Chapter

Blockchain-Empowered Mobile Edge Intelligence, Machine Learning and Secure Data Sharing

Yao Du, Shuxiao Miao, Zitian Tong, Victoria Lemieux and Zehua Wang

Abstract

Driven by recent advancements in machine learning, mobile edge computing (MEC) and the Internet of things (IoT), artificial intelligence (AI) has become an emerging technology. Traditional machine learning approaches require the training data to be collected and processed in centralized servers. With the advent of new decentralized machine learning approaches and mobile edge computing, the IoT on-device data training has now become possible. To realize AI at the edge of the network, IoT devices can offload training tasks to MEC servers. However, those distributed frameworks of edge intelligence also introduce some new challenges, such as user privacy and data security. To handle these problems, blockchain has been considered as a promising solution. As a distributed smart ledger, blockchain is renowned for high scalability, privacy-preserving, and decentralization. This technology is also featured with automated script execution and immutable data records in a trusted manner. In recent years, as quantum computers become more and more promising, blockchain is also facing potential threats from quantum algorithms. In this chapter, we provide an overview of the current state-of-the-art in these cutting-edge technologies by summarizing the available literature in the research field of blockchain-based MEC, machine learning, secure data sharing, and basic introduction of post-quantum blockchain. We also discuss the real-world use cases and outline the challenges of blockchain-empowered intelligence.

Keywords: blockchain technology, mobile edge computing (MEC), distributed machine learning, internet of things (IoT), data security and privacy

1. Introduction

In the past few years, machine learning and blockchain have been known as two of the most emerging research areas. Machine learning is the practice of building learning models on the computers to parse data, and provide human-like predictions or decisions for some real-world problems. Blockchain, on the other hand, has the capability to store and process data, preserve data integrity, and govern peers accessibility without needing any centralized administration. Those two research areas are heavily data driven and each of those technologies has its own advantages and bottlenecks. In this chapter, we review some novel research on combining blockchain and machine learning, and identify how their short-comings can be

addressed by merging these different ecosystems. Several machine learning techniques such as supervised machine learning, deep reinforcement learning and federated learning are considered as good alternative solutions to the Blockchain related research. We also discuss how the researchers make these two technologies work collaboratively to solve some real-world problems.

The Internet of things (IoT) is a well-known technology for research and industry. Devices in this network can still sense and respond to the environment without users' intervention. Enabling artificial intelligence (AI) in IoT has emerged as a hot research topic [1]. However, machine learning is a kind of computational task which is a heavy workload for the IoT devices (IoTDs). Usually, these low-cost IoT devices are battery-powered devices. On the one hand, computational tasks execution (e.g., training machine learning models) consumes considerable energy. On the other hand, the required powerful microchips are not suitable for IoTDs with compact physical size.

Mobile edge computing (MEC) is a solution to the above challenges. By offloading complex learning tasks to the edge of Internet, IoTDs could perform machine learning algorithms to realize AI. The original MEC was proposed by ETSI in 2014. The description of MEC was "A new platform provides IT and cloud computing capabilities within the Radio Access Network (RAN) in close proximity to mobile subscribers" [2]. We focus on the edge computing within the RAN in this chapter because it has been a standard across different industries. It will help readers to learn blockchain-enabled mobile edge intelligence in the most practical scenario. However, security and privacy issues must still be considered [3]. The IoT data leakage may lead to malicious attacks on individuals. Fortunately, blockchain has potential and is suitable for MEC [4]. The integration of MEC and blockchain is a win-win solution. For one thing, blockchain provides MEC with data security and privacy. For another, MEC can improve blockchain's scalability and effectiveness.

The main contributions of this chapter are listed as follows:

- We first focus on the security and privacy-preserving features of blockchain. The consensus mechanisms, permissioned blockchain and zero-knowledge proof are jointly introduced to give a general understanding for readers;
- We describe the blockchain-enabled mobile edge intelligence in the scenario of IoT systems. The potential of blockchain in edge intelligence is included;
- The combination of blockchain and AI is further given in a two-way manner. Real world applications of blockchain in AI are summarized;
- Discussions of blockchain's threat are illustrated for future research. For example, the threat of quantum computing and its related research is surveyed in this chapter.

The rest of this chapter is organized as follows. In Section 2, we introduce the security and privacy-preserving features of blockchain. Next, the blockchain-enabled edge intelligence is discussed in Section 3. Then, some blockchain and machine learning combined research is summarized in Section 4. Finally, we discuss some threats for blockchain-enabled systems and conclude this chapter.

2. The security and privacy-preserving features of Blockchain

Blockchain is famous for its security, and the most well-known social experiment of blockchain today is Bitcoin. As a revolutionary invention, Bitcoin certainly

caught many investor's attention. One index that can be used to determine the popularity of Bitcoin is the total number of wallets created on the Bitcoin networks[1]. This index is currently at record high (around 65.015 million). Unlike traditional banking systems where a person can only have a limited number of bank accounts, Bitcoin allows users to create accounts with just a few commands/clicks without the involvement of any government issued identity verification process. Therefore, we would not be able to find out how many people tried Bitcoins or engaged in the Bitcoin network service. There is another number that can show the impact of Bitcoin, which is the total hashrate (TH/s) of the Bitcoin network[2], this number is also at its record high, about 153.019 million (TH/s) now. Mining hashrate is one of the key security metrics of the Bitcoin network. The bigger the hashrate number or hash power in a network, the greater its security and its overall resistance to attacks. There is no way for us to calculate the actual hashrate on the network. However, from the block difficulty, we can give an estimate of its total hash power [5]. Hash power is delivered by Bitcoin miners, whose computers join the blockchain network to compute the problems together. This mechanism is often called proof-of-work (PoW) and it costs a lot of power and electricity. A study published on Nature Climate Change in 2018 estimated that Bitcoin mining alone could push up global warming by 2 degrees Celsius [6].

At this moment, a single Bitcoin is worth around 40,000 US dollars. The questions are, what are people buying it for? Are there any reasons why mining mechanisms are so energy hungry? Are there any alternative ways to design systems? In the following paragraphs, we will explain to you how Bitcoin achieves its state-of-the-art secure distributed ledger and how it allows people on the boundary of trust to work together. Next, we will introduce you to another concept and discuss how 5G edge devices could benefit from blockchain security.

2.1 Security feature

2.1.1 Proof-of-Work (PoW Consensus Algorithm)

PoW is the underlying consensus algorithm of Bitcoin [7]. A consensus algorithm in computer science is a process used to achieve agreement on a single data value among distributed processes or systems [8]. This term is commonly used by distributed systems. It explains that in the modern computing era, how multiple servers could work together with high levels of security and fewer errors. In more detail, some servers (or nodes) may fail or may be unreliable in other ways (e.g., being hacked, losing data, running in idle). Therefore, consensus algorithms must be fault tolerant and resilient. Consensus mechanisms function a bit like constitutions in the human world - guiding decisions about what's acceptable among interacting parties. This is the core of a blockchain system. PoW is commonly recognized as a secure consensus algorithm [7]. It's a consensus mechanism that heavily relies on computing power and cryptographic hash function (also known as CHF, a mathematical algorithm that maps data of arbitrary size to a bit array of a fixed size). Before diving into this consensus model, one needs to be familiar with the following two concepts, the Crash-Fault Tolerance (CFT) and the Byzantine-Fault Tolerance (BFT).

The Crash-Fault Tolerance (CFT). Just as it states in its name, it can be resilient toward crash/halt events. Suppose that your system has been damaged or lost

[1] https://www.blockchain.com/

[2] One trillion (1,000,000,000,000) hashes per second.

connection, the CFT based system will still function and give the result that you expect [9]. The CFT fault model has been discussed by academics for a number of years long time and is mature in industrial use cases. Most cloud based companies implemented different CFT methods to prevent the critical problems. We still occasionally hear news about collapse/maintenance of servers of Amazon, Alibaba or Microsoft and developers make some open source or free projects to show you the real-time status of their servers (e.g., the downdetector[3]).

Byzantine-Fault Tolerance (BFT) is more complicated than CFT. The name Byzantine-Fault Tolerance is derived from a paper published by Leslie Lamport, Robert Shostak and Marshall Pease on SRI International called The Byzantine Generals Problems [10].

Converting the story above into a computer system use case, a distributed system should be resilient to the case when a small portion of the computers in the network are malicious. Every non-malicious entity has the same status (including action). Companies' server systems are mostly CFT because they set up each node/server in the network and they are very confident that the chances of having malicious nodes are low. Furthermore, they have backup systems that can recover from the previous loss. However for Bitcoin, everyone can hop-on and hop-off the Bitcoin chain. So how do we protect the network and the ledger system's integrity, making sure no one is taking extra money that does not belong to them or preventing one's money from being stolen [7]. This is a typical BFT question.

The PoW solves the problem of determining representation in majority decision making. It's a one-CPU-one-vote proposed by Satoshi Nakamoto [7], the pseudonymous founder of Bitcoin. Around every 10 minutes, the network will wrap around all transactions that happened within the 10 minutes. As illustrated in **Figure 1**, it uses a cryptographic hash function to hash previous block's hash, Nonce and transactions together to form a new hash block. Each node will try different nonces (numbers) to find a certain number of zeros in front of the hash result (mining difficulty). This process is called mining, it is power consuming and no less energy consuming, mathematically proven secure short cut has been found yet.

The beauty of PoW is that the result can be instantly verified but it will be very difficult to tamper with unless the malicious nodes occupy 51 percent of the total computing power of the network [11]. With increasing numbers of miners joining the mining and significant numbers of investments in this area, the difficulty of tampering with the Bitcoin network becomes harder and harder. However, a lot of criticisms about blockchain also arose in the past decades, especially about its efficiency, energy consumption and its economic model. Environmentalists disagree with this mechanism due to the fact that the annual electricity consumption of the Bitcoin network is nearly 120 gigawatts (GW) per second. Equivalent to 49.440 wind turbines (412 turbines per GW) when generating power at peak production per second [12]. There is another focus on Bitcoin PoW mechanisms which is about the ASIC miners. Since the Bitcoin mining mechanism is like solving a math puzzle,

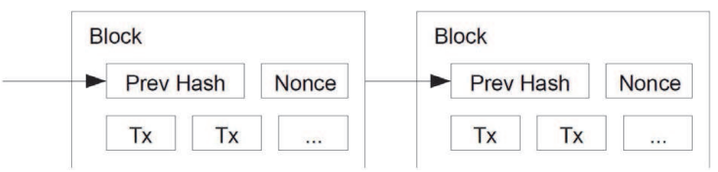

Figure 1.
Blockchain Structure [7].

[3] https://www.isitdownrightnow.com/

developers moved from using CPU to using Application-Specific Integrated Circuit (ASIC) machines to mine Bitcoin. This shift significantly increased the Bitcoin mining difficulty since ASIC is a dedicated computing circuit that is purely designed for mining purposes [13]. Therefore, the ASIC's performance is much better than the General Purposes Computing Unit (CPU). This brings a huge barrier for beginners to join the mining, and it will further enhance the Bitcoin mining centralization, not to mention that the Bitcoin miner market is in a relatively monopoly situation, as 66% of market share of miners are occupied by Bitmain[4].

2.1.2 Alternative consensus mechanisms

Due to the above drawbacks and concerns over PoW mechanisms, designers have developed a new consensus mechanism called Proof-of-Stake (PoS) where miners have been incentivized based on how much "work (hash power)" they have contributed. In contrast, the PoS mechanism asks miners to bet tokens in order to participate in the new block generation. This concept was first discussed in 2012 by Peercoin [14, 15], and had later become a popular discussion and experiment among many cryptocurrencies.

Compared with the PoW mechanism, PoS is simpler. The more you stake, the higher the influence you have on determining the next block [14]. The assumption is based on the premise that high staking nodes are less likely to lie because of high losses for them if they tried to tamper with the chain. Under this scenario, nodes are no longer needed to solve cryptographic puzzles. Apparently, compared with PoW, PoS is more environmentally friendly. Besides, less computation will further enhance the network transaction speed as well as the throughput [16]. There are currently two types of PoS consensus models: Chain-based Proof-of-Stake and Consortium Consensus model [14]. Chain-based Proof-of-Stake chooses availability over consistency [17]. The algorithm pseudo-randomly selects a validator during each time slot. Validators will then have the right to create a single block and point it back to the previous longest chain. Consortium Consensus Model chooses consistency over availability. During each voting procedure, every node counts proportionally to the stake it bets.

Apparently, the richer nodes have higher chances of getting the reward. In order to avoid the monopoly situation, a random selection model is required for most PoS algorithms. Each token has their own token economy and some of them include token age design, where tokens being staked for a longer time will be more likely to be selected. In general, the network wants holders to stake validation tokens as long as possible and act as hosts.

With rapid adoption of 5G networks by different countries and regions, edge computing and edge devices will play an important role in the network. Blockchain is currently the state-of-the-art secure network system and has many use cases in edge computing [18]. In the upcoming 5G era, more and more devices will have access to the network, since one of the main goals of 5G is to support the IoT [19, 20]. As predicted, data transmission rate and volume will exponentially grow and thus to have a secure communication channel and a consensus algorithm for edge devices have been identified in recent research papers. Edge devices for 5G network are often not designed for doing heavy computation. Thus, a new consensus model is needed for the 5G era. PoS as one of the successful consensus models has potential in the IoT era due to its simpler structure, high security feature and completely decentralized characteristics. Besides PoS, Delegated Proof-of-Stake

[4] https://www.bitmain.com/

(DPoS) is another possible consensus algorithm for 5G use cases with greater scalability and faster transactions. However, DPoS is not completely decentralized; it is an intermediate solution finding the balance between centralization and decentralization [21].

2.2 Privacy-preserving features

In 2020, a Netfliex documentary called The Social Dilemma raised awareness about risks to our personal privacy. The Social Dilemma exposes audiences to shocking facts about how social media apps are currently using intelligence algorithms to control user's behaviours, as a result, making users addicted to their own content, and gathering user's data to target users with ads without any regulatory supervision [22].

Traditional banking systems often require many documents to set up one account. However, registering a public blockchain network normally does not require any identity verification and there is no limitation on how many accounts that you can build and there is no cost associated with making an account. Bitcoin (BTC) and Ethereum (ETH) are currently the most popular public blockchain networks[5]. When you send Ether (the cryptocurrency in Ethereum) on Ethereum platform, the sender and receiver are both just wallet addresses, hashes of a public key. Each transaction will be broadcasted on the mainnet.

2.2.1 Permissioned Blockchain network

Blockchain has many user scenarios. As for Bitcoin, it brings people to work together even if they are all on the boundary of trust. Users in the Bitcoin network have no need to trust each other at the beginning and anyone can hop-on and hop-off the network. Public blockchain networks are mostly targeting monetary systems and have their own token economics. However, public blockchain networks are often very slow and cannot be used in specific scenarios due to complex consensus algorithms to prevent malicious attacks. To make blockchain networks be more useful and specific to each use case, developers proposed permissioned blockchain network ideas. Permissioned blockchains usually involve a consortium of organizations who are in charge of verifying the transition history instead of asking pseudonymous miners to participate in the mining process [23]. Permissioned blockchains are often popular in the industries that rely on digital data, for example, supply chain management, liquidation in the financial industry, manufacturing industry. These industries take data security, data privacy and role definition seriously and are keen on pursuing higher efficiency. The operation of these industries is often similar to a chain reaction; one mistake in one process will cause sequential reaction in the following processes.

Public blockchain networks are open to anyone, where permissioned blockchains require identity verification as an extra security layer. In a nutshell, nodes on permissioned blockchains are verified and their roles in the network are predefined.

Permissioned networks can be used to protect sensitive data. Public blockchain networks set all users/nodes with equal amounts of power. In contrast, a permissioned blockchain network can have a more complicated internal structure to ensure data security, and access controls to specify that only nodes with permission can retrieve.

---

[5] https://coinmarketcap.com/, a website to track the market cap of all cryptocurrencies

2.2.2 Zero-knowledge proof and zk-SNARK

People may wonder whether there are mechanisms that can be used by a public blockchain network to hide some transactions or protect one's address from being traced. Zero-knowledge proof (ZKP) is a proof that allows a prover to prove the knowledge of a secret to a verifier without revealing it. The verifier should receive no knowledge before verification and after the verification [24]. This sounds unreal because in the real world, we gain trust in third parties through revealing our private messages or information such as date of birth, secret key or password. There is a famous story on ZKP. It was about two mathematicians who both claimed that they found the solution equation of a formula. However, Neither of them wanted to reveal it to the public. They later conducted a competition in which both drafted a question for their competitor and they would solve the question from each other by using their own method and to show their solutions. Verifiers only needed to check whether their solutions were correct to determine who actually found the solution equation of that formula. As a result, neither party revealed any information to the verifier, but the verifier still had sufficient evidence to determine who actually knew the solution.

Generally speaking, ZKP has two categories, the interactive and non-interactive ZKPs. Interactive ZKP is more intuitive. It requires intervention between individuals (or computer systems) to prove their knowledge and the individual validating the proof. For example, the method used by the mathematician competition is based on interactive ZKP. Interactive ZKP already has many applications in the communication industry, and such a system requires a stable and continuous communication channel. Non-interactive proof requires none of that, it takes less time and only one message is enough [25]. It's more efficient and can be optimized for IoT systems. Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) is a type of non-interactive ZKP and has been used by cryptocurrency Zcash as its core privacy-preserving mechanism. In a nutshell, Zcash can hide some transactions to make the blockchain more privacy focused, and external parties will not be able to trace many accounts' transaction history. However, researchers from Carnegie Mellon University found that 99.9% of Zcash and 30% of Monero (another privacy-preserving token) transactions were traceable because users may not use them properly [26, 27].

3. Blockchain-enabled edge intelligence for IoT

In this section, we introduce the potential and applications of blockchain in edge intelligence. To be specific, we aim at describing how AI could be implemented on the edge of the Internet and how blockchain could improve the mobile edge intelligence. We first introduce offloading strategies and the MEC architecture for readers. Then, we list how blockchain can improve mobile edge intelligence in terms of data security. Finally, we describe the blockchain-enabled resources allocation and market trading in the mobile edge intelligence systems with the constrains of energy supply, computational power, and the size of training data.

3.1 Tasks offloading in Blockchain systems

Although the PoW can secure transaction records in Bitcoin and similar blockchain networks, it is still very challenging to implement this kind of consensus mechanism for securing AI applications because it is a computational intensive task. To be specific, realizing blockchain-enabled AI for edge devices (i.e., edge

intelligence) requires two kinds of tasks to be executed. On one hand, mining process is necessary for establishing consensus among distributed IoTDs. On the other hand, data training will be performed at each IoTD in a decentralized manner.

However, IoTDs are energy-constrained and unable to process complex computational tasks. Fortunately, edge computing is capable of handling this issue. The main idea of realizing blockchain-enabled AI on the edge network is to use different offloading strategies for IoTDs. As illustrated in **Figure 2**, one can see that computing tasks can be offloaded from IoTDs to MEC servers located in different places, including small-cell base stations, cellular base stations, and the cloud data center [28]. As the distance between IoTD and MEC server becomes shorter, the computing capability decreases.

However, data leakage and other security issues impose great challenges to MEC, especially for MEC-enabled blockchain and AI applications. In [3], authors discussed the privacy issues in MEC-enabled blockchain networks. Data processing and mining tasks were offloaded to nearby servers. Moreover, the privacy level was modeled in this paper. The trade-off and optimization among energy consumption, privacy, and latency were jointly considered. Furthermore, [29] investigated the trust mechanism for edge network by using blockchain technology. Selfish edge attacks were discussed in this paper. The selfish attack means MEC servers provided the IoTDs with fake service and less computational resources. To deal with this attack, the authors explored the blockchain-based reputation record system, wherein selection of the miner relies upon the reputation of the MEC servers.

As the growth of IoTDs and AI applications becomes explosive, it becomes challenging to coordinate tasks offloading in wireless networks, especially for the ultra-dense wireless network [30]. To deal with this problem, authors in [30] proposed a decentralized platform based on blockchain. Computational tasks were first published and recorded in this platform, then user matching was evaluated and conducted based on the tradeoff between service latency and energy consumption. Moreover, offloading mode selection was discussed in [31], including offload tasks to a nearby server or a group of users. The content caching strategy was studied to handle the traffic issue in blockchain wireless networks. Furthermore, content caching could be used to extend the block capability of a blockchain platform. To be specific, hashed blocks were cached in MEC servers [32]. Then, images and even videos could be stored into the block for AI applications. Authors in [33] further optimized and proposed a block size adaptation scheme for video transcoding.

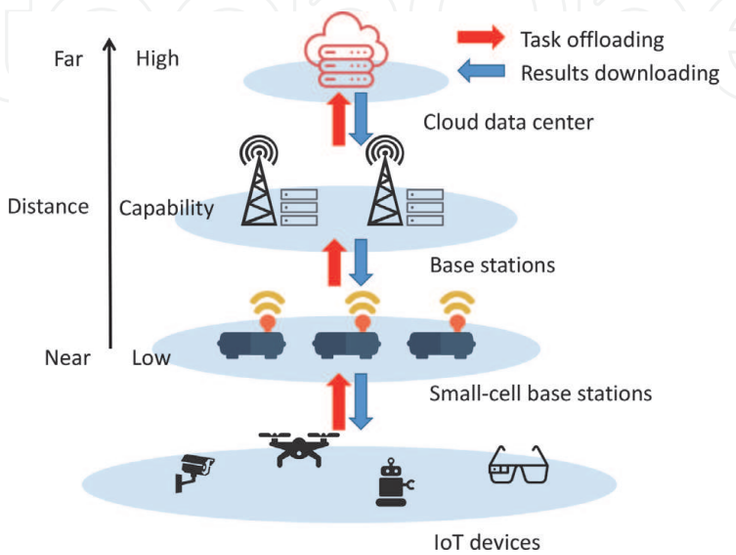

Figure 2.
MEC architecture for IoT devices.

Another issue is cooperation incentive. As mentioned above, nearby MEC servers have limited resources to share. The cooperation computation offloading research was discussed in [34]. To incentivize and establish this kind cooperation, a coin loaning strategy was given for IoTDs in [35]. Besides, most related research ignored the real need of IoTDs and blockchain-enabled AI applications. For example, fast transaction writing and uploading are critical for low-latency applications [36]. In another scenario, the revenue (e.g., tokens) may be treated as the first priority in the computing cooperation. Moreover, the scalability and efficiency should be considered in offloading strategies. To solve this issue, blockchain technology and the directed acyclic graph were explored in [37].

3.2 Blockchain-enabled data security for mobile edge intelligence

IoT data contains sensitive information related to individuals. Therefore, IoT data security is critical in establishing AI applications based on IoTDs. As described in the previous part, blockchain-based MEC is a key solution to enable AI for IoTDs. To secure IoT data and MEC, blockchain is a promising strategy. To be specific, authentication, secure communication, data privacy, and data integrity are four main strategies to enable IoT securtiy in the scenario of MEC.

Although blockchain-enabled edge intelligence is a cutting-edge technology to enable AI applications for IoT systems, it is vulnerable when facing malicious attacks. Authentication of identities in blockchain-enabled MEC system was discussed in [38]. The authors proposed a digital validation strategy based on group signature scheme. In this way, the identities of block creators were verified and authenticated to prevent edge intelligence from false records. Moreover, to manage privacy and data leakage issues, authors in [39] discussed the authentication for federated learning (FL) peers in the edge computing context. By exploring blockchain technology and smart contract, the FL and differential privacy technique were proposed in this article.

Secure data sharing is another aspect of data security for edge intelligence. The basic idea of secure data sharing is that data should be stored and shared in a trusted way. Consortium blockchain was discussed in [40] for the secure and efficient data sharing. Different from a public blockchain network, the consensus process is performed on a group of pre-determined edge nodes in consortium blockchain. The proposed model contained two kinds of smart contracts, including data storage smart contract and information sharing smart contract, allowing the auditing and governance of data sharing. Besides, the data sharing problem was transformed into a machine learning problem in [41]. FL was explored in this article to share the learning model rather than raw data.

The integrity of data should be considered in edge intelligence. As illustrated in **Figure 3**, any false information may do harm to the global ML model. For example, poisoning attack and input attack are two major types of issues in data integrity in AI application. The first one normally occurs in the initial stage of AI model training. By manipulating training data, the AI model would be ineffective. The latter one tends to use manipulated data to shape and affect the AI model output in a way desired by attackers. The design of blockchains naturally protects data integrity because any tampering of previous data recorded are not permissioned. MEC servers were used to validate and store blockchain data in [42] for data integrity. The data acquisition process for IoT system was discussed in this article. To be specific, the identity of a data sender was verified in this process. IoT data were recorded and stored in blockchain only if the validation was successful. Additionally, verifiable integrity of IoT data could be realized by blockchain [43].

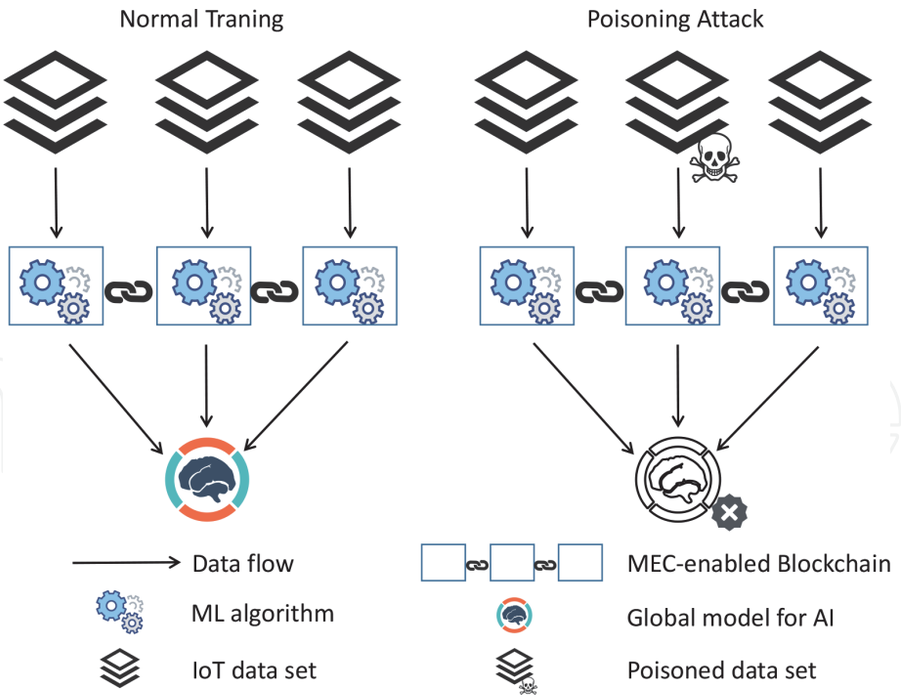

Figure 3.
Poisoning attack on blockchain-enable edge intelligence.

As we have discussed in the previous part, protection of privacy presents great challenges for mobile edge computing. Sensitive data should not be shared to any trustless third parties. The decentralization of privacy was discussed in [44]. The off-chain storage technique was used in the blockchain for privacy-preserving purposes. Furthermore, the topology of the edge intelligence network is another kind of sensitive information. A heterogeneous MEC system was proposed in [45] to provide MEC network topology with protections. FL was used in [41] to solve the privacy issue in data sharing. Differential strategy was further integrated into FL to prevent the leakage of sensitive IoT information. In terms of industrial IoT systems, authors in [46] explored the privacy issue in industry 4.0. ML models were trained on the sensitive data in industrial IoT systems. Therefore, the establishment of trustworthiness and privacy-preservation was a critical aspect in designing AI applications for industry 4.0 aspect. By jointly exploring the Ethereum blockchain, smart contracts, differential privacy, and FL, the authors proposed a novel blockchain named PriModChain to handle the privacy and security issues in industrial IoT systems.

3.3 Blockchain-based market for mobile edge intelligence

In the social layer, blockchain is a promising technology for peer-to-peer resources trading. As is shown in **Figure 4**, energy, information, and computing power are three major resources in blockchain-enabled markets. As we have discussed, MEC servers are more powerful than the IoTDs in terms of storage and computing power. However, IoTDs are far more than MEC servers. That means resources are still very limited on the edge of Internet. Therefore, resources allocation is critical for blockchain-enabled edge intelligence. Fortunately, blockchain can establish an open market among IoTDs and MEC serves, enabling resources trading according to the need in system level.

Energy trading is important and useful in IoT systems. This is because IoTDs are energy-constrained. Different from the MEC servers with the constant power supply, IoTDs are battery-powered and not very convenient to recharge.

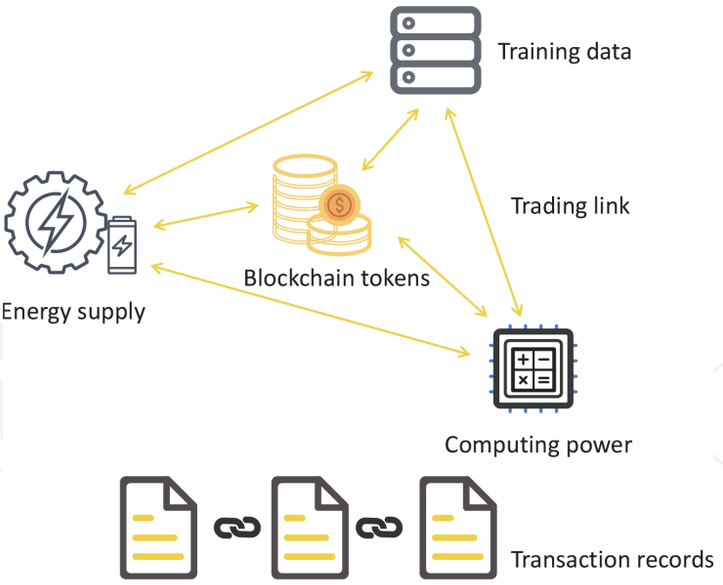

Figure 4.
Blockchain-enabled resources market for edge intelligence.

Energy-knowledge trading was discussed in [47]. On-device Al applications would be useless when IoTDs' battery is exhausted. Therefore, authors in this paper proposed a wireless way to power IoTDs. A permissioned blockchain was used for peer-to-peer (P2P) resources trading between energy power and training data sets.

Marketing is not only a platform to trade resources but also an effective solution to incentivize IoTDs and MEC servers into this blockchain-enabled platform. FL training market was studied in [48]. The idea of using blockchain is to establish a decentralized and fair market among MEC servers groups. A smart contract based resources trading market was further proposed in this article to ensure automatic transactions.

Content market is another topic for blockchain-enabled edge intelligence. To be specific, video transcoding and content delivery were investigated in [49]. A decentralized market was established by blockchain among trustless entities in a content delivery network. Content price, offloading cost, and content quality were jointly considered in this article. Furthermore, the willingness of MEC caching was discussed in [50]. In general, blockchain incited MEC servers by satisfying their expected rewards.

Last but not least, data is another type of digital asset, especially for AI applications. To be specific, data ownership is critical in the performance evaluation of AI training. Authors in [51] investigated the data ownership in AI training. Transactions among data owners, AI developers, and service providers were recorded in the proposed blockchain system. In this way, trading and data usage actions became traceable and verifiable. Thus, the ownership of training data sets was well-preserved. Nevertheless, for some types of sensitive transactions, where the existence of a transnational relationship between two parties may need to remain private, residual privacy concerns remain when all intervention is recorded on the ledger.

4. Blockchain and machine learning combined research

4.1 Machine learning for Blockchain industry

4.1.1 Blockchain security attack detection

One thing the public are concerned with respect to blockchain is its security performance. Although blockchain utilizes cryptography and consensus to enforce

network security and privacy, it is still not immune to potential attacks. In 2017, the Bitcoin researchers [5] found out that the Bitcoin network is vulnerable to some state of the art attacks, even though it has been successfully running for 8 years. In 2019, some vulnerabilities in the Ethereum network were exposed and it was reported that the network has experienced several attacks such as 51% attacks and data breaching attacks [52].

Machine learning has been considered as one of the tools to improve the blockchain security. Scicchitano *et al.* in [53] introduced an unsupervised machine learning approach to identify anomalies in the activities of the blockchain network. The proposed anomaly detection system constructs a neural encoder-decoder model and the model is capable of summarizing the status of the ledger sequence-by-sequence. The system has the ability to detect the difference of the statuses between standard situation and anomalous situation and trigger the alert accordingly.

Somdip Dey [54] was interested in improving the blockchain consensus mechanism. By utilizing game theory and supervised machine learning algorithm, an improved Proof-of-Work consensus is introduced to prevent any quantifiable attacks. By analyzing the attacker's activities and rewards, a utility/payoff function can be derived and fed into a supervised machine learning model. This machine learning model has the ability to detect whether an attack is bound to happen or not - based on the value of the commodity/service. If the attack is likely to happen, the machine learning agent has the ability to prevent the blockchain confirmation until a new block of fair transactions is generated again.

Hou *et al.* [55] proposed a framework called SquirRL. This is a deep reinforcement learning framework that can be used to analyze the blockchain rewards. Even though SquirRL is used to detect the adversary activities in the network, the framework can automate vulnerability detection in the blockchain incentive mechanisms. When the theoretical analysis is infeasible, SquirRL can serve as a powerful tool for the blockchain engineers to verify the protocol designs during their development phrases.

4.1.2 Cryptocurrency and mining

Thanks to the blockchain and cryptography, the emergence of cryptocurrency has drawn a lot of attention. Unlike fiat money and stocks, the cryptocurrencies have shown significantly unstable fluctuations and have disrupted the investment industries. Researchers have made steady progress on how to improve the profit in the cryptocurrency by applying machine learning models to analyze market performance or network data.

One main direction in this research area is to utilize the machine learning models to predict the prices of cryptocurrencies. However, the data source and the detail techniques may vary. Kim *et al.* [56] introduced a method that can help predicting the cryptocurrencies fluctuations. The proposed method collects user online posts and comments that are related to the cryptocurrency market activities, and conducts an association analysis between the collected data and the fluctuations in the prices of the cryptocurrencies. The final model shows about 74% weighted average precision in the Bitcoin and Ethereum markets. Madan *et al.* [57] intended to automate Bitcoin trading via supervised machine learning algorithms by using random forest and binomial logistic regression to support vector machine. Their learning method is trained with the Bitcoin price index and the final result achieves above 55% precision. Jang and Lee [58] used Bayesian Neural Network algorithm to train the supervised learning model. The training data for their empirical study includes cryptocurrency market prices and volumes, blockchain attributes, financial stock market information and global currency ratio. Their research presents a

promising result of anticipating the Bitcoin price time series and explaining the high volatility of the Bitcoin market. McNally *et al.* [59] assembled two different deep learning models to forecast Bitcoin price - with Recurrent Neural Network (RNN) and Long-Short Term Memory (LSTM) algorithm. Both models achieve about 50% accuracy in the simulations but the LSTM model has the capability to acknowledge the market dependencies in the long term period. Jourdan *et al.* [60] formulated a few conditional dependencies induced by the block design of the Bitcoin protocol, and propose a probabilistic graphical model to predict the value of UTXOs, which record the number of Bitcoins in each transaction.

Another direction in this research area is to improve the mining strategies and power efficiencies using machine learning approaches. Wang *et al.* [61] employed Reinforcement Learning algorithm to dynamically analyze the profits of different mining strategies and discover the optimal mining strategies over time-varying blockchain networks. Some researchers demonstrate that the Bitcoin Mining can be quantified as a Markov Decision Process (MDP), and different reinforcement learning algorithms can be applied to construct the MDP model [62, 63]. Other than that, Nguyen *et al.* [64] present a reinforcement learning-based offloading scheme that assists mobile miners to determine optimal offloading decisions, reduce energy consumption, and avoid network latency.

4.1.3 Transaction entity classification

The Bitcoin has become an alternative medium of value exchange. Behind the screens, some users have taken advantage of the Bitcoin network for their illegal purposes. With the CoinJoin mixing service, Bitcoin has been recognized as a safe currency in the dark net markets and it can also be used for money laundering. In this case, there is an urgent need to develop transaction and address tracing systems. Machine learning has been considered as a powerful tool to perform cryptocurrency address clustering and labeling for detecting illegal activities.

In 2017, Yin and Vatrapu [65] built several different classifiers using supervised machine learning models, to identify the Bitcoin addresses that are related to criminal activities. The next year, Harlev *et al.* [66] also introduced a supervised learning model with the gradient boosting algorithm. All those learning models can achieve accuracy of 75% in the simulation of the address clustering. Besides that, Akcora *et al.* [67] proposed an efficient and tractable framework called BitcoinHeist. By applying topological data analysis into the past records of transactions, BitcoinHeist can automate the prediction of new ransomware transactions in an address cluster, and detect new ransomware that has no past records.

4.2 Blockchain-enabled machine learning model

While machine learning systems have become powerful tools to solve real-world problems, people started to question its trustworthiness. First of all, machine learning systems might be susceptible to data poisoning attacks. The hackers might try to manipulate the system performance by altering the collected data or inserting constructed poison instances. Secondly, it is difficult for humans to understand decisions made by the machine learning systems if there is no traceable logs or training histories. Thirdly, centralized servers are still heavily required for completing the model training processes. Finally, the model construction stages are not automated and the human involvement may bring biases into the final system. Blockchains and smart contracts have shown great potential to solve those challenges.

4.2.1 Blockchain for data security

Blockchain is known for keeping data secure and safe. With reliable and traceable data stored on the blockchain, the researchers can ensure that machine learning algorithms will produce the most trusted and credible results. Muhammad *et al.* [68] introduced a federated learning system called Biscotti. Biscotti utilizes blockchain and cryptographic primitives to coordinate a privacy-preserving federated learning process between peering clients. While all the training iterations are stored in the blockchain, only the peer-verified updates are committed into the final model. The training data are stored with the data providers locally. This system is able to protect the privacy of an individual client's data as well as defend data poisoning attacks.

Mugunthan *et al.* [69] provided a privacy-preserving federated learning system called BlockFlow. The system incorporates differential privacy, introduces a novel auditing mechanism for model contribution, and uses smart contracts to incentivize positive behaviors. However, the system does not have the capability to detect any anomalies during the learning process. To address that issue, Desai *et al.* [70] came up with another blockchain-based federated learning framework called BlockFLA. After the learning algorithm is deployed, the BlockFLA framework utilizes smart contracts to automatically detect and discourage any backdoor attacks by holding the responsible parties accountable. Both frameworks ensure that the machine learning algorithms are resilient to malicious adversaries.

In 2018, Chen *et al.* [71] proposed a secure supervised machine learning system called LearningChain. In LearningChain, they developed a differential privacy mechanism for the local gradient computing process to protect the privacy of individual data providers, and a l-nearest aggregation scheme to defend against Byzantine attacks in the global gradient's aggregation process. In the next year, Kim *et al.* [72] pointed out that the LearningChain system has several limitations such as low computation efficiency, zero support on non-deterministic function computations, and weak privacy preservation. To revolve those issues in a systematic way, they developed an improved distributed machine learning model for permissioned blockchains. With a differentially private stochastic gradient descent method and an error-based aggregation rule as core primitives, their model provides better defences on the byzantine attacks and has the capability to handle the learning algorithm with non-deterministic functions defined. Besides that, Zhou [73] also introduced a similar system called PIRATE to provide distributed machine learning algorithms with byzantine-resiliency but the system is designed for 5G networks.

4.2.2 Blockchain for system improvement

Blockchains and smart contracts can also be utilized to improve the machine learning processes and eliminate human involvements. Ouyang *et al.* [74] implemented a novel federated learning collaboration framework: Learning Markets. In the Learning Markets, blockchain creates a trustless environment for collaboration and transaction. The learning task provider simply needs to publish the initial task to the markets and deposit the rewards in the network. The data providers and trainers participate in the learning process by depositing an entrance fee, uploading/downloading the data on IPFS network, and contributing their computation power. Several predefined smart contracts serve as network agents to maintain the collaboration relationships and market mechanisms.

Kim *et al.* [75] proposed an on-device blockchain-based Federated learning architecture called BlockFL. Data on user devices are processed locally and the local updates are accumulated on the blockchain. The global model updates are

calculated based on the user updates recorded on each block. Their architecture mainly focuses on the latency minimization and system scalability. They also indicate that the system may not be able to retrieve all the local model updates on time due to network delay or intermittent availability problems.

Muhammad *et al.* [76] gave a complete list of requirements for the blockchain enabled federated learning framework, including penalisation, decentralization, fine-grained Federated Learning, incentive mechanisms, trust, activity monitoring, heterogeneity and context-awareness, model synchronization, and communication and bandwidth-efficiency. They also introduce a term called reputation (which is similar to the Proof of Stake) and describe how this attribute works in their proposed framework.

Besides that, some researchers in this subsection work on designing new blockchain mechanisms for the distributed machine learning tasks. Felipe *et al.* [77] invented a new protocol called Proof-of-Learning, which achieves distributed consensus by ranking machine learning systems for a given machine learning task. The aim of this protocol is to mitigate the computational consumption in solving hashing-based puzzles and still ensure the data integrity. Toyoda *et al.* [78] improved the common incentive mechanism in the current blockchain network and make it more applicable to the blockchain network when the machine learning tasks are involved.

4.3 Combined research for real world scenarios

Instead of proposing innovative and theoretical designs, some researchers intend to figure out how this combined research can be applied on some real-world problems. Their contribution establishes a bridge between this new research area and the traditional industries such as transportation, hospital management, supply chain, etc.

4.3.1 Transportation

Pokhrel and Choi [79] developed a mathematical framework that adapts the blockchain-based federated learning design into the autonomous vehicle industry. They utilize the consensus mechanism and a renewal reward approach to enable on-vehicle machine learning training in the distributed network. The on-vehicle updates and global models are maintained in the blockchain, which are visible to and verifiable by every vehicle. Rewards are distributed to the vehicle owners based on the size of their updates accepted into the global model. They also discussed the limitations of this design and the performance of the system based on the simulations and numerical analysis.

Hua *et al.* [80] tried to apply federated learning algorithm into the heavy haul railway management. In their research, the train controls are quantified into multiple classes and the individual train data is applicable to the SVM based mixed kernel. The global model is administered by the smart contract. This research resolves the data island issue in this industry and the asynchronous collaborative learning algorithm is designed without involving a central server.

4.3.2 Healthcare

The healthcare industry has long been an early adopter of and benefited greatly from technological advances. Chen et al. in [81] proposed a blockchain based disease-classification framework called Health-Chain. In the Health-Chain system, multiple institutes can train the model with their patient records, collaborate

asynchronously in the blockchain network and contribute to the global model with privacy preserved. The researchers implement the system in two disease recognition tasks, breast cancer diagnosis and ECG arrhythmia classification, and both simulations demonstrate promising results.

Kumar *et al.* [82] proposed a similar but more elaborate supervised machine learning framework on detecting COVID-19 patients. The proposed framework can utilize up-to-date data which improves the recognition of CT images. Both researchers above mainly focus on building the machine learning models and the blockchain is used for enforcing the consensuses across research institutes and aggregating the training models.

Rahman *et al.* [83] gave a complete picture of how the blockchain can be employed in the Internet of Health Things (IoHT) area. In their framework, smart contracts are used to manage the training plan, trust management, participant authentication and the device data encryption. The framework design has high security and scalability level in the IoHT health management area.

4.3.3 Supply chain

Kamble *et al.* [84] built a prediction model using the machine learning technique to calculate an organization's probability of successful blockchain adoption (BA) within the supply chain industry. The researchers focus on explaining the intent of BA by using the psychological constructs from the literature on technology adoption. The learning model can help managers to predict the readiness of their organizations.

Mao *et al.* [85] developed a blockchain-based credit evaluation system to strengthen the efficiency of supervision and management in the food supply chain. The system collects credit evaluation from the traders on the blockchain, analyzes the evaluation directly via a deep learning network, and provides the credit results for the supervision and management of regulators.

Yong *et al.* [86] proposed a detailed" vaccine blockchain" system based on blockchain and machine learning technologies. The vaccine system is designed to support tracing the vaccine inventory and preventing supply record fraud. The machine learning model can also provide suggestions to the immunization practitioners and recipients.

5. Discussions and conclusion

5.1 Current threads in Blockchain research

Blockchain systems are designed to be distributed. Ironically, most blockchain networks are facing problems on centralization. For example, PoW mechanism relies on the success of mining mechanism. The higher the hashrate is, the more resilient the Bitcoin is against attacks. However, on the market side, mining a Bitcoin becomes increasingly harder. In order to gain more reward, miners share their hash power under a common mining pool. As shown in **Figure 5**, the top 4 mining pools currently contribute to more than 50% of the entire hash power.

In other words, if a hacker controls or manipulates the top4 mining pools, they might be able to perform 51% of the attacks. This is known as mining pool attacks. Besides directly controlling the mining pool, multiple variations of mining pool attacks have also been proposed. Selfish mining, for instance, refers to when miners who find the next block withhold the information and then release multiple valid blocks at once, resulting in other miners losing their block rewards and blocks.

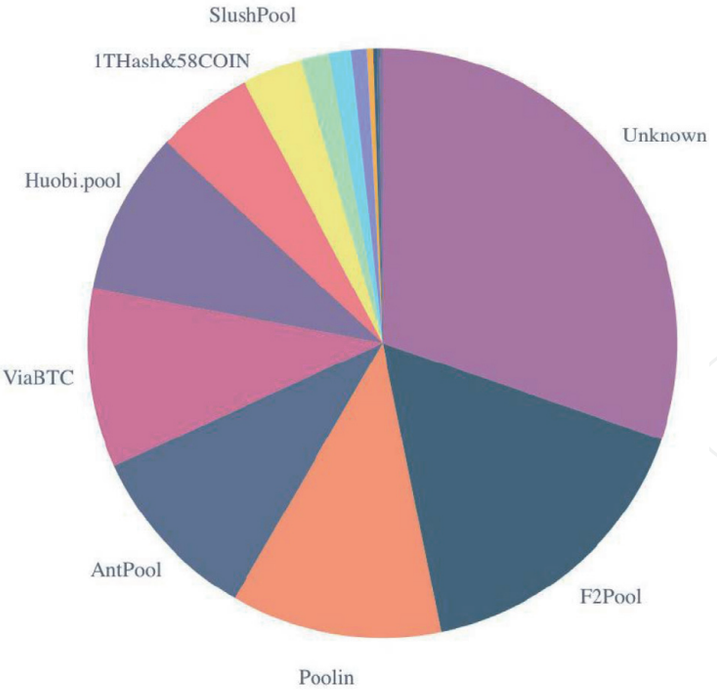

Figure 5.
Bitcoin Main Network Hashrate Distribution [87].

Many upgraded versions of mining pool attacks have been brought forth, such as Fork-after-Withhold (FAW) [88].

Ideally speaking, blockchain is resilient to Denial-of-Service Attack (DDoS) due to its distributed characteristics. However, the network layer is not completely decentralized. It includes routers, Internet Service Provider (ISP) for mining pools and cloud services. More than 60% of the Bitcoin nodes are hosted in less than 100 IP prefixes [89]. Such attacks on network layers are easier to perform and could have a larger impact on the entire blockchain network. *Hijacking Bitcoin: Routing Attacks on Cryptocurrencies* by Apostolaki *et al.* had talked about network layer attacks, partitioning attacks, and delay attacks [89].

5.2 Quantum computing

The existence and advancement of quantum computers will bring a massive change to our current technology industry, from cryptography [90], artificial intelligence [91] to computer architecture [92]. Nowadays, small to intermediate-scale quantum computers already exist in universities and industry laboratories (Noisy intermediate Scale quantum devices, often called NISQ [93]). Such noisy devices with about 50 qubits are promising to demonstrate quantum supremacy in the following years [94]. Quantum computers are devices using quantum phenomena such as superposition and entanglement to perform calculation. Quantum computers are believed to solve certain computational problems, such as integer factorization, substantially faster than traditional computers [94].

Blockchain security heavily relies on asymmetric encryption [90]. Besides, hash functions are commonly used by most blockchain networks in order to compress the content of all information. Both hash functions and asymmetric encryption are threatened by the evolution of quantum computers due to shor's algorithm [90], a polynomial-time solution to integer factorization problems invented by Peter Shor in 1994 [95]. Asymmetric encryption or public key encryption was designed based on elliptic curve cryptography (ECC) [90]. Quantum computers dominate ECDSA

(Elliptic Curve Digital Signature Algorithm), a secure and efficient tool used in Bitcoin systems [7]. Hence, a quantum resilient and high efficiency algorithm is needed for future Bitcoin/blockchain development [90].

Another algorithm that will bring a huge impact on blockchain is called Grover's algorithm. Grover's algorithm is a quantum computing algorithm that can quadratically speed up the unstructured search problem [96]. Furthermore, this algorithm has been used as a general trick or subroutine to obtain quadratic run time improvements for many other algorithms [97]. Firstly, grover's algorithm can be used to find collisions in hash functions, causing hash function to lose security. Secondly, Grover's algorithm can be used to accelerate mining because of its efficiency in searching for nonces, resulting in biasing in computational power and further recreating entire blockchains to manipulate the historical transactions [90].

Last but not least, to successfully implement Shor's algorithm, it will require more than 5,000 qubits to factor cryptographically significant numbers [98]. That is only without considering the error correction properties of quantum mechanisms. With error correction, the requirement may go up to as high as a million. In addition to the large number of qubits, it also requires hundreds of millions of gate operations [98]. This requirement is nearly impossible to achieve today, as Google's best quantum computer can only reach 54 qubits in 2019. Note that there are many approaches to build quantum computers; the qubits numbers referred to here is based on digitized adiabatic quantum computers with a superconducting circuit [99]. Another famous approach is using quantum annealing [100], led by D-Wave.

5.3 Conclusion

In this part, we reviewed and summarized the state-of-the-art research papers related to combining blockchain and AI in different scenarios. We provided a survey about how blockchain network could be integrated into the MEC technology. With security and privacy-preserving features, blockchain could be an effective solution to secure the aspects of data sharing and resources allocation in AI applications, especially for mobile edge intelligence. Besides, we introduced multiple research papers with respect to how machine learning and blockchain collaborate with each other. While machine learning can be utilized to improve network security and stability of blockchain, blockchain can also automate the model learning process and protect sensitive training data. We further discussed some threats that would challenge blockchain systems, including malicious attacks and quantum computing. Overall, this chapter demonstrates that Blockchain and AI researches are still at an early stage. Once all the bottlenecks and challenges in this combined research area are addressed, blockchain network could become a necessary and important platform to enable and improve AI applications across different industries.

Acknowledgements

This work was supported by Blockchain@UBC and Natural Sciences and Engineering Research Council of Canada (CREATE Program grant 528125).

DOI: http://dx.doi.org/10.5772/intechopen.96618

Author details

Yao Du†, Shuxiao Miao†, Zitian Tong†, Victoria Lemieux and Zehua Wang*
Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver, BC, Canada

*Address all correspondence to: zwang@ece.ubc.ca

† These authors contributed equally.

References

[1] Jameel F, Javaid U, Khan WU, Aman MN, Pervaiz H, Jantti R. Reinforcement Learning in Blockchain-Enabled IIoT Networks: A Survey of Recent Advances and Open Challenges. Sustainability. 2020;12(12):5161.

[2] Patel M, Naughton B, Chan C, Sprecher N, Abeta S, Neal A, et al. Mobile-edge computing introductory technical white paper. White paper, mobile-edge computing (MEC) industry initiative. 2014;29:854–864.

[3] Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Privacy-Preserved Task Offloading in Mobile Blockchain With Deep Reinforcement Learning. IEEE Transactions on Network and Service Management. 2020;17(4):2536–2549.

[4] Xiong Z, Zhang Y, Niyato D, Wang P, Han Z. When Mobile Blockchain Meets Edge Computing. IEEE Communications Magazine. 2018; 56(8):33–39.

[5] Conti M, Sandeep Kumar E, Lal C, Ruj S. A Survey on Security and Privacy Issues of Bitcoin. IEEE Communications Surveys Tutorials. 2018;20(4):3416–3452.

[6] Worrall E. Study: Bitcoin Mining Could Push Global Warming Over the 2C Threshold; 2018. Copyright - Copyright Newstex Oct 29, 2018; Last updated - 2019-07-08.

[7] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. bitcoin.org; 2008.

[8] Ferdous MS, Chowdhury MJM, Hoque MA, Colman A. Blockchain Consensus Algorithms: A Survey; 2020.

[9] Tseng L. Recent Results on Fault-Tolerant Consensus in Message-Passing Networks; 2016.

[10] Lamport L, Shostak R, Pease M. The Byzantine Generals Problem. ACM transactions on programming languages and systems. 1982;4(3):382–401.

[11] Gupta KD, Rahman A, Poudyal S, Huda MN, Mahmud MAP. A Hybrid POW-POS Implementation Against 51 percent Attack in Cryptocurrency System. In: 2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom); 2019. p. 396–403.

[12] Küfeoğlu S, Özkuran M. Bitcoin mining: A global review of energy and power demand. Energy research social science. 2019;58:101273.

[13] Wang YZ, Wu J, Chen SH, Chao MC, Yang CH. Micro-Architecture Optimization for Low-Power Bitcoin Mining ASICs. IEEE; 2019. p. 1–4.

[14] Saleh F. Blockchain without Waste: Proof-of-Stake. The Review of financial studies. 2020.

[15] King S, Nadal S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake; 2012.

[16] Lepore C, Ceria M, Visconti A, Rao UP, Shah KA, Zanolini L. A Survey on Blockchain Consensus with a Performance Comparison of PoW, PoS and Pure PoS. Mathematics (Basel). 2020;8(1782):1782.

[17] Reijsbergen D, Szalachowski P, Ke J, Li Z, Zhou J. LaKSA: A Probabilistic Proof-of-Stake Protocol; 2021.

[18] Mistry I, Tanwar S, Tyagi S, Kumar N. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. Mechanical systems and signal processing. 2020;135:106382.

[19] Yazdinejad A, Srivastava G, Parizi RM, Dehghantanha A, Karimipour H, Karizno SR. SLPoW: Secure and Low Latency Proof of Work Protocol for Blockchain in Green IoT Networks. In: 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring); 2020. p. 1–5.

[20] Varga P, Peto J, Franko A, Balla D, Haja D, Janky F, et al. 5G support for Industrial IoT Applications - Challenges, Solutions, and Research gaps. Sensors (Basel, Switzerland). 2020;20(3):828.

[21] Fan K, Ren Y, Wang Y, Li H, Yang Y. Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G. IET communications. 2018;12(5): 527–532.

[22] in Media BBSL, Communications, Lecturer DB. Netflix's The Social Dilemma highlights the problem with social media, but what's the solution?; 2020. Available from: https://theconversation.com.

[23] Podgorelec B, Kersic V, Turkanovic M. Analysis of Fault Tolerance in Permissioned Blockchain Networks. IEEE; 2019. p. 1–6.

[24] Goldwasser S, Micali S, Rackoff C. The Knowledge Complexity of Interactive Proof Systems. SIAM Journal on Computing. 1989 02;18(1):186–23. Copyright - Copyright] © 1989 Society for Industrial and Applied Mathematics; Last updated - 2012-02-05.

[25] D RR, Adam S, Katerina S. Toward Non-interactive Zero-Knowledge Proofs for NP from LWE. Journal of cryptology. 2021;34(1).

[26] Kumar A, Fischer C, Tople S, Saxena P. In: A Traceability Analysis of Monero's Blockchain. Cham: Springer International Publishing; 2017. p. 153–173.

[27] hour ago Major Russian Bank Sberbank Files Application to Launch Its Own Stablecoin — Possibly Pegged to the Fiat Ruble ALTCOINS — 20 hours ago PCMASEWSBMPA, to be a Digital Bank in Gibraltar Biden Administration Reported to Be Lining up a Former Ripple Advisor as the Next Bank Regulator Bitcoin Near 'Extreme Bubble' but Tesla More Vulnerable: Deutsche Bank Survey Russia Prohibits Government Officials From Owning Crypto CCXS. Not So Private: 99% of Zcash and Dash Transactions Traceable, Says Chainalysis – Altcoins Bitcoin News; 2020. Available from: https://news.bitcoin.com/.

[28] Abbas N, Zhang Y, Taherkordi A, Skeie T. Mobile Edge Computing: A Survey. IEEE Internet of Things Journal. 2018 Feb;5(1):450–465.

[29] Xiao L, Ding Y, Jiang D, Huang J, Wang D, Li J, et al. A Reinforcement Learning and Blockchain-Based Trust Mechanism for Edge Networks. IEEE Transactions on Communications. 2020; 68(9):5460–5470.

[30] Seng S, Li X, Luo C, Ji H, Zhang H. A D2D-assisted MEC Computation Offloading in the Blockchain-Based Framework for UDNs. In: ICC 2019–2019 IEEE International Conference on Communications (ICC). New York: IEEE; 2019. .

[31] Liu M, Yu FR, Teng Y, Leung VCM, Song M. Joint Computation Offloading and Content Caching for Wireless Blockchain Networks. In: IEEE Infocom 2018 - IEEE Conference on Computer Communications Workshops (infocom Wkshps). New York: IEEE; 2018. p. 517–522.

[32] Liu M, Yu FR, Teng Y, Leung VCM, Song M. Computation Offloading and Content Caching in Wireless Blockchain Networks With Mobile Edge Computing. IEEE Transactions on

Vehicular Technology. 2018;67(11): 11008–11021.

[33] Liu M, Yu FR, Teng Y, Leung VCM, Song M. Distributed Resource Allocation in Blockchain-Based Video Streaming Systems With Mobile Edge Computing. IEEE Transactions on Wireless Communications. 2019;18(1): 695–708.

[34] Feng J, Yu FR, Pei Q, Chu X, Du J, Zhu L. Cooperative Computation Offloading and Resource Allocation for Blockchain-Enabled Mobile-Edge Computing: A Deep Reinforcement Learning Approach. IEEE Internet of Things Journal. 2020;7(7):6214–6228.

[35] Zhang Z, Hong Z, Chen W, Zheng Z, Chen X. Joint Computation Offloading and Coin Loaning for Blockchain-Empowered Mobile-Edge Computing. IEEE Internet of Things Journal. 2019;6(6):9934–9950.

[36] Liu W, Cao B, Zhang L, Peng M, Daneshmand M. A Distributed Game Theoretic Approach for Blockchain-based Offloading Strategy. In: ICC 2020–2020 IEEE International Conference on Communications (ICC); 2020. p. 1–6.

[37] Hassija V, Chamola V, Gupta V, Chalapathi GSS. A Blockchain based Framework for Secure Data Offloading in Tactile Internet Environment. In: 2020 International Wireless Communications and Mobile Computing (IWCMC); 2020. p. 1836–1841.

[38] Zhang S, Lee J. A Group Signature and Authentication Scheme for Blockchain-Based Mobile-Edge Computing. IEEE Internet of Things Journal. 2020 May;7(5):4557–4565.

[39] Rahman MA, Hossain MS, Islam MS, Alrajeh NA, Muhammad G. Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach. IEEE ACCESS. 2020;8:205071–205087.

[40] Kang J, Yu R, Huang X, Wu M, Maharjan S, Xie S, et al. Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks. IEEE Internet of Things Journal. 2019 Jun;6(3):4660–4670.

[41] Lu Y, Huang X, Dai Y, Maharjan S, Zhang Y. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. IEEE Transactions on Industrial Informatics. 2019;16(6):4177–4186.

[42] Islam A, Shin SY. BUAV: A Blockchain Based Secure UAV-Assisted Data Acquisition Scheme in Internet of Things. Journal of Communications and Networks. 2019;21(5):491–502.

[43] Zhang W, Lu Q, Yu Q, Li Z, Liu Y, Lo SK, et al. Blockchain-based Federated Learning for Device Failure Detection in Industrial IoT. IEEE Internet of Things Journal. 2020.

[44] Zyskind G, Nathan O, Pentland A. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In: 2015 IEEE Security and Privacy Workshops; 2015. p. 180–184.

[45] Yang H, Liang Y, Yuan J, Yao Q, Yu A, Zhang J. Distributed Blockchain-Based Trusted Multidomain Collaboration for Mobile Edge Computing in 5G and Beyond. IEEE Transactions on Industrial Informatics. 2020;16(11):7094–7104.

[46] Arachchige PCM, Bertok P, Khalil I, Liu D, Camtepe S, Atiquzzaman M. A Trustworthy Privacy Preserving Framework for Machine Learning in Industrial IoT Systems. IEEE Transactions on Industrial Informatics. 2020 Sep;16(9):6092–6102.

[47] Lin X, Wu J, Bashir AK, Li J, Yang W, Piran J. Blockchain-Based

Incentive Energy-Knowledge Trading in IoT: Joint Power Transfer and AI Design. IEEE Internet of Things Journal. 2020:1–14.

[48] Fan S, Zhang H, Zeng Y, Cai W. Hybrid Blockchain-Based Resource Trading System for Federated Learning in Edge Computing. IEEE Internet of Things Journal. 2020.

[49] Liu Y, Yu FR, Li X, Ji H, Leung VCM. Resource Allocation for Video Transcoding and Delivery Based on Mobile Edge Computing and Blockchain. In: 2018 IEEE Global Communications Conference (GLOBECOM); 2018. p. 1–6.

[50] Zhang R, Yu FR, Liu J, Huang T, Liu Y. Deep Reinforcement Learning (DRL)-Based Device-to-Device (D2D) Caching With Blockchain and Mobile Edge Computing. IEEE Transactions on Wireless Communications. 2020;19(10): 6469–6485.

[51] Somy NB, Kannan K, Arya V, Hans S, Singh A, Lohia P, et al. Ownership Preserving AI Market Places Using Blockchain. In: 2019 IEEE International Conference on Blockchain (Blockchain); 2019. p. 156–165.

[52] Chen H, Pendleton M, Njilla L, Xu S. A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses. ACM Comput Surv. 2020 Jun;53(3).

[53] Scicchitano F, Liguori A, Guarascio M, Ritacco E, Manco G. A Deep Learning Approach for Detecting Security Attacks on Blockchain; 2020. .

[54] Dey S. Securing Majority-Attack in Blockchain Using Machine Learning and Algorithmic Game Theory: A Proof of Work. In: 2018 10th Computer Science and Electronic Engineering (CEEC); 2018. p. 7–10.

[55] Hou C, Zhou M, Ji Y, Daian P, Tramer F, Fanti G, et al.. SquirRL: Automating Attack Analysis on Blockchain Incentive Mechanisms with Deep Reinforcement Learning; 2020.

[56] Kim YB, Kim JG, Kim W, Im JH, Kim TH, Kang SJ, et al. Predicting Fluctuations in Cryptocurrency Transactions Based on User Comments and Replies. PLOS ONE. 2016 08;11(8): 1–17.

[57] Madan I. Automated Bitcoin Trading via Machine Learning Algorithms; 2014. .

[58] Jang H, Lee J. An Empirical Study on Modeling and Prediction of Bitcoin Prices With Bayesian Neural Networks Based on Blockchain Information. IEEE Access. 2018;6:5427–5437.

[59] McNally S, Roche J, Caton S. Predicting the Price of Bitcoin Using Machine Learning. In: 2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP); 2018. p. 339–343.

[60] Jourdan M, Blandin S, Wynter L, Deshpande P. A Probabilistic Model of the Bitcoin Blockchain. In: 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW); 2019. p. 2784–2792.

[61] Wang T, Liew SC, Zhang S. When Blockchain Meets AI: Optimal Mining Strategy Achieved By Machine Learning. CoRR. 2019;abs/1911.12942.

[62] Eyal I, Sirer EG. Majority is not Enough: Bitcoin Mining is Vulnerable. CoRR. 2013;abs/1311.0243. Available from: http://arxiv.org/abs/1311.0243.

[63] Sapirshtein A, Sompolinsky Y, Zohar A. Optimal Selfish Mining Strategies in Bitcoin. CoRR. 2015;abs/1507.06183. Available from: http://arxiv.org/abs/1507.06183.

[64] Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Privacy-Preserved Task

Offloading in Mobile Blockchain With Deep Reinforcement Learning. IEEE Transactions on Network and Service Management. 2020 Dec;17(4):2536–2549.

[65] Sun Yin H, Vatrapu R. A first estimation of the proportion of cybercriminal entities in the bitcoin ecosystem using supervised machine learning. In: 2017 IEEE International Conference on Big Data (Big Data); 2017. p. 3690–3699.

[66] Harlev MA, Yin H, Langenheldt KC, Mukkamala R, Vatrapu R. Breaking Bad: De-Anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning. In: HICSS; 2018.

[67] Akcora CG, Li Y, Gel YR, Kantarcioglu M. BitcoinHeist: Topological Data Analysis for Ransomware Prediction on the Bitcoin Blockchain. In: Bessiere C, editor. Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence, IJCAI-20. International Joint Conferences on Artificial Intelligence Organization; 2020. p. 4439–4445. Special Track on AI in FinTech.

[68] Shayan M, Fung C, Yoon CJM, Beschastnikh I. Biscotti: A Ledger for Private and Secure Peer-to-Peer Machine Learning. CoRR. 2018;abs/1811.09904. Available from: http://arxiv.org/abs/1811.09904.

[69] Mugunthan V, Rahman R, Kagal L. BlockFLow: An Accountable and Privacy-Preserving Solution for Federated Learning; 2020.

[70] Desai HB, Ozdayi MS, Kantarcioglu M. BlockFLA: Accountable Federated Learning via Hybrid Blockchain Architecture; 2020.

[71] Chen X, Ji J, Luo C, Liao W, Li P. When Machine Learning Meets Blockchain: A Decentralized, Privacy-preserving and Secure Design. In: 2018 IEEE International Conference on Big Data (Big Data); 2018. p. 1178–1187.

[72] Kim H, Kim S, Hwang JY, Seo C. Efficient Privacy-Preserving Machine Learning for Blockchain Network. IEEE Access. 2019;7:136481–136495.

[73] Zhou S, Huang H, Chen W, Zheng Z, Guo S. PIRATE: A Blockchain-based Secure Framework of Distributed Machine Learning in 5G Networks. CoRR. 2019;abs/1912.07860. Available from: http://arxiv.org/abs/1912.07860.

[74] Ouyang L, Yuan Y, Wang FY. Learning Markets: An AI Collaboration Framework Based on Blockchain and Smart Contracts. IEEE Internet of Things Journal. 2020.

[75] Kim H, Park J, Bennis M, Kim S. Blockchained On-Device Federated Learning. IEEE Communications Letters. 2020;24(6):1279–1283.

[76] ur Rehman MH, Salah K, Damiani E, Svetinovic D. Towards Blockchain-Based Reputation-Aware Federated Learning. In: IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS); 2020. p. 183–188.

[77] Bravo-Marquez F, Reeves S, Ugarte M. Proof-of-Learning: A Blockchain Consensus Mechanism Based on Machine Learning Competitions. In: 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON); 2019. p. 119–124.

[78] Toyoda K, Zhang AN. Mechanism Design for An Incentive-aware Blockchain-enabled Federated Learning Platform. In: 2019 IEEE International Conference on Big Data (Big Data); 2019. p. 395–403.

[79] Pokhrel SR, Choi J. Federated Learning With Blockchain for

Autonomous Vehicles: Analysis and Design Challenges. IEEE Transactions on Communications. 2020;68(8):4734–4746.

[80] Hua G, Zhu L, Wu J, Shen C, Zhou L, Lin Q. Blockchain-Based Federated Learning for Intelligent Control in Heavy Haul Railway. IEEE Access. 2020;8:176830–176839.

[81] 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. p. 5469–5473.

[82] Kumar R, Khan AA, Zhang S, Kumar J, Yang T, Golalirz NA, et al.. Blockchain-Federated-Learning and Deep Learning Models for COVID-19 detection using CT Imaging; 2020.

[83] Rahman MA, Hossain MS, Islam MS, Alrajeh NA, Muhammad G. Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach. IEEE Access. 2020; 8:205071–205087.

[84] Kamble S, Gunasekaran A, Kumar V, Belhadi A, Foropon C. A machine learning based approach for predicting blockchain adoption in supply Chain. Technological Forecasting and Social Change. 2020 11.

[85] Mao D, Wang F, Hao Z, Li H. Credit Evaluation System Based on Blockchain for Multiple Stakeholders in the Food Supply Chain. International Journal of Environmental Research and Public Health. 2018 08;15:1627.

[86] Yong B, Shen J, Liu X, Li F, Chen H, Zhou Q. An intelligent blockchain-based system for safe vaccine supply and supervision. International Journal of Information Management. 2020;52: 102024. Available from: http://www.sciencedirect.com/science/article/pii/S0268401219304505.

[87] blockchain com. Hashrate Distribution: An estimation of hashrate distribution amongst the largest mining pools; 2021. https://www.blockchain.com/pools.

[88] Kwon Y, Kim D, Son Y, Vasserman E, Kim Y. Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin. 2017.

[89] Apostolaki M, Zohar A, Vanbever L. Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. IEEE; 2017. p. 375–392.

[90] Fernández-Caramès TM, Fraga-Lamas P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. IEEE Access. 2020; 8:21091–21116.

[91] Choi J, Oh S, Kim J. The Useful Quantum Computing Techniques for Artificial Intelligence Engineers. In: 2020 International Conference on Information Networking (ICOIN); 2020. p. 1–3.

[92] Riesebos L, Fu X, Moueddenne AA, Lao L, Varsamopoulos S, Ashraf I, et al. Quantum Accelerated Computer Architectures. In: 2019 IEEE International Symposium on Circuits and Systems (ISCAS); 2019. p. 1–4.

[93] Tanimoto T, Matsuo S, Kawakami S, Tabuchi Y, Hirokawa M, Inoue K. How Many Trials Do We Need for Reliable NISQ Computing? In: 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI); 2020. p. 288–290.

[94] Arute F, Arya K, Babbush R, Bacon D, Bardin J, Barends R, et al. Quantum supremacy using a programmable superconducting processor. Nature. 2019 10;574:505–510.

[95] Shor PW. Polynomial-Time Algorithms for Prime Factorization and

Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing. 1997 Oct;26(5):1484–1509.

[96] Grover L. Fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on the Theory of Computing. 1996 06.

[97] Team TQ. Grover's Algorithm. Data 100 at UC Berkeley; 2021. Available from: https://qiskit.org/textbook/ch-algorithms/grover.html.

[98] Guerreschi GG, Matsuura AY. QAOA for Max-Cut requires hundreds of qubits for quantum speed-up. Scientific Reports. 2019 May;9(1).

[99] Barends R, Shabani A, Lamata L, Kelly J, Mezzacapo A, Heras UL, et al. Digitized adiabatic quantum computing with a superconducting circuit. Nature. 2016 Jun;534(7606):222–226.

[100] DE FALCO D, TAMASCELLI D. AN INTRODUCTION TO QUANTUM ANNEALING. vol. 45. Les Ulis: EDP Sciences; 2011. p. 99–116.