

Blockchain for AI: A Disruptive Integration

Ruijiao Tian
School of Software
Shandong University

Jinan, China
202015210@mail.sdu.edu.cn

Lanju Kong*
School of Software
Shandong University
Dareway Software Co., Ltd
Jinan, China
klj@sdu.edu.cn

Xinping Min
School of Software
Shandong University
Jinan, China
minxinping0105@126.com

Yunhao Qu
School of Software
Shandong University
Jinan, China
y.h.qu1@nefu.edu.cn

Abstract—Artificial intelligence (AI) and blockchain are two of the most disruptive technologies in recent years. Blockchain is widely regarded as a trust machine because of its decentralization, non-tampering, anonymity and traceability. AI provides machines with cognitive functions, including learning, reasoning, and adaptation based on the collected data, which enables human-like machines possess intelligence and decision-making capabilities. Also, both technologies are data-driven, and thus there are rapidly growing interests in integrating them for trustworthy artificial intelligence and intelligent blockchain. In this paper, we review the related research on the integration of AI and blockchain, mainly analyzing how blockchain technology can improve AI from five aspects and pointing out the future research direction of these two technologies. And our research shows that blockchain can drive various components of AI including data, algorithms, and computational power to higher levels.

Keywords—Blockchain, Smart contract, Artificial intelligence, Federated Learning, Machine learning,

I. INTRODUCTION

Artificial intelligence(AI), a promising technological solution for big data analysis, enables automatic identification and intelligent decision-making with the help of many task-oriented techniques. A large number of intelligent applications have emerged in many industries such as medical and health, intelligent transportation and financial management. However, over 70 years of research and development, the deployed complex AI systems are starting to face complicated external issues ranging from security to ethics, especially susceptibility to biases and adversarial attacks [1].

When an AI system correctly makes decisions on a subset of data, but performs poorly in the entire population, the susceptibility to biases increases. Although these biases are statistical in nature, they may lead to social biases and harm the interests of a certain community. On the other hand, when some malicious actors try to manipulate data, leading to wrong decisions (such as misclassification or bad clusters), an adversarial attack on the AI system will occur. There are more and more adversarial attacks against machine learning, especially deep neural networks. These attacks come in different flavors such as data set poisoning, adversarial examples, and side-channel attacks [2]. Malicious participants may manipulate the environment around the system or input samples to cause random or targeted misclassifications. The demand for resisting potential biases and adversarial attacks is rapidly increasing.

On the other hand, blockchain has gradually evolved from an encrypted digital currency to a trusted Blockchain as a Service (BaaS) platform in recent years. Various industries are enthusiastic about the blockchain, and actively explore the blockchain-plus industry application innovation model. As a distributed, non-tamperable and verifiable transaction ledger, the blockchain guarantees the security of operations through transaction records and decentralized consensus in an untrusted decentralized environment, provides access to data, transactions and logs in a secure and trusted manner, and builds a trust foundation between multiple agents in a low-cost manner without a trusted third party.

Blockchain technology can largely meet the requirements of trusted AI for resilience against biases and adversarial attacks. The natural decentralized and distributed trustworthiness of blockchain provides new ideas for designing machine Learning algorithms, and interdisciplinary research combining the two technologies will be full of promise. In order to assist researchers find out the latest research results, we summarize existing efforts and discuss the promising future of their integration. The main contributions of this paper is summarized as follows.

- We give an overview of blockchain and AI, and provide an in-depth analysis of what blockchain can offer AI systems, showing that the two technologies can efficiently collaborate.
- We have categorized and summarized the research efforts related to integrating blockchain with AI systems from five perspectives.
- We outline open research challenges of adopting blockchain in future AI applications.

The rest of the paper is organized as follows. Section II discusses the background of blockchain and AI technologies. Section III presents the detailed analysis of how blockchain helps in transforming AI techniques in five aspects. A discussion of further research directions is in Section IV. Section V concludes the paper.

II. BACKGROUND

A. Blockchain and Artificial Intelligence Overview

Since Satoshi Nakamoto [3] published the Bitcoin white paper in 2008, blockchain as the underlying technology of

Bitcoin has received extensive attention and discussion. In a narrow sense, blockchain can be seen as an open, distributed digital ledger, which efficiently records transactions between parties in a verifiable and tamper-proof manner. However, in a broader sense, blockchain can be regarded as a underlying framework. We consider only the high-level representation of the framework, which can be divided into data layer, network layer, and application layer [4].

At the data layer, data structures and algorithms such as hashes, Merkle trees and signatures define the basic units of the blockchain. From a data structure perspective, each block contains a set of data records or transactions, a hash of the previous block and a timestamp, which make it difficult to modify the records. The network layer generally refers to the entire blockchain interaction environment, including the distributed peer-to-peer network protocols and the consensus mechanism. The application layer provides a variety of applications. The most common application is digital cryptocurrency represented by Bitcoin [3] while another widespread application is smart contract [5], which relies on the decentralized consensus mechanism of blockchain, allowing mutually untrusted users to complete data exchange or transaction without any third-party trusted authorization and supervision.

AI is showing transformative impact in many fields and industries, and its recent renaissance has benefited from breakthroughs in machine learning. The explosion of available data and ever-increasing computing power promote the training of machine learning algorithms more effective. As a branch of AI, machine learning mainly studies data-driven prediction model that automatically uses sample data to learn a mathematical model and uses this mathematical model to make predictions on unknown data. Data training often adopts centralized learning, distributed learning or federated learning [6]. Distributed machine learning is currently one of the most popular research areas. Especially with the rise of big data, the distributed deployment of computational models to multiple machines for simultaneous computation becomes a necessary solution. Federated learning is a special distributed machine learning framework. It collaborates with thousands of participants for iterative training of a specific machine learning model in a distributed manner.

However, with the development of network attack and defense techniques, all phases of machine learning (data collection, model training, model prediction) are vulnerable to attackers. Attackers can generate more autonomous malware and more deceptive exploits by machine learning or obtain private information about training data, which has stimulated the interest of related researchers in exploring secure and interpretable improvements in machine learning.

B. Blockchain for AI

Derived from the components of the data and network layers outlined above, blockchain provides several features that could be the key to enhancing AI [7].

Decentralized: blockchain adopts a purely mathematical approach to establish trust relationships among distributed nodes, forming a decentralized and trusted distributed system. All

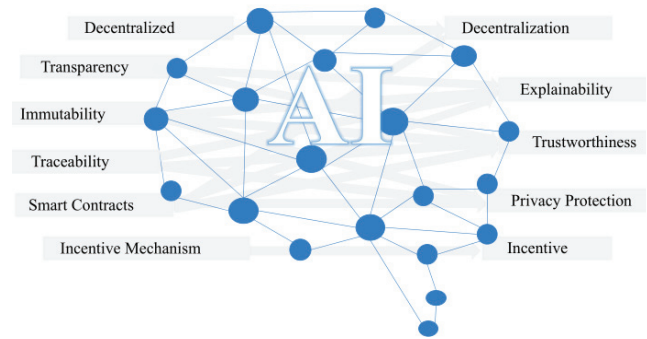


Fig. 1. Blockchain for AI

activities are done based on the distributed network, which achieve complete decentralization.

Transparency: All transactions are stored in a publicly auditable, append-only and transparent ledger. Ledger status, transaction and function call logs are stored in a secure, tamper-proof, decentralized manner which is accessible to all stakeholders involved.

Immutability: The blockchain ledger consists of timestamped blocks, each of which contains a set of transactions and references the hash of the block before it. Each block is protected by a cryptographic hash and any change in one of these blocks will invalidate the entire blockchain.

Traceability: Each participating node or user in the blockchain must cryptographically sign each transaction or function and each signed item must be verified by the mining node of blockchain.

Smart Contracts: Smart Contracts are codes that manage the interactions between different participants, allowing the execution of business logic in an automated, trusted and decentralized manner.

Incentive Mechanism: A perfect system lies firstly in its incentives and secondly in its constraints. In Bitcoin [3], a new block is formed after the mining is successful, and the miner who is recognized as the winner receives tokens. This incentive mechanism is conducive to building a complete ecosystem and provides guarantees for system security.

The marriage of these two technologies could complement each other to revolutionize the next digital generation [8]. As shown in Fig.1, due to the characteristics of the blockchain, we think, it will bring decentralization, explainability, trustworthiness, incentive and privacy to AI.

III. INTEGRATING BLOCKCHAIN WITH AI SYSTEMS

A. Decentralization

Algorithms is the key to AI, but most machine learning and deep learning algorithms are based on huge data sets and centralized training models, which are vulnerable to attacks or malicious operations, with the consequence of untrustworthy models and wasted computing power. As an emerging machine learning technology, Federated Learning realizes the iterative training in a distributed manner with multiple participants. However, due to the existence of the central server, the essence of its centralization has not changed. It has been noted that these

central server-based learning frameworks suffer from the following fundamental problems [9]:

Single-point-of-attack: The central server can easily become an obvious target of attack. If the central server is damaged, the entire network is at risk of being compromised.

Party join and departure: Participants cannot join or leave the network freely at any time. Each time any party joins or leaves the network for a short time, the process is interrupted and the server needs to handle network recovery.

Lack of fairness: The existing framework is based on the assumption that all parties contribute equally. In fact, one party may contribute more high-quality data, while the other party may contribute nothing. However, at the end of the training, all parties are allowed to obtain the same global model.

The outstanding advantage of blockchain technology lies in its decentralized design. Through the encryption algorithms, timestamps, tree structures, consensus mechanisms, and reward mechanisms, it realizes decentralized point-to-point transactions in a distributed network, which solves the problems of poor reliability, low security, high cost, and low efficiency in the current centralized model. At present, a lot of research work have taken the blockchain as the underlying infrastructure of federated learning.

For the problem of possible malicious attacks on the central server of federal learning, the work of [10] proposes a blockchain-based decentralized federated learning framework. The framework uses the blockchain for global and local model storage, and smart contracts replace the central server to perform the aggregation of local model to achieve decentralization. The committee consensus mechanism is designed, and the role of the committee members is to validate the local model updates and select the best to save in the blockchain. As a result, malicious updates can be ignored. Based on the consortium blockchain, nodes with permissions can enter and exit at any time without affecting the model training, and nodes with historical malicious behavior will no longer be allowed to join, which effectively reduce malicious attacks. In order to effectively ensure the notarization of the consensus process, committee members are replaced in each round.

Lyu et al. [11] propose replacing the centralized server with a distributed collaboration framework to parallelize the calculation between all parties and implement a completely decentralized privacy protection deep learning framework, called DPPDL, which records all operations as transactions in blockchain, including uploading and downloading artificial samples or gradients. Similarly, a decentralized federal learning method called chainFL is realized in [12].

Also, the blockchain-based decentralized storage infrastructure helps to achieve encrypted and secure data storage, which we will discuss in part of trustworthy data. In summary, the introduction of blockchain enables distributed machine learning to be fully decentralized, and the operations of central server such as update aggregation, client selection, and global model maintenance are all replaced by blockchain. A series of problems such as the bandwidth requirements of the communication between server and clients, the stability of the server, and the collection of private data from clients by server

have been effectively solved. Of course, due to the limitations of the blockchain, mainly in terms of slow block-out speed and long confirmation time, further research is still going on.

B. Explainability

For AI, the lack of explanation of decisions made by algorithms is a major drawback. For example, deep learning does not provide control or reasoning about its internal processes or outputs, which represents a black-box solution that is more susceptible to biases and adversarial attacks[13].

A promising solution for black-box AI is to move trust from a single predictive system to a set of distributed predictors that provide predictions and explanations. For example, the systems based on smart contracts of blockchain can make credible and accurate decision results which are verified and validated by all mining nodes and cannot be tampered with once they are written to the chain, and all entities can track and verify them.

Sarpatwar et al. [14] describe how to use blockchain to track training models to obtain more credible AI. Specifically, they use the blockchain to track the source and history of the data, learning models, metadata of all related activities, and operations between different participants. The blockchain data include the history of model creation, the data hash of the model and the potential contributions of various participants. Then, the model be passed to different groups or other organizations in the same groups, and each organization can read the historical source of the model from the blockchain and choose to retrain the model with additional data. Organizations can also read the results of model iterations completed by different teams from the blockchain to see if previous training data has adversely affected the results.

Peng et al. [15] propose a verifiable and auditable federated learning framework VFChain based on the blockchain system. Specifically, the committee summarizes the updated model and records verifiable evidence on the blockchain to provide explainability. To improve the efficiency of the search for verifiable evidence and to support secure rotation of the committee, the authors also design a new authentication data structure for the blockchain. Majeed et al. [16] design a federated learning architecture FLchain which provides a separate channel for each learning task. During the training process, the local model parameters for each iteration will be packaged into blocks as transactions and stored on the channel-specific ledger. The coefficients of the global model are updated synchronously with the generation of blocks in the FLchain and stored securely in the Merkle tree, the root of which is stored in the block header. Based on the Merkle tree, the global model parameters can be regenerated and verified in any iteration stage from the source block to the tail block, maintaining the auditability of the model iteration process in an immutable manner. However, the limitation of the approach is that the user device relies on the honesty of its corresponding edge device to forward transactions to the blockchain network.

C. Trustworthiness

With the two characteristics of trustworthiness and decentralization, blockchain build a foundation of trust in a cost-effective manner, in which multiple participants are able to share data in a trusted manner. This subsection will discuss how

to use blockchain to solve the trustworthiness issues of AI, including trustworthiness of the nodes involved in the training and data.

Trustworthy node: In distributed machine learning, multiple device nodes are dispersed in a network, and they collaborate on training tasks or jointly make intelligent group decisions. However, both the device itself and inter-device communication may be subject to various network security attacks, such as the possibility of device failure or malicious intent. It is important to design a mechanism to measure the reliability of nodes. One common mechanism is to construct a reputation system, that is building perceptions and expectations of future behavior based on previous behavior. For example, Kang et al. [17] focus on the problem of how to select reliable nodes in federation learning, where participating nodes may slack off or upload wrong parameters, implementing a distributed and tamper-evident reputation management model based on the blockchain. For a particular mobile device, the task publisher integrates its direct and indirect reputation opinions to generate an integrated reputation value, which is used as an important indicator for the subsequent selection of reliable participating nodes.

Also, Calvaresi et al. [18] propose to use another parallel blockchain ledger to store the relevant evaluation information between the service provider and the requester. By storing immutable calculation processes and based on these calculations, the smart contract updates the reputation of the agent in a transparent way, which realizes the reputation management of the smart contract. And the work of [19] points out that the complexity of fine-grained federated learning systems based on mobile edge computing leads to multiform (i.e. raw data, preprocessed data or training model) and multilevel (i.e. users, sensors, edge devices, fog nodes, blockchain networks and cloud service providers) heterogeneity. This enormous heterogeneity creates an urgent need to design a fully collaborative, trustworthy, and reliable fine-grained federation learning system. The authors propose a blockchain-based decentralized federation learning technique that introduces a reputation mechanism to ensure trusted collaborative training in a mobile edge computing environment. Also due to the consensus mechanism and the implicit property of non-repudiation, it further ensures that all participants can trust each other.

Trustworthy data: Currently, the data set used to train usually come from the third party. The lack of attention to the data may be subject to different types of attacks when using models. Specifically, in machine learning, training on biased data will produce a biased model, which will lead to a variety of errors and biased results. It is not easy to read the code or interpret the parameters of the model to determine if they are corrupted by toxic training data. This requires a mechanism to track the history of the data set to ensure the correctness and effectiveness of the training results.

In [20], a blockchain-based system for collecting training data and recording the learning process of intelligent robots is proposed, which ensures that the training information of the robots remains trustworthy. However, the authors have not implemented the system, and plan to implement and test its performance in a real environment in future work. The work of [21] proposes a blockchain-based trusted federated learning

architecture to realize the accountability. The authors design a smart contract-driven data-model provenance registry to track and record local data for local model training, and map the data and local model version to the corresponding global model version for audit. In addition, they propose a weighted sampler algorithm for data sets, which improves the fairness of data sets and models affected by heterogeneous distributions.

On the other hand, AI applications need to process, transform, and store large data sets. However, in the case of large data sets, centralized data management methods are very inefficient, and when it comes to sensitive personal data, centralized storage will become highly sensitive in terms of privacy and security. Blockchain has now been foreseen as a trusted platform for storing data. In order to enhance the privacy, trustworthiness and efficiency of data storage, transmission, and management in AI computing scenarios, blockchain can be regarded as a potential solution, which can use a variety of encryption algorithms and establish a collaborative relationship between multiple parties.

For the problem that the data used for machine learning algorithms from the variable database, the data and results cannot be completely trusted, Wang et al. [22] propose to use blockchain technology to build a trusted machine learning system that is capable of storing data in a permanent and unchanging manner. The smart contract is used to automate the machine learning process. Also, in order to make full use of the framework to improve data processing efficiency, the authors design a three-step method. Firstly, train a lightweight machine learning model on the server layer, then the trained model is saved in a special binary data format, finally, the stream layer takes this binary data as input and scores the input in an online fashion.

Machine learning algorithms rely on data to learn, infer and make final decisions. When collecting data from a reliable and trusted platform, machine learning algorithms will work well. In blockchain, data can be stored and processed by cryptographic signature and consensus, and the data transformation history can be effectively traced. This tamper-evident and effectively traceable nature provides a new direction to solve the problem of data reliability in machine learning.

D. Incentive

Traditional incentives require a credible central authority to audit participants behavior and arbitrate their rewards, failing to provide public auditability and decision fairness [23]. Noteworthy, in blockchain, nodes receive tokens and reach consensus based on mining results which ensures public auditability. Introducing appropriate incentives from the blockchain and designing transparent and cost-effective implementations will hopefully increase the motivation of all parties in a distributed machine learning system.

For example, in [10], to prevent nodes from only downloading the latest global model without participating in the training in federated learning, the authors propose that nodes must pay a fee when they get the latest global model. At the same time, nodes are rewarded when their local models are uploaded to chain, or when they become committee members for excellent performance. Such a mechanism promotes nodes to provide

local model more frequently, which in turn keeps the global model updated. And numerous global models will attract more nodes to participate, eventually forming a virtuous circle.

Toyoda et al. [24] introduce the concept of competition to blockchain-based federated learning so that only nodes that contribute are rewarded, which prevents nodes from deviating from the protocol. The article provides a complete theoretical analysis of the optimal reward policy based on competition theory. Behera et al. [25] propose using the open and transparent characteristics of smart contracts to define an incentive rule for participants based on scalar federal contributions. In turn, it overcomes challenge of the lack of fairness, transparency and universal recognition of reward rules. Similarly, Weng et al. [26] propose a framework DeepChain based on incentive mechanism of blockchain and cryptographic primitives. Through value-driven incentive mechanisms, participants are encouraged to act honestly, especially in gradient collection and parameter updating.

Based on the incentives of blockchain, it is expected that machine learning systems can obtain the best data and models and become more intelligent. Eventually it forms an open market where anyone can sell their data and protect data privacy, developers can get the best data for their algorithms, while the model can be shared and used by the nodes on the chain, and the whole system achieve a virtuous circle.

E. Privacy Protection

AI has revolutionized data extraction techniques and achieved breakthrough success in various applications such as autonomous driving and facial recognition. These applications often require clients to extract data from a distributed environment, leading to serious data privacy issues. Differential privacy and cryptography are two widely used methods to protect privacy [27]. Some experimental work now focuses on minimizing the side effects of these two approaches, while continuing the search for a novel approach that balances data privacy protection with flexible privacy requirements.

Xuhui et al. [28] analyze the privacy and security issues of the nonlinear learning model in distributed machine learning, and propose a distributed security machine learning system LearningChain that supports privacy protection based on blockchain technology. A decentralized stochastic gradient descent (SGD) algorithm is designed to learn a generic prediction model on blockchain. In decentralized SGD, a differential privacy-based mechanism is developed to protect the data privacy of all parties, and an l-nearest aggregation algorithm is proposed to protect the system from potential Byzantine attacks. Also, Awan et al. [29] design a blockchain-based privacy protection framework, which performs gradient aggregation based on cryptographic protocols. A variant of the Paillier cryptosystem which supports additive homomorphic encryption and proxy re-encryption can aggregate encrypted local model updates and convert them to a recoverable form, effectively protecting data privacy. Youyang et al. [30] propose a novel type of blockchain-supported federated learning (FL-Block) scheme to balance privacy and efficiency issues. It allows terminal devices to exchange global models on the blockchain with local models updates. By using the proof-of-work consensus mechanism of the blockchain, autonomous

machine learning is achieved without any central authorization to coordinate and maintain, effectively protecting private data.

In terms of data privacy protection mechanisms, technologies such as differential privacy and homomorphic encryption are still the most effective means for blockchain-based distributed learning and training.

IV. OPEN RESEARCH DIRECTIONS

Blockchain can offer a decentralized market and platform for various components of artificial intelligence, including data, algorithms, and computing capabilities, provide safe and efficient solutions for data storage, transmission, and management in the machine learning process, and ensure the training process more transparent and interpretable. TABLE 1. briefly summarizes the relevant research work.

While categorizing and summarizing the research in this filed, we have identified further open research directions discussed below.

Improve the scalability of blockchain: Although we have discussed many advantages of introducing blockchain technology into AI, many technical challenges related to blockchain itself need to be further studied which will limit the practical application to a certain extent. Most of the technical challenges related to blockchain focus on the performance, especially transaction throughput, transaction confirmation delay, block capacity and so on. Among them, the consensus mechanism is a key which ensures the validity and consistency when the distributed nodes process transactions and create block. Therefore, it is also crucial to improve the consensus efficiency of the blockchain.

The trade-off between computational efficiency and data privacy: The goal of protecting security and privacy is not a new topic, and blockchain has key characteristics such as anonymity,

TABLE I. BLOCKCHAIN RESEARCH FOR AI

Scenario	Decentralized	Explainable	Trust	Incentive	Privacy
[10]FL	✓			✓	
[11]DL	✓				✓
[12]FL	✓				✓
[14]ML		✓			
[15]FL		✓			
[16] FL		✓			
[17] FL			✓	✓	
[18]Robot			✓		
[19] FL	✓		✓	✓	
[20]Robot			✓		
[21] FL			✓		
[22]CV			✓		
[24] FL				✓	
[25] FL				✓	
[26]DL				✓	✓
[28] FL					✓
[29]ML	✓				✓
[30] FL					✓

decentralization and security, so it is considered to be able to deal with the security and privacy problems in the system efficiently and reliably. However, using blockchain to improve the privacy and security is often accompanied by the design of relevant cryptographic algorithms. And these algorithms need further design and research to reduce the impact on the computational efficiency of the system.

V. CONCLUSION

This article reviews the research progress of the integration of blockchain and AI. The combination of the two ensures improved data security and collective intelligence due to decentralization and decision storage mechanisms, increased trust of multiparty decision-making systems with various consensus protocols. We believe that interdisciplinary research combining the two technologies is full of potential, and the alliance is expected to create a variety of possibilities.

ACKNOWLEDGMENT

Supported by the National Research and Development Plan (NO.2021YFF0704102); the National Natural Science Foundation, China (NO.61772316); the major Science and Technology Innovation of Shandong Province (No.2019JZZY010109,2020CXGC010106,No.2021CXGC010108); the Industrial Experts Program of Spring City; National Social Science Fund (No.20BJY131).

REFERENCES

- [1] M. R. Frank, D. Wang, M. Cebrian, and I. Rahwan, "The evolution of citation graphs in artificial intelligence research," *Nature Machine Intelligence*, vol. 1, no. 2, pp. 79–85, 2019.
- [2] N. Papernot, P. McDaniel, S. Jha, M. Fredrikson, Z. B. Celik, and A. Swami, "The limitations of deep learning in adversarial settings," in 2016 IEEE European symposium on security and privacy (EuroS&P). IEEE, 2016, pp. 372–387.
- [3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.
- [4] W. Gao, W. G. Hatcher, and W. Yu, "A survey of blockchain: Techniques, applications, and challenges," in 2018 27th international conference on computer communication and networks. IEEE, 2018, pp. 1–11.
- [5] G. Wood et al., "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.
- [6] Z. L. TanZuowen, "Survey on privacy-preserving techniques for machine learning," *Journal of Software*, vol. 31, no. 7, p. 21272156, 2020.
- [7] M. Nassar, K. Salah, M. H. ur Rehman, and D. Svetinovic, "Blockchain for explainable and trustworthy artificial intelligence," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 10, no. 1, p. e1340, 2020.
- [8] N. A. Team, "Nebula ai (nbai)—decentralized ai blockchain whitepaper," 2018.
- [9] C. Fromknecht, D. Velicanu, and S. Yakoubov, "A decentralized publickey infrastructure with identity retention." *IACR Cryptol. ePrint Arch.*, vol. 2014, p. 803, 2014.
- [10] Y. Li, C. Chen, N. Liu, H. Huang, Z. Zheng, and Q. Yan, "A blockchain-based decentralized federated learning framework with committee consensus," *IEEE Network*, vol. 35, no. 1, pp. 234–241, 2020.
- [11] L. Lyu, J. Yu, K. Nandakumar, Y. Li, X. Ma, and J. Jin, "Towards fair and decentralized privacy-preserving deep learning with blockchain," *arXiv preprint arXiv:1906.01167*, pp. 1–13, 2019.
- [12] C. Korkmaz, H. E. Kocas, A. Uysal, A. Masry, O. Ozkasap, and B. Akgun, "Chain fl: Decentralized federated machine learning via blockchain," in 2020 Second International Conference on Blockchain Computing and Applications (BCCA). IEEE, 2020, pp. 140–146.
- [13] C. Olah, A. Satyanarayan, I. Johnson, S. Carter, L. Schubert, K. Ye, and A. Mordvintsev, "The building blocks of interpretability," *Distill*, vol. 3, no. 3, p. e10, 2018.
- [14] K. Sarpatwar, R. Vaculin, H. Min, G. Su, T. Heath, G. Ganapavarapu, and D. Dillenberger, "Towards enabling trusted artificial intelligence via blockchain," in *Policy-based autonomic data governance*. Springer, 2019, pp. 137–153.
- [15] Z. Peng, J. Xu, X. Chu, S. Gao, Y. Yao, R. Gu, and Y. Tang, "Vfchain: Enabling verifiable and auditable federated learning via blockchain systems," *IEEE Transactions on Network Science and Engineering*, 2021.
- [16] U. Majeed and C. S. Hong, "Flchain: Federated learning via mec-enabled blockchain network," in 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS). IEEE, 2019, pp. 1–4.
- [17] J. Kang, Z. Xiong, D. Niyato, S. Xie, and J. Zhang, "Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10 700–10 714, 2019.
- [18] D. Calvaresi, A. Dubovitskaya, D. Retaggi, A. F. Dragoni, and M. Schumacher, "Trusted registration, negotiation, and service evaluation in multi-agent systems throughout the blockchain technology," in 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), 2018, pp. 56–63.
- [19] M. H. ur Rehman, K. Salah, E. Damiani, and D. Svetinovic, "Towards blockchain-based reputation-aware federated learning," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2020, pp. 183–188.
- [20] K. Wang et al., "A smart robot training data acquisition and learning process recording system based on blockchain," *Open Access Library Journal*, vol. 7, no. 09, p. 1, 2020.
- [21] S. K. Lo, Y. Liu, Q. Lu, C. Wang, X. Xu, H.-Y. Paik, and L. Zhu, "Blockchain-based trustworthy federated learning architecture," *arXiv preprint arXiv:2108.06912*, 2021.
- [22] T. Wang, M. Du, X. Wu, and T. He, "An analytical framework for trusted machine learning and computer vision running with blockchain," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*, 2020, pp. 6–7.
- [23] U. Shevade, H. H. Song, L. Qiu, and Y. Zhang, "Incentive-aware routing in dtms," in 2008 IEEE international conference on network protocols. IEEE, 2008, pp. 238–247.
- [24] K. Toyoda, J. Zhao, A. N. S. Zhang, and P. T. Mathiopoulos, "Blockchain-enabled federated learning with mechanism design," *IEEE Access*, vol. 8, pp. 219 744–219 756, 2020.
- [25] M. R. Behera, S. Upadhyay, and S. Shetty, "Federated learning using smart contracts on blockchains, based on reward driven approach," *arXiv preprint arXiv:2107.10243*, 2021.
- [26] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, "Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive," *IEEE Transactions on Dependable and Secure Computing*, 2019.
- [27] M. Asad, A. Moustafa, and C. Yu, "A critical evaluation of privacy and security threats in federated learning," *Sensors*, vol. 20, no. 24, p. 7182, 2020.
- [28] X. Chen, J. Ji, C. Luo, W. Liao, and P. Li, "When machine learning meets blockchain: A decentralized, privacy-preserving and secure design," in 2018 IEEE International Conference on Big Data (Big Data). IEEE, 2018, pp. 1178–1187.
- [29] S. Awan, F. Li, B. Luo, and M. Liu, "Poster: A reliable and accountable privacy-preserving federated learning framework using the blockchain," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 2561–2563.
- [30] Y. Qu, L. Gao, T. H. Luan, Y. Xiang, S. Yu, B. Li, and G. Zheng, "Decentralized privacy using blockchain-enabled federated learning in fog computing," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5171–5183, 2020.