Cluster Computing (2022) 25:2585–2599
https://doi.org/10.1007/s10586-021-03424-y

Blockchain-based federated learning methodologies in smart environments

Dong Li[1,2] · Zai Luo[2] · Bo Cao[1]

Received: 27 June 2021 / Revised: 30 August 2021 / Accepted: 19 September 2021 / Published online: 2 November 2021

Abstract
Blockchain technology is an undeniable ledger technology that stores transactions in high-security chains of blocks. Blockchain can solve security and privacy issues in a variety of domains. With the rapid development of smart environments and complicated contracts between users and intelligent devices, federated learning (FL) is a new paradigm to improve accuracy and precision factors of data mining by supporting information privacy and security. Much sensitive information such as patient health records, safety industrial information, and banking personal information in various domains of the Internet of Things (IoT) including smart city, smart healthcare, and smart industry should be collected and gathered to train and test with high potential privacy and secured manner. Using blockchain technology to the adaption of intelligent learning can influence maintaining and sustaining information security and privacy. Finally, blockchain-based FL mechanisms are very hot topics and cut of scientific edge in data science and artificial intelligence. This research proposes a systematic study on the discussion of privacy and security in the field of blockchain-based FL methodologies on the scientific databases to provide an objective road map of the status of this issue. According to the analytical results of this research, blockchain-based FL has been grown significantly during these 5 years and blockchain technology has been used more to solve problems related to patient healthcare records, image retrieval, cancer datasets, industrial equipment, and economical information in the field of IoT applications and smart environments.

Keywords Blockchain · Federated learning · Privacy · Security · Internet of Things (IoT)

1 Introduction

In the digital age, almost all business models have been undergone unprecedented changes thanks to many advances in information and communication technology such as Internet of Things (IoT) [1]. An outstanding technology that has changed traditional business models is blockchain technology. In 2008, Nakamoto introduced bitcoin in a white paper [2]. Bitcoin is a digital currency that is working based on public Decentralized and undeniable ledger known as blockchain. Blockchain current situation is often compared to that of the Internet in the mid-1990s, When the Internet was still in its basic steps and its value and potential was not yet understood. But some countries have realized the importance of blockchain technology in recent years and had set up research institutes in this zone. To discover the high potential of blockchain, in smart environments such as industry, medical systems, smart city and transportations, much attention has been paid to it and a lot of research studies have been done in this field. There are many uses for blockchain and many articles have been published about the uses of blockchain [3].

On the other hand, federated learning (FL) is known data analysis technique to achieve high potential privacy and security in safety-critical systems such as smart medical and healthcare systems, industrial environments and

✉ Dong Li
18158513269@163.com; li3269@yahoo.com

Zai Luo
luozai@cjlu.edu.cn

Bo Cao
cb527125268@163.com

[1] BULL, 32 Sanhai Road, Guanhaiwei Town, Cixi, Ningbo City 315300, Zhejiang, China

[2] College of Metrology & Measurement Engineering, China Jiliang University, 258 Xueyuan Street, Xiasha Higher Education Park, Hangzhou 310018, Zhejiang, China

smart cities. Recently, FL is known as one of the important artificial intelligence techniques that was proposed and applied by many research studies [4, 5]. As a specific and professional machine learning methodology, FL can update and renew the required training parameters and save all dataset on the local devices. By dividing data records on selected physical or virtual machines in each federated zone, datasets can be trained with high speed process and safe condition to detect unstructured and unknown patterns [6]. By rapid train and test procedures with collaborative learning, a high accuracy with supporting privacy can be guaranteed for existing datasets. There are many advantages to using the FL for the conceptual learning of smart environments [7].

Since the blockchain technology can enhance quality of security and privacy factors to gain training and analyzing sensitive and critical information, applying this technology to use FL mechanisms can guarantee high potential data analytic on the collaborative learning with minimum response time and cost [8]. In other words, blockchain as a core technology in smart environments can join to federate learning procedure to support the security and privacy subjects [9]. Various research studies have been published on vulnerabilities in smart contracts, attacking contracts and stealing cryptocurrencies such as blockchain and Ethereum technologies [10]. Privacy issues like the possibility of identifying users and quantity of transactions are other important points for users. A review of those studies using systematic review and survey studies in the field of blockchain and FL shows that although this field has been considered by various researchers in recent years, but a review of articles shows that a comprehensive study in the field of security and privacy of blockchain research papers indexed in the ISI is not done [11]. For example, Tseng and his partners [12] reviewed the area of blockchain between 2013 and 2018. They have suggested that blockchain could be used as a solution to IoT security issues. Authors in [13] have studied on security-aware models of blockchain between on the Web of Science database on the application of blockchain in power systems. Conti and other researchers [14] have analyzed Bitcoin articles over an 8-year period from 2012 to 2019. Sisi and his partner [15] have focused on energy-aware blockchain strategies and analysis in both Scopus and Web of Science databases. They focused more on content analysis to evaluate Quality of Service (QoS) factors. Considering the blockchain science articles, nothing has been done in the field of security and privacy so far. Therefore, due to the importance of security and privacy challenges, it is necessary to study blockchain-based FL methodologies using systematic review. Finally, authors [16] proposed a comprehensive survey on FL mechanisms and technical aspects of collaborative learning. Analytical results showed that augmented reality and image processing are most popular case studies on applying FL mechanisms.

Given the breadth of the above research and review studies in this area, gaining an overview of this research can help to better understand the main challenges and open issues of blockchain-based FL [17]. For this purpose, a comprehensive review analysis is presented to classify technical aspects of blockchain-based FL methodologies. This classification includes a series of methods for analyzing scientific publications using various mathematical and statistical tools and analysis of smart environments. This type of systematic analysis of research studies helps us to better identify important issues, emerging trends, and influential people in the field of blockchain-based FL methodologies to make appropriate decisions for future research in that area. Privacy and security topics in blockchain are among the most challenging issues in collaborative learning. Therefore, the purpose of the present research analyzes a systematic review of blockchain-based FL methodologies that indexed in the scientific databases. The research community is consisting of 1226 records that had been entered by blockchain researchers in the field of FL in Web of Science indexes over 4 years period (between 2018 and 2021). In this article, the most influential countries, the network of cooperation between countries, top researchers, and some technical aspects of this field have been examined for 41 research studies.

The remaining sections of this paper can be shown as follows: Sect. 2 presents the detailed systematic methodology for the blockchain-based FL techniques that concentrate on effective technical analysis. Section 2.1 demonstrates a technical taxonomy and classification of existing approaches and algorithms. Section 3 analyzes and discusses the evaluation factors, aspects, issues, and existing algorithms for each category. Section 4 shows the research direction and main challenges of blockchain-based FL as well. Section 5 concludes the article with major findings and possible scope of future works.

2 Research methodology and finding appropriate content

This section is among the applied research studies in which systematic techniques and analysis of blockchain-based FL have been used. The statistical population of this study consists of all blockchain-based studies in the field of FL, which are in English language and Web of Science indexes, over 4 years between 2018 and 2021 [18]; To obtain the records of this research, first, using the search strategy introduced in all blockchain field research in the period 2018 to 2021, 1226 items had been identified.

Finally, 41 research studies were selected for inclusion and exclusion goals.

According to Fig. 1, important keywords related to the field of blockchain and FL have been applied. Finally, the following search strategy has been obtained, which includes all security and privacy research studies in blockchain-based FL.

Using the above search strategy, 1226 research records have obtained. After retrieving security and privacy records in Blockchain-based FL techniques, 41 research studies have been considered to analyze in this review. In this section, based on the purposes and questions of the research, various analyzes have been performed, which are stated below. Based on inclusion and exclusion methods existing questions will be answered in statistical and analytical report:

1. Which blockchain types have been applied to the existing FL methodologies?
2. Which FL environments have been studied in the field of blockchain technology for smart environments?
3. Which FL implementation was carried out to cooperation of blockchain technology in smart environments?
4. What are the researchers with the most citations in the field of blockchain-based FL methodologies?
5. What has been the quantitative research studies of QoS in the field of blockchain-based FL?
6. What are the most common pairs of words in the blockchain zone?

Table 1 shows the centrality values, which present each keyword's capacity to connect other keywords within the network as an intermediary. "Blockchain" and "FL" are the top two keywords in terms of between centrality values in general for the past 4 years.

2.1 Blockchain-based federated learning techniques

Blockchain is a decentralized storage system that works without any central authority and stores data in the form of a list of blocks that are linked using the cryptographic hash of the previous block [19]. Data in the blockchain is stored in the form of blocks linked together to form an immutable chain. Every time a new transaction occurs in the blockchain, it is added to the ledger and sent to all network peers [20]. As the blockchain is a decentralized solution that it is natural to extend the concept of a data file system and use a blockchain for the specification of authorization policies. In this paper, we address the main challenges, technical analysis, and research directions of blockchain-based FL techniques. To the best of our knowledge, there exists no approach which handles the case of reviewing this topic [21]. We have mapped our proposed review to categorize existing blockchain techniques, FL environments, implementation and evaluation algorithms, and models to apply blockchain technology on FL in smart environments.

To introduce a brief conceptual definition for blockchain, we divided blockchain into four models including public, private, hybrid, and consortium. In a public blockchain, all data stored in a system are visible to all the nodes. A chain of blocks starts from the genesis block, and all blocks are connected through a cryptographic hash function. Each block contains a header and a series of transactions, and each header contains link pointers of the previous block. So if anyone wants to tamper with any block, he has to change all the headers that point to the previous node, so this feature makes blockchain immutable and tampers resistant. Blockchain uses different consensus algorithms for adding a block in a chain. The main idea behind consensus is to make all peers agree on

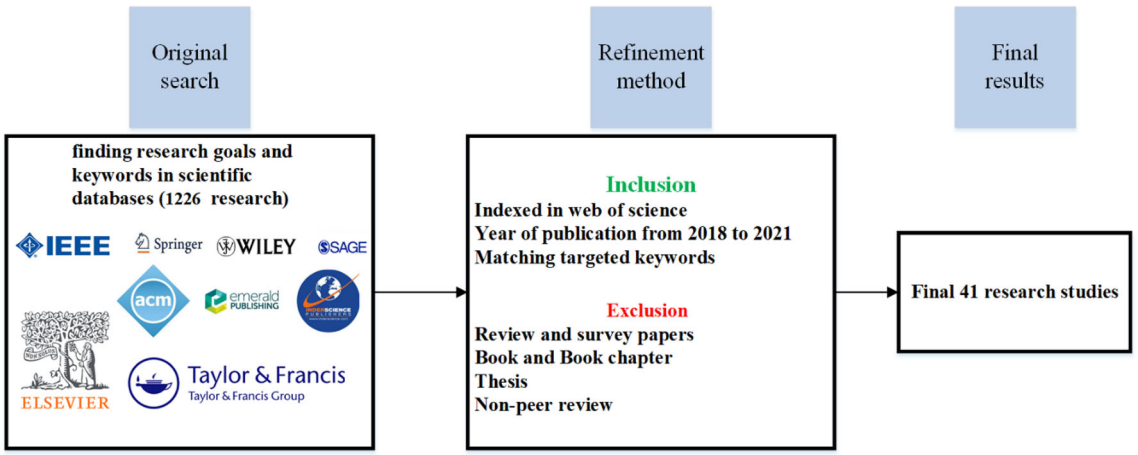

Fig. 1 Paper selection strategy

Table 1 Statistical view of search-based finding report for blockchain and federated learning strategies

Keywords	Number of studies before applying inclusion and exclusion method	Total number of selected papers
"Blockchain"	2435	287
"Federated learning"	1633	154
"Blockchain" + "Federated learning"	1226	41

one dataset. Proof of work (PoW) [22], Byzantine Fault Tolerance algorithm [23], and the Ripple algorithm [24] are some famous consensus algorithms used in different application depending upon the requirements. Bitcoin uses the PoW consensus algorithm to add blocks in a chain. In this algorithm, each node in the network calculates a hash value. In hyper ledger blockchain technology, blocks are divided into sub-categories based on a set of numbers and labels. In federated training, each sub-category is identified using its label to check one point training and supporting privacy [25].

Due to the above-mentioned FL concept, the main advantages of blockchain technologies are applied to the training and gathering of models to avoid network anomalies and intrusion aspects. For example, to increase prediction of anomalies and attacks, hybrid blockchain technology can be useful to support privacy and security of information without decreasing data access level [26]. Also, blockchain technology is one of important solutions to evaluate malware detection by supporting privacy of information [27]. Figure 2 shows the proposed taxonomy for blockchain-based FL methodologies in smart environments. In this taxonomy, FL methodologies are divided into public FL and private FL environments. There are many various entities to collaborate with together with low computing and power quantities in public FL environments. In public blockchain mechanism, just vertical FL approach is analyzed [28]. For sensitive medical information, banking and supply chain information and transportation data, private blockchain mechanisms are applied with respect to evaluation of horizontal FL and federated transfer learning approaches [29].

2.2 Blockchain-based vertical federated learning techniques

In [30], authors suggested a federal learning algorithm with Blockchain capability for sharing knowledge on the Internet of Vehicles. They have provided a categorized blockchain model for training procedure in a vertical federation learning method to evaluate information of vehicles. The hierarchical federation learning algorithm is designed to respond to the distribution pattern and the need for Internet of Vehicle (IoV) privacy [31]. The proposed hierarchy algorithm can improve data sharing between vehicles and training quality. In addition, the active blockchain framework can counter some malicious attacks effectively [32]. The experimental result shows that the blockchain hierarchical framework is able not only to increase the reliability and security of knowledge sharing but also to be compatible with large-scale vehicle networks with different regional characteristics. Their proposed hierarchical

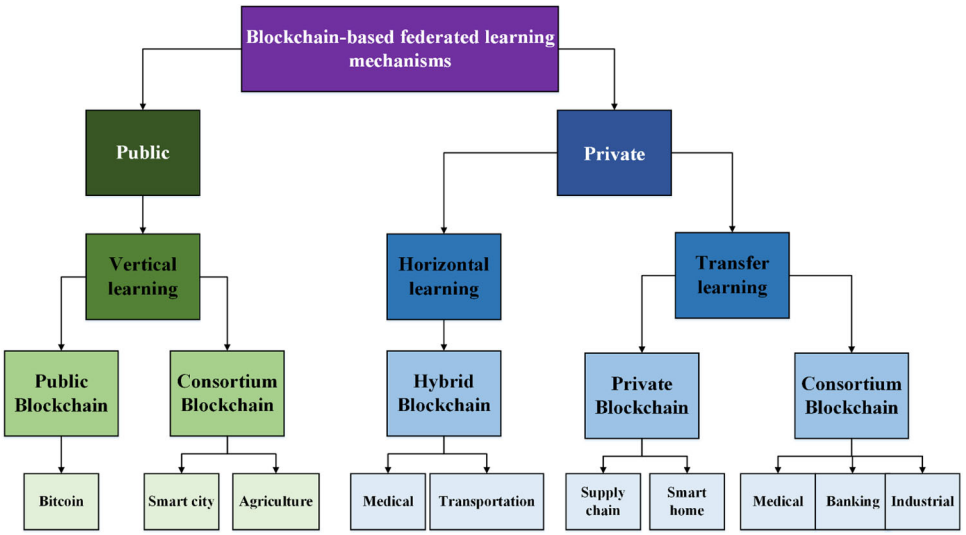

Fig. 2 Comprehensive taxonomy on blockchain-based FL mechanisms

federation learning algorithm improved accuracy factor than conventional federation learning algorithms and the proposed blockchain model can support security against malicious attacks between the sharing information procedures [33].

In [34], authors presented a blockchain technology for fog computing and problems in IoT that could be solved using FL. They found that fog computing works as a combination of cloud computing and edge computing, and can reduce problems such as network congestion, latency, local autonomy, and more. In this model, the devices upload the available local information to the fog servers, where global updates are generated. While only update pointers are stored on this chain, the distributed hash table (DHT) table is used to save data and ensure the production of blocks. They were able to achieve lower time of accuracy in several evaluation methods, which improves performance. Finally, after obtaining the desired results, they intend to expand the model by optimizing the trade-off between privacy and performance to arrive at more general scenarios, as well as using game theory and the Markov decision process to optimally compute.

In other work [35], authors presented a model of machine learning called federated learning or FL. Features of this model include low latency, secure privacy, and optimal power consumption, which have recently been approved and recommended by Google. However, one of the problems of this model is that if only one of the trainers sends incomplete data into the blockchain network, the network and the learning process may fail. This model was proposed to replace the older FL model used to build a decentralized ecosystem.

In [36], authors have provided a FL protocol to Encourage workers which collect and store models in blockchain-enabled FL. In this paper, they propose a mechanism-design-oriented FL protocol (MD) on a Blockchain model to make a rule. This rule, makes the system (FL Blockchain network) reach specific goals. In the system, workers must be exerted irreversible and costly efforts to update models and reward workers based on the quality of their works (all data which improve models). They used mathematical proofs of the effectiveness of their method. Among the advantages of their proposed way, we can mention such things as implementation will be feasible and mathematically guarantee that system workers will expend effort and will not be lazy. They aim to recognize system performances & operational costs (latency, etc.) in the future. On the other hand, like Ethereum, they implement their design on top of a network (Public blockchain network).

In other study [37], authors suggested a resource trading scheme based on combined blockchain for FL in the field of Edge Computing. The suggested system is based on a combination of consortium blockchain and public blockchain and employs payment channel method to deal with public blockchain presentation problem and a Data Quality-Driven Reverse Auction (DQDRA) designation to assist auctions in edge nodes. The simulation utilizes a budget-practicable method named DQDRA and makes a comparison between this and traditional methods namely greedy and random procedure. Based on the simulation results, the suggested system fulfills budget-practicability, computational productivity, security, and individual reasonableness.

Authors [38] have proposed a new system that collected different concepts like IoT devices/cloud/blockchain/nodes. In this system, the authors introduce a new algorithm called "CREAT" that uses edge nodes on their local data to increase caching mechanism without nodes access to other node's data. Also, for the warranty of that data, the authors combine FL and blockchain. The authors tested and simulated algorithms on 1 m real datasets from MovieLens. The result of compared algorithms shows advantages like boost training processes/good cache efficiency besides increasing cache size/lower time for upload after compressions.

In [39], authors presented a new method based on defense organization for creating a connection between the army and the community in an IoT environment. The proposed methodology uses an algorithm to meet the training challenges to achieve high accuracy and avoid a specific model. The purpose of this paper is to provide a defensive framework for a sustainable community using blockchain technology and federation learning as a service model and the effectiveness of this procedure is satisfactory. Evaluation and model of empirical results indicate that this method is more promising in terms of precision and miss compared to the base method. The advantages of this can be attended and for its disadvantages, we can point to the endangerment of organizational challenges and national security.

Authors in this study [40] designed a framework on basis of Blockchain which is decentralized and also learning federated. This method wont fail in state of doesn't have a main node (Server node) which the failure on it cause the fail entire the system. The Authors designed method has advantages of reducing failure risk to zero and bring privacy in safe state. Also they developed an approach on model training which cause in better privacy, accuracy and robustness. In training method, they developed the building design of system. This model help accuracy in training with total utilizes of the given information. The main advantage of this paper which has proved by the Experimental test that Privacy, Accuracy and system powerfulness would become more and more betters that past.

Authors [41] suggested an automated Blockchain-based Federated Learning (BFL) architecture a privacy and impressive vehicle connectivity, in which localized on-Vehicle Machine Learning (oVML) project changes shared and validated in a decentralized manner. The authors created a computational structure that incorporates manageable system and BFL variables to quantify their impact on system efficiency. The authors provided several computational and simulations result that highlighted numerous non-observations and perspectives for responsive BFL architecture. The authors improved FL with blockchain for automated vehicles' efficiency and safety. The BFL architecture allows effective connectivity of automated vehicles which local oVML training materials share and validate the changes in a completely distributed manner. The authors reduced device reprieve by using channel dynamics, demonstrating that the suggested concept of modifying the bloc entrance rate is observably operational and able of driving the device dynamics to the optimal processing stage.

2.3 Blockchain-based horizontal federated learning techniques

In this study [42], authors presented a method called FL. They believe that this model is capable to not only keep artificial intelligence secure but also protect the primary information while improving the system. For that purpose, they used limited and global blockchain method. Limited method registries the upcoming levels of the procedures by time and date; Device to Device (D2D) facilitates the task and decreases time. Global method improves the effectiveness and provides privacy and validation by confronting system defects. In the future, authors would perceive the dynamic form of segments of the model and protect them against probable threats to optimize that into a more secure and capable method.

In [43], authors propose a unique FL architecture (FL-an idea that supports a model that uses distributed devices that work on a big scale, to benefit the cooperated model from good local databases-) by benefiting from the blockchain. It's a 2 part design consist of an evaluation of numbers and an algorithm that selects participants that helps the FL to choose the devices of each turn of the training. This 2 part architecture helps to solve a big problem—which is when they want to transmit a model of an FL model, there is a lack of security and also every part of the process can get attacked by hackers—with connecting fields of blockchain and FL. As the result of this paper, the proposed algorithm defeated other algorithms in terms of the proficiency of updating the model. For future work, the authors want to design a more proficient strategy of selecting to improve the FL framework which is assisted by blockchain.

In [44], authors proposed a blockchain-based defense technology for different security perspectives in FL systems. The proposed blockchain algorithm simplifies the learning procedure and gives safety versus the attacks named model poisoning. In this study, the simulation implements Keras and Tensorflow in calculating algorithm productivity, and FL is executed through the MNIST dataset that has 60,000 handwritten digit figures and also 10,000 verification figures. The authors provided a potential technology that enhances the security during FL. The suggested algorithm exposes greater speed, security, and convergence.

In [45], authors suggested a decentralized and safe blockchain-based mechanism in FL. The provided mechanism utilizes Elastic Weight Consolidation to authorize optimal learning of the successive assignments, and Ethereum to authorize decentralization, homomorphic encryption, and differential privacy algorithms to authorize the safety and secrecy, and finally uses Gaussian Process (GP) hyperparameter optimization technique and a rewarding based on deposit to make the mechanism financially practicable. The efficacy evaluation is done through the implementation of a 5*5 involution layer neural network construction and the mechanism training is guaranteed through using MNIST dataset with 60,000 schooling cases and 10,000 testing cases of 28*28 pictures of 10 handwritten figures. The authors provided an efficient system with high safety and privacy and an increased training level.

In other work, authors [46] propose an FL learning structure based on blockchain which allows using secure, trusty FL as a method to solve the problem of centralized FL which has many security problems with chances of privacy leaks in the process of gathering unprocessed data in the model. In this structure proposed by the authors, the updated model of divided vehicles gets authenticated with the help of miners to resolve the problem of untrustworthy updates for the model. And after that, it is saved and kept in the blockchain. For more protection on the blockchain, an alternative method that adds noise is used for the FL based on the blockchain. As the result, the authors found out the method is sufficient and can be useful for traffic control systems and departments like the police. For further work, they want to improve the sufficiency and also the accuracy of the described structure.

In [47], authors proposed a FL method built on a credibility model to help home product producers develop a machine learning algorithm focused on data from consumers. The authors used blockchain to substitute the conventional FL device's distributed aggregator. The authors described the framework they designed for intelligent house system producers that want to create a machine learning algorithm utilizing information in their

users' mobile products to evaluate their users' habits and optimize their technology and goods. The authors developed the framework using several cutting-edge technologies, such as a mobile cloud server, blockchain, cloud storage, and FL. The authors show in experiments that their standardization strategy surpasses cluster standardization when devices are subject to varying levels of confidentiality security.

In other study [48], authors proposed an amalgamation technique inclusive of blockchain and FL to tackle endpoint menaces by appraising MNIST datasets in local data. To facilitate the ensued data, some important functions were implemented thus, comparing to the former approaches, endpoint menaces diminished; conversely the classifying ameliorated and demonstrated a supple while steady discharge. The authors plan to provide a fresh enterprise counting further clients alongside, concentrating on sorting out a selection and its hazard later in their incoming research.

In [49], authors presented an approach that optimizes the FL model. FL is a secure indoctrinating model that uses client information to form an understanding algorithm. regardless of providing info security, FL faces some issues such as congestion of variant information and models that lead to system impose and latency and lack of client assurance as well. To overcome those obstacles, the authors suggested an approach that uses blockchain to involve each client as a node. They realize that the method above, not only upgrades the FL model in terms of required time, precision and resistance but also is more capable than other resembling approaches based on the simulations implemented.

In [50], authors provided a new method based on a machine learning model through a set of data distributed to several owners in an IoT environment. This new design proposes an intelligent agent using the concept of an intelligent contract. This proposed design is efficient and is based on trust and the stochastic gradient descent algorithm is used. The purpose of this article creating a link between a multi-factor system, blockchain, and FL. Evaluations show that this method is safe and effective. The advantages of this method include privacy and its disadvantages include the lack of an incentive mechanism that will be part of the author's plans.

In [51], authors proposed a blockchain-based FL for digital twin environment between edge computing and IoT systems, which integrates digital twins with edge networks. To improve communication security and data privacy protection in the proposed model, they propose a blockchain-enabled FL scheme. They suggested an asynchronous method to apply blockchain on digital twin FL for managing customers and allocation of IoT resources to increase the efficiency of smart environments. The proposed scheme in this paper will significantly improve both communication efficiency and data protection for IoT applications, according to theoretical research and numerical results.

Authors in this work [52] proposed a crowdsourcing framework named CrowdSFL, by integrating blockchain, accompanied by FL with presenting a pristine cipher algorithm by carrying out trials, utilizing empirical medical datasets (e.g. BWCD–HDD) in truffle environment on Ethereum platform and Python, in addition to juxtaposing it to Secure-SVM. The proposed commission successfully fulfill the writers' main goal by strengthening safety and seclusion issues alongside enhancing validity, coherence, and time overhead; even though, the expenses of its application transpired excessively which will be resolved later in their incoming research besides the improvements in its practicality.

Authors in another work [53] provided an autonomic blockchain-based federated learning (BFL) model. This model had made to provide better privacy and Vehicle communication grillwork. BFL on vehicles provides machine learning with no need for any intensive schooling datum or harmony by employing the meeting of the working blockchain. They used two assumptions Calculation and verification time in oVML and Proof of work conforms to the Poisson flow. The experimental results show that delay decrements when SNR gains, which it records by numeral and filing computer simulation outcomes.

2.4 Blockchain-based federated transfer learning techniques

In [54], authors have provided a way to Improvement the data security of Federated Learning called "FLchain". In this paper, they used a concept of channels and transfer data with a Model called "The Global Model State" in Blockchain Network. In FLchain use MEC-enabled Blockchain Network and implement methods such as Device Register, Models update, Models Consensus, and more. For machine learning on global models, the FLchain platform made an Exclusive Channel per model and The Models will be store in the distributed server (Blockchain) [55] with high security rather than store in single data storage. Global Models stored in a Merkle Patricia Tree. The cons of this platform are that The Data publisher Devices (user devices) depend on the integrity of devices at the edge of their network to data transfer with the blockchain network. They aim to optimize data computing, latency time, requirements in storage platforms in the future. On the other hand, they implement a mechanism for data miner nodes group and devices in FLchain.

Authors in this study [56] presented a machine learning method called FL. It is a distributed machine learning method that allows ML models to be taught on decentralized private data. FL saves network bandwidth by preventing the transfer of large amounts of training data and also protects data privacy due to the local nature of training Machine learning (ML) models. FL is used in applications such as the Google Keyboard to predict the next word, hospital health care such as predicting death and length of hospital stay, or the telecommunications industry such as cores and network edges. They created an FL server and two FL clients to display a demo scenario. Another model is built on an HP server that creates a channel with three similar nodes. Results show In the blockchain protocol, the accuracy of the model trained by the FL is very close to the centralized training, and this protocol can provide a secure connection and communication between the server and the clients.

In [57], author have proposed multi-agent systems (MAS) that perform different activities by dividing tasks into separate objects. Data security in MAS is provided in the BLOCKCHAIN system and encryption techniques. In this paper, research on the learning of medical things (LoMT) a new architecture based on a MAS is performed. The components of the LOMT model include architecture and agent, which is an architecture based on the creation of factors by connecting to cloud infrastructure, and the agent is an agent of an independent object in which it reacts to the environment. Types of agent models include Learning Agent (LA), Data management agent (DMA), and Indirect agent (IA). LA is based on database-labeled records, and DMA performs medical data management and IA performs classification based on DMA demand. In experimental studies, the performance in different environments and the accuracy and time required for the performance of these agents were measured.

In [58], authors suggested a framework for utilizing data to boost position projections without jeopardizing the security of the clients who produce this data. The authors recommended using FL to practice remotely on a customer's smart devices while also detecting and combating the risk of harmful operators or enemies intentionally reporting inappropriate information to harm the training method. To maintain the security of the learning method the authors recommended using a blockchain rather than the intensive server. The authors explained how to capture, store, and use this information to learning in a federated platform built on a stable blockchain. The authors hope to present their project for a holistic system that integrates device location data through FL to provide customers with reliable position services (centered on position forecasting). The authors described areas where better work should be done, such as using positional or central conditional security strategies to protect against offensives.

Authors in this study [59] proposed a prototype for an integrated blockchain-organized machine learning infrastructure for private information FL in healthcare and modern medical usefulness. In an FL system information is just saved on computers and the framework is modified dependent on other people's information as well as your information specifically on your computer. The authors investigate a more comprehensive hybrid of utilization, with a focus on consolidating the learning mechanism as well as the accountability and incentive system that blockchain may provide in the machine learning system. The disadvantage of this paper is that the accuracy of one's information to the system can be calculated in a number of aspects thus, more analysis and experiments can be performed to establish reward structures that favor participants while increasing the model's performance and preventing bias.

In this work [60], author suggested a new procedure based on using a new mechanism design in strategic cases moving to achieve the desired goals when employees act rationally. The proposed methodology uses an algorithm to meet the training challenges to achieve high accuracy. The purpose of this article is to achieve the desired goals to educate participants and maximize their productivity. And in this way, blockchain technology and learning of the federation have been used. Evaluations show that this method preserves the privacy of user data to some extent compared to previous methods. One of the advantages of this method is that applicants cannot control the behavior of employees who are equipped with blockchain and one of its disadvantages is the lack of a mechanism to encourage workers.

Authors in this study [61] presented a reputation-based FL technique that the IoT devices get trained and update trained model on datasets. These models solve some problems such as communication cost, latency optimization, and privacy-preservation. They also compared FL and Fine-grained the FL method using the cloud, multi-cloud servers, and data centers. In this paper, they have mentioned the importance of FL and the role it has in personalizing model training for mobile users, and they proposed the idea of reputation-aware decentralized along with the blockchain technology led to other research for future works.

In [62], authors provided a new model based on a deeply distributed, safe, and equitable framework called the Deep chain is a value-based incentive mechanism that strengthens the motivation to participate. In this model, the deep learning algorithm is used and is also a secure and decentralized model. The purpose of this research is to create an incentive mechanism that can control the

education process. Evaluations show that the results of this model are promising. The disadvantages of this method include data privacy, and its disadvantages include security problems.

In [63], authors suggested a blockchain-based model in industrial IoT (IIoT) systems to guarantee client data privacy. The authors showcase a platform architecture for failure detection in IIoT utilizing blockchain-based FL systems, providing the integrity of client data. Each client in the architecture builds a Merkle tree with each leaf node representing a client data record and stores the tree root on a blockchain regularly. To refer to the data heterogeneity problem in IIoT failure detection, the authors suggested a new centroid weighted FL algorithm by notice to the space and positive classification of features of each client dataset.

In [64], authors provided a decentralized cognitive computing (D2C) approach which is a simulation of mankind's resolution and thinking system for a device to be independent. However; lack of security, effectivity, and scant motivation in information sharing are major defects in this method which leads to being problematic. The authors considered using FL and blockchain together. FL prevents security threats and blockchain stimulates information sharing. Investigations have declared the advantage of this approach among other similar methods. In the future, they will expand that into a widely used approach by creating a bonus mechanism as well.

In [65], authors presented a method to learn blockchain-based federation to implement shared heterogeneous machine learning between distributed agents who own data. This method performs distributed machine learning without a trusted central server. They proposed a blockchain-based learning framework, which enables various operators to train smart driving models without sharing data. This method uses intelligent control based on a support vector machine (SVM). They developed an intelligent control model for heavy trains through a fusion algorithm. Performance evaluation of the proposed method is introduced through simulation results. First, compare the training results of the federation participant data after learning. Second SVM simulation results: As the training period increases, the accuracy of the training continuously increases. They provided a China-based framework to protect the privacy and security of user data. The experimental results show that this FL method can train the better model with more data.

Authors in this study [66] have proposed a decentralized FL method called Chain FL, composed of miners and training servers which replaces Ethereum Blockchain with the common centralized way of saving data. Chain FL allows users to anonymously keep training data on their servers and uses a plan which separates huge model parameters into tiny smart contracts. There are significant subjects that have been studied in the article; fault-tolerant which may appear from low-quality data and to prevent that and also terminating harmful users and improve management of large data.

Authors in this work [67] used FL system which can improve thread detection by gathering data. They presented a solution in which the parties in FL can be held accountable and then described a permission blockchain-based FL method where has gradual updates to a detection machine learning model which can enhance the security and decrease malicious activities. For initial testing they compared centralized versus FL, then they created an experimental setup which was a Linux-based deployment configuration, and also researched FL with blockchain support. They found out that the performance of blockchain is tied to the complexity of neural networks at the core of FL. Finally, they assumed that the blockchain is not compromised directly.

In [68], authors have proposed BlockFL architecture to solving data security issue of users that collected by companies. It uses EOS blockchain by proof of concept (POC) consensus mechanism and gives rewards to users for data analytics without data collection issues. The authors introduced the Class-Sampled Validation-Error Scheme (CSVES) via smart contract and implemented it in python and hyper ledger then they simulated their project with MNIST dataset and used ten devices. The result of simulations proves that blockchain doesn't interfere with FL. In the future authors will study others validation layouts.

In [69], authors have proposed a federate Learning Architecture for Providers to reducing the privacy concern of addresses and the load volume of transmission. The Author Also developed a componential topology in Blockchain to improve the model parameters reliability and security which includes DAG and permitted Blockchain. In addition, they provided a schema for improving efficiency with Deep Reinforcement Learning. They proposed Algorithms in componential Empowered FL based on Blockchain and Deep Deterministic Policy Gradient-Based on Node Selection. The proposed method improved learning efficiency and accuracy.

In [70], authors provided Internet of Health Things (IoHT) privacy methods in the field of FL and Differential Privacy (DP). Blockchain management to provide data source and use an in-depth learning process for loHt data is described in this paper. This paper presented an FL framework as a COVID-19-based radiometric detection tool and the development of secure encryption schemes for patient information by upgrading Blockchain layers in the FL field. The authors presented an FL framework as a COVID-19-based radiometric detection tool and the development of secure encryption schemes for patient

information by upgrading Blockchain layers in the FL field. Blockchain was used to track data in symptom management and COVID-19 diagnosis. One of the modules as deep learning for COVID-19 detection is biometric modules. The mentioned programs consume medium to high energy levels. These approaches are useful for maintaining the privacy of personal data in the field of health.

Authors [71] suggested a trustworthy designation of choosing workers through FL in mobile networks. The suggested designation was based on reputation metric for choosing workers reliably and utilized a model named multi-weight subjective reasoning to plan to calculate the reputation operatively, and consortium blockchain algorithm to protect reputation administration. The simulation was done through the MNIST dataset, which is specified for grouping digits and has 60,000 schooling cases and 10,000 test cases, and used Tensorflow 1.12.0. The authors focused on making the worker choosing process reliable. The numerical results prove that the proposed designation is capable of adding trustworthy FL to the field of mobile networks.

Authors in another work [72] suggested a decentralized blockchain-based FL framework named BAFFLE, which is aggregate free. To adjust round interpretation, model accumulation, and renew the tasks, BAFFLE uses Smart Contracts and takes advantage of the score and bid technique to increase computational accomplishment. To evaluate the proposed environment, the authors examined it on a private Ethereum system, and to run the case study the authors used the New York City taxi dataset to increase taxi driver income through BAFFLE. The proposed environment was proved to decrease the gas costs and increase the scalability and efficiency of computations.

In [73], authors provided a solution that integrates (FL) and blockchain to warrant both datum solitude and network safety and provided a frame to decentralize polar automaton acquirement models; a meeting blockchain solution as a secondary script of solitude used to bond reliable shared schooling on the fog. The authors presented an allied Blockchain FL relying upon VNet architecture supports meeting flow. The remonstrative vehicle solitude is guaranteed by adopting blockchain ability with the FL via fog meeting. The gifted results were relying on using MATLAB and Simulink dramaturgy. Authors will carry out rather experiments by thinking several FL algorithms and accept the ensemble acquisition material along with FL in surplus to experimenting proposed out with several datum sets.

In [74], authors combined Blockchain technology and FL using Python, creating Biscotti with the goal of privacy and maintaining the accuracy of FL at the same time. In FL, there are certain difficulties, such as Sybil attacks, poisonings, information leakage attacks, and also utility loss with differential privacies. Biscotti fulfills three different roles. As a noise, it provides a group of noise to prevent leakage. As a verifier, it receives masked updates and uses multi-KRUM to filter out the poisoned update. And finally, as an aggregator, it uses a secret sharing scheme to aggregate the update and create a new block with aggregated gradient. This scheme is extensible, fault lenient, and can maintain across common attacks. It can assure the privacy of each applicant and also control the global model's behavior in the presence of 30% of attackers. Biscotti uses Proof-of-Service as consensus and peer gain stake by providing stochastic gradient descent update or by facilitating the consensus process. Each peer is connected to a subset that allows flooding-based dissemination of the block. Therefore, the peer can be offline during training and join later.

3 Discussion and technical analysis

In this section, a technical analysis and analytical discussion is presented for existing blockchain-based FL techniques. Based on previous defined questions in Sect. 2, we answer these questions based on some technical and statistical results as follows:

1. Which blockchain types have been applied to the existing FL methodologies?

Figure 3 illustrates the percentage of existing blockchain technologies in FL environments. As it observed consortium monopolizes the maximum percentage by 20 research studies. The hybrid blockchain technology, private, and public have 12, 6, and 3 articles respectively. Also, Fig. 4 shows a statistical percentage on the usage of different blockchain technologies. With respect to flexibility f consortium technology medical systems, banking transformations and defense critical systems can use this technology in FL approach.

2. Which FL environments have been studied in the field of blockchain technology for smart environments?

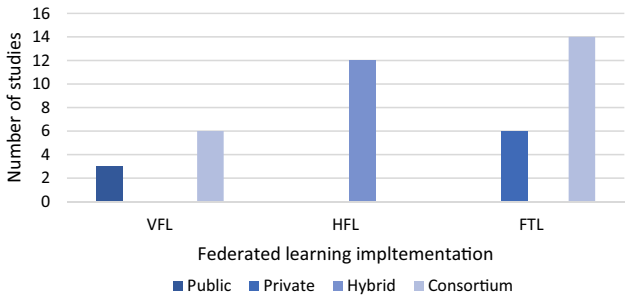

Fig. 3 Variety of blockchain technologies for existing federated learning techniques

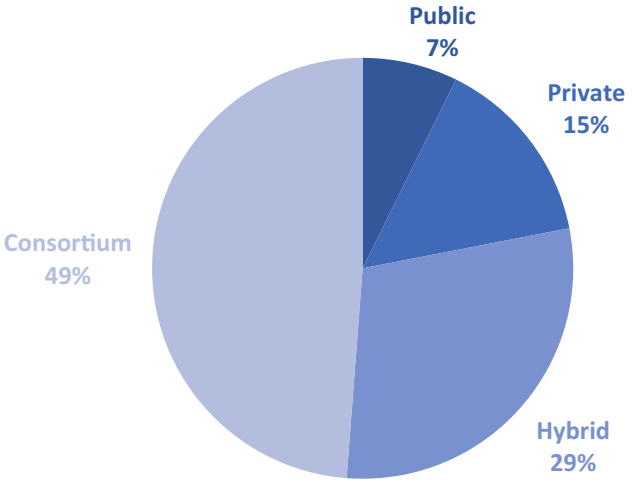

Fig. 4 Statistical view on blockchain technologies in federated learning concept

Based on Fig. 5, Federated Transfer Learning (FTL) method is used more than Horizontal Federated Learning (HFL) and Vertical Federated Learning (VFL) methods. The HFL method is refer to a homogenous environments with a basic learning approach that aids to share same features with different various samples. On the other hand, The VFL method is applied to a heterogeneous environments with respect to huge number of different set of features. In this literature, we observed that the FTL method is used more in the smart environments because this method is suitable for smart applications where overlapping features and users create some problem accessibilities on intelligent devices. According to Table 2, a list of existing FL methods is presented with full name and their abbreviations.

3. Which FL implementation was carried out to cooperation of blockchain technology in smart environments?

According to Fig. 6, FL implementations have been categorized into public and private level. Also, privacy factor in both methods is based on horizontal, vertical and

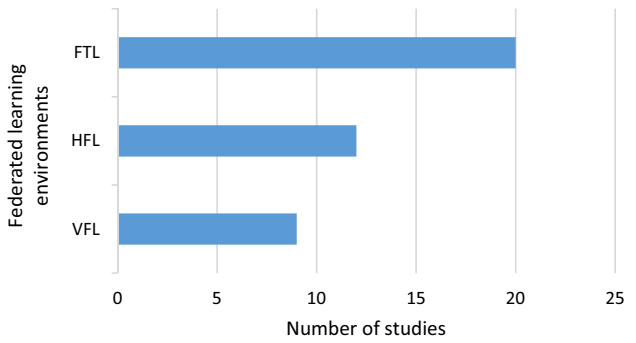

Fig. 5 Percentage of the federated learning environments for blockchain technologies

Table 2 List of applied federated learning algorithms with full name

Abbreviation	Full name
CFL	Chain Federated learning
FGFL	Fine-Grained Federated Learning
AFL	Auditable Federated Learning
CEFL	Communication-Efficient Federated Learning
RFL	Reward Federated Learning
RFL	Reputation-Aware Federated Learning
RAFL	Reliability-aware Federated Learning
IFL	Incentive-aware Federated Learning

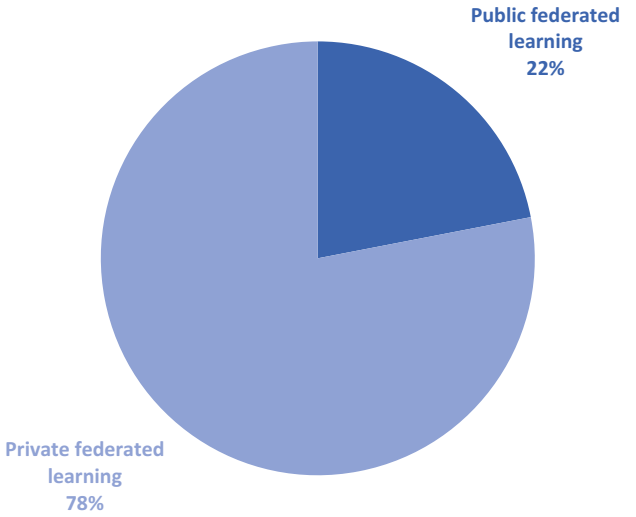

Fig. 6 Comparison of federated learning implementations with blockchain technology

transfer learning methods of FL. We can see that private FL implementation has highest research direction on this field based on blockchain technology aspects.

4. What are the researchers with the most citations in the field of blockchain-based FL methodologies?

Based on Table 3, a list of most highly cited researcher is shown in the field of blockchain-based FL methodologies. This report is based on google scholar database and technical interests of each researcher.

5. What has been the quantitative research studies of QoS in the field of blockchain-based FL?

Figure 7 shows that the existing case studies have been assessed based on main quality factors including accuracy, latency, time, security, privacy, and energy consumption. Eventually, we observed that accuracy was the most important quality factor that has been evaluated and energy consumption has minimum usage than the other QoS factors. Totally, we examined six main QoS factors in

Table 3 List of most highly cited researchers in federated learning and blockchain technologies

Cited by	Researcher
70,242	Qiang Yang
29,942	Bhaskar Krishnamachari
26,062	Yaochu Jin
20,242	Mary Lacity
17,074	Jin Li
9344	Hasnaine Siddique
8281	Dongning Guo
6565	Rong Yu
6481	Yaser Jararweh
5784	Behrad Bagheri

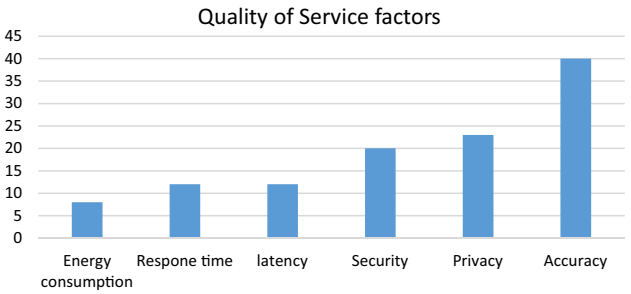

Fig. 7 Variety of evaluated QoS factors in blockchain-based federated learning techniques

blockchain-based FL techniques. However, other factors could be evaluated, such as reliability, precision and scalability issues, performance efficiency, etc.

6. What are the most common pairs of words in the blockchain zone?

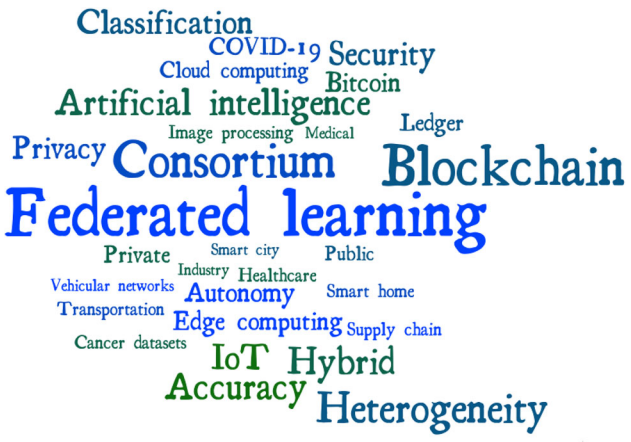

Fig. 8 Variety of technical keywords in blockchain-based federated learning case studies

According to Fig. 8, existing hot keywords of this review have been shown to check the priority of each topic, algorithm and technical concept for existing smart environments. This is observable that smart city, smart industry, medical systems and supply chain management are cut of edge case studies as open issues.

4 Future work and open issues

In this section, there exist hot and new innovations and open challenges in the blockchain-based FL which should be analyzed and evaluated comprehensively to support optimal use cases on them. We explain existing issues with respect to blockchain technology and FL environments as follows:

- Energy-aware FL has some challenges such as finding a deep relationship between energy consumption features and reliability factors. Applying a standard and optimal blockchain framework is a main open issue to support minimum failures in the smart environments [75].
- In medical IoT environments, the historical-based feature selection on the private health records is an open issue to achieve the optimal accuracy of the prediction procedure. Also, to enhance the security of medical records, a hybrid blockchain model is necessary as new open issues in the FL techniques [76].
- Time management in FL approaches is a main challenge for real-time IoT applications [77]. Also, to achieve the optimal QoS factors, meta-heuristic algorithms can more consider for evaluating accuracy and redundancy of prediction procedure in the federated transfer learning method.
- Consortium blockchain-based horizontal FL has some open issues such as data-centric evolutionary cryptography, data filtering, and extracting dependency matrix for important features in training methods by FL.
- Formal analysis on conceptual privacy aspects is one of important open issues that researchers can discuss and evaluate sensitive data in FL strategies [78].

5 Conclusion and limitations

The research focused on blockchain-based FL techniques in smart environments by examining the past 4 years to identify the changes and evolution in this field. This review analyzed existing research studies based on 1226 articles. Finally, this research selected the co-evolution between the two main fields by investigating the blockchain studies from a FL perspective. This review used Scopus database because it is a frequently preferred database in similar

studies and it is a comprehensive database. This may cause studies not listed on Scopus to be excluded in this research. Future studies may include the ISI Web of Science and similar reliable databases in the research. To obtain more valid and reliable results, only journal articles were used within the scope of the database. Therefore, future studies may include other types of publications, such as book chapters and conference papers, to capture a more holistic perspective. Analytical results showed that there are many open issues and challenges on new case studies to apply blockchain technology for prediction of unstructured patterns using FL techniques. Finally, the experimental results show that there are many gaps and new challenges to evaluate light weight blockchain methodologies by applying tensor flow process, meta-heuristic algorithms and evolutionary methods in FL environments. Also, categorizing vertical and horizontal FL mechanisms help researchers that can find optimal solutions to improve accuracy factor in sequential training procedure based on data set type. Medical information and healthcare data are important environments to improve accuracy factor, privacy and decrease error rate using FL.

Author contributions Not applicable

Funding Not applicable.

Data availability Not applicable.

Code availability Not applicable.

Declarations

Conflict of interest No conflict of interest.

References

1. Khalid, U., Asim, M., Baker, T., Hung, P.C.K., Tariq, M.A., Rafferty, L.: A decentralized lightweight blockchain-based authentication mechanism for IoT systems. Cluster Comput. **23**(3), 2067–2087 (2020). https://doi.org/10.1007/s10586-020-03058-6
2. Nakamoto, S.: Re: bitcoin P2P e-cash paper. Cryptogr. Mail. List (2008)
3. Shen, H., Zhang, M., Wang, H., Guo, F., Susilo, W.: A cloud-aided privacy-preserving multi-dimensional data comparison protocol. Inf. Sci. (Ny). **545**, 739–752 (2021)
4. Yang, Q., Liu, Y., Chen, T., Tong, Y.: Federated machine learning: concept and applications. ACM Trans. Intell. Syst. Technol. **10**(2), 1–19 (2019)
5. Khan, L.U., Saad, W., Han, Z., Hossain, E., Hong, C.S.: Federated learning for internet of things: Recent advances, taxonomy, and open challenges. IEEE Commun. Surv. Tutorials (2021)
6. Wang, P., Wang, L., Leung, H., Zhang, G.: Super-resolution mapping based on spatial–spectral correlation for spectral imagery. IEEE Trans. Geosci. Remote Sens. **59**(3), 2256–2268 (2020)
7. Zhou, W., Lv, Y., Lei, J., Yu, L.: Global and local-contrast guides content-aware fusion for RGB-D saliency prediction. IEEE Trans. Syst. Man Cybern. Syst. (2019)
8. Lim, W.Y.B., et al.: Federated learning in mobile edge networks: a comprehensive survey. IEEE Commun. Surv. Tutorials **22**(3), 2031–2063 (2020)
9. Li, D., Deng, L., Cai, Z., Souri, A.: Blockchain as a service models in the Internet of Things management: systematic review. Trans. Emerg. Telecommun. Technol. (2020). https://doi.org/10.1002/ett.4139
10. He, Y., Dai, L., Zhang, H.: Multi-branch deep residual learning for clustering and beamforming in user-centric network. IEEE Commun. Lett. **24**(10), 2221–2225 (2020)
11. Zarrin, J., Wen Phang, H., Babu Saheer, L., Zarrin, B.: Blockchain for decentralization of internet: prospects, trends, and challenges. Cluster Comput. (2021). https://doi.org/10.1007/s10586-021-03301-8
12. Tseng, L., Yao, X., Otoum, S., Aloqaily, M., Jararweh, Y.: Blockchain-based database in an IoT environment: challenges, opportunities, and analysis. Cluster Comput. **23**(3), 2151–2165 (2020). https://doi.org/10.1007/s10586-020-03138-7
13. Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q.: A survey on the security of blockchain systems. Future Gener. Comput. Syst. **107**, 841–853 (2020)
14. Conti, M., Kumar, E.S., Lal, C., Ruj, S.: A survey on security and privacy issues of bitcoin. IEEE Commun. Surv. Tutorials **20**(4), 3416–3452 (2018)
15. Sisi, Z., Souri, A.: Blockchain technology for energy-aware mobile crowd sensing approaches in Internet of Things. Trans. Emerg. Telecommun. Technol. (2021). https://doi.org/10.1002/ett.4217
16. Aledhari, M., Razzak, R., Parizi, R.M., Saeed, F.: Federated learning: a survey on enabling technologies, protocols, and applications. IEEE Access **8**, 140699–140725 (2020)
17. Weng, L., He, Y., Peng, J., Zheng, J., Li, X.: Deep cascading network architecture for robust automatic modulation classification. Neurocomputing **455**, 308–324 (2021)
18. Kordestani, H., Zhang, C., Masri, S.F., Shadabfar, M.: An empirical time-domain trend line-based bridge signal decomposing algorithm using Savitzky–Golay filter. Struct. Control Heal. Monit. **28**(7), e2750 (2021)
19. Lv, Z., Qiao, L., Hossain, M.S., Choi, B.J.: Analysis of using blockchain to protect the privacy of drone big data. IEEE Netw. **35**(1), 44–49 (2021)
20. Cai, K., Chen, H., Ai, W., Miao, X., Lin, Q., Feng, Q.: Feedback convolutional network for intelligent data fusion based on near-infrared collaborative IoT technology. IEEE Trans. Ind. Inf. (2021)
21. Lv, Z., Singh, A.K., Li, J.: Deep learning for security problems in 5G heterogeneous networks. IEEE Netw. **35**(2), 67–73 (2021)
22. Keenan, T.P.: Alice in blockchains: surprising security pitfalls in PoW and PoS blockchain systems. In: 2017 15th Annual Conference on Privacy, Security and Trust (PST), pp. 400–4002 (2017)
23. Chinnathambi, S., Santhanam, A., Rajarathinam, J., Senthilkumar, M.: Scheduling and checkpointing optimization algorithm for Byzantine fault tolerance in cloud clusters. Cluster Comput. **22**(6), 14637–14650 (2019)
24. Zhou, Y., Yu, Z., Lan, Y., Guo, Y., Chen, R.: An anonymous transmission algorithm named ripple spreading for blockchain. In: Proceedings of the: 2020 The 2nd International Conference on Blockchain Technology, pp. 34–38 (2020)

25. Lv, Z., Qiao, L., Song, H.: Analysis of the security of internet of multimedia things. ACM Trans. Multimed. Comput. Commun. Appl. **16**(3s), 1–16 (2020)
26. Lv, Z., Qiao, L., Li, J., Song, H.: Deep-learning-enabled security issues in the Internet of Things. IEEE Internet Things J. **8**(12), 9531–9538 (2020)
27. Safarkhanlou, A., Souri, A., Norouzi, M., Sardroud, S.E.H.: Formalizing and verification of an antivirus protection service using model checking. Proc. Comput. Sci. **57**, 1324–1331 (2015)
28. Lv, Z., Chen, D., Lou, R., Song, H.: Industrial security solution for virtual reality. IEEE Internet Things J. **8**(8), 6273–6281 (2020)
29. Lv, Z., Lou, R., Li, J., Singh, A.K., Song, H.: Big data analytics for 6G-enabled massive internet of things. IEEE Internet Things J. **8**(7), 5350–5359 (2021)
30. Chai, H., Leng, S., Chen, Y., Zhang, K.: A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles. IEEE Trans. Intell. Transp. Syst. (2020)
31. Wang, P., Liu, Y.: SEMA: Secure and efficient message authentication protocol for VANETs. IEEE Syst. J. **15**(1), 846–855 (2021)
32. Lv, S., Liu, Y.: PLVA: privacy-preserving and lightweight V2I authentication protocol. IEEE Trans. Intell. Transp. Syst. (2021)
33. Sheng, H., et al.: Near-online tracking with co-occurrence constraints in blockchain-based edge computing. IEEE Internet Things J. **8**(4), 2193–2207 (2020)
34. Qu, Y., et al.: Decentralized privacy using blockchain-enabled federated learning in fog computing. IEEE Internet Things J. **7**(6), 5171–5183 (2020)
35. Bao, X., Su, C., Xiong, Y., Huang, W., Hu, Y.: Flchain: a blockchain for auditable federated learning with trust and incentive. In: 2019 5th International Conference on Big Data Computing and Communications (BIGCOM), pp. 151–159 (2019)
36. Toyoda, K., Zhao, J., Zhang, A.N.S., Mathiopoulos, P.T.: Blockchain-enabled federated learning with mechanism design. IEEE Access **8**, 219744–219756 (2020)
37. Fan, S., Zhang, H., Zeng, Y., Cai, W.: Hybrid blockchain-based resource trading system for federated learning in edge computing. IEEE Internet Things J. (2020)
38. Cui, L., et al.: CREAT: blockchain-assisted compression algorithm of federated learning for content caching in edge computing. IEEE Internet Things J. (2020)
39. Sharma, P.K., Park, J.H., Cho, K.: Blockchain and federated learning-based distributed computing defence framework for sustainable society. Sustain. Cities Soc. **59**, 102220 (2020)
40. Wu, X., Wang, Z., Zhao, J., Zhang, Y., Wu, Y.: FedBC: blockchain-based decentralized federated learning. In: 2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), pp. 217–221 (2020). https://doi.org/10.1109/ICAICA50127.2020.9182705
41. Pokhrel, S.R., Choi, J.: Federated learning with blockchain for autonomous vehicles: analysis and design challenges. IEEE Trans. Commun. **68**(8), 4734–4746 (2020)
42. Feng, L., Yang, Z., Guo, S., Qiu, X., Li, W., Yu, P.: Two-layered blockchain architecture for federated learning over mobile edge network. IEEE Netw. (2021)
43. Zhang, K., Huang, H., Guo, S., Zhou, X.: Blockchain-based participant selection for federated learning. In: International Conference on Blockchain and Trustworthy Systems, pp. 112–125 (2020)
44. Short, A.R., Leligou, H.C., Papoutsidakis, M., Theocharis, E.: Using blockchain technologies to improve security in Federated Learning Systems. In: 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 1183–1188 (2020)
45. Kumar, S., Dutta, S., Chatturvedi, S., Bhatia, M.P.S.: Strategies for enhancing training and privacy in blockchain enabled federated learning. In: 2020 IEEE Sixth International Conference on Multimedia Big Data (BigMM), pp. 333–340 (2020)
46. Qi, Y., Hossain, M.S., Nie, J., Li, X.: Privacy-preserving blockchain-based federated learning for traffic flow prediction. Futur. Gener. Comput. Syst. **117**, 328–337 (2021)
47. Zhao, Y., et al.: Privacy-preserving blockchain-based federated learning for IoT devices. IEEE Internet Things J. (2020)
48. Sun, Y., Esaki, H., Ochiai, H.: Blockchain-based federated learning against end-point adversarial data corruption. In: 2020 19th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 729–734 (2020)
49. Kim, Y.J., Hong, C.S.: Blockchain-based node-aware dynamic weighting methods for improving federated learning performance. In: 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), pp. 1–4 (2019)
50. Zhang, Z., Yang, T., Liu, Y.: SABlockFL: a blockchain-based smart agent system architecture and its application in federated learning. Int. J. Crowd Sci. (2020)
51. Lu, Y., Huang, X., Zhang, K., Maharjan, S., Zhang, Y.: Communication-efficient federated learning and permissioned blockchain for digital twin edge networks. IEEE Internet Things J. (2020)
52. Li, Z., Liu, J., Hao, J., Wang, H., Xian, M.: CrowdSFL: a secure crowd computing framework based on blockchain and federated learning. Electronics **9**(5), 773 (2020)
53. Pokhrel, S.R., Choi, J.: A decentralized federated learning approach for connected autonomous vehicles. In: 2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pp. 1–6 (2020)
54. Majeed, U., Hong, C.S.: FLchain: federated learning via MEC-enabled blockchain network. In: 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), pp. 1–4 (2019)
55. Luo, J., Li, M., Liu, X., Tian, W., Zhong, S., Shi, K.: Stabilization analysis for fuzzy systems with a switched sampled-data control. J. Franklin Inst. **357**(1), 39–58 (2020)
56. Zhang, Q., Palacharla, P., Sekiya, M., Suga, J., Katagiri, T.: A blockchain based protocol for federated learning. In: 2020 IEEE 28th International Conference on Network Protocols (ICNP), pp. 1–2 (2020)
57. Połap, D., Srivastava, G., Yu, K.: Agent architecture of an intelligent medical system based on federated learning and blockchain technology. J. Inf. Secur. Appl. **58**, 102748 (2021)
58. Halim, S.M., Khan, L., Thuraisingham, B.: Next - location prediction using federated learning on a blockchain. In: 2020 IEEE Second International Conference on Cognitive Machine Intelligence (CogMI), pp. 244–250 (2020). https://doi.org/10.1109/CogMI50398.2020.00038
59. Passerat-Palmbach, J., et al.: "Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data. In: 2020 IEEE International Conference on Blockchain (Blockchain), pp. 550–555 (2020)
60. Toyoda, K., Zhang, A.N.: Mechanism design for an incentive-aware blockchain-enabled federated learning platform. In: 2019 IEEE International Conference on Big Data (Big Data), pp. 395–403 (2019)
61. ur Rehman, M.H., Salah, K., Damiani, E., Svetinovic, D.: Towards blockchain-based reputation-aware federated learning. In: IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 183–188 (2020)

62. Weng, J., Weng, J., Zhang, J., Li, M., Zhang, Y., Luo, W.: Deepchain: auditable and privacy-preserving deep learning with blockchain-based incentive. IEEE Trans. Dependable Secur. Comput. (2019)
63. Zhang, W., et al.: Blockchain-based federated learning for device failure detection in industrial IoT. IEEE Internet Things J. (2020)
64. Qu, Y., Pokhrel, S.R., Garg, S., Gao, L., Xiang, Y.: A blockchained federated learning framework for cognitive computing in industry 4.0 networks. IEEE Trans. Ind. Informatics (2020)
65. Hua, G., Zhu, L., Wu, J., Shen, C., Zhou, L., Lin, Q.: Blockchain-based federated learning for intelligent control in heavy haul railway. IEEE Access **8**, 176830–176839 (2020)
66. Korkmaz, C., Kocas, H.E., Uysal, A., Masry, A., Ozkasap, O., Akgun, B.: Chain FL: decentralized federated machine learning via blockchain. In: 2020 Second International Conference on Blockchain Computing and Applications (BCCA), pp. 140–146 (2020)
67. Preuveneers, D., Rimmer, V., Tsingenopoulos, I., Spooren, J., Joosen, W., Ilie-Zudor, E.: Chained anomaly detection models for federated learning: an intrusion detection case study. Appl. Sci. **8**(12), 2663 (2018)
68. Martinez, I., Francis, S., Hafid, A.S.: Record and reward federated learning contributions with blockchain. In: 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 50–57 (2019)
69. Lu, Y., Huang, X., Zhang, K., Maharjan, S., Zhang, Y.: Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. IEEE Trans. Veh. Technol. **69**(4), 4298–4311 (2020). https://doi.org/10.1109/TVT.2020.2973651
70. Rahman, M.A., Hossain, M.S., Islam, M.S., Alrajeh, N.A., Muhammad, G.: Secure and provenance enhanced internet of health things framework: a blockchain managed federated learning approach. IEEE Access. **8**, 205071–205087 (2020). https://doi.org/10.1109/ACCESS.2020.3037474
71. Kang, J., Xiong, Z., Niyato, D., Zou, Y., Zhang, Y., Guizani, M.: Reliable federated learning for mobile networks. IEEE Wirel. Commun. **27**(2), 72–80 (2020)
72. Ramanan, P., Nakayama, K.: Baffle: blockchain based aggregator free federated learning. In: 2020 IEEE International Conference on Blockchain (Blockchain), pp. 72–81 (2020)
73. Otoum, S., Ridhawi, I.Al, Mouftah, H.T.: Blockchain-supported federated learning for trustworthy vehicular networks. In: GLOBECOM 2020–2020 IEEE Global Communications Conference, pp. 1–6 (2020)
74. Shayan, M., Fung, C., Yoon, C.J.M., Beschastnikh, I.: Biscotti: a blockchain system for private and secure federated learning. IEEE Trans. Parallel Distrib. Syst. (2020)
75. Zhao, C., Liu, X., Zhong, S., Shi, K., Liao, D., Zhong, Q.: Secure consensus of multi-agent systems with redundant signal and communication interference via distributed dynamic event-triggered control. ISA Trans. **112**, 89–98 (2021)
76. Zhao, C., Zhong, S., Zhong, Q., Shi, K.: Synchronization of Markovian complex networks with input mode delay and Markovian directed communication via distributed dynamic event-triggered control. Nonlinear Anal. Hybrid Syst. **36**, 100883 (2020)
77. Zhao, C., Zhong, S., Zhang, X., Zhong, Q., Shi, K.: Novel results on nonfragile sampled-data exponential synchronization for delayed complex dynamical networks. Int. J. Robust Nonlinear Control **30**(10), 4022–4042 (2020)
78. Souri, A., Rahmani, A.M., Navimipour, N.J., Rezaei, R.: A symbolic model checking approach in formal verification of distributed systems. Human-Centric Comput. Inf. Sci. (2019). https://doi.org/10.1186/s13673-019-0165-x

Dong Li received the Bachelor's degree in Measurement & Control Technology and Instrument from Tianjin University of Technology and Education in 2015, and the master degree in Instrument Engineering from China Jiliang University in 2018. During the Master's degree, her postgraduate research topic is image processing and motion control of AGV.

Zai Luo Graduated from Department of precision instruments and machinery, Hefei University of Technology, and got the PhD in Engineering. Professor of China Jiliang University, Director of Key Laboratory of testing technology and instrument for key parts of automobile brake system in mechanical industry, Standing member and Deputy Secretary-general of Measurement and Control Professional Committee of China Instrument and Control Society.

Bo Cao received the Bachelor's degree in Counter Exhibition Management Major from Henan Normal University and received the master degree in Engineering Management Major from University of Shanghai for Science and Technology. During the Master's degree, his The research problem is the digitalization system of enterprise quality management system.