IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 13 May 2024, accepted 16 June 2024, date of publication 19 June 2024, date of current version 26 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3416458

RESEARCH ARTICLE

Decentralized Deepfake Task Management Algorithm Based on Blockchain and Edge Computing

YANG YANG[1], NORISMA BINTI IDRIS[1], DINGGUO YU[2], CHANG LIU[3], AND HUI WU[3]

[1]Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur 50603, Malaysia
[2]College of Media Engineering, Communication University of Zhejiang, Hangzhou 310000, China
[3]Institute of Intelligent Media Technology, Communication University of Zhejiang, Hangzhou 310000, China

Corresponding author: Dingguo Yu (yann@cuz.edu.cn)

This work was supported in part by the National Social Science Fund of China under Grant 22BSH025; in part by the National Natural Science Foundation of China under Grant 62206241; in part by the Key Research and Development Program of Zhejiang Province, China, under Grant 2021C03138; and in part by the Medium and Long-Term Science and Technology Plan for Radio, Television, and Online Audiovisuals under Grant 2022AD0400.

ABSTRACT Centralized deepfake service providers have large amounts of computing power and training data, giving them the ability to produce high-quality deepfake content. However, once these service providers are attacked or malfunction, it may lead to the collapse of the entire deepfake ecosystem, making deepfake a potential threat to data security. This monopoly development has led to the uneven distribution of deepfake resources, which in turn has brought about the risk of single points of failure. To deal with the problem, this paper proposes a decentralized deepfake task management algorithm (DD-TMA) based on blockchain and edge computing. The blockchain in this algorithm can provide a decentralized storage and management platform to ensure that the data and models of deepfake tasks will not be tampered with or lost. Edge computing can distribute tasks to edge devices close to the data source for processing, reducing data transmission delays and bandwidth consumption, and improving the efficiency and security of deepfake tasks. The paper innovatively integrates blockchain, federated computing, and edge computing. Firstly, the algorithm establishes a decentralized computing platform based on blockchain. Subsequently, it enhances computing power during the execution of decentralized deepfake tasks through the integration of federated computing and edge computing. Finally, the algorithm increases the active performers of decentralized deepfake tasks through gamification, thereby improving task execution efficiency. Experiments conducted in this study on public data sets demonstrate that the algorithm is efficient, robust, and reusable. Compared with other algorithms, the efficiency of DD-TMA is improved by more than 20% and the stability is improved by more than 13%. This algorithm proves effective in solving the problems encountered in the execution of centralized deepfake tasks. The research provides new ideas for future evaluations of decentralized deepfake effects based on different strategies.

INDEX TERMS Deepfake, monopolistic development, blockchain, edge computing, federated computing.

I. INTRODUCTION

This paper will give a preliminary introduction to this research from four aspects: background, motivation, previous studies and structure of paper.

The associate editor coordinating the review of this manuscript and approving it for publication was Mehdi Sookhak.

A. BACKGROUND

The Artificial Intelligence Generate Content (AIGC) utilizes artificial intelligence such as Natural Language Progress (NLP) and Generative Adversarial Networks (GANs) to automatically and quickly create digital content including but not limited to text, images, and audio [1], [2]. Professional Generated Content (PGC) and User Generated Content (UGC) have their own drawbacks when facing AIGC:

Although the quality of digital content based on PGC is very good, its production speed is too slow compared to AIGC; With the explosion of short videos, although the production speed of UGC will increase due to the large number of producers, the quality of content is low and varies greatly. Nowadays, AIGC is not only needed by individual users, but also by innovative industries, such as the Metaverse [3]. Early research on AIGC was not very outstanding. On the one hand, it was limited by the hardware performance at the time, on the other hand, it was limited by the efficiency of the algorithm, and most importantly, it was limited by the scale of data that could be used for training.

In the field of deepfake image, as AIGC integrates the research results of GANs [3] and NLP [4], greater progress has occurred. AIGC is fully capable of producing deepfake images that humans cannot distinguish from real images. NVIDIA [5] has been early in this field. They have achieved high-resolution, controllable deepfake image generation, and this technology is still being upgraded. At the same time, deepmind [6] also released new products. Its specialty is the production of continuous videos, and its performance in the multi-modal field is very good. The research [7] used a literature review method and summarized 112 articles related to deepfake detection, clearly elaborating on the possible abuse of deepfake technology, especially in the creation of false information, political disputes, the spread of hate, and the harassment and blackmail of individuals. potential risks. However, its references are not up-to-date and may not cover recent deepfake detection methods due to the rapid development of technology.

In recent research, the emergence of diffusion models [8] has accelerated the development of deepfake image. This technology uses incremental noise addition to generate images that are more realistic, more beautiful, and more indistinguishable to the ordinary eyes. Moreover, the development of large-scale language models similar to ChatGPT [9] has also improved to a certain extent the correlation and consistency between the input prompt words and the generated images during deepfake image production. At the same time, many excellent products based on deepmind have emerged in the industry. These products are simple and easy to use. Even an ordinary person can generate very realistic deepfake images. The best among them are Stable Diffusion [10], Midjourney [11], and Make-A-Video [12].

In general, in the field of deepfake image, AIGC has the advantage of being far ahead in data creation compared to traditional PGC and UGC. Because it can not only ensure the degree of automation and speed of creation, but also enable customized creation to fully meet the personalized needs of users. If the progress of AIGC is used in the right field, the social and economic value it can create are immeasurable.

B. MOTIVATION

The paper proposes deepfake task management because the increasingly popular deepfake can easily cause privacy leaks and personal security risks, and can easily bring false information and public misleading. This research is also a global regulatory need to deal with deepfake.

Gartner's survey [13] shows that the data generated by AIGC will account for more than 10% of all data generation in 2025. On the positive side, the data generated by these AIGC enriches the diversity of data on the Internet, and can be beneficially applied to news reporting, online games and social fields. However, those with bad intentions will maliciously use the data in areas such as political rumors and personal attacks, triggering unprecedented security and privacy crises.

Firstly, deepfake image can expose private content by copying Original image. We all know that image generation models must rely on a large amount of image training data, and these training data will inevitably have private content, such as face images. Facts have proven that current large-scale image generation models have powerful original data recording capabilities [14], [15], which can partially or even completely copy the original image. This means that the image generated by AIGC has a high probability of partially or completely exposing the private and sensitive information contained in the Original image. For example, the model developed by [16] has the ability to output photos of real people, which is undoubtedly a huge threat to personal privacy. Therefore, risk management of the output of real personal photos is very urgent.

Secondly, deepfake images generated for malicious purposes often contain a large amount of false information. The information can both threaten individuals and deceive the public [17]. For example, in the research [18], deepfake generated an image of Trump blaming Obama, which does not exist in reality. This kind of information seriously misleads the public and, if not controlled, may lead to unnecessary wars. For example, in the sensitive area of Ukraine, deepfake is used to create images containing political rumors [19]. Therefore, it is very important to provide effective technology to verify the authenticity of this type of image, so as to proactively prevent and manage this potential threat.

Thirdly, as deepfake image is booming in both positive and negative aspects, regulatory agencies around the world have also begun to regulate deepfake image. Italy, France, etc. have expressed concerns about deepfake image and have begun related investigations [20]. In particular, China has introduced temporary measures for the management of AIGC, which is an important step in supervision [21]. Therefore, even from the standpoint of policy formulation, research on deepfake images is also very urgent.

The decentralized approach proposed in the paper applies the security and privacy of decentralization, data traceability and transparency, and can optimize computing performance and resource allocation, promoting broad participation and diversity.

In summary, for this study, the following motivations support our research: Data generated by artificial intelligence-generated content will account for more than

10% of all data generation in 2025. The increase of these data enriches the diversity of Internet data and can be beneficially applied in news reporting, online games and social fields. However, the malicious use of this data may trigger unprecedented security and privacy crises, and there should be corresponding research to deal with the malicious use of this part of the data. Deepfake images generated by AIGC may expose private content by copying the original image. Current large-scale image generation models have powerful raw data recording capabilities and can partially or completely replicate the original image, thereby exposing private and sensitive information contained in the original image with a high probability. This poses a huge threat to personal privacy, so it is very urgent to achieve risk management for the output of real personal photos. Deepfake images generated for malicious purposes often contain a large amount of false information that may threaten individuals and mislead the public. This kind of information seriously misleads the public and, if left unchecked, could lead to unnecessary conflicts. Therefore, it is important to provide effective techniques to verify the authenticity of such images in order to proactively prevent and manage this potential threat.

C. PREVIOUS STUDIES

In terms of the working principle of deepfake image, the research [22] conducted a detailed study on the design principles of deepfake image and comprehensively explored the classification issues of deepfake image in terms of security and privacy. At the same time, this work examines the deepfake image model and all ownership issues of the generated deepfake images, with a focus on obscene images. However, they provide no countermeasures for the use of such generated images.

In terms of the management of deepfake image, the research [23] believes that deepfake image technology has been abused and violated personal privacy. By forging videos or images of real scenes, criminals can create false information and slander or deceive individuals. Moreover, the false content produced by deepfake image may confuse social cognition, making it difficult for people to distinguish between real and false information, destroying the credibility of the information. However, this research does not fully address the risk management of deepfake image at the source of information. The research [24] summarized many specific implementation details of deepfake image technology, also discussed the huge risks brought by deepfake image, and proposed a blockchain-based response strategy. However, they only focused on Original image data and did not pay attention to the data generated by deepfake.

Applying BlockChain and Edge Computing to deepfake research, the research [25] proposed an innovative solution by combining blockchain with deep learning to establish a distributed deep fake detection system across multiple ICPs. By using blockchain technology, the system is decentralized and does not rely on a single ICP. Such a design helps prevent manipulation and abuse of power and improves the robustness of the system. However, due to the need for collaboration and consensus among multiple ICPs, there may be performance issues. The research [26] proposed a deep fake face video detection method that uses a combination of frequency domain features and spatial domain features. In order to improve the generalization ability of the detection model and respond to malicious attacks, the article introduces blockchain technology to implement an incentive mechanism. However, the article used the deepfake detection and Celeb-DF data sets for experiments, but these two data sets may have their limitations and may not necessarily fully cover all possible forgery situations on the Internet. The limitations of these two data sets are: first, they mainly contain some specific celebrity facial images and lack data in other fields, such as animals, natural landscapes, etc., resulting in insufficient generalization ability of the model in other fields. Second, the data size of these two datasets is relatively small. Third, these data sets are composed of images from different sources. There may be some images with low quality or labeling errors, which will affect the training effect of the model.

D. RESEARCH GAP AND THE OBJECTIVES OF THE WORK

According to the above content, the current research gaps for deepfake task management are: First, although current research focuses on the generation and detection algorithms of deepfake technology, it has not yet delved into the personal privacy data protection and data security issues that may be included in the generated content. The lack of a targeted privacy protection mechanism may lead to the risk of leaking personal privacy in the generated content. Second, current research mainly focuses on the generation and detection algorithms of deepfake technology, but there has not been in-depth research on how to verify the credibility and authenticity of deepfake content. The lack of an effective verification mechanism may call into question the authenticity of deepfake content.

Deepfake task management involves several key processes of blockchain and game theory. First, Deepfake Service Providers (DSPs) issue tasks through smart contracts, specifying parameters such as diffusion model network structure, local training rounds, global training rounds, learning rate, and data set size. Second, to incentivize participation, the smart contract also sets the payment price for deepfake training nodes. However, due to the resource heterogeneity of edge services, formulating a unified payment price is challenging. Then, in response to this problem, the paper proposed a resource competition mechanism based on game theory to optimize resource allocation and maximize benefits.

During the training process, first, the deepfake training node accepts the task, executes the diffusion model network structure, and completes the specified local training rounds. After training is completed, the node publishes the local

diffusion model parameters to the blockchain network for aggregation. These aggregated parameters are then shared with other training nodes to initiate the next round of training. After training is completed, the DSP obtains the trained federated diffusion model from the blockchain and uses it to reason based on user input to generate deepfake digital content by gradually removing noise from the data. Blockchain technology, with its decentralization, security and transparency, effectively solves problems such as task release, resource competition, model parameter sharing and inference. The use of smart contracts ensures the transparency and credibility of task release, while providing a safe and fast payment method to motivate participants. In addition, blockchain ensures fairness and transparency in resource allocation and helps develop optimal resource allocation strategies.

In response to the above and the resulting research gap, the goals of this study are: first, to explore how to combine blockchain technology with the deepfake image content generation process, further integrating the concept of edge computing, and through the implementation of smart contracts, Enable decentralized management of generated content to ensure content interoperability and traceability. Second, edge computing is introduced to optimize the computing performance of the generation process. By loading model training tasks to edge nodes, the load on centralized servers is reduced and the overall response speed of the decentralized system is improved. Third, decentralized model training is enabled in edge computing environments through federated diffusion models, promoting broader participation and increasing the diversity of generated content. Construct a resource allocation mechanism, consider edge computing nodes, achieve effective allocation of edge resources, and further improve the efficiency and performance of deep fake image content generation in a distributed environment.

E. STRUCTURE OF PAPER

This paper explores the integration of blockchain technology and edge computing with the process of deepfake image content production. The aim is to achieve decentralized management of generated content, ensuring interoperability and traceability through smart contracts. Additionally, edge computing is introduced to optimize the computing performance, reduce the load on centralized servers, and improve the overall response speed of the decentralized system. The federated diffusion model facilitates decentralized model training, promoting wider participation and increasing the diversity of generated content. The resource allocation mechanism considers edge computing nodes for effective resource management, enhancing efficiency and performance in a decentralized environment. This comprehensive approach aims to merge blockchain, edge computing, and deepfake technology to enhance security, efficiency, and innovation in decentralized content generation.

This paper is divided into 4 parts, the summary of each part is as follows:

1) Part 1: Background and Motivation This section delves into the background of blockchain technology, edge computing, and deepfake image generation, highlighting their significance and potential applications in modern technological development. It examines the motivations behind this research direction, identifying the issues and challenges at the intersection of these technologies, setting the stage for the detailed discussions that follow.
2) Part 2: Algorithm Proposal This part introduces the proposed algorithm for deepfake image risk management, integrating blockchain and edge computing. It details the key steps involved in deepfake generation within blockchain and edge computing environments, focusing on decentralized systems. The principles, design considerations, and expected outcomes of the algorithm are thoroughly examined, providing a comprehensive understanding of its workings.
3) Part 3: Experimental Results A series of experiments are conducted to verify the effectiveness and performance of the proposed algorithm. This section presents detailed experimental analyses, demonstrating the feasibility and superiority of the method. The results are discussed to validate the claims made about the algorithm's efficiency and performance improvements.
4) Part 4: Conclusion and Future Work The final part summarizes the main findings of the paper, offering prospects for future research. It reflects on the experiences and lessons learned during the research process. The section concludes with a list of references cited throughout the paper, providing a resource for further study.

II. ALGORITHMS AND MODELS

This study proposes DD-TMA. First, the principle of deepfake image generation is analyzed by studying mathematical models, and then blockchain is applied to achieve decentralized management and improve the reliability and transparency of original image risk management. Finally, the resource allocation optimization strategy based on edge computing provides help for the practical application of the algorithm. The flow chart of the algorithm is shown in Figure 1.

A. OVERVIEW OF THE ALGORITHM

1) This paper introduces an innovative algorithm that integrates blockchain and edge computing technologies to create a decentralized model for managing deepfake image generation.
2) By using blockchain and smart contracts, the paper ensures decentralized management, enhancing the reliability and transparency of handling original images and addressing associated risks.
3) The paper employs edge computing to optimize the computing performance and response speed, reducing

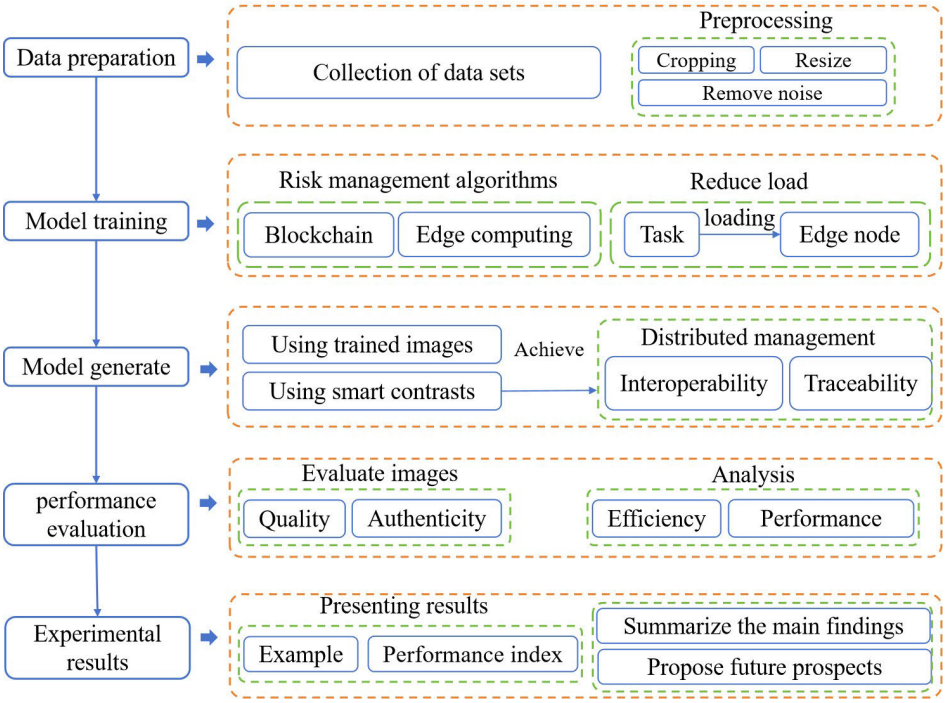

FIGURE 1. Flow chart of the algorithm.

the load on centralized servers through decentralized model training.

4) Through in-depth research on edge computing and a resource allocation optimization strategy, the paper validates the practical application and effectiveness of the proposed algorithm in a decentralized environment.

B. CONSTRUCTION OF THE MODEL

The paper innovatively proposes a decentralized content generation system model, and adopts hierarchical structure management for this model. The model mainly includes data layer, blockchain layer, computing layer and application layer.

Deepfake service providers whose data layer consists of edge devices train federated models through federated learning to generate deepfake digital content. The blockchain layer consists of edge servers with strong computing capabilities, and manages deepfake tasks and model parameters through smart contracts and decentralized ledgers. The computing layer is also composed of edge servers, which are responsible for participating in collaborative training of deepfake tasks and submitting training results. Finally, the application layer consists of users sending tasks to Deepfake Service Providers(DSPs) and receiving application content. The decentralized content generation system model is shown in the Figure 2.

In the model proposed in the paper, the data layer consists of edge devices with limited computing and storage resources such as smartphones, IoT devices, and embedded systems [27]. It can reduce the delay and dependency of data transmission. This model combines these edge devices collectively called DSPs. This model introduces federated learning. These devices are distributed through the blockchain layer and computing layer, and perform federated learning to achieve distributed model training and train federated models that can generate deepfake digital content.

The blockchain layer of the model consists of edge servers with strong computing power, which are called miners. The model releases deepfake tasks through smart contracts and decentralized ledgers, and automatically collects and aggregates deepfake model parameters, and finally submits deepfake tasks.

The computing layer of the model also consists of edge servers with strong computing capabilities called deepfake training nodes. They join deepfake tasks through smart contracts for collaborative training, mainly contributing a large amount of computing resources and local data. Finally, the aggregated deepfake model parameters are obtained, multiple rounds of iterations are performed, and the deepfake training results are submitted.

The application layer of the model consists of users, who send task types and prompt words to DSPs. DSPs perform inference through the trained model and return the generated deepfake digital content.

This decentralized content system model achieves a highly collaborative content generation and application process through a hierarchical structure, allowing each layer to play a key role in specific functions and tasks. The data layer enables edge devices to contribute to training through federated

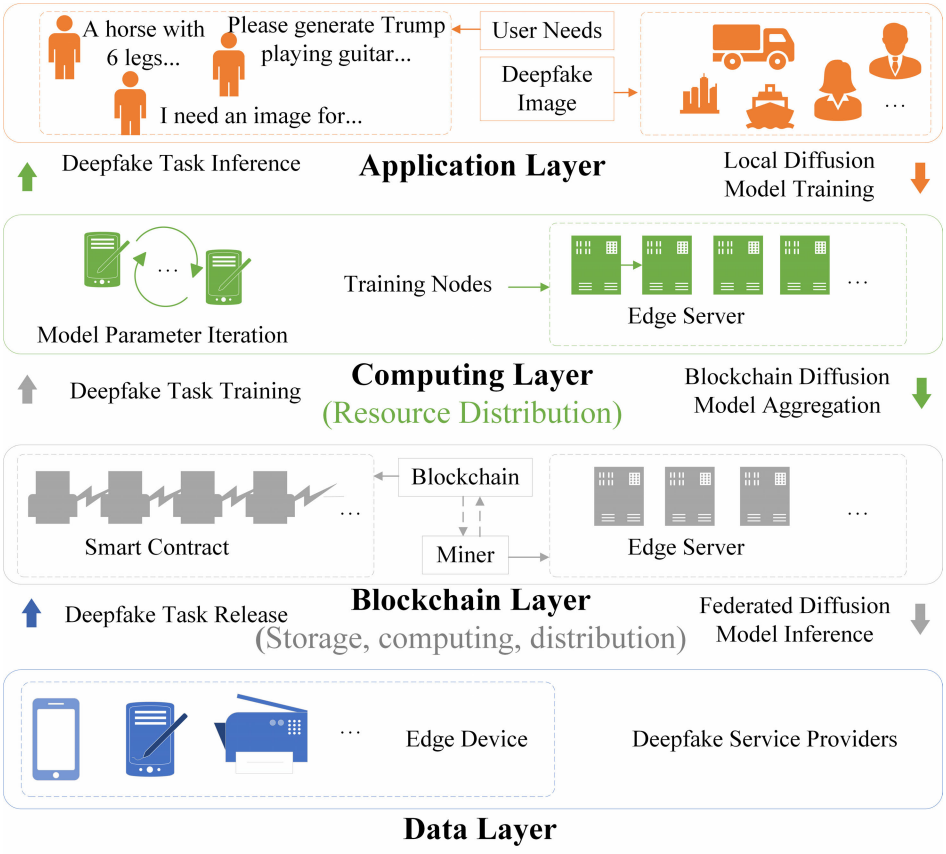

FIGURE 2. Decentralized content generation system model.

learning. The blockchain layer ensures the security and transparency of tasks and model parameters. The computing layer provides powerful computing resource support, while the application layer connects users and systems to facilitate collaborative work between them., realizing efficient, safe and transparent deepfake digital content generation.

C. MODEL INNOVATION

1) When deepfake tasks are released, DSPs can release tasks through smart contracts. The parameters given by the task include the diffusion model network structure, local training rounds, global training rounds, learning rate, data set size, etc. The smart contract also sets a payment price to encourage deepfake training nodes to join collaborative training. However, edge services have the characteristics of resource heterogeneity [28], and it is difficult for DSPs to formulate a unified price to pay for the computing resources paid by deepfake training nodes. Therefore, this paper innovatively proposes a resource competition mechanism based on game theory [29], which can find the optimal allocation strategy and find the space to maximize benefits.
2) During deepfake task training, the deepfake training node first accepts the task, then executes the diffusion model network structure, and finally executes the diffusion model training for which the local training round has been specified. After the training is completed, the deepfake training node publishes the local diffusion model parameters to the blockchain network for aggregation. The aggregated model parameters will be shared with other deepfake training nodes through the blockchain to start the next round of diffusion model training.
3) During deepfake task inference, after the deepfake task training is completed, DSPs can obtain the trained federated diffusion model through the blockchain and perform inference based on the deepfake request input by the user. During the inference process, the federated diffusion model gradually removes noise from the data and generates deepfake digital content.
4) Blockchain has the characteristics of decentralization, security, and transparency, and can well solve problems such as task release, resource competition, model parameter sharing, and inference involved in deep forgery tasks. This paper innovatively uses blockchain for the following reasons: 1) The DSPs proposed in this paper can issue tasks through smart contracts and set payment prices to encourage deep forgery training nodes to participate in collaborative training. The smart contract function of blockchain technology

TABLE 1. Symbols of equations.

symbol	definition
d_{step}	The data for the diffusion step
n_{step}	Parameters regulating the equal reduction
d_{step-1}	Data from the previous diffusion step
g_{step}	Samples taken from gaussian noise
d_0	Raw data
g	Randomly generated noise samples
$out()$	Diffusion model network
o	Local diffusion model training results
$loss()$	Loss function
$l.back()$	Back propagation
$l.step()$	Updating the local gradient
dif_i	Parameters of the on-chain diffusion model
$\|Data_i\|$	Local data size
$\|Data\|$	Total local data size
$o(dif)_{min}$	Local diffusion model minima
dif	On-chain model diffusion parameters
$node_i$	Deepfake training nodes
$data_{node_i}$	Training data for federated inference models
cyc_{node_i}	Number of CPU cycles
fre_{node_i}	CPU operating frequency
qua_{node_i}	Federated Inference model quality
pri_{node_i}	The resource price paid by DSPs
use_{node_i}	Utility function
$log_2(1+qua_{node_i})$	Satisfaction of DSPs
$qua_{node_i}prinode_i$	The expenditure of DSPs to train the model
qua_{node_i}	Federated Inference model quality
pri_{node_i}	The price paid for the resource

can ensure the transparency and credibility of task release. At the same time, the payment mechanism implemented through smart contracts can also provide a safe and fast payment method to motivate node participants in DD-TMA. 2) Due to the resource heterogeneity of edge services, it is difficult to set a unified payment price. This paper proposes a resource competition mechanism based on game theory. The use of blockchain technology can ensure the fairness and transparency of resource allocation and help find the optimal resource allocation strategy.

D. RESEARCH BASED ON DECENTRALIZATION

In order to encourage deepfake training nodes to participate in solving deepfake tasks and maximize the benefits of both parties to the transaction, this paper proposes a resource allocation mechanism based on Stackelberg game. This paper performs Stackelberg modeling on DSPs and deepfake training nodes, and uses the blockchain to store, distribute and calculate optimal resource allocation strategies. By maximizing the utility of both parties in the game, the benefits of both parties in the transaction are maximized. The symbols of equations in this part are explained in detail as shown in Table 1.

Stackelberg game is mainly used to describe the strategic interaction between leaders and followers. First, the leader formulates his optimal strategy, and then the followers choose his optimal response strategy knowing the leader's strategy. Second, leaders will definitely pursue maximization of their own interests, while followers also hope to obtain maximum benefits through reasonable responses. Third, the strategic selection and interaction between leaders and followers may achieve the overall optimal configuration of interests.

The reasons why this paper uses Stackelberg game are: first, this paper needs to solve the deep forgery task and hopes to encourage deep forgery training nodes to actively participate and maximize the interests of both parties. Second, the game is suitable for models describing strategic interactions between leaders (resource allocators) and followers (deepfake training nodes). Third, by using this model, this paper can better understand the conflict of interests and coordination between the two parties, and then propose a more effective resource allocation mechanism to maximize the interests of both parties.

The generation of decentralized content mainly includes three stages: Training of local diffusion model, aggregation of on-chain diffusion model and reasoning for the federated diffusion model. Among them, training of local diffusion model is to train the same diffusion model through the local data and computing resources of multiple edge devices, and input the local data with added noise to the diffusion model. The diffusion model needs to predict the added noise. Aggregation of on-chain diffusion model is that multiple edge devices share the locally trained diffusion model through the blockchain, and then obtain the global diffusion model through aggregation. The edge device uses the global diffusion model to start the next new iteration until the global training round required by the task is reached. After the training is completed, reasoning for the federated diffusion model is the task publisher who can use the federated diffusion model to infer and predict the noise added to the data [30], and restore the data by removing the noise.

1) TRAINING OF LOCAL DIFFUSION MODEL

After receiving the deepfake task on the blockchain, the edge device performs the diffusion process locally, that is, adding Gaussian noise to the local data in multiple diffusion steps. In each diffusion step, noise is added to the data d_{step-1} of the previous diffusion step $step-1$ to obtain the data d_{step} of the next diffusion step $step$. Continue this diffusion step until the data becomes pure noise. The paper sets n_{step} as a parameter that adjusts the degree of added noise to be reduced by an equal amount. The smaller its value, the more noise is added, that is, the smaller the proportion of original data, the greater the proportion of pure noise. The paper sets g_{step} to be samples obtained from normally distributed Gaussian noise. The noise addition process is shown in equation (1).

$$d_{step} = \sqrt{n_{step}} d_{step-1} + \sqrt{1-n_{step}} g_{step} \tag{1}$$

Among them, the original data is defined as d_0, and the randomly generated noise sample is defined as g, then the relationship between d_{step} and d_0 is as shown in equation (2).

$$\begin{aligned} d_{step} &= \sqrt{n_{step} n_{step-1} \cdots n_2 n_1} d_0 \\ &\quad + \sqrt{1 - n_{step} n_{step-1} \cdots n_2 n_1} g \\ &= \sqrt{\overline{n_{step}}} d_0 + \sqrt{1-\overline{n_{step}}} g \end{aligned} \tag{2}$$

According to the calculation of equation (1) and equation (2), d_{step} can be obtained. By inputting the diffusion step $step$ and data d_{step} into the diffusion model network $out()$, the local diffusion model training result o can be obtained. As shown in equation (3).

$$o = out(step, d_{step}) \tag{3}$$

By inputting the output o of the diffusion model and the added randomly generated noise sample g into the loss calculation function $loss()$ for loss calculation, the loss value l can be obtained, as shown in equation (4).

$$l = loss(o, g) \tag{4}$$

2) AGGREGATION OF ON-CHAIN DIFFUSION MODEL

The paper defines back propagation as $l.back()$ and updating the local gradient as $l.step()$. After multiple edge devices train the local diffusion model o, define dif_i as the on-chain diffusion model parameter, and then $o(dif_i)$ is the local diffusion model corresponding to the parameter. Then share $o(dif_i)$ to the blockchain network, perform on-chain diffusion model parameter aggregation based on the local data size $|Data_i|$, set the total size of local data to $|Data|$, and set the minimum value of the local diffusion model to $o(dif)_{min}$. As shown in equation (5).

$$o(dif)_{min} = \frac{1}{n}\sum_{i=1}^{n} o(dif_i) \tag{5}$$

Among them, the paper defines the on-chain model diffusion parameter after parameter aggregation as dif, as shown in equation (6).

$$dif = \frac{|Data_i| dif_i}{|Data|} \tag{6}$$

According to the requirements of the task on the deepfake chain, perform a specified number of local iterations and global aggregation to obtain the global federated diffusion model $o(dif)$ after the aggregation of the on-chain diffusion model, where dif is the on-chain model diffusion parameter selected by the global federated diffusion model, and then It is fed back to the publisher of the deepfake task.

3) REASONING FOR THE FEDERATED DIFFUSION MODEL

After the publisher of the deepfake task obtains the global federated diffusion model, he randomly generates noise g, uses $o(dif)$ to predict the added noise, removes the obtained noise result from d_{step}, and deduces the data d_{step-1} of the previous diffusion step until the original data d_0 is restored. As shown in equation (7).

$$d_{step-1} = +\frac{1}{\sqrt{n_{step}}}(d_{step} - \frac{1-n_{step}}{\sqrt{1-\overline{n}_{step}}} o(dif)_{min}(d_{step}, step)) + \sqrt{1-n_{step}}g \tag{7}$$

E. RESEARCH BASED ON EDGE COMPUTING

1) MODELING BASED ON DSPS AND DEEPFAKE TRAINING NODES

The paper stipulates that the deepfake training node is $node_i$, the training data used to train the federated inference model is $data_{node_i}$, the number of CPU work cycles required to train individual data samples is set to cyc_{node_i}, the CPU working frequency is set to fre_{node_i}, and the trained federation the quality of the inference model is qua_{node_i}, and the resource price paid by DSPs is set to pri_{node_i}. Therefore, the utility function of deepfake training node $node_i$ is set to use_{node_i}. As shown in equation (8).

$$use_{node_i} = qua_{node_i} pri_{node_i} - qua_{node_i}{}^2 cyc_{node_i} data_{node_i} fre_{node_i}{}^2, \quad qua_{node_i} \in [0, 1] \tag{8}$$

Among them, $qua_{node_i} pri_{node_i}$ represents the income obtained by deepfake training node $node_i$, and $qua_{node_i}{}^2 cyc_{node_i} data_{node_i} fre_{node_i}{}^2$ represents the computing resources consumed by deepfake training node $node_i$ when executing deepfake tasks published on the blockchain.

The utility function of DSPs is set to use_0. As shown in equation (9).

$$use_0 = \sum_{i=1}^{N} log_2(1 + qua_{node_i}) - \sum_{i=1}^{N} qua_{node_i} pri_{node_i}, pri_{node_i} \geq 0 \tag{9}$$

Among them, $log_2(1 + qua_{node_i})$ represents the DSPs' satisfaction with the federated inference model obtained by the task, and $qua_{node_i} pri_{node_i}$ represents the DSPs' expenditure on training the model. The utility function use_0 of a single deepfake training node $node_i$ for DSPs is shown in equation (10).

$$use_0 = log_2(1 + qua_{node_i}) - qua_{node_i} pri_{node_i} \tag{10}$$

2) OPTIMAL PAYMENT STRATEGIES

In order to solve the above utility function, this paper models the interaction process between DSPs and deepfake training nodes as a Stackelberg game process of two nodes. And through smart contracts, the strategies of both parties to the transaction are automatically executed to maximize the benefits of both parties. This paper divides the game process into two stages. In the first stage, deepfake training node $node_i$ determines the federated inference model quality is qua_{node_i} and shares qua_{node_i} with DSPs through the blockchain. In the second stage, DSPs determine the resource price pri_{node_i} to be paid based on qua_{node_i} to solve the optimal payment strategy. The following is the process of solving the optimal payment strategy.

Firstly, the paper finds the first-order derivative $\frac{\partial use node_i}{\partial use qua_{node_i}}$ and the second-order derivative $\frac{\partial^2 use node_i}{\partial use qua^2_{node_i}}$ for the utility

function use_{node_i} of deepfake training node $node_i$. As shown in equation (11) and equation (12).

$$\frac{\partial_{usenode_i}}{\partial_{use_{qua_{node_i}}}} = pri_{node_i} - 2qua_{node_i}cyc_{node_i}data_{node_i}fre^2_{node_i} \tag{11}$$

$$\frac{\partial^2_{usenode_i}}{\partial_{use_{qua^2_{node_i}}}} = -2cyc_{node_i}data_{node_i}fre^2_{node_i} \tag{12}$$

Among them, the second derivative $\frac{\partial^2_{usenode_i}}{\partial_{use_{qua^2_{node_i}}}} < 0$, the paper can get the first derivative $\frac{\partial_{usenode_i}}{\partial_{use_{qua_{node_i}}}}$ monotonically decreasing, and when $qua_{node_i} = 0$, the first derivative $\frac{\partial_{usenode_i}}{\partial_{use_{qua_{node_i}}}} = pri_{node_i} \geq 0$. When $qua_{node_i} = 1$, $\frac{\partial_{use_{node_i}}}{\partial_{use_{qua_{node_i}}}} = pri_{node_i} - 2cyc_{node_i}data_{node_i}fre^2_{node_i}$ may be greater than 0 or less than 0. This paper will discuss it according to the situation.

Case 1: When $qua_{node_i} = 1$ and $pri_{node_i} \geq 2cyc_{node_i}data_{node_i}fre^2_{node_i}$, the first derivative $\frac{\partial_{usenode_i}}{\partial_{use_{qua_{node_i}}}} \geq 0$ and use_{node_i} increase monotonically. The maximum value $maxuse_{node_i}$ of the utility function use_{node_i} is shown in equation (13).

$$maxuse_{node_i} = pri_{node_i} - 2cyc_{node_i}data_{node_i}fre^2_{node_i}, qua_{node_i} = 1 \tag{13}$$

At this time, the utility function use_0 of a single deepfake training node $node_i$ for DSPs is shown in equation (14).

$$use_0 = log_2 2 - pri_{node_i} \tag{14}$$

Since $\frac{\partial_{use_0}}{\partial_{pri_{node_i}}} = -1 < 0$, use_0 is monotonically decreasing, so when $pri_{node_i} = 2cyc_{node_i}data_{node_i}fre^2_{node_i}$, the maximum value of use_0, $maxuse_0$, can be calculated. As shown in equation (15).

$$maxuse_0 = log_2 2 - 2cyc_{node_i}data_{node_i}fre^2_{node_i} \tag{15}$$

Case 2: When $qua_{node_i} = 1$ and $0 < pri_{node_i} < 2cyc_{node_i}data_{node_i}fre^2_{node_i}$, $\frac{\partial_{usenode_i}}{\partial_{use_{qua_{node_i}}}} < 0$, $node_i$ have a maximum utility, as shown in equation (16).

$$\frac{\partial_{usenode_i}}{\partial_{use_{qua_{node_i}}}} = pri_{node_i} - 2cyc_{node_i}data_{node_i}fre^2_{node_i} = 0,$$
$$qua_{node_i} = \frac{pri_{node_i}}{2cyc_{node_i}data_{node_i}fre^2_{node_i}} \tag{16}$$

At this time, the utility function use_0 of a single deepfake training node $nonde_i$ for DSPs is shown in equation (17).

$$use_0 = log_2(1 + \frac{pri_{node_i}}{2cyc_{node_i}data_{node_i}fre^2_{node_i}}) - \frac{pri^2_{node_i}}{2cyc_{node_i}data_{node_i}fre^2_{node_i}} \tag{17}$$

Its first derivative $\frac{\partial_{usenode_i}}{\partial_{use_{qua_{node_i}}}}$ and second derivative $\frac{\partial^2_{usenode_i}}{\partial_{use_{qua^2_{node_i}}}}$ are shown in equation (18) and equation (19).

$$\frac{\partial_{usenode_i}}{\partial_{use_{qua_{node_i}}}} = \frac{1}{2cyc_{node_i}data_{node_i}fre^2_{node_i}} + pri_{node_i} - \frac{pri_{node_i}}{cyc_{node_i}data_{node_i}fre^2_{node_i}} \tag{18}$$

$$\frac{\partial^2_{usenode_i}}{\partial_{use_{qua^2_{node_i}}}} = -\frac{1}{(2cyc_{node_i}data_{node_i}fre^2_{node_i} + pri_{node_i})^2} - \frac{1}{cyc_{node_i}data_{node_i}fre^2_{node_i} + pri_{node_i})^2} \tag{19}$$

Among them, $\frac{\partial^2_{usenode_i}}{\partial_{use_{qua^2_{node_i}}}} < 0$, then $\frac{\partial_{usenode_i}}{\partial_{use_{qua_{node_i}}}}$ decreases monotonically, and use_0 has a maximum utility such that $\frac{\partial_{usenode_i}}{\partial_{use_{qua_{node_i}}}} = 0$. This study uses $Karush - Kuhn - Tucker$ to solve the objective function, as shown in equation (20).

$$KKT = -log_2(1 + \frac{pri_{node_i}}{2cyc_{node_i}data_{node_i}fre^2_{node_i}}) + \frac{pri_{node_i}}{cyc_{node_i}data_{node_i}fre^2_{node_i}} - l_1 pri_{node_i} + l_2(pri_{node_i} - 2cyc_{node_i}data_{node_i}fre^2_{node_i}) \tag{20}$$

Among them, l_1 and l_2 are Lagrange multipliers. According to the calculation of KKT, the $Karush - Kuhn - Tucker$ conditions can be obtained as shown in equation (21), equation (22) and equation (23).

$$\frac{\partial_{KKT}}{\partial_{pri_{node_i}}} = -\frac{1}{2cyc_{node_i}data_{node_i}fre^2_{node_i} + pri_{node_i}} + \frac{pri_{node_i}}{cyc_{node_i}data_{node_i}fre^2_{node_i}} - l_1 + l_2 = 0 \tag{21}$$

$$l_1 pri_{node_i} = 0, l_1 \geq 0, pri_{node_i} \geq 0 \tag{22}$$

$$l_2(pri_{node_i} - 2cyc_{node_i}data_{node_i}fre^2_{node_i}) = 0, \quad l_2 \geq 0, pri_{node_i} \leq 2cyc_{node_i}data_{node_i}fre^2_{node_i} \tag{23}$$

Finally, in this study, $cyc_{node_i}data_{node_i}fre^2_{node_i}$ is recorded as C, then $(pri_{node_i}, qua_{node_i})$ can be calculated, as shown in equation (24).

$$(pri_{node_i}, qua_{node_i}) = \begin{cases} (\sqrt{C(1+C)} - C, \frac{pri_{node_i}}{2C}), C > \frac{1}{8} \\ (2C, 1), C \leq \frac{1}{8} \end{cases} \tag{24}$$

In this study, by substituting the calculated value of $(pri_{node_i}, qua_{node_i})$ into equation (8) and equation (9), the value of the utility function use_{node_i} of the deepfake training node $node_i$ and the value of the utility function use_0 of the DSPs can be calculated, that is, the optimal utility can be calculated.

III. EXPERIMENT

In order to demonstrate the effectiveness of the mathematical model proposed in this paper, this paper arranged decentralized content generation experiments and resource allocation experiments. In order to make the experimental results convincing, the paper sets the local training rounds of federated diffusion model inference in the decentralized content generation experiment to 10 rounds, the global training rounds to 100 rounds, the diffusion steps to 1000 times, and the number of edge devices to 20. In addition, the paper sets 100 deepfake training nodes in the resource allocation experiment. A single deepfake training node is used for the federated inference model.

This paper conducted many experiments and made many adjustments to the training rounds and parameters to be selected, and finally decided to use these parameters. First, the Local training rounds are set to 10 to ensure that each edge device fully trains and learns the data locally to improve the model's local feature learning capabilities and reduce the computational load of each round of training. Global training rounds are set to 100 rounds in order to fully utilize the local model update information of all devices in the entire network to achieve global convergence and optimization of the model. Second, the Diffusion steps are set to 1,000 times to ensure that the model can fully integrate the local model information of each device after multiple iterative diffusions and improve the performance and performance of the model in the entire network. Third, the Number of edge devices is set to 20 to simulate a relatively large-scale edge computing environment to test the performance and scalability of the model in processing large-scale data and multi-device collaboration. The Number of deepfake training nodes is set to 100 in order to simulate a larger-scale training data set to test the generalization ability and effect of the model when processing large-scale data.

The data is $data_{node_i}$. The number of CPU working cycles required to train a separate data sample cyc_{node_i} and the CPU working frequency fre_{node_i} are from the uniform distribution. Random sampling, its value range is shown in equation (25).

$$\begin{cases} data_{node_i} \in [0.8, 1.2] \\ cyc_{node_i} \in [0.4, 0.5] \\ fre_{node_i} \in [0.1, 0.2] \end{cases} \tag{25}$$

A. DECENTRALIZED CONTENT GENERATION EXPERIMENT

In order to prove the universal effectiveness of the algorithm proposed in this paper, this paper selected 3 public data sets for this experiment. They are E-MNIST, F-MNIST, and KMNIST. The three datasets contain different types of data such as numbers, letters, and fashion items. Use them to test the diversity and adaptability of algorithms to different data representations. These datasets are widely used in the machine learning community and are suitable for benchmarking the performance of algorithms against existing methods. These datasets contain data relevant to real-world applications such as digit recognition, letter recognition, and fashion item classification. By using these datasets, the performance of the algorithm in real-world scenarios can be evaluated. This study will globally iterate 100 rounds of training loss values and decentralized content generation results under the conditions of independent and identical distribution and non-independent and identical distribution. As the training rounds increase, the loss value changes as shown in Figure 3 and Figure 4.

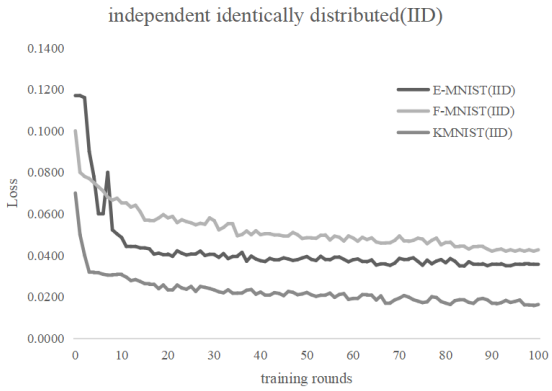

FIGURE 3. Decentralized Content Generation Training (IID).

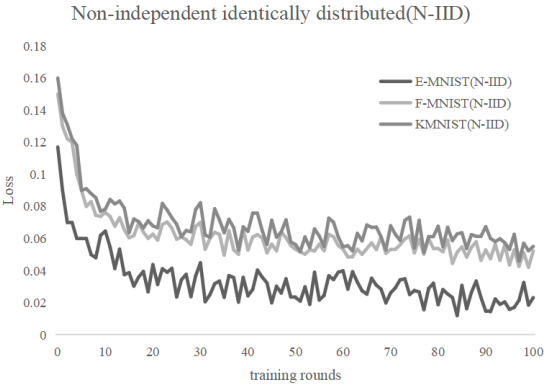

FIGURE 4. Decentralized Content Generation Training (N-IID).

Under independent and identically distributed conditions, some experimental results of three public data sets E-MNIST, F-MNIST and KMNIST after global iterations of 0, 20 and 100 times of training are shown in the Figure 5, Figure 6 and Figure 7. The paper analyzed in detail the value of the training node utility under the condition of independent and identical distribution in different sets of experiments with training rounds of 0, 20 and 100 times respectively. Among them, training round 100 is proposed by this paper, and also represents the algorithm effect of the training node utility corresponding to the algorithm proposed in this paper, as shown in Table 2.

Under non-independent and identically distributed conditions, some experimental results of three public data sets E-MNIST, F-MNIST and KMNIST after 100 global iterations of training are shown in the Figure 8, Figure 9 and Figure 10. The paper analyzed in detail the value of the training node utility under the condition of non-independent and identical distribution in different sets of experiments with

TABLE 2. Independent and identical distribution in different sets.

Data set	E-MNIST			F-MNIST			KMNIST		
Training rounds	0	20	**100 (DD-TMA)**	0	20	**100 (DD-TMA)**	0	20	**100 (DD-TMA)**
training node utility	0.08	0.65	**0.88**	0.12	0.68	**0.86**	0.07	0.71	**0.90**
clarity of the image	poor	very poor	**good**	very poor	average	**Excellent**	very poor	average	**Excellent**

TABLE 3. Non-independent and identical distribution in different sets.

Data set	E-MNIST			F-MNIST			KMNIST		
Training rounds	0	20	**100 (DD-TMA)**	0	20	**100 (DD-TMA)**	0	20	**100 (DD-TMA)**
training node utility	0.24	0.69	**0.81**	0.31	0.68	**0.82**	0.17	0.63	**0.81**
clarity of the image	poor	very poor	**good**	poor	average	**Excellent**	very poor	poor	**good**

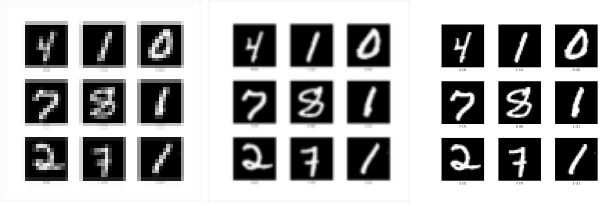

FIGURE 5. Independent and identically distributed-E-MNIST, (a)Training Rounds 0,(b)Training Rounds 20,(c)Training Rounds 100.

FIGURE 6. Independent and identically distributed-F-MNIST, (a)Training Rounds 0,(b)Training Rounds 20,(c)Training Rounds 100.

FIGURE 7. Independent and identically distributed-KMNIST, (a)Training Rounds 0,(b)Training Rounds 20,(c)Training Rounds 100.

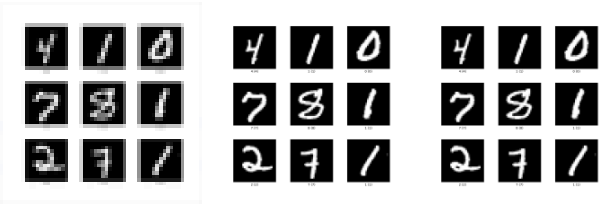

FIGURE 8. Non-independent and identically distributed-E-MNIST, (a)Training Rounds 0,(b)Training Rounds 20,(c)Training Rounds 100.

FIGURE 9. Non-independent and identically distributed-F-MNIST, (a)Training Rounds 0,(b)Training Rounds 20,(c)Training Rounds 100.

training rounds of 0, 20 and 100 times respectively, as shown in Table 3.

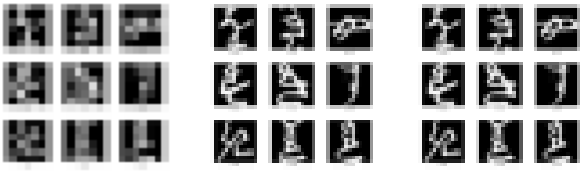

FIGURE 10. Non-independent and identically distributed-KMNIST, (a)Training Rounds 0,(b)Training Rounds 20,(c)Training Rounds 100.

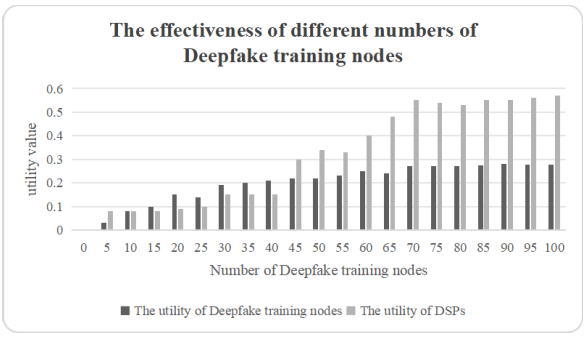

FIGURE 11. Decentralized Content Generation Training (IID).

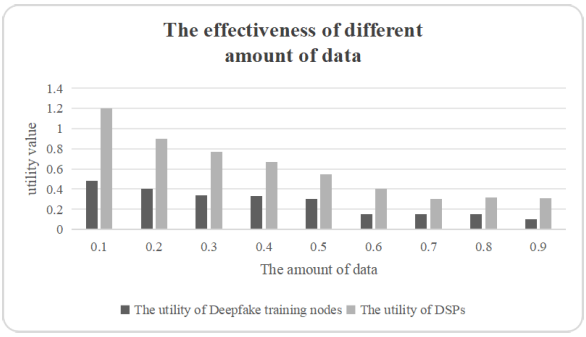

FIGURE 12. Decentralized Content Generation Training (N-IID).

B. RESOURCE ALLOCATION EXPERIMENT

In order to prove the robustness of the algorithm proposed in this paper, the paper designs the changes in the utility of deepfake training nodes and the utility of DSPs under different deepfake training nodes and different total amounts of data. The experimental results are shown in the Figure 11 and Figure 12.

According to the experimental results, under the condition of independent and identical distribution, the training loss value of the federated diffusion model is smaller and the quality of the generated images is higher. Because the

TABLE 4. Comparison of loss value and standard deviation.

	E-MNIST		F-MNIST		KMNIST	
Loss and standard deviation	$\overline{loss}_{E-MNIST}$	$\sigma_{E-MNIST}$	$\overline{loss}_{F-MNIST}$	$\sigma_{F-MNIST}$	$\overline{loss}_{KMNIST}$	σ_{KMNIST}
DD-TMA	**0.371**	0.188	**0.581**	**0.252**	**0.298**	**0.185**
RFRL	0.455	0.277	0.775	0.286	0.389	0.235
GDIUS	0.521	0.207	0.719	0.298	0.403	0.216
DmyT	0.400	**0.154**	0.610	0.267	0.311	0.187
Progress	23.63%	13.12%	20.71%	12.57%	23.38%	14.95%

TABLE 5. Comparison of utility.

	A	B	C	D
DD_TMA	0.25	0.59	0.21	0.35
RFRL	0.16	0.48	0.15	0.28
GDIUS	0.24	0.47	0.14	0.27
DmyT	0.19	0.51	0.21	0.28
Progress	21.33%	17.51%	20.63%	20.95%

data distribution of different devices is the same under independent distribution conditions, the federated diffusion model can be better controlled for global noise training. On the contrary, under non-independent and identically distributed conditions, since the data distribution of different devices is different, the federated diffusion model will over fit the local data and cannot fully utilize the data of other devices to train the global noise, resulting in greater training time. loss. Therefore, the more accurate the federated diffusion model predicts noise, the better it will be at understanding the noise during the inference phase, so the quality of the generated images will be higher.

C. COMPARISON OF EXPERIMENTAL RESULTS

In order to prove the effectiveness of DD-TMA, this paper will use three data sets E-MNIST, F-MNIST, and KMNIST to conduct experiments. In addition, this paper selects three algorithms RFRL [31], GDIUS [32] and DmyT [33] for comparison. The comparison of results is divided into two parts: comparison of loss value and its stability and comparison of utility.

1) COMPARISON OF THE FIRST PART

As the number of training times increases, the loss value gradually becomes stable. This paper compares the average value $\overline{loss}_{Extending-MNIST}$, $\overline{loss}_{Fashion-MNIST}$ and $\overline{loss}_{KMNIST}$ of the loss value of 100-200 global iterations, and uses this value to observe the loss value representing the respective algorithm. Then, by calculating the standard deviation $\sigma_{Extending-MNIST}$, $\sigma_{Fashion-MNIST}$ and σ_{KMNIST} of these loss values, observe the stability of the loss value within this interval.

2) COMPARISON OF THE SECOND PART

As the number of deepfake training nodes increases, the utility of nodes and the utility of DSPs gradually stabilize. This paper compares the node utility average $\overline{nodes}$ and the DSPs utility average $\overline{DSPs}$ in the case of 70-100 nodes. In addition, as the total amount of data increases, the utility of nodes and the utility of DSPs gradually stabilize. This paper compares the average node utility $utility_{nodes}$ and the average utility $utility_{DSPs}$ of DSPs when some data occupy 0.6-0.9 of the total data volume.

The paper set up two sets of experiments to verify and compare the effectiveness of the DD-TMA algorithm. In the first set of experiments, the paper compared the average and standard deviation of the training loss values to verify the loss effect and stability of DD-TMA. In the second set of experiments, the paper compared the utility values of DD-TMA training nodes under different training nodes and different amounts of data to verify the utility value of the training nodes in the algorithm. The higher the utility value, the It shows that edge devices in this algorithm are more involved in calculations. The comparison of experimental results is shown in Table 4 and Table 5.

Based on the comparison of experimental results, the following conclusions can be drawn.

1) In the Comparison of the first part, after this paper conducted experiments on three data sets, DD-TMA obtained the lowest average loss value after 100-200 global iterations of training, which shows that DD-TMA has the lowest training loss. Compared with other algorithms, the effect of DD-TMA is improved by 22.57% on average. At the same time, within this range of iterations, the standard deviation of the loss value calculated based on DD-TMA is also the smallest. This shows that as the number of iterations increases, the stability of the loss value of DD-TMA increases on average compared to other algorithms. 13.55%.
2) In the comparison of the second part, when there are 70-100 deepfake training nodes, the average node utility value based on DD-TMA and the average utility value of DSPs are at the highest level, indicating that both training nodes and DSPs are Used effectively. Compared with other algorithms, the average utility value of DD-TMA has increased by 20.98%. When the data volume occupies the range of 0.6-0.9 of the total data volume, the average utility value of training nodes and the average utility value of DSPs are also at the highest level, proving that the utility based on DD-TMA is excellent. Compared with other algorithms, the average utility value of DD-TMA has increased by 19.23%.

The experimental results of DD-TMA, RFRL, GDIUS and DmyT on three data sets E-MNIST, F-MNIST and KMNIST

prove that under the same conditions, DD-TMA proposed in this paper not only has the lowest training loss value, but also has better results as the number of iterations increases. Hair is stable. At the same time, in decentralized deployment, the utilization efficiency of edge devices is also the highest.

IV. CONCLUSION

In view of the shortcoming that centralized deepfake service providers are particularly prone to single points of failure, this study proposes a decentralized deepfake task management algorithm based on blockchain and edge computing. This research innovatively introduces blockchain, smart contracts and edge computing. First, a platform is built using a decentralized blockchain, and smart contracts are used to automatically distribute deepfake tasks. In order to cope with the problem of insufficient data and computing resources during the execution of deep forgery tasks, this study proposes an innovative decentralized generation mechanism based on blockchain and federated propagation model. This mechanism makes full use of the computing advantages of deep forgery task participants in edge computing and achieves effective utilization of data and computing resources. Finally, in order to encourage all nodes to actively participate in deepfake tasks, this study innovatively proposes a game-based resource allocation mechanism to actively increase deepfake task participants. Next, this research will continue to explore the performance indicators when blockchain, smart contracts and edge computing are simultaneously carried out in a task, as well as the dynamic proportion adjustment of each technology in the same task, hoping to stimulate stronger decentralization. Maximize the potential of deepfake task completion.

REFERENCES

[1] Z. Guo, Z. Zhu, Y. Li, S. Cao, H. Chen, and G. Wang, "AI assisted fashion design: A review," *IEEE Access*, vol. 11, pp. 88403–88415, 2023.
[2] J. Zhou, Z. Liang, Y. Fang, and Z. Zhou, "Exploring public response to ChatGPT with sentiment analysis and knowledge mapping," *IEEE Access*, vol. 12, pp. 50504–50516, 2024.
[3] H. Ning, H. Wang, Y. Lin, W. Wang, S. Dhelim, F. Farha, J. Ding, and M. Daneshmand, "A survey on the metaverse: The state-of-the-art, technologies, applications, and challenges," *IEEE Internet Things J.*, vol. 10, no. 16, pp. 14671–14688, Jul. 2023.
[4] Z. Liu, M. He, Z. Jiang, Z. Wu, H. Dai, L. Zhang, S. Luo, T. Han, X. Li, X. Jiang, D. Zhu, X. Cai, B. Ge, W. Liu, J. Liu, D. Shen, and T. Liu, "Survey on natural language processing in medical image analysis," *J. Central South Univ. Med. Sci.*, vol. 47, no. 8, pp. 981–993, 2022.
[5] A. Sauer, K. Schwarz, and A. Geiger, "StyleGAN-XL: Scaling StyleGAN to large diverse datasets," in *Special Interest Group Comput. Graph. Interact. Techn. Conf. Proc.*, Aug. 2022, pp. 1–10.
[6] Y. Seo, K. Lee, S. L. James, and P. Abbeel, "Reinforcement learning with action-free pre-training from videos," in *Proc. Int. Conf. Mach. Learn.*, 2022, pp. 19561–19579.
[7] M. S. Rana, M. N. Nobi, B. Murali, and A. H. Sung, "Deepfake detection: A systematic literature review," *IEEE Access*, vol. 10, pp. 25494–25513, 2022.
[8] L. Yang, Z. Zhang, Y. Song, S. Hong, R. Xu, Y. Zhao, W. Zhang, B. Cui, and M.-H. Yang, "Diffusion models: A comprehensive survey of methods and applications," *ACM Comput. Surveys*, vol. 56, no. 4, pp. 1–39, Apr. 2024.
[9] J. Yang, H. B. Li, and D. Wei, "The impact of ChatGPT and LLMs on medical imaging stakeholders: Perspectives and use cases," *Meta-Radiology*, vol. 1, no. 1, Jun. 2023, Art. no. 100007.
[10] A. Borji, "Generated faces in the wild: Quantitative comparison of stable diffusion, midjourney and DALL-E 2," 2022, *arXiv:2210.00586*.
[11] B. Çeken and O. Şen, *Grafik Tasarım Sektöründe Yapay Zekanın Kullanılması* (Midjourney), 2023.
[12] U. Singer, A. Polyak, T. Hayes, X. Yin, J. An, S. Zhang, Q. Hu, H. Yang, O. Ashual, O. Gafni, D. Parikh, S. Gupta, and Y. Taigman, "Make-A-video: Text-to-video generation without text-video data," 2022, *arXiv:2209.14792*.
[13] Y. Zhao, L. Li, H. Jia, and S. Wu, "Opportunities and challenges of artificial intelligence generated content on the development of new digital economy in metaverse," in *Proc. 2nd Int. Conf. Artif. Intell.*, 2023, pp. 473–480.
[14] N. Carlini, F. Tramèr, E. Wallace, M. Jagielski, A. Herbert-Voss, K. Lee, A. Roberts, T. Brown, D. Song, Ú. Erlingsson, A. Oprea, and C. Raffel, "Extracting training data from large language models," in *Proc. 30th USENIX Secur. Symp.*, 2021, pp. 2633–2650.
[15] N. Carlini, J. Hayes, M. Nasr, M. Jagielski, V. Sehwag, F. Tramer, B. Balle, D. Ippolito, and E. Wallace, "Extracting training data from diffusion models," in *Proc. 32nd USENIX Secur. Symp.*, 2023, pp. 5253–5270.
[16] A. V. Savchenko, K. V. Demochkin, and I. S. Grechikhin, "Preference prediction based on a photo gallery analysis with scene recognition and object detection," *Pattern Recognit.*, vol. 121, Jan. 2022, Art. no. 108248.
[17] T. Wang, Y. Zhang, S. Qi, R. Zhao, Z. Xia, and J. Weng, "Security and privacy on generative data in AIGC: A survey," 2023, *arXiv:2309.09435*.
[18] A. Broinowski, "The future is hackable: Apocalypse and euphoria in a deepfake world," *Griffith REVIEW*, vol. 1, no. 79, pp. 9–19, 2023.
[19] J. Twomey, D. Ching, M. P. Aylett, M. Quayle, C. Linehan, and G. Murphy, "Do deepfake videos undermine our epistemic trust? A thematic analysis of tweets that discuss deepfakes in the Russian invasion of Ukraine," *PLoS One*, vol. 18, no. 10, Oct. 2023, Art. no. e0291668.
[20] X. Li, Y. Fan, and S. Cheng, "AIGC in China: Current developments and future outlook," 2023, *arXiv:2308.08451*.
[21] N. Su, "Research on multiparty participation collaborative supervision strategy of AIGC," in *Proc. IEEE 13th Int. Conf. Electron. Inf. Emergency Commun. (ICEIEC)*, Jul. 2023, pp. 268–272.
[22] A. Raza, K. Munir, and M. Almutairi, "A novel deep learning approach for deepfake image detection," *Appl. Sci.*, vol. 12, no. 19, p. 9820, Sep. 2022.
[23] S. Rashid Ahmed, E. Sonuç, M. Rashid Ahmed, and A. Deniz Duru, "Analysis survey on deepfake detection and recognition with convolutional neural networks," in *Proc. Int. Congr. Hum.-Comput. Interact., Optim. Robotic Appl.*, Jun. 2022, pp. 1–7.
[24] C. Chen, Z. Wu, Y. Lai, W. Ou, T. Liao, and Z. Zheng, "Challenges and remedies to privacy and security in AIGC: Exploring the potential of privacy computing, blockchain, and beyond," 2023, *arXiv:2306.00419*.
[25] N. Choi and H. Kim, "DDS: Deepfake detection system through collective intelligence and deep-learning model in blockchain environment," *Appl. Sci.*, vol. 13, no. 4, p. 2122, Feb. 2023.
[26] D. Mao, S. Zhao, and Z. Hao, "A shared updatable method of content regulation for deepfake videos based on blockchain," *Int. J. Speech Technol.*, vol. 52, no. 13, pp. 15557–15574, Oct. 2022.
[27] A. Concilio, I. Dimino, and R. Pecora, "SARISTU: Adaptive trailing edge device (ATED) design process review," *Chin. J. Aeronaut.*, vol. 34, no. 7, pp. 187–210, Jul. 2021.
[28] D. Giagkos, A. Tzenetopoulos, D. Masouros, D. Soudris, and S. Xydis, "Darly: Deep reinforcement learning for QoS-aware scheduling under resource heterogeneity optimizing serverless video analytics," in *Proc. IEEE 16th Int. Conf. Cloud Comput.*, Jul. 2023, pp. 1–3.
[29] A. Stein, M. Salvioli, H. Garjani, J. Dubbeldam, Y. Viossat, J. S. Brown, and K. Stanková, "Stackelberg evolutionary game theory: How to manage evolving systems," *Phil. Trans. Roy. Soc. B, Biol. Sci.*, vol. 378, no. 1876, May 2023, Art. no. 20210495.
[30] K. Tam, L. Li, B. Han, C. Xu, and H. Fu, "Federated noisy client learning," *IEEE Trans. Neural Netw. Learn. Syst.*, pp. 1–14, 2024.
[31] Y.-C. Liu, C.-M. Chang, I.-H. Chen, Y.-R. Ku, and J.-C. Chen, "An experimental evaluation of recent face recognition losses for deepfake detection," in *Proc. 25th Int. Conf. Pattern Recognit.*, Jul. 2021, vol. 15, no. 7, pp. 9827–9834.
[32] S. Kanwal, S. Tehsin, and S. Saif, "Exposing AI generated deepfake images using Siamese network with triplet loss," *Comput. Informat.*, vol. 41, no. 6, pp. 1541–1562, 2022.
[33] N. Beuve, W. Hamidouche, and O. Deforges, "DmyT: Dummy triplet loss for deepfake detection," in *Proc. 1st Workshop Synth. Multimedia Audiovisual Deepfake Gener. Detection*, Oct. 2021, pp. 17–24.

YANG YANG received the master's degree in 2019. He is currently pursuing the Ph.D. degree.

He mainly studies urban computing, smart transportation, and blockchain technology. He has published six SCI/EI indexed articles, two articles in Chinese core journals, obtained five national invention patents, and participated in the drafting of one industry standard.

NORISMA BINTI IDRIS received the master's and Ph.D. degrees from Universiti Malaya.

Her research interests include lexical analysis, text normalization, text summarization, machine translation, and sentiment analysis.

DINGGUO YU received the master's and Ph.D. degrees from Tongji University.

In the past five years, he has presided over seven scientific research projects at all levels and published more than 30 articles in internationally renowned journals, such as *Knowledge-Based Systems* (KBS). His research interests include media convergence, media big data and artificial intelligence, and computational communication.

CHANG LIU received the master's and Ph.D. degrees from Northwestern Polytechnical University (NWPU). Her research interests include intelligent processing of media data and intelligent processing of audience feedback. On the one hand, from the perspective of brain cognition, further creative development of artificial intelligence technology plays an important role in improving the level of intelligent media technology. On the other hand, the study of media effects from the perspective of brain cognition will be conducive to a deep understanding and control of the influence of media and the realization of scientific media.

HUI WU received the Ph.D. degree in geography and geographical information systems from the University of Chinese Academy of Sciences, in 2014, and the Institute of Geographical Sciences and Natural Resources, Chinese Academy of Sciences. His research interests include watershed simulation, resource spatial allocation optimization, culture and culture in the context of intelligent media technology, and technology integration.