Application of Blockchain Based on Deep Learning Algorithm in Enterprise Internet of Things System

Liang Guo

Department of Mathematics and Information Engineering, Liaocheng University Dongchang College, Shandong, Liaocheng 252000, China

Correspondence should be addressed to Liang Guo; 20140131@nxmu.edu.cn

Received 7 July 2022; Revised 28 July 2022; Accepted 12 August 2022; Published 30 August 2022

1. Introduction

Scientific and technological progress is the power source of social and economic development, and it is also the main development goal. In recent years, with the continuous progress of Internet technology in China, the application of new technologies has brought new opportunities and challenges to all fields of economic development [1]. Artificial intelligence based on deep learning can quickly process a large amount of information, and even partially replace artificial intelligence for intelligent prediction and decision-making, so as to effectively improve the efficiency of transaction processing, so as to achieve economies of scale [2]. In recent decades, terminal intelligence, communication technology, cloud computing, and big data technology have developed rapidly. Affected by the above technologies, Internet of Things technology has developed rapidly in the fields of smart home, smart city, and autonomous driving [3, 4]. At present, the number of Internet of Things terminals entering the network continues to grow. Cloud computing is limited by network bandwidth, delay, and other factors, and there are still many deficiencies in the data processing of edge nodes. At the same time, the consumer-oriented Internet of Things is developing rapidly, and its demand for IoT terminals and applications is growing. Driven by internal and external factors, edge computing is developing rapidly [5]. Blockchain has the characteristics of distributed data storage, point-to-point transmission, consensus mechanism, encryption algorithm, and smart contract. It is a new kind of distributed infrastructure. The blockchain structure facilitates the storage and tracking of data. In order to ensure
the consistency of network data in a distributed environment, the blockchain uses a deep learning algorithm to generate block update registers [6]. Modern cryptographic technology ensures the security of blockchain data sending and storage. Using smart contracts to write automated scripts can build distributed applications. Blockchain adopts distributed consensus to maintain all system data at the same time, so as to effectively resist malicious attacks. Therefore, blockchain technology can help the enterprise Internet of Things system build a safe and reliable network environment [7]. The technical characteristics of blockchain technology, such as decentralization, data invariance, traceability, public-private key signature, and smart contract, naturally meet the needs of enterprise Internet of Things systems, and it is hoped to break through the reliance on third-party systems, so as to reduce transaction costs and improve operation efficiency [8]. The progress of Internet information technology such as blockchain has played an important role in promoting the innovation of enterprise Internet of Things system, providing new ideas for truly solving the pain points of the development of the real economy, and effectively optimizing the development and innovation methods of system applications [9].

2. Related Work

The literature believes that public chain is the original concept of blockchain technology, which means that everyone can participate in it. Compared with traditional trading systems, using public chain can save transaction costs and liberate productivity in data mining and data sharing. The literature believes that the smart contract designed based on blockchain technology has the characteristics of automatic execution [10]. If the smart contract is executed, the code hash value and digital signature will be copied into the smart contract at the same time, so the accuracy of contract execution can be improved. Blockchain is a technology that does not need to rely on intermediaries to reach a credit consensus [11]. Decentralization is the main feature of blockchain. Literature studies have found that the main reasons for the high cost of remittances in Africa are imperfect payment systems and poor market information. It is proposed to use blockchain technology to build a system without financial intermediary participation, such as bitcoin, to reduce costs and increase efficiency [12]. The literature combs the academic research on the consensus mechanism and compares the blockchain consensus mechanism with traditional technologies. The application of blockchain technology such as decentralization, tamper resistance, consensus mechanism, and smart contract seems to be a perfect solution, but this is not the case [13, 14]. The weakness of the pow algorithm and uncertain potential security limitations are pointed out in the literature. At present, the research on the application value of blockchain technology is more theoretical and lacks quantitative or empirical research and analysis, but these theories provide direction for the application of blockchain technology and lay the foundation for further research [15]. We need to seek the results of using blockchain technology in various disciplines, including computer, economic, and social research [16]. A multilevel secure Internet of Things model based on blockchain is proposed in the literature. According to the model description, the Internet of Things system is composed of two layers: the edge layer and the top layer above the edge layer. The definition of the edge layer is a local area network, which is composed of multiple devices under the control of a central node [17]. The edge layer node maintains a NoSQL database to store edge layer object information, including UUID, identity information, status dataset, function set, and format document. There is no central node at the top level, so each data node is independent and self-managed. The data exchange between nodes is recorded in the blockchain registers maintained by all nodes. Blockchain consensus algorithms have different choices. This mode ensures the security of the Internet of Things deployed in the wide area environment, but this scheme increases the cost of the whole network and requires a lot of time and resources to maintain the smart contract [18]. In order to solve the security problem of the industrial Internet of Things, the literature has designed an integrated identity management system based on blockchain and implemented the access control mechanism by using edge computing [19]. The system uses lightweight self-authentication password to detect the registration and authentication of network entities [20]. Each entity in the system has an identity, and each identity corresponds to a unique implicit certificate. Identity information and certificates are stored in the blockchain network to ensure that they are not deleted or tampered with. The literature uses convolutional neural network (CNN) technology to provide a wide range of video data storage and real-time monitoring [21]. Compared with the traditional video surveillance system, this system has many technical advantages, and there is still room for improvement in data access control and large-scale testing.

3. Analysis of Blockchain Technology Based on Deep Learning Algorithm

3.1. Principle and Model of Deep Learning Algorithm. Deep learning is one of the key technologies in the outbreak of artificial intelligence. It has made progress in the field of computer vision and natural language processing, which has brought AI technology into a new stage of explosive development. The wide and deep model consists of wide components and deep components. Its frame structure is shown in Figure 1.

It can be seen from Figure 1 that the wide component is a generalized linear model, and its shape is shown in the following formula:

\[ y = W^T [x, \Phi(x)] + b, \]  

where \( x \) is the original feature, \( \Phi(x) \) is the cross-product feature, \( b \) is the default polarization value, and \( W \) is the weight parameter.

Deep neural network is a part of deep. The neural network first learns low dimensional dense embeddings for the feature vector and then uses the original dense feature as
the input of the network. The calculation of each hidden layer is shown in the following formula:

\[
a^{(l+1)} = f(W^{l}a^{l} + b^{l}),
\]

where \(a^{l}, W^{l}, \) and \(b^{l}\) represent the activation, weight, and polarization values of the first layer of the hidden layer, respectively, and \(f\) represents the activation function. The loss function is logistic loss. At this time, the prediction result of the wide and deep model is shown in the following formula:

\[
p(y = 1 \mid x) = \sigma(w_{\text{wide}}^{T}[x, \Phi(x)] + w_{\text{deep}}^{T}a^{T} + b),
\]

where \(\sigma\) represents sigmoid function, \(\Phi(x)\) represents the cross-product function, and \(a^{T}\) represents the activation value of the last layer.

Wide and deep is a common type of training, and joint training is different from integrated training. In integrated training, each model is trained separately, and the results are combined after training. Compared with joint training, integrated training requires that each part of the training be trained independently and summarized only when certain requirements are met, so the size of the model is larger. The wide component of joint training only uses a small part of the training sample set as the training set and uses its eigenvector to carry out product crossover to make up for the memory defects of deep components.

3.2. Blockchain Data Structure. Since its inception in 2008, blockchain technology has been regarded as a technology for sharing data between untrusted parties. A common form of blockchain is chain blockchain. This blockchain structure is the basis of different blockchain structures and the common feature of other blockchains. Blockchain is composed of interrelated block records. The order of blocks corresponds to the order of time stamps stored internally, as shown in Figure 2.
3.3. Hash Algorithm Design of Blockchain. Hash algorithm is an important technology in the field of information technology, which is widely used in blockchain. After binary data of any length is mapped to the hash function, it is converted to fixed-length output, and the output value is the hash value of the data. There are many hash functions, and the hash algorithm is the most widely used in blockchain technology. Using this algorithm, binary data of any length can be converted into hash values of 256 bits and 32 bytes. The hash algorithm has the advantages of unidirectional, random, timing, fixed length, and so on.

(1) Unidirectionality: the output data can be easily extracted from the input data, but the input data cannot be calculated from the output data.

(2) Randomness: even if the input data is only slightly modified, the output data may change greatly, so different input data will not produce the same hash value.

(3) Timing: any input data with different lengths will consume approximately the same time period through the same type of hash calculation.

(4) Fixed length: any input data with different lengths can generate output data with the same length after the hash calculation of the same type.

Hash function is usually defined according to the generated hash value. There are two main methods. Hash based on addition and multiplication is achieved by returning data elements and then adding each initial value associated with the data elements. Usually, the value of an element is multiplied by a prime number.

The following formulas provide a hash calculation method based on addition and multiplication:

\[ h(m) = h^{-1}(m \oplus p), \]
\[ h(m) = \sum_{i=0}^{m} m_i \otimes p_i, \]
\[ h(m) = h^{-1} \otimes (m \oplus p), \]
\[ h(m) = \prod_{i=0}^{m} m_i \otimes p_i. \]

Like additive hashing, shift-based hashing also uses each element of the data string, but unlike additive hashing, shift-based hashing algorithms prefer to transmit data. It is usually a combination of left and right transfer operations, and the number of transfers is the quality. The result of each shift is only some additional aggregation operations, and the final result of shift calculation is the final result of change hash calculation. The formula of the shift hash algorithm is shown in the following formulas:

\[ h(m) = h^{-1} \otimes (m \ll q), \]
\[ h(m) = \sum_{i=0}^{m} (m_i \ll p_i) \otimes (m_i \gg q_i), \]
\[ h(m) = \prod_{i=0}^{m} (m_i \ll p_i) \otimes (m_i \gg q_i). \]

Merkel is a binary hash tree. In the Merkel tree, each leaf node is the hash value of a transaction. This article takes the Merkel tree with only four leaves as an example.
Table 1: Comparison of common consensus algorithms.

<table>
<thead>
<tr>
<th>Feature</th>
<th>PoS</th>
<th>PoW</th>
<th>DPoS</th>
<th>PBFT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction throughput</td>
<td>General</td>
<td>Low</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Fault tolerance</td>
<td>&lt;50%</td>
<td>&lt;50%</td>
<td>&lt;50%</td>
<td>&lt;33%</td>
</tr>
<tr>
<td>Single transaction speed</td>
<td>min 10</td>
<td>min s</td>
<td>ms</td>
<td></td>
</tr>
<tr>
<td>Number of supported nodes</td>
<td>Many</td>
<td>Many</td>
<td>Many</td>
<td>Less</td>
</tr>
<tr>
<td>Byzantine fault tolerance</td>
<td>Support</td>
<td>Support</td>
<td>Support</td>
<td>Support</td>
</tr>
<tr>
<td>Computing resource consumption</td>
<td>General</td>
<td>High</td>
<td>General</td>
<td>Low</td>
</tr>
<tr>
<td>Network resource consumption</td>
<td>General</td>
<td>Lower</td>
<td>General</td>
<td>High</td>
</tr>
</tbody>
</table>

1. Use the sha256 hash algorithm twice to calculate the hash value of each transaction and calculate the hash value of each transaction. Here, four hash values of $H_A$, $H_B$, $H_C$, and $H_D$ can be calculated, that is, the four-leaf nodes of the Merkel tree. article paper takes $H_A$ calculation as an example:

$$H_A = SHA256(SHA256("trade"A)).$$ (11)

2. Combine the hash values of two leaf nodes $H_A$ and $H_B$. This article takes $H_{AB}$ calculation as an example:

$$H_{AB} = SHA256(SHA256 (H_A + H_B)).$$ (12)

3. Perform the same combined hash calculation as in step (2) on the existing two hash values $H_{AB}$ and $H_{CD}$, and finally, get a new hash value $H_{ABCD}$. The calculation of $H_{ABCD}$ is as follows:

$$H_{ABCD} = SHA256(SHA256(H_{AB} + H_{CD})).$$ (13)

At present, the workload proof mechanism is considered to be the most efficient blockchain consensus algorithm, but it takes a long time to reach a consensus, which will consume a lot of computing power and resources, so it is not suitable for large-scale promotion and application. The characteristics of various consensus algorithms widely used in blockchain are shown in Table 1.

There are four private nodes in the experimental system chain. Each node needs real-time data sharing, with high data rate and low hardware computing power. Through comprehensive analysis, the PBFT consensus algorithm is the most suitable for this experimental system, so it is selected as the private chain consensus algorithm of this system to build the private chain of this system.

4. Architecture Design of Enterprise Internet of Things Based on Related Technologies

4.1. System Architecture. This article proposes a distributed Internet of Things system based on blockchain technology and edge computing, which is composed of a device layer, an edge layer, and an application layer. The device layer is composed of various intelligent and nonintelligent IoT terminals, forming a distributed IoT database. The edge layer is composed of multiple edge computing servers, and blockchain is used as the network infrastructure to connect each node of the edge computing server. After the data collected from the device is processed by the edge layer computing framework, part of the data is processed by the edge server and returned to the terminal device for local service closed-loop, and the other part of the data is uploaded to the application layer cloud computing center as the basic data of the top-level application. The application layer is equivalent to the cloud computing hub of the traditional Internet of things architecture, and responsible for the design of top-level business logic and application deployment. The overall architecture of the enterprise Internet of Things system based on blockchain and deep learning technology is shown in Figure 4.

4.2. Equipment Level Design. The IoT terminal at the device level is a bridge connecting the physical world and cyberspace. Terminal devices detect changes in the world's physical environment and digitally transmit analog data to higher-level IoT applications. According to the intelligent degree of terminal equipment, it can be divided into intelligent equipment and limited resource equipment. Intelligent devices have specific computing and storage capabilities, and can perform preprocessing, encryption, data transmission, and other functions independently. On the other hand, equipment with limited resources can only recognize and collect environmental data and convert analog signals into digital signals. In the distributed Internet of Things, we roughly divide IoT terminals into two types of devices: acquisition devices and execution devices. The collection equipment is the producer of data, and the execution equipment is the consumer of data. Therefore, the terminal device can be a collection device, an execution device, or have two identities at the same time. The terminal is connected to the adjacent edge computing server through NB-IoT, Lora, WiFi, NFC, and other communication protocols.

4.3. Edge Layer Design. Edge computing servers are all over the Internet of Things. To meet the requirements of internal data security processing, we have implemented Edge X Foundry computing framework, Hyperledger Fabric blockchain, and trusted platform deployment based on microservice architecture.

As an excellent open-source edge computing framework, Edge X Foundry provides device services for device-level terminals through a variety of communication protocols. Users can write Edge X Foundry control commands to manage their devices, and their devices send their production data through the restful API. Edge X Foundry publishes data to edge or cloud applications for further processing according to certain rules. Edge X Foundry is based on the microservice architecture. Each microservice is logically independent and functionally decoupled. The core service layer of Edge X Foundry is divided into an equipment service layer, a basic service layer, a support service layer, and an export service layer. To ensure the stability of Edge X Foundry during operation, it also provides security and...
system management services. Each layer of Edge X Foundry has several components that communicate with each other through the restful API. In the edge computing environment, we adopt the key functions required to define the Edge X Foundry concept and integrate them into the design platform. From the perspective of users, the functions of the edge computing framework can be obtained as a collection of APIs. With excellent interface design, rich protocol support, and heterogeneous data processing capabilities, Edge X Foundry plays the role of edge-level data processing. Although Edge X Foundry provides security services, this service is only for single-point devices and is not applicable to the entire edge computing network, so we have introduced blockchain technology.

Blockchain network realizes a secure, reliable, and decentralized intelligent system in the edge environment, and solves the security and privacy problems in edge computing. A blockchain network is shared by multiple server edge nodes, and each node, as a network participant, can communicate with other nodes in the blockchain network. Due to the limited computing capacity of some terminal devices, they cannot participate in blockchain business. We use the edge server to provide blockchain services for terminal devices. The identity information of all these terminals is recorded and stored in the blockchain network through the edge server. Once the blockchain verifies the identity information, the authorized final entity can read the blockchain data, but the data can only be written to the edge server, which helps to avoid excessive data exposure. Users can access the edge server to edit smart contracts to create blockchain applications that meet the needs of terminal devices. In the edge computing environment, device identity information, access control information, and access control policies are stored in the decentralized blockchain network, which can effectively prevent data corruption.

4.4. Performance Parameter Index Design. For fragment content, in the process of verifying the consensus of new blocks, it is defined that the block manufacturer generates a local block with a maximum size of $B_t$ (bytes) within each packaging interval $T_n$ of the block. If the average transaction size is $b_t$, the block header size is $B_{lk}$, and the number of slices is $k$, the scalability within the slice can be obtained as follows:

$$\Phi(B_t, T_{II}) = \frac{1}{k} \sum_{i=1}^{K} \left( \frac{B_l - B_{l_2}}{B_{l_1}} \right) b_l$$

(14)

If the transaction reaches a consensus within the shard, a local block will be formed. The shard will transfer the local block to the directory shard for final consensus and write it into the final blockchain. In the final consensus stage, check the blocks formed by $K$ partitions, define the partition producer in the block directory, and generate a final block with a maximum size of $B_F$ (bytes) within each block interval period $T_F$. If the average transaction size is $b_F$, the block...
Because the blockchain transaction consensus is divided into two processes—the number of transactions that each process can handle is represented by the scalability of internal partitions and directory partitions, and assuming that the scalability of internal partitions and directory partitions are the same, it is recorded as $T_t'$, and that the block header size is the same, it is recorded as $B_{Ht}$. Then, the scalability of the whole blockchain is recorded as

$$\Phi(B, T) = \Phi(B_t, T_{II}) + \Phi(B_{Ht}, T_{Ht})$$

$$= \sum_{i=1}^{k} \left( \frac{\left( B_t - B_{Ht} \right)}{B_{t}} \right) / T_t + \frac{\left( B_{Ht} - B_{Ht}' \right)}{B_{Ht}}$$

(16)

The total propagation time of the internal consensus of the partition is

$$T^{k}_{in, p} = \frac{1}{M} \left( T^{k}_{in, prepare} + T^{k}_{in, prepare} + T^{k}_{in, commit} \right)$$

$$= \frac{1}{M} \max_{i \in [1, \ldots, k]} \left( \min_{j \in p} \left( \frac{MB}{R_{n,j,p,j}} \right), \zeta \right) + \min_{j \in [1, \ldots, k]} \left( \frac{MB}{R_{n,j,p,j}}, \zeta \right)$$

Where, $n_i, p$ represents the master node $p$ in the slice $i$, $n_{s,j}$ represents the node $j$ in the slice $i$, and $R_{n_i,p,n_{s,j}}$ represents the transmission rate between the master node $p$ and the replica node $j$ in the slice $i$.

Assuming that the computing power of the replica node is $C_{r,p}$, the processing time of the internal consensus verification fragment of the replica node is

$$T^{k}_{in, rec} = \frac{[MC + 4(N_i - 1)a]}{C_{r,p}}$$

(18)

In addition, the process of checking the master node and the replica is the same. Therefore, the verification time of each message in the intraslice consensus request can be expressed as

$$T^{k}_{f} = \frac{1}{M} \left( T^{k}_{f, request} + T^{k}_{f, prepare} + T^{k}_{f, prepare} + T^{k}_{f, commit} + T^{k}_{f, apply} \right)$$

$$= \frac{1}{M} \left( \min_{i \in [1, \ldots, k]} \left( \max_{n_{s,j} \in [1, \ldots, C]} \left( \frac{MB}{R_{n,s,j,p,s,j}} \right), \zeta \right) + \min_{n_{s,j} \in [1, \ldots, C]} \left( \frac{MB}{R_{n,s,j,p,s,j}} \right), \zeta \right)$$

$$+ \min_{n_{s,j} \in [1, \ldots, C]} \left( \frac{MB}{R_{n,s,j,p,s,j}} \right), \zeta \right) + \min_{n_{s,j} \in [1, \ldots, C]} \left( \frac{MB}{R_{n,s,j,p,s,j}} \right), \zeta \right)$$

(20)

where $n_{ds,p}$ represents the master node $p$ in the directory partition, $n_{DS,j}$ represents the node $j$ in the directory partition, and $R_{DS,p,DS,j}$ represents the transmission rate between the master node $p$ and the replica node $j$ in the directory partition.

The final consensus must go through five steps: (1) the final stage of requesting consensus—fragmentation starts with requesting directory fragmentation; (2) the process of checking the master node and the replica node occurs; (3) the final stage of requesting consensus; (4) the
consensus process. The time required for each step includes message expansion time and message verification time. Then, the segmented blocks of the segmented blockchain based on the PBFT consensus algorithm can be expressed as

\[ T_{\text{total}} = T_I + T_{\text{con}} + T_I + T_{m} + T_f = T_I + T_{m} + T_f \]

(24)

The above formula calculates the blockchain delay based on PBFT consensus. The consensus delay of blockchain transactions must be completed within a limited number of consecutive block intervals \( U \) is usually taken as 5~7) to make the blockchain consistent.

\[ T_{\text{total}} \leq uT^I. \]

(25)

5. System Security Design and Implementation

5.1. DataSource. First, 130000 Ethereum transactions were crawled from Etherscan, of which 100000 transactions were used as the training set, 15000 transactions as the verification set, and the remaining 15000 transactions as the test set. The web3.js tool is used to view and deploy transactions. The programming language used in the experiment is Python 3.7, and the deep learning framework is PyTorch-1.4.0, CUDA version 10.1, and CuDNN 7501. The transaction characteristics of the training set are shown in Table 2.

5.2. System Test. Since the automatic coding network is used to embed and retrieve information, the generated secret transactions may not be successfully sent to the blockchain. If the generated secret transaction cannot be deployed, Alice can reset the transaction attributes and merge again. In addition, the extracted secret information does not have to be the same as the original information, so it is necessary to calculate the success rate of embedding and extracting secret information. The average embedding capacity of 100000 transactions and the corresponding embedding success rate and extraction success rate are shown in Table 3.

The unit of embedded capacity in Table 3 is the embedded byte size of each transaction. The embedding success rate is the percentage of 100000 transactions successfully executed. The extraction success rate is the ratio of the number of retrieved correct information bytes to the number of embedded information bytes. It can be seen from Table 3 that with the increase in embedding amount, the success rate of embedding and extracting secret information decreases. Whether it is 4 bytes or 8 bytes of secret information, it has a higher embedding capacity, embedding success rate, and successful extraction rate. If the embedded capacity increases to 10 bytes, the success rate of extracting information decreases to 0.81. Therefore, it is best to embed 8 bytes of secret information in each transaction.
5.3. System Safety Analysis. Ethereum transactions are deployed directly on the blockchain, so the stability of this scheme is equivalent to the tamper resistance of the blockchain itself. After the training generator and extractor, Alice and Bob must save the trained network model parameter file (pt format). Before the two communicators disclose the stored model parameters, the attacker will not be able to crack the secret information. Therefore, deep learning based on blockchain steganography has high security.

6. Conclusion

As an application paradigm integrating distributed databases, P2P networks, consensus, and encryption algorithms, blockchain is characterized by good decentralization and openness, which can prevent tampering, complete anonymity, and trace data. In addition to the relevant characteristics of blockchain itself, fragmented blockchain is also more efficient than single chain blockchain, so it has better prospects in the application of value chain management. With the development of economy, enterprises have formed a value chain in the process of manufacturing products or completing services, thus improving the efficiency of enterprises. Using blockchain technology in the commercial Internet of Things system can improve the operation efficiency of the commercial Internet of Things and reduce the operation cost. In this context, after introducing the deep learning algorithm, this article expounds the efficiency of data collection and the reliability of data storage in the modern Internet of things system, and summarizes the basic business logic of the Internet of Things. A blockchain-based enterprise Internet of Things system model is proposed. Based on the in-depth study of the business development and business needs of modern Internet of Things, combined with the current blockchain hotspot technology, this article uses the deep learning algorithm to model and proposes a business development-oriented enterprise Internet of Things system model. It provides specific guidance for manufacturers on how to widely use technology to improve the functions of the Internet of Things system and reduce operating costs in the future.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

All the authors do not have any possible conflicts of interest.

Acknowledgments

The research was supported by the project Research on curriculum Reform of Industry University Cooperation for Software Engineering Major under New Engineering (Project no. 202002191027).

References


