEE, Cambridge, UK, March 2018.

[53] T. Liu, J. Ge, Y. Wu et al., "A new bitcoin address association method using a two-level learner model," in *Proceedings of the International Conference on Algorithms and Architectures for Parallel Processing*, pp. 349–364, Springer, Heidelberg, Germany, January 2019.

[54] W. Shao, H. Li, M. Chen et al., "Identifying bitcoin users using deep neural network," in *Proceedings of the International Conference on Algorithms and Architectures for Parallel Processing*, pp. 178–192, Springer, Guangzhou, China, December 2018.

[55] B. Yong, J. Shen, X. Liu et al., "An intelligent blockchain-based system for safe vaccine supply and supervision," *International Journal of Information Management*, vol. 52, Article ID 102024, 2020.

[56] Z. Fu, P. Dong, and Y. Ju, "An intelligent electric vehicle charging system for new energy companies based on consortium blockchain," *Journal of Cleaner Production*, vol. 261, Article ID 121219, 2020.

[57] D. Mao, F. Wang, Z. Hao et al., "Credit evaluation system based on blockchain for multiple stakeholders in the food supply chain," *International Journal of Environmental Research and Public Health*, vol. 15, no. 8, p. 1627, 2018.

[58] M. Pawlak and A. Poniszewska-Marańda, "Blockchain e-voting system with the use of intelligent agent approach," in *Proceedings of the 17th International Conference on Advances in Mobile Computing & Multimedia*, pp. 145–154, New York, NY, USA, December 2019.

[59] N. C. Luong, Z. Xiong, P. Wang et al., "Optimal auction for edge computing resource management in mobile blockchain networks: a deep learning approach," in *Proceedings of the 2018 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, Kansas City, MO, USA, December 2018.

[60] 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 of Things Journal*, vol. 7, no. 3, pp. 1974–1993, 2019.

[61] S. Mao, S. Leng, S. Maharjan et al., "Energy efficiency and delay tradeoff for wireless powered mobile-edge computing systems with multi-access schemes," *IEEE Transactions on Wireless Communications*, vol. 19, no. 3, pp. 1855–1867, 2019.

[62] S. Mao, J. Wu, L. Liu, D. Lan, and A. Taherkordi, "Energy-efficient cooperative communication and computation for wireless powered mobile-edge computing," *IEEE Systems Journal*, 2020.

[63] J. Feng, F. R. Yu, Q. Pei et al., "Cooperative computation offloading and resource allocation for blockchain-enabled mobile edge computing: a deep reinforcement learning approach," *IEEE Internet of Things Journal*, vol. 7, 2019.

[64] 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 Transactions on Intelligent Transportation Systems*, 2020.

[65] N. Q. Hieu, T. T. Anh, N. C. Luong et al., "Resource management for blockchain-enabled federated learning: a deep reinforcement learning approach," 2020, https://arxiv.org/abs/2004.04104.

[66] Y. Zhai, X. Zheng, and S. Ai, "Integrating blockchain and broad learning for smart energy innovation: design and experiment," *Academic Journal of Computing & Information Science*, vol. 3, no. 1, 2020.

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

[68] A. Bugday, A. Ozsoy, S. M. Öztaner et al., "Creating consensus group using online learning based reputation in blockchain networks," *Pervasive and Mobile Computing*, vol. 59, Article ID 101056, 2019.

[69] H. Ruparel, S. Chiplunkar, S. Shah et al., "GeoSharding—A machine learning-based sharding protocol," in *Proceedings of the*, pp. 105–118, Springer, Mumbai, India, June 2020.

[70] M. Liu, F. R. Yu, Y. Teng et al., "Performance optimization for blockchain-enabled industrial Internet of Things (IIoT) systems: a deep reinforcement learning approach," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3559–3570, 2019.

[71] J. Kang, Z. Xiong, C. Jiang et al., "Scalable and communication-efficient decentralized federated edge learning with multi-blockchain framework," 2020, https://arxiv.org/abs/2008.04743.

[72] S. He, W. Tian, J. Zhang et al., "A high efficient approach for power disturbance waveform compression in the view of heisenberg uncertainty," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 5, pp. 2580–2591, 2018.

[73] S. He, Y. Zhang, R. Zhu et al., "Electric signature detection and analysis for power equipment failure monitoring in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 17, 2020.

[74] A. Dua, N. Kumar, A. K. Das, and W. Susilo, "Secure message communication protocol among vehicles in smart city," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4359–4373, 2017.

[75] L. Liu, C. Chen, T. Qiu et al., "A data dissemination scheme based on clustering and probabilistic broadcasting in VANETs," *Vehicular Communications*, vol. 13, pp. 78–88, 2018.

[76] J. Du, F. R. Yu, X. Chu et al., "Computation offloading and resource allocation in vehicular networks based on dual-side cost minimization," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1079–1092, 2018.

[77] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Secure data sharing and searching at the edge of cloud-assisted internet of things," *IEEE Cloud Computing*, vol. 4, no. 1, pp. 34–42, 2017.

[78] L. Liu, C. Chen, Q. Pei et al., "Vehicular edge computing and networking: a survey," *Mobile Networks and Applications*, pp. 1–24, 2020.