Discover Artificial Intelligence

Discover

Review

Leveraging machine learning and blockchain in E-commerce and beyond: benefits, models, and application

Hrag Jebamikyous[1] · Menglu Li[1] · Yoga Suhas[1] · Rasha Kashef[1]

Received: 8 November 2022 / Accepted: 23 December 2022
Published online: 10 January 2023

Abstract
Blockchain technology (BT) allows market participants to keep track of digital transactions without central recordkeeping. The features of blockchain, including decentralization, persistency, and attack resistance, allow data security and privacy. Machine learning (ML) involves the analytical platform on a massive amount of data to provide precise decisions. Since data reliability, integration, and data security are crucial in machine learning, the emergence of blockchain technology and machine learning has become a unique, most disruptive, and trending research in the last few years, achieving comparable and precise performance. The combination of blockchain and machine learning (BT–ML) has been applied across different applications to assist decision-makers in retrieving valuable data insights while preserving privacy and integration. This paper summarizes the state-of-the-art research in combing BT and ML in e-commerce and other various applications, including healthcare, smart transportation, and the Internet of Things (IoT). The challenges and benefits of integrating machine learning and blockchain technologies are outlined in the paper. We also discuss the advantages and limitations of current algorithms in the BT–ML integration. This paper provides a roadmap for researchers to pave the way for current and future research directions in combing the BT and ML research areas.

Keywords Blockchain · Machine learning · e-commerce · IoT · Healthcare · Transportations

1 Introduction

Blockchain and machine learning are two leading research areas in the second decade of the twenty-first century. The first use of blockchain technology served as the public transaction ledger of the cryptocurrency Bitcoin [1]. Other cryptocurrencies, such as Ethereum, also use blockchain technology to record transactions. A peer-to-peer network manages the blockchain records without the need for a trusted authority or central server. Recently, the blockchain has been applied to several other areas. For example, the blockchain-based smart contract can execute and enforce the terms of an agreement between untrusted parties [2]. At the same time, it can reduce the transaction costs of reaching an agreement [3]. Blockchain is also employed in supply chain management. Walmart used the blockchain solution based on Hyperledger Fabric and built two blockchain pilots in China and the Americas to track food safety [4]. Other areas, such as financial services, energy resources, and healthcare, are those industries interested in blockchain technology [5]. While living in a digital world that produces a large amount of data, big data's manual processing is time-consuming. Machine learning technology becomes popular to deal with all kinds of data because it can learn from the historical data and improve automatically without explicit programming [6]. Machine learning algorithms mainly consist of three categories: supervised

✉ Rasha Kashef, rkashef@ryerson.ca; hjebamikyous@ryerson.ca; menglu.li@ryerson.ca; yoga.kuruba@ryerson.ca | [1]Electrical, Computer, and Biomedical Engineering Department, Toronto Metropolitan University, Toronto, Canada.

learning, unsupervised learning, and reinforcement learning. Labeled data train the supervised learning algorithm. It is widely used for classification and prediction tasks, such as pattern recognition [7] and price prediction [8]. Unsupervised learning is usually applied for anomaly detection by using cluster analysis. The application of reinforcement learning is in personalized recommendation systems [9] and gaming [10]. Blockchain technology provides a decentralized, secure, and trusted system for data storage, and machine learning can process and analyze a massive amount of data. Therefore, the idea of combining blockchain and machine learning is emerging recently to achieve secure, efficient, and sustainable real-time systems, which has been addressed in various research studies. For instance, Zhang et al. [11] integrated machine learning and blockchain in accounting, re-engineering accounting procedures, and improved accounting efficiency. Machine learning-aided blockchain is also applied in healthcare [12]. Shrivastava and Kumar [13] stated the application areas of combining blockchain and machine learning technologies in other applications, including supply chain, smart contracts, and transportation. Existing literature on combining blockchain and machine learning techniques primarily focuses on single focused industrial applications with no intensive background in other applications or the combined theory. For example, [14] mainly focus on its application of IoT security. [15] provided a survey on combining blockchain and machine learning in electronic health record systems. To address the research gap in providing a broader literature review, we provide a comprehensive overview of the theory of combining BT and ML and list the state-of-the-art techniques in selected application areas. In this paper, application research areas as healthcare, smart transportation, E-commerce, and the Internet of Things (IoT) are addressed since these fields deal with big data and security challenges. The main contributions of this paper are summarized as:

- The paper discusses the basic concepts and key features of BT and ML.
- This article illustrates the algorithms and benefits of integrating BT and ML.
- The paper outlines the practical application areas of combining BT and ML.

The rest of this paper is organized as follows: The background of blockchain and machine learning is introduced in Sects. 2 and 3, respectively; Sect. 4 presents the adoption of BT-ML integrations in various applications with challenges and limitations; Sect. 5 discusses the main key points in the literature; Sect. 6 outlines the conclusion, and Sect. 7 discusses the main challenges in the literature as well as future research directions.

2 The blockchain

Satoshi Nakamoto introduced blockchain in 2008 [16] such that each block in the chain contains several valid transactions, and the blocks are hashed and encoded into a Merkle tree [1]. Each blockchain block is linked to the previous one by storing the cryptographic hash of the last block. Each recorded transaction into the chain is unchangeable with a time-stamped. The chain is traceable, and each transaction block is linked to the previous record of the transaction. Once a new transaction is added to the chain, it cannot be erased. Since there is no central server in the network, a blockchain database is managed using a peer-to-peer network. A copy of the blockchain is available to every individual within the network. Therefore, any change to the chain, such as adding a new transaction, must be cross verified by all other network participants. Only the transaction that receives the majority of consensus from other participants can be added into the chain,otherwise, the particular transaction will be considered a fraud attack. The blockchain's invention is designed to eliminate the role of a central server or a trusted authority. The idea of decentralization has inspired many applications that are not limited to cryptocurrencies, such as healthcare and the Internet of things [5]. Zheng et al. [17] summarized four critical characteristics of blockchain, which are decentralization, persistence, anonymity, and audibility. The consensus algorithm applied in the blockchain achieves decentralization, ensuring data consistency in a distributed network. The decentralization structure eliminates the transaction cost and the performance bottlenecks caused by the trusted authority. The blockchain's persistence is reflected in the fact that transactions in the chain cannot be changed and deleted, and invalid transactions can be easily detected. Also, the participants in the blockchain do not need to reveal their real identities. They can use a generated address in the blockchain network to obtain anonymity. The characteristic of audibility is achieved by the blockchain's linked structure so that each transaction in the chain can be tracked. Gao et al. [18] mentioned the other two features of the blockchain, which are fault tolerance, and attack resistance. The blockchain network can be categorized into three types: public blockchains, private blockchains, and consortium blockchains [19]. The public blockchain is a fully decentralized system such that anyone is allowed to join the chain and participate in the consensus. Each transaction stays anonymous and transparent to every participant. Bitcoin and Ethereum are examples

of public blockchain [20]. The private blockchain is centralized such that a central organization can decide who can join the blockchain. The advantages of private blockchain are that the network's output is fast and provides privacy [21]. Hyperledger Fabric is a well-known private permissioned blockchain platform [20]. The consortium blockchain is a multi-centralized and scalable system. Multiple organizations or groups control the consortium blockchain network to preserve security and privacy. The drawback of the consortium is that any member's misconduct may compromise the entire network.

3 Machine learning

Machine learning (ML), as a subset of artificial intelligence (AI), is a computer algorithm that can accomplish tasks without being explicitly programmed [6]. Machine learning builds a mathematical model based on the historical data features, and the model gets trained and updated when exposed to new sample data. The ML model learns patterns, adjusts actions, and makes decisions automatically without human assistance. The digital world produces a grant amount of data, and it is impossible to process and analyze all kinds of data by a human. Machine learning can automatically process a large amount of data and extract features of relevant data. The main advantage of machine learning is that it keeps learning from the new training data, and it can improve itself if the algorithm produces unexpected outputs. Machine learning techniques are widely used to achieve tasks such as classification, anomaly detection, and prediction. Face/emotion recognition [22], credit card fraud detection [23], sentiment analysis [13], and marketing recommendation system [24] are the well-known applications of ML in daily life. Machine learning techniques are mainly categorized into supervised learning, unsupervised learning, and reinforcement learning [25]. Supervised learning algorithms need labeled training data to build the mathematical model. After both input data and their desired outputs are fed into the model, the model extracts the relationship between the input data and the corresponding label. Then the algorithm can determine the work for the unseen input data correctly. Supervised learning is commonly used to forecast or classify a specific outcome of interest [26]. Unlike supervised learning, the unsupervised learning algorithm uses unlabeled data to train the model. Unsupervised learning tries to find the dataset's hidden insights and structure and split the data with similarities into one category. Cluster analysis is one of the main techniques in unsupervised learning. After clustering, similar data are in the same cluster, and they are different from the data in other groups. This is an efficient way to detect abnormal data points because it does not fit into any cluster. The reinforcement learning algorithm learns by interacting with an external environment, and the machine may know its behaviours from the feedback received from the ground. Different machine learning techniques are suitable to achieve various tasks. For example, supervised and unsupervised learning algorithms are useful for data analysis, and reinforcement learning is preferred for solving decision-making problems [27]. Recently, deep understanding has become a popular approach for achieving ongoing tasks. Deep learning technology is based on artificial neural networks. The neural network contains multiple layers so that it can extract higher-level features from the inputs. The widely used architectures for deep learning are Deep Multilayer Perceptron, Convolutional Neural Network, and Recurrent Neural Network. Since its ability to provide a high-level abstraction for data modeling, deep understanding has been applied to areas as image recognition and natural language processing [28].

4 Combining blockchain and machine learning

Blockchain technology (BT) enjoys many features, including decentralization, persistence, and transparency. The blockchain can provide a new opportunity for machine learning algorithms to offer trustful decisions while preserving user's data and information. In this section, applications of combining blockchain and machine learning technologies are discussed in E-commerce, and different areas including: healthcare, smart transportation, and IoT. In addition, we provide a comparative study among various selected research applications that combine machine learning and blockchain. The comparison is based on the contribution, the machine learning category and algorithm used, the type of the adopted blockchain, validation measures, and limitations.

4.1 BT-ML in E-commerce

Blockchain technology plays an essential role in e-commerce, supply chain, and financial platforms. Lai [29] proposes an application of a blockchain in the supply chain. The work provides a solution to centralized cross-border e-commerce logistics while solving capital and information flow issues. The blockchain's decentralized property plays an essential role in dividing the process, and hence, the failure at one level in the supply chain cannot stop the whole process. The proposed solution is empirically evaluated in China's cross-border logistics supply chain. Zhang [30] explores the advantages of using blockchain in financial transactions for the agriculture domain. The author believes that blockchain can help build the most robust credit system and improvement in information asymmetric. The author has constructed and cost a reduced financial system exclusively for agriculture by improving transaction reliability and efficiency. The author evaluated the proposed solution in an agriculture enterprise and found it improved 2.3% growth in finance and reduced the risk rate. The green supply chain is a trend and necessity in the current e-commerce organizations. There is a lot of motivation from the governments as well to promote the green supply chain. In addition, [31] explore the credibility modeling of e-commerce networks using blockchain and data mining. Trusted computing base (TCB) unified management and scheduling security with response latency is analyzed. Signpost, independence is achieved.

E-commerce is an exciting domain where blockchain and machine learning would secure and automate the e-commerce domain. This section provides the related research work that uses blockchain and artificial intelligence to deal with automatic transactions focusing on contributions and limitations. In [32], financial transactions using a blockchain under an artificial neural network of deep learning are introduced. To improve the backpropagation algorithm's convergence speed, the solution studies the autoencoder and restricted Boltzmann machine to find suitable initial values. It is found that unsupervised autoencoders performed better with an accuracy of 59%. The research shows how to apply the deep learning methods in financial transactions that use a blockchain. However, this paper has not demonstrated the generalization ability of the deep learning model. Thus, the solution is restricted only to the analysis of blockchain-based transactions that have a predictive nature. A cross-border e-commerce supply chain framework using a blockchain is presented [33]. This research essentially focuses on the traceability of products and transactions in the supply chain. The framework includes a multi-chain structure model, a data management model, and a block structure model. Security factors such as information anchoring, key distribution, information encryption, and anti-counterfeiting methods are also addressed. However, the proposed method is not evaluated in a real business setup, and there is no data mining strategy explained in the paper. The standard process is familiar to logistic finance (LF), in e-commerce, that combines logistics and financial services. The LFs depend on third-party logistics (3PL) to avoid financial risks. However, PL worsens the entry threshold for other 3PL. Li et al. [34] proposes a blockchain-based logistics finance execution platform (BcLFEP) integrated with LF. The object-oriented method (OOM) is used to design workflows and resource management, and a hybrid finite-state machine-based smart contract (HFSM-SC) is implemented to synchronize the job. A case study is studied by implementing the proposed BcLFEP solution. The authors have studied the feasibility and effectiveness in terms of latency. However, the solution is not tested with different e-commerce data. Guo et al. [35] proposes a green closed-loop supply chain for online and offline sales modes. The problem involves solving nonlinear optimization,therefore, the authors used a genetic algorithm (GA and particle swarm optimization (PSO to find an approximate solution. Optimization aims to find the optimal ratio of manufacturing and remanufacturing lots. The paper has set up a theoretical foundation for green supply chain management. However, there is a gap in analyzing the factors that affect the manufacture, for example, supply–demand constraints, etc. Dalila and Abdullah [36] tackled the problem of detecting malicious transactions by building four classifiers, namely, Random Forest, Bayes Network, Naïve Bayes, and Adaboost and tested it on the Elliptic dataset, which is a graph network built from Bitcoin transactions. The dataset consists of three classes: 'licit', 'illicit', and 'unknown', and it is partially labeled,the authors applied the unsupervised K-Mean clustering algorithm to cluster the unlabeled data into two clusters, "licit" and "illicit". When combining K-Mean clustering with Random Forest, they achieved promising results. Results are evaluated using True Positive Rate (TP), True Negative Rate (TN), Precision, Recall, Receiver Operating Characteristic curve (ROC), and the precision-recall curve (PRC). Madhuparna et al. [37] performed a comparative study of various supervised learning algorithms such as Support Vector Machine (SVM), Naïve Bayes (NB), Decision Trees (DT), Multilayer Perceptron (MLP), Logistic Regression (LR), Random Forest (RF), Deep Neural Network (DNN), and Ada Boost to classify the transactions in a Blockchain network into fraudulent and legitimate transactions. Support Vector Machine, Random Forest, and Ada Boost achieved 97% accuracy. A comparative study among various selected BT-ML research in E-commerce is shown in Table 1.

Table 1 Contributions, limitations, measures, BT Types and ML methods of BT-ML in E-commerce

References	Contributions	ML category and techniques	Validation measures	Blockchain Type	Limitations
Gao and Su [32]	• Finds suitable initial values to speed up the convergence • Unsupervised autoencoders performed better	• It uses unsupervised learning algorithms • It uses autoencoders and a Restricted Boltzmann Machine	• Accuracy = 59%	• Consortium	• No demonstration of the generalization ability of the used model • the solutions are restricted to only for the analysis of blockchain-based transactions that have a predictive nature
Liu and Li [33]	• The use of the traceability of products and transactions in the supply chain	• Supervised learning • The framework includes a multi-chain structure supervised machine learning model, a data management model, and a block structure model	• Accuracy	• Public	• The proposed method is not evaluated in a real business setup • Data mining strategy is not explained in the paper
Li et al. [34]	• The blockchain-based logistics finance execution platform (BcLFEP) is integrated with logistics finance (LF) • The object-oriented method (OOM) is used to design workflows and resource management	• Unsupervised Learning • It uses a hybrid finite-state machine-based smart contract (HFSM-SC) to synchronize the job	• Transaction Throughput	• Private	• The solution is not tested with different e-commerce data
Guo et al. [35]	• The green closed-loop supply chain for online and offline sales modes • Finds an approximate solution to optimize nonlinear function	• Semi-supervised learning • It uses Genetic Algorithm and Particle Swarm Optimization	• Fitness value	• Public	• There is a gap in analyzing the factors that affect the manufacture
Dalila and Abdullah [36]	• Uses four different classifiers to classify bitcoin transactions into 'licit', 'illicit', or 'unknown' • Uses K-Means to cluster the unlabeled data	• Supervised and unsupervised learning • It uses Random Forest, Bayes Network, Naïve Bayes, and AdaBoost to classify and K-Means to cluster	• TP, TN, Precision, Recall, ROC, PRC	• Public	• They did not test the classifiers on a fully labeled dataset
Madhuparna et al. [37]	• It classifies transactions into 'legitimate' or 'fraudulent'	• Supervised learning • It uses SVM, NB, DT, MLP, LR, RF, DNN, and AdaBoost	• Accuracy = 97% (Highest accuracy)	• Public	• No deep validation analysis is provided

4.2 BT-ML in healthcare

Applying machine learning and data analysis to current medical data can help learn the disease pattern and detect potential disease in minimum time [38]. Except for its massive amount, one of the most critical characteristics of medical data is its privacy. Due to privacy concerns, all medical data are not available on any decentralized system for accessing [38]. In this case, it is hard to gather a larger dataset to train machine learning models, limiting the quality of research in the healthcare area [12]. Therefore, applying blockchain in healthcare is a big trend recently to solve security and privacy concerns. Because blockchain is a transparent and decentralized distributed system, it can provide a more secure environment for healthcare data without compromising data reliability [12]. Safer data can be used to train better machine learning models. One of the applications of combining blockchain and machine learning in healthcare is the electronic health record (EHR) system. Zheng et al. [39] proposed a blockchain-based personal health data sharing system. The system collects and encrypts personal health data from wearables and mobile devices and stores the cloud's data in an encrypted format. The Ethereum platform is used for data sharing transaction components. The system also contains a data quality inspection module based on machine learning techniques. For example, the module can distinguish sleep data from other daily activities. The machine learning-based module can also filter the noise data to control data quality. Therefore, this system allows users to control and share their health data in a secure way. The high-quality healthcare data collected by the system can also benefit the research works. The EHR system that [40] proposed involves an anonymous blockchain. This system uses a permissioned blockchain, such as Multichain to control access to the system. For example, patients' medical data and medical records from multiple healthcare institutions will be kept anonymous in the EHR system. Therefore, the communication of medical data between institutions will become more comfortable and quicker. Research institutions can easily access anonymous medical data to apply machine learning techniques for research purposes. This anonymous blockchain-based EHR ensures medical data security and provides a massive anonymous medical dataset for machine learning and data mining techniques, which benefits the healthcare industry's research work. Zhang et al. [41] also proposed a model to solve privacy concerns for applying machine learning techniques onto medical data, such as the medical image. The model [42] proposed a multi-Blockchain-based distributed machine learning architecture (MBDML). Each blockchain stores a deep learning training model so that the MBDML supports solving multi-task model training problems. Also, there are communication channels between each blockchain. The training process on one blockchain may optimize the model on its neighbour blockchain. The MBDML supports researchers to train multiple machine learning models collaboratively without sharing patient private data. The framework, Health-Chain, [43], proposed another way to apply machine learning on cross-institution data for disease diagnosis. The Health-Chain uses a decentralized Stochastic Gradient Descent algorithm on the blockchain. Chen et al. [43] have designed a gradient delay compensation method to solve the asynchronous problem in this blockchain-based learning system. Lee and Yang [44] have designed a fingernail analysis management system using machine learning and blockchain technology. The nail appearance reflects the human body's condition so that processing fingernails can be used for disease prediction. This fingernail analysis management uses the histogram of oriented gradients (HOG) and local binary pattern (LBP) to extract the biometric features. Support Vector Machines (SVM) and Deep Neural networks are used as classifiers to predict health conditions based on the nails' image. In this management system, the data of nails are stored using blockchain data so that any change or manipulation of the data will be tracked. Then, the privacy and correctness of personal data can be secured. Juneja and Marafat [45] applied blockchain and deep learning to develop a patient-specific arrhythmias classification application. Monitoring a patient with the symptoms of arrhythmias requires processing large amounts of data for a long time. The Stacked Denoising Autoencoders (SDA) are used to extract features from the electrocardiogram data and distinguish the abnormal heartbeats from the normal beats. Blockchain technology is an access control manager that verifies patient identities and controls the access required by the SDA classifier to the patient data during the retraining process. The proposed system [45] increases the classification accuracy and private data security for continuous remote systems. The research project funded by the European Commission designed a blockchain-based AI system called "CareAI" [46]. The medical data from multiple institutions, such as libraries or research centers, are stored on the blockchain, so the "CareAI" system can apply a machine learning training model to those massive data. It can diagnose within seconds whether the blood sample is infectious or not. The state-of-the-art algorithms of integrating the blockchain and machine learning in healthcare have been employed in practice, for example, the FeatureCloud platform in the EU [47]. Table 2 provides a comparative study among various selected BT-ML research in healthcare systems.

Table 2 Contributions, limitations, measures, BT Types and ML methods of BT-ML in Healthcare

References	Contributions	ML category and techniques	Validation measures	Blockchain type	Limitations
Zheng et al. [39]	• It filters the noising data to ensure high quality • The data stored on the cloud are encrypted to enhance the data security • It supports large size of datasets	• Supervised learning • It uses quality validation algorithms to classify the quality of different types of data and eliminate noises and meaningless data	• Accuracy	• Public	• Third-party cloud storage is not full-trusted • Data may be leaked on purpose by the users who can decrypt the data
Lee and Yang [44]	• The image processing using deep learning helps disease diagnosis • The blockchain technique can ensure the privacy and integrity of personal data	• Supervised learning • It uses Support Vector Machine (SVM), Random Forest Tree, and Deep Neural Networks as classifiers	• Accuracy = 70.6%	• Private	• Data may be leaked in the public blockchain ledger
Juneja and Marafat [45]	• BT is used as an access control manager; patients control their data • The retraining SDA technique increases the accuracy of arrhythmia detection	• Sunsupervised learning • It uses Stacked Denoising Autoencoders (SDA) for Arrhythmia classification	• Accuracy = 99.15% for VEB & 98.55% for SVEB	• Private	• The system faces the risk of malicious attacks
EU Science Hub Duricic [46]	• A massive medical dataset is accessed for machine learning training, building a powerful disease classification model	• Supervised learning • The prototype of the "CareAI" classification system is built for testing	• Accuracy	• Public	• The user's data in the CareAI system will be stored on the blockchain, but they may not access their data
Zhang et al. [22]	• The multi-blockchain model supports the training of multiple machine learning models collaboratively • All institutions on the chain have access to the massive shared medical dataset	• Supervised learning • It uses the medical image segmentation model Unet and the deep learning model ResNet for medical image detection and classification tasks	• Dice coefficient = (0.82, 0.62), Area Under the Curve (AUC) = (0.96, 0.95)	• Consortium	• The additional training is asynchronous, which may cause communication delay or message loss
Chen et al. [43]	• The decentralized machine learning framework allows multiple institutions to train a classification model collaboratively • The model provides a solution to address the asynchronous issues	• Supervised learning • It uses Logistic Regression and a three-layer Neural Network for medical image classification	• Accuracy	• Hybrid	• The institutions on the chain may not have access to their data

4.3 BT-ML in smart transportation

Recently, artificial intelligence-based machine learning technologies have been widely used in developing smart transportation. Traffic Data and different modes of transportation are collected and processed to provide users with more accurate information and build safer transport networks. For example, applying smart transportation technology can let users use a navigation system to find the best route based on the real-time condition, be guided to an empty parking space by a smart sign, or let the traffic management office detect and respond promptly to traffic incidents [48]. All of these applications require machine learning technologies to analyze a large amount of data. It also raises a problem: the security and privacy of data during the analyzing and sharing process. Therefore, the blockchain technique is introduced to smart transportation to overcome the safety challenges mainly. Hassija et al. [49] purposed a blockchain-based secure crowdsourcing model to predict road traffic congestion, which deploys a neural network-based smart contract onto the blockchain network. This traffic congestion prediction model is based on crowdsourcing technology, one of the most significant components used in Google Maps. However, crowdsourcing has two main disadvantages: user privacy issues and the lack of motivation for users to participate. Then an incentive mechanism is created to motivate users to share data within the network. They choose to use an Ethereum based smart contract to validate and store the users' data sharing. All the live shared data are fed in an LSTM neural network, and the historical data are used to train a feed-forward ANN model. After considering the estimation results from these two neural network models, the model can produce a highly accurate traffic jam prediction during the experiment. Hua et al. [50] combined the blockchain and machine learning to achieve intelligent control in a massive rail system. To replace manual control with smart management, the system needs an extensive dataset to train the control model. Then Hua et al. [50] proposed to use a blockchain smart contract to let distributed railway operators share their data with security and privacy. They introduced a distributed machine learning technique that optimizes the classic support vector machine (SVM) based on the historical driving data stored in the blockchain without a trusted central server. In their model, the SVM's kernel function is composed of polynomial and radial basis function kernel functions to map the dataset to a high dimension to make it linearly separable the kernel function is updated dynamically. Smart transportation involves the Internet of vehicles and data sharing within the network. The current challenges are to guarantee the shared data's security and privacy and ensure machine learning-based algorithms work properly in a distributed vehicular system [51]. To solve these challenges Chai et al. [51] proposed a hierarchical blockchain framework combined with a hierarchical federated learning algorithm. Because of multiple layers in the framework, the model can be deployed on large-scale vehicular networks with several regional characteristics [51]. Zhang et al. [41] worked on the distributed software-defined vehicular ad hoc networks (SDVs). Current distributed SDVs need multiple controllers in the traditional consensus mechanisms, which brings extra overheads and a scalability problem. Therefore, they used a permissioned blockchain system on the distributed SDV, which overcomes data sharing security issues without the massive overheads in the consensus process. They also applied a dueling deep reinforcement learning model to learn information about the distributed SDV, such as the trust features of blockchain nodes, the number of consensus nodes, and each vehicle's trust features. After training, the reinforcement learning model can determine the best policy to maximize the network [41]. Gandhi and Salvi [52] proposed to integrate machine learning and blockchain in the training process of the self-driving car. Currently, most self-driving cars are trained individually using machine learning algorithms, such as reinforcement learning. The authors proposed a concept of collective learning to accelerate the training process such that each self-driving car is connected to a shared public ledger. Each vehicle is exposed to a large training database and can share its learning experience. Table 3 provides a comparative study among various selected research applications that combined machine learning and blockchain algorithms in transportation systems.

4.4 BT-ML in IoT

We investigate the effectiveness of the blockchain and machine learning method to address the security issues in the IoT. In this section, we present the research works that explored the application of blockchain and machine learning to strengthen security in the IoT. Initially, we explore applying blockchain in IoT, as shown in Table 4. Cryptography plays an essential role in secured communication. In recent times, online trading has become a trend. Therefore, the vulnerabilities of communication are increased for different kinds of attacks. Prajapati and Chaudhari [53] proposes

Table 3 Contributions, limitations, measures, BT Types and ML methods of BT-ML in transportation

References	Contributions	ML category and techniques	Validation measures	Blockchain type	Limitations
Hassija et al. [49]	• Use a neural network technique to calculate traffic congestions' actual probability based on live and historical data • An Ethereum based smart contract is used to enhance data security • Propose an incentive model to motivate users to share data	• Supervised learning • It uses Long Short Term Memory (LSTM) and three-layer Artificial Neural Network (ANN) to predict the probability of traffic jam	• Accuracy	• Public	• Even though this model focuses on improving traffic jam prediction accuracy, it has not been tested on a large dataset
Hua et al. [50]	• Use the blockchain technique to protect user data privacy and security • The distributed machine learning framework can process extensive data efficiently and perform more accurate results with more data	• Supervised learning • It uses Support Vector Machine (SVM) to perform intelligent control in a massive haul rail system	• Accuracy = 95%	• Private	• The system faces the risk of malicious attacks
Chai et al. [51]	• The hierarchical framework supports the scalability of the proposed model • The model can protect the security of data from malicious attacks during the process of data sharing	• Supervised learning • It uses a Hierarchical Federated Learning algorithm for knowledge sharing among vehicles	• Accuracy	• Private	• The datasets used for the experiment are not related to the Internet of Vehicles
Zhang et al. [42]	• Use the blockchain technique to build the distributed SDVs and increase their scalability • The reinforcement learning technique with a reward mechanism is applied to increase the proposed framework's throughput and effectiveness	• Reinforcement learning • It uses a novel Dueling Deep Q-Learning (DDQL) to learn about the SDVs	• Accuracy and Throughput of block-SDV	• Private	• The framework is only tested by simulation without a real-world dataset
Gandhi and Salvi [52]	• Blockchain is used to enlarge the training set of machine learning algorithms • The cumbersome and repetitive training task for each self-driving car can be eliminated	• Reinforcement learning • It does not provide an algorithm	• Accuracy	• Public	• There is no experiment presented

a key block chaining method to derive the keys for advanced symmetric key encryption. The technique uses blockchain to introduce randomness into the system to enhance security as well as robustness. The National Institute of Standards and Technology statistical test suite is used to evaluate the proposed method. The popularity of the Internet of Things (IoT) motivates many companies to develop new IoT devices; thus, the data storage for the IoT devices also increases in a steady phase. Given the sensitivity of the data, it is necessary to protect the IoT data from hackers. Liu and Zhang [54] proposes an Ellipse Curve Cryptography (ECC) using blockchain, and for storage, the paper introduces data compression reconstruction to improve the information storage speed for IoT devices. The authors compare the performance of the ECC with the Digital Signature Algorithm (DSA) and Rivest-Shamir-Adelman (RSA) encryption, and the experimental result shows that ECC with the blockchain method performs 89.8% better. Sun and Zhang [55] proposes the application of the blockchain-based big data platform in smart cities. The research contributes to lowering carbon emissions and thus improves the green environment. A Blockchain is employed to build a decentralized peer-to-peer trust service system. Therefore, governments can share official documents digitally without compromising security. The proposed solution is studied empirically in a smart city at Hefei. Their research promoted healthy and sustainable development while ensuring the life of the environment. The equality and range of query operations use Searchable Symmetric Encryption (SSE). In SSE, forward privacy is not addressed. Wei et al. [56] proposes a forward secure SSE scheme. The index structure of the proposed method consists of keyed-block chains. The new solution enables us to add and delete the instances in one cycle,thus, it improves the speed. The experiment results show that secure forward SSE is 300 times faster than the previous solutions. IoT devices come with the challenge of limited storage, and it is a requirement to distribute the IoT data for future usage. However, third-party storage can pose a privacy risk. Moin et al. [57] proposed a distributed storage using blockchain. The authors have studied the strengths, weaknesses, opportunities, and threats (SWOT) of a blockchain-based IoT environment. Besides, the authors explored the application of blockchain in bitcoin transactions and security challenges. The solution includes various extra packet bits to ensure security, affecting the data store and retrieving latency. Communication Things Network (CTN) is a paradigm of a network formed by IoT devices. When a more significant number of IoT devices are added, then those devices will create complex CTN. The complex CTN is vulnerable to various attacks. Rathee et al. [58] proposes a hybrid industrial IoT framework using a blockchain. Between the sender and receiver, a blockchain layer is introduced to safeguard the transaction. The authors have tested the vulnerability of transactions to the attacks and found the proposed solution avoided 89% of various attacks compared to the usual CTN without blockchain. However, there is no evaluation of complexity analysis for churn, and there is no emphasis on handshakes when new devices are added. Qu et al. [59] proposed blockchain-based IoT device credibility verification framework includes blockchain structures (BCS) to verify any given IoT devices. The Blockchain entity is formed to share the keys securely. When a device requests a resolution of other entities, the blockchain module asks for approval from all the network devices. Based on the majority, the key will be shared by the blockchain module. The experiment shows a secured method,however, there is no evidence of congestion handling when the network grows. Table 4 provides a comparative study among various selected research applications that combined machine learning and blockchain algorithms in the Internet of Things.

Integrating blockchain technology and machine learning in an IoT environment has received great attention in the last decade. Chao et al. [60] proposed a blockchain-based collective Q-learning (CQL) approach to address the challenges of integrating machine learning (ML) with IoT, such as centralized ML training, the requirement of heavy computing power, and poor ML training efficiency. The proposed method uses lightweight IoT nodes to train parts of the learning layers and uses blockchain to share the learning results among the nodes in a verifiable manner. The winner IoT node has a minimum reduced percentage of the learning loss function, known as the Proof of Learning (PoL) consensus protocol. The experimental results have proven the proposed method's superiority. The delay-tolerant data plays a crucial role in the machine-to-machine (M2M) communication-based IoT. It prioritizes the stability and security of data transmission and powerful data computing, caching, and processing. Meng et al. [61] proposed a dueling deep Q-network (DQN) based join optimization framework for security, caching, and computation of delay-tolerant data in M2M communication networks. DQN is used to achieve maximum system rewards, such as better data interaction security, efficient data processing, and lower network costs, by selecting the optimal Blockchain systems, computing, and caching servers. Muhammad et al. [62] proposed a distributed machine learning-based intrusion detection (ID) system in the Internet of Things (IoT) using Blockchain technology. Spectral partitioning is used to divide the IoT network into multiple autonomous systems to perform traffic monitoring for intrusion detection in a distributed manner. The intrusion detection system is based on the SVM algorithm trained on prominent IoT datasets and evaluated by simulation. To overcome the challenges such as privacy, centralization, and scalability that slow the adoption of smart cities Kumar et al. [63],

Table 4 Applications of the blockchain in IoT

References	Contributions	Blockchain type	Limitations
Prajapati and Chaudhari [53]	• The paper proposes a key block chaining to derive symmetric key encryption • The technique uses blockchain to introduce randomness into the system to enhance the security as well as the robustness	• Private	• The proposed method is resource-intensive • The security level depends on the protocol chosen
Liu and Zhang [54]	• The paper proposes an Ellipse Curve Cryptography (ECC) using blockchain • The paper introduces data compression reconstruction to improve the information storage speed for IoT devices • The results show that ECC performs 89.8%	• Public	• This method provides secure storage, but it adds additional keys to security • Increasing data allows the overhead header to grow exponentially
Sun and Zhang [55]	• The paper proposes the application of blockchain-based big data in smart cities • The research contributes to lowering carbon emissions and the green environment • The research's fundamental motive is to promote healthy and sustainable development	• Public, Private, Alliance	• There is no accurate information about data and performance evaluation
Wei et al. [56]	• The paper proposes a secure SSE scheme • The new solution enables us to add and delete the instances in one cycle; thus, it improves the speed • The experiment results show that secure forward SSE is 300 times faster than the previous solutions	• Private	• There is no explanation about handling orphan keyed-block chains
Moin et al. [57]	• A distributed storage using blockchain is proposed • The authors provided the strengths, weaknesses, opportunities, and threats of a blockchain-based IoT environment	• Public	• The solution includes various extra packet bits to ensure security, affecting the data store and retrieving latency
Rathee et al. [58]	• A hybrid industrial IoT framework using blockchain is provided • Between the sender and receiver, a blockchain layer safeguards the transaction • The authors have tested the vulnerability of transactions to the attacks and found the proposed solution avoided 89% of various attacks compared to CTN	• Public	• There is no evaluation of complexity analysis for churn, and there is no emphasis on handshakes when new devices are added
Qu et al. [59]	• The paper presents a framework that includes blockchain structures (BCS) to verify any given IoT devices	• Private	• There is no evidence of congestion handling when the network grows to billions or more paths

presented a Privacy-Preserving and Secure Framework (PPSF) for IoT-based smart cities. The proposed method is based on two mechanisms: a two-level privacy scheme and an intrusion detection (ID) system. The two-level privacy scheme consists of a Blockchain module designed for the IoT data transmission in a secure manner and Principle Component Analysis (PCA) technique to transform the raw IoT data into a new shape. The intrusion detection system is based on the Gradient Boosting Anomaly Detector (GBAD) trained and evaluated on two IoT network datasets, ToN-IoT and BoT-IoT. Their experimental results have proven the superiority of the proposed method over recent approaches in Blockchain and Non-Blockchain systems. We compare the BT-ML work in IoT in terms of contributions, limitations, validation measures, ML category and methods, and the Blockchain type, as shown in Table 5.

5 Discussion

Combining Blockchain with machine learning has shown a significant impact in different application domains and industries. For example, machine learning techniques bring benefits to the medical area as healthcare usually involves a large amount of data. Processing medical data by humans will be time-consuming. Simultaneously keeping the patient's health records and information in a secure environment is a crucial task. Thus, combining blockchain and machine learning technologies in healthcare solves both security and privacy problem and provides an automated solution to analyze the merging medical data from different sources. In healthcare applications, various blockchains are used, including public and private. We have observed a research gap in using hybrid and consortium BT types in healthcare-related work. We have also found that most research papers use supervised learning related to the disease diagnosis and prediction of healthcare-related problems. In transportation, blockchain technology plays a significant role in protecting data security and privacy during data sharing. With the support of blockchain, machine learning techniques can be performed in a distributed way. Combining Blockchain with machine learning in the smart transportation domain solve the privacy and security problems, the accurate prediction of traffic congestion, as well as increasing the scalability of the machine learning models used in the autonomous vehicles; especially that there is an extensive shared training database under a variety of scenarios. Most of the literature uses public and private blockchain. Related work in Bt-ML in smart transportation uses supervised and reinforcement learning algorithms, such as Long Short Term Memory (LSTM), Artificial Neural Network (ANN), Support Vector Machine (SVM), and Dueling Deep Q-Learning (DDQL) to perform various tasks. We have also observed a gap in using unsupervised learning in most intelligent transportation research work that combines BT and ML. Combining Blockchain with machine learning in the e-commerce industry provides alternative solutions to privacy and security challenges. Combined Bt-ML optimizes manufacturing in supply chain management. Recent related work shows that the state-of-the-art supervised, unsupervised, and semi-supervised learning algorithms are used to cluster the unlabeled data, classify bitcoin transactions into fraudulent or legitimate, and predict financial trends. Most of the blockchain types that are used in e-commerce related research use public BT. We have also observed that there is a limitation in most of the BT-ML related work, including the proper validation in the combined models. Finally, in the era of IoT, adopting blockchain helps organizations and enterprises to achieve a sustainable level of privacy-aware solutions. Various BT-ML studies in IoT have used supervised, unsupervised, and semi-supervised learning algorithms such as Support Vector Machine, Principal Component Analysis, and Deep Q-learning to improve data interaction security and privacy-preserving for IoT-based intelligent cities and intrusion detection IoT networks. We have observed that hybrid and consortium BT types are not widely used in IoT-related work. Overall, we have also observed that the current BT-ML integrated systems focus on data security and performance accuracy, with prohibited computational complexity and additional overhead.

6 Conclusion

There is a need to investigate the aggregation of the blockchain technology with machine learning techniques due to the unique features of the blockchain, such as decentralization, persistence, and transparency, and the smart process and decisions obtained using machine learning algorithms. This paper provides a comprehensive survey that explains the key concepts and features of blockchain and machine learning technologies and reviews the state-of-the-art applications of combining the two technologies in E-commerce and other applications including the emerging IoT. One of the common characteristics of these four selected areas is that they involve large numbers of partners and big data in the system. This paper discusses the significant advantages in each application area, outlines the benefits of integrating

Table 5 Contributions, limitations, measures, BT types and ML methods of BT-ML in IoT

References	Contributions	ML category and techniques	Validation measures	Blockchain type	Limitations
Chao et al. [60]	• A blockchain-based collective Q-learning approach in IoT applications • Tackled the safety and heavy computing requirements of integrating ML in IoT	• Reinforcement learning • It uses a Q-learning algorithm	• Minimum reduced percentage of learning loss function	• Public	• They did not test the proposed method on more than one scenario
Meng et al. [61]	• A Dueling Deep Q-network (DQN) is used as an optimization framework • The proposed method results in better security of data interaction, lower network costs, and more efficient data processing	• Reinforcement learning • It uses the Deep Q-Network algorithm	• System Rewards	• Private	• The proposed method was not evaluated in a real-world scenario
Muhammad et al. [62]	• The paper proposes a distributed machine learning-based intrusion detection system in IoT using Blockchain	• Supervised learning algorithm • It uses the SVM algorithm	• Accuracy, Precision, Recall, ROC curve, AUC, F1 score	• Public	• The proposed solution was not compared with other machine learning algorithms
Kumar et al. [63]	• Privacy-Preserving and Secure Framework using Blockchain-based Machine Learning for IoT based smart cities is presented	• supervised and unsupervised learning • It uses PCA and GBAD	• Precision, Recall, F1 score, False Alarm Rate (FAR)	• Public	• The efficiency of the proposed method was not assessed

machine learning and blockchain, and addresses limitations. In summary, as machine learning has a strong ability to process big data and the reliable feature of blockchain to store data, combining these two technologies can access data more securely and privately to produce more secure classification or prediction decisions.

7 Challenges and future directions

Challenges in combining Blockchain and machine Learning include the accuracy/sustainability/scalability of the ML model and the security/suitability/memory/infrastructure of the Blockchain. With a large amount of Big data available in various domains, the accuracy, sustainability, and scalability of the adopted machine learning model play a crucial role in the entire decision-making process. Thus, ensuring proper choice of the invoked ML methods and analyzing the vulnerability and scalability level of these methods are mandatory tasks to ensure sustainable and efficient decision-making intelligent systems. The most common security issue in Blockchains consists of the possible compromise of the consensus protocol due to attacks. The mining power of a few nodes will have the power to control which blocks should be added to the network. This issue is present in public blockchains only. It is essential to understand the blockchain architecture before using it in any application because the blockchain architecture is designed for applications with untrusted data sources. If optimum performance is required, then a centralized database is a better option. As new blocks are added to the network, the size of the blockchain keeps growing, which creates significant memory constraints on the devices. The storage of irrelevant or useless data wastes substantial computational and memory resources. Hence the storage management is a critical issue in most blockchains. It is crucial to enhance the infrastructure and build the hardware and network infrastructure specific for blockchains, such as decentralized storage, network administration, communication protocol, and network administration, to enhance the performance of many blockchain-based applications. Future directions include the investigation of the relationship between the network size and the communication/computational overhead, the relationship of the accuracy of the adopted ML algorithm based on the type of the used blockchain, and the impact of attacks on the network as related to the sustainability of the adopted ML model. In addition, expanding the combined BT–ML work to hybrid and consortium blockchain worths future investigations.

Acknowledgements Not applicable.

Author contributions All authors contributed equally. All authors read and approve the final manuscript.

Funding This project is funded by Toronto Metropolitan Univeristy, Start-up Fund.

Data availability and Code availability Not applicable: no datasets used in this survey paper.

Declarations

Ethics approval and consent to participate Not applicable: no human or animals are used in this study.

Competing interests Authors declare no conflict of interest.

References

1. The Economist. Blockchains: The great chain of being sure about things. The Economist. Archived from the original on 3 July 2016. Accessed 18 June 2016.
2. Alharby M, Moorsel A. Blockchain Based Smart Contracts: A Systematic Mapping Study. Computer Sci Inform Technol. 2017a;45:5.
3. Shermin V. Disrupting governance with blockchains and smart contracts. Strateg Chang. 2017;26(5):499–509.
4. AlDarwish M. Machine Learning. ML. http://www.contrib.andrew.cmu.edu/~mndarwis/ML.html.

5. Abbas QE, Sung-Bong J. A Survey of Blockchain and Its Applications. In: 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), 2019.
6. Samuel AL. Some studies in machine learning using the game of checkers. IBM J Res Dev. 1959;3(3):210–29.
7. Kulkarni SR, Rajendran B. Spiking neural networks for handwritten digit recognition—Supervised learning and network optimization. Neural Netw. 2018;103:118–27.
8. Hu Y, Ni J, Wen L. A hybrid deep learning approach by integrating LSTM-ANN networks with GARCH model for copper price volatility prediction. Physica A. 2020;557: 124907.
9. Gao R, Xia H, Li J, Liu D, Chen S, Chun G. DRCGR: Deep Reinforcement Learning Framework Incorporating CNN and GAN-Based for Interactive Recommendation. In: 2019 IEEE International Conference on Data Mining (ICDM), 2019.
10. Silver D, Huang A, Maddison CJ, Guez A, Sifre L, Driessche GVD, Schrittwieser J, Antonoglou I, Panneershelvam V, Lanctot M, Dieleman S, Grewe D, Nham J, Kalchbrenner N, Sutskever I, Lillicrap T, Leach M, Kavukcuoglu K, Graepel T, Hassabis D. Mastering the game of Go with deep neural networks and tree search. Nature. 2016;529(7587):484–9.
11. Zhang J, Yin Z, Chen P, Nichele S. Emotion recognition using multi-modal data and machine learning techniques: a tutorial and review. Inform Fusion. 2020a;59:103–26.
12. Vyas S, Gupta M, Yadav R. Converging blockchain and machine learning for healthcare. In: 2019 Amity international conference on artificial intelligence (AICAI); 2019.
13. Shrivastava V, Kumar S. Utilizing block chain technology in various application areas of machine learning. In: 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon); 2019.
14. Mohanta BK, Jena D, Satapathy U, Patnaik S. Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things. 2020;11: 100227.
15. Shi S, He D, Li L, Kumar N, Khan MK, Choo K-KR. Applications of blockchain in ensuring the security and privacy of electronic health record systems: a survey. Comput Secur. 2020;97: 101966.
16. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System (PDF). Archived (PDF) from the original on 20 March 2014. 2008; bitcoin.org.
17. Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE international congress on Big Data (BigData Congress); 2017.
18. Gao W, Hatcher W, Yu W. A Survey of Blockchain: Techniques, Applications, and Challenges. In: 2018a 27th International Conference on Computer Communication and Networks (ICCCN). 2018a.
19. Ali O, Ally M, Clutterbuck A, Dwivedi Y. The state of play of blockchain technology in the financial services sector: A systematic literature review. Int J Inf Manag. 2020;54:102199.
20. Yang R, Wakefield R, Lyu S, Jayasuriya S, Han F, Yi X, Yang X, Amarasinghe G, Chen S. Public and private blockchain in construction business process and information integration. Autom Constr. 2020;118: 103276.
21. Abu-Elezz I, Hassan A, Nazeemudeen A, Househ M, Abd-Alrazaq A. The benefits and threats of blockchain technology in healthcare: A scoping review. Int J Med Informatics. 2020;142:104246.
22. Zhang Y, Xiong F, Xie Y, Fan X, Gu H. The impact of artificial intelligence and blockchain on the accounting profession. IEEE Access. 2020b;8:110461–77.
23. Adityasundar N, SaiAbhigna T, Lakshman B, Phaneendra D, MohanKumar N. Credit card fraud detection using machine learning classification algorithms over highly imbalanced data. J Sci Technol. 2020;05(03):138–46.
24. Fernández-García AJ, Iribarne L, Corral A, Criado J, Wang JZ. A recommender system for component-based applications using machine learning techniques. Knowl-Based Syst. 2019;164:68–84.
25. Athmaja S, Hanumanthappa M, Kavitha V. A survey of machine learning algorithms for big data analytics. In: 2017b International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2017b.
26. Jiang T, Gradus JL, Rosellini AJ. Supervised machine learning: a brief primer. Behav Ther. 2020;51(5):675–87.
27. Qiu J, Wu Q, Ding G, Xu Y, Feng S. Erratum to: A survey of machine learning for big data processing. EURASIP J Adv Signal Processing. 2016;1:2016.
28. Ozbayoglu AM, Gudelek MU, Sezer OB. Deep learning for financial applications : a survey. Appl Soft Comput. 2020;93: 106384.
29. Lai J. Research on Cross-Border E-Commerce Logistics Supply Under Block Chain. In: 2019 International Conference on Computer Network, Electronic and Automation (ICCNEA). 2019.
30. Zhang D. The innovation research of contract farming financing mode under the block chain technology. J Clean Prod. 2020;270: 122194.
31. Jiang L, Dong K. Credibility Modelling of E-commerce Networks Based on Block-chain and Massive Data Mining. In: 2020 Fourth International Conference on Inventive Systems and Control (ICISC), 2020.
32. Gao W, Su C. Analysis on blockchain financial transaction under artificial neural network of deep learning. J Comput Appl Math. 2020;380: 112991.
33. Liu Z, Li Z. A blockchain-based framework of cross-border e-commerce supply chain. Int J Inf Manage. 2020;52: 102059.
34. Li M, Shao S, Ye Q, Xu G, Huang GQ. Blockchain-enabled logistics finance execution platform for capital-constrained E-commerce retail. Robotics Comput Integr Manuf. 2020;65: 101962.
35. Guo J, Yu H, Gen M. Research on green closed-loop supply chain with the consideration of double subsidy in e-commerce environment. Comput Ind Eng. 2020;149: 106779.
36. Dalila B, Abdullah AKA. Enhancing the security of financial transactions in Blockchain by using machine learning techniques: towards a sophisticated security tool for banking and finance. First Int Conf Smart Syst Emerg Technol (SMARTTECH). 2020;2020:110–5.
37. Madhuparna B, Tulasi SSC, Bhawana R. Comparative study of machine learning algorithms for fraud detection in blockchain. In: 2021 5th international conference on computing methodologies and communication (ICCMC); 2021, p. 539–41.
38. Pardakhe NV, Deshmukh VM. Machine learning and blockchain techniques used in healthcare system. In: 2019 IEEE Pune Section International Conference (PuneCon), 2019.

39. Zheng X, Mukkamala RR, Vatrapu R, Ordieres-Mere J. Blockchain-based personal health data sharing system using cloud storage. In: 2018c IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom); 2018c.
40. Hanley M, Tewari H. Managing Lifetime Healthcare Data on the Blockchain. In: 2018b IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 2018b.
41. Zhang W, Wang Q, Li M. Medical image collaborative training based on multi-blockchain. In: 2019b IEEE International conference on bioinformatics and biomedicine (BIBM); 2019b.
42. Zhang D, Yu FR, Yang R. Blockchain-based distributed software-defined vehicular networks: a dueling deep ${Q}$ -learning approach. IEEE Trans Cogn Commun Netw. 2019a;5(4):1086–100.
43. Chen X, Wang X, Yang K. Asynchronous Blockchain-based Privacy-preserving Training Framework for Disease Diagnosis. In: 2019 IEEE International Conference on Big Data (Big Data). 2019.
44. Lee SH, Yang CS. Fingernail analysis management system using microscopy sensor and blockchain technology. Int J Distrib Sens Netw. 2018;14(3):155014771876704.
45. Juneja A, Marefat M. Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification. In: 2018 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI), 2018.
46. Duricic A. CareAI: A Solution for African Healthcare?. Masters of Media. 2018. http://mastersofmedia.hum.uva.nl/blog/author/anjaduricic/. Accessed 1 Sept 2020.
47. FeatureCloud. Revolutionising CloudCommunication. FeatureCloud, 2020. https://featurecloud.eu/. Accessed 01 Nov 2020.
48. Tomás JP, Keysight F, Blackman J. What is smart transportation?. Enterprise IoT Insights. https://enterpriseiotinsights.com/20170626/transportation/20170625transportationwhat-smart-transportation-tag23-tag99. Accessed 27 Sept 2020.
49. Hassija V, Gupta V, Garg S, Chamola V. Traffic Jam Probability Estimation Based on Blockchain and Deep Neural Networks. In: IEEE Transactions on Intelligent Transportation Systems, pp. 1–10, 2020.
50. Hua G, Zhu L, Wu J, Shen C, Zhou L, Lin Q. Blockchain-Based Federated Learning for Intelligent Control in Heavy Haul Railway. In: IEEE Access. p. 1–1, 2020.
51. Chai H, Leng S, Chen Y, Zhang K. A Hierarchical Blockchain-Enabled Federated Learning Algorithm for Knowledge Sharing in Internet of Vehicles. In: IEEE Transactions on Intelligent Transportation Systems. p. 1–12. 2020.
52. Gandhi GM, Salvi. Artificial Intelligence Integrated Blockchain For Training Autonomous Cars. In: 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM). 2019.
53. Prajapati P, Chaudhari K. KBC: Multiple key generation using key block chaining. Procedia Computer Science. 2020;167:1960–9.
54. Liu Y, Zhang S. Information security and storage of Internet of Things based on block chains. Futur Gener Comput Syst. 2020;106:296–303.
55. Sun M, Zhang J. Research on the application of block chain big data platform in the construction of new smart city for low carbon emission and green environment. Comput Commun. 2020;149:332–42.
56. Wei Y, Lv S, Guo X, Liu Z, Huang Y, Li B. FSSE: Forward secure searchable encryption with keyed-block chains. Inf Sci. 2019;500:113–26.
57. Moin S, Karim A, Safdar Z, Safdar K, Ahmed E, Imran M. Securing IoTs in distributed blockchain: analysis, requirements and open issues. Futur Gener Comput Syst. 2019;100:325–43.
58. Rathee G, Sharma A, Kumar R, Iqbal R. A secure communicating things network framework for industrial IoT using blockchain technology. Ad Hoc Netw. 2019;94: 101933.
59. Qu C, Tao M, Zhang J, Hong X, Yuan R. Blockchain based credibility verification method for IoT Entities. Security Commun Netw. 2018;2018:1–11.
60. Chao Q, Wang X, Yao H, Du J, Yu F, Guo S. Networking Integrated Cloud-Edge-End in IoT: A Blockchain-Assisted Collective Q-Learning Approach. IEEE Internet of Things J. 2020;8:9.
61. Meng L, Richard Y, Pengbo S, Wenjun W, Yanhua Z. Resource optimization for delay-tolerant data in blockchain-enabled iot with edge computing: a deep reinforcement learning approach. IEEE Internet Things J. 2020;7(10):9399–412.
62. Muhammad AC, Hassan KQ, Chrysostomos C, Marios L. Utilizing blockchain for distributed machine learning based intrusion detection in internet of things. In: 2020 16th international conference on distributed computing in sensor systems (DCOSS), 2020, p. 429–35.
63. Kumar P, Kumar R, Srivastava G, Gupta G, Tripathi R, Gadekallu T, Xiong N. PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven Smart Cities. IEEE Trans Netw Sci Eng. 2021;34:56.