IEEE Open Journal of the Computer Society

Received 16 August 2023; accepted 8 September 2023. Date of publication 18 September 2023;
date of current version 27 November 2023. The review of this article was arranged by Associate Editor Deze Zeng.

Digital Object Identifier 10.1109/OJCS.2023.3315835

Towards Reliable Utilization of AIGC: Blockchain-Empowered Ownership Verification Mechanism

CHUAN CHEN [1] (Member, IEEE), YIHAO LI [1], ZIHOU WU [1], MINGFENG XU [1], RUI WANG [1], AND ZIBIN ZHENG [2] (Fellow, IEEE)

[1]School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou 510275, China
[2]School of Software Engineering, Sun Yat-sen University, Zhuhai 519000, China

CORRESPONDING AUTHOR: ZIBIN ZHENG (e-mail: zhzibin@mail.sysu.edu.cn).

This work was supported in part by the National Natural Science Foundation of China under Grant 62176269, in part by the Guangzhou Science and Technology Program under Grant 2023A04J0314, and in part by the Sun Yat-Sen University Young Faculty Development Program under Grant 23ptpy109.

ABSTRACT With the development of the blockchain technology, a decentralized and de-trusted network paradigm has been constructed, enabling multiple digital assets like NFT, to be permanently recorded and authenticated by blockchain. Also, the uniqueness and verifiability of these assets allows them to flow and generate value between any network entities. With the emergence of AI Generative Content (AIGC), the ownership of models and generative contents, which are also digital assets, has not been well protected. Both because the black-box nature of neural networks makes it difficult to mark models' ownership and because the lack of a reliable third-party verification platform. Meanwhile, the existing model-attack threat and raising ethical problems driven the research on model watermark embedding for traceability and verification, and thus the reliable basic algorithm and the verification platform are needed. In this survey, while emphasizing the importance and reason of the ownership protection in AIGC and summarizing the recent research using model watermarking, we will also introduce the achievements of blockchain in copyright in order to summarize the research history and point out future direction of model copyright validation from both the underlying technology and the supporting platform.

INDEX TERMS Blockchain, copyright, federated learning, ownership, AIGC.

I. INTRODUCTION

With the rapid development of AIGC, the issue of legal use and copyright protection of the model began to enter people's realization. Researchers begin to study how to design a reliable copyright verification mechanism for the deep learning model and how to provide a infrastructure for verification. In this section, we will introduce the background of the emergence of the AIGC system and the threat it will face during the training and utilization process, which makes the ownership verification mechanism necessary to provide a secure environment. Then, the application of blockchain will be introduced to search the possibility of the combination with the model copyright protection.

A. MACHINE LEARNING SYSTEM AND ISSUE

Nowadays, data flourishes in both amount and source. The Internet, for example, contains vast valuable information that can be used to analyze the behavior of a specific user by training deep learning models. The rapid growth of the computational capacity and data storage ability make it more convenient to build large models. In order to provide better service while fully utilize the data produced by human activity, researchers begin to build kinds of machine learning system to build artificial intelligence to augment working efficient or for the purpose of studying. For instance, we can use an open-source project named YOLO [70] to train our own image segmentation model conveniently. Recent compelling generative models like GPT-4 [64] and stable-diffusion [72]

also provide us with a more convenient AI tools to produce contents. Due to the huge requirement of training data, the integrate process of AIGC from training, deployment to online-service requires the support of a series of machine learning systems, which is also full of challenges to be faced and precautions to be taken in the face of malicious attackers.

From the training process of a deep learning model, various attacks have threatened the safety and privacy of the model and training data. Take the cooperative training paradigm federated learning as an example. During the training, malicious participants threat the global model and entire machine learning system by attack method to disrupt or to leak the global model to infringe the interests of other normal participants. In the FL system, the global model is trained by unreliable devices with their private data, which means the system can be damaged by many kinds of failure including the non-malicious failure like the central server breakdown or noisy training dataset, and the adversarial failure like the byzantine attack. These failures could severely sabotage the training process and reduce the model performance if we ignore them. We may implement the trace for those byzantine or malicious node with the help of ownership verification and trace the leaker with the specific fingerprint planted in the model [77].

Another risk of the AIGC system is data leakage. Nowadays, with the model reuse attack, the attacker can just simply copy the others' model and get some profit from the training process or distribution process of the model or generative contents. Meanwhile, training data is another precious resource. The large generative model needs lots of training data to achieve good performance. When it comes to federated learning system, the training data leakage problem is actually generating differential privacy (DP) among the framework [22]. By using DP strategy, one can disturb their upload models to prevent other achieving the original model parameters. However, as we keep encrypting the local model and data, it becomes harder to get a well-performed model. Another way to protect private training data in defense of the data abuse, we can plant a specific fingerprint into our own data to mark models which is trained based on these data. Under these circumstances, the malicious model and unauthorized use will be recorded and detected once they participate in the training process.

B. BLOCKCHAIN AND PROBLEMS

While the model ownership verification mechanism is required to solve many challenges during the production of AIGC, the blockchain system was designed to permanently keep the transaction information and thus grow many ownership and copyright application on it.

Blockchain originates from online transactions. It was first proposed by in 2008 for processing transactional information of Bitcoin [62] in P2P networks. With the progress of the era, blockchain has attracted broad attentions. Previous studies have argued that blockchain should not be limited to being synonymous with Bitcoin or cryptocurrency, but rather be explored and applied in various domains to leverage the advantages of blockchain technology. Recent empirical evidence has alighted with these assertions.

Copyright protection is recognized as a significant application of blockchain technology. The distinct consensus mechanism employed by blockchain guarantees consistency in decentralized systems, thereby presenting promising prospect, even in the absence of a central authority. Savelyev [75] raised several key issues in copyright protection, such as copyright transparency, control over digital copies, license issuance, and argued that blockchain technology can effectively address them. At the application level, researchers have proposed corresponding blockchain-based solutions for various issues, such as code copyright protection [39], integrated circuit IP core protection [53], and numerous others. With the iterative advancement of blockchain technology, the emergence of non-fungible token (NFT) signifies a new era for copyright protection. Wang et al. [87] have provided a comprehensive discourse on the principles and prospects of NFT. Leveraging smart contracts based on blockchains, NFT enables efficient and convenient proof of ownership for virtual assets or intellectual property rights. Guadamuz [33] combines the technological perspective with the legal perspective to discuss the relationship between NFT and copyright protection. With these applications on copyright recording and verification, we decide to explore the possibility of combining the blockchain with the model ownership verification.

In summary, the contributions of this article are listed as follows:

- This article summarizes basic technologies of the model ownership verification.
- This article summarizes the challenges and the solution of the AIGC system and specifically presents the ownership verification method.
- This article points out a possible route for constructing a reliable model verification mechanism towards a more proper utilization of AIGC.

The article will be organized as follows: the second chapter will introduce some basic technology for the whole procedure of building a AIGC system with ownership verification. Some key technology like federated learning, blockchain and model watermark technology will be introduced. Chapter 3 will list the risk faced by the existing AIGC system and some related works resolving these problems. The next chapter explore the potential of the blockchain to provide a reliable ownership verification platform to give a more reliable platform for fixing the facing risk introduced in chapter 3. And the last chapter will give the summary of the article and describe the future work to provide a more robust and reliable AIGC system built on ownership verification platform.

II. PRELIMINARY

A. FEDERATED LEARNING

Federated learning (FL) [60] is a typical cooperative machine learning paradigm. The FL appears under the consequence

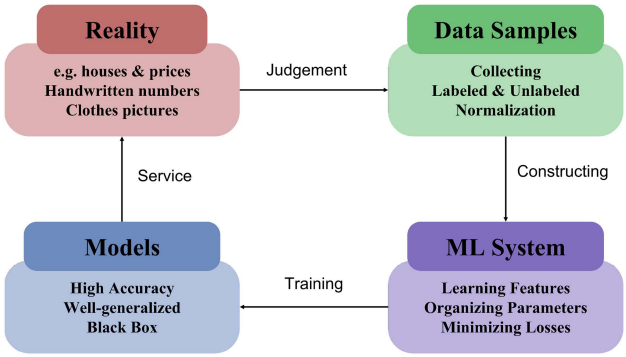


FIGURE 1. Federated Learning Flow Chart: The data derived from the real world (red block) is preprocessed and becomes dataset and used by the machine learning system.

which the traditional method training way may encounter obstacles in gathering information and protecting data privacy and the single trainer may also face the problem of lacking the dataset. FL enables multiple clients to train a global model without leaking their private training data. Due to the great amount of training dataset used in generative models and other artificial intelligence system, the existing federated learning framework such as FedML [36] provides individuals and smaller companies with a chance to build their own large model [92], [88]. To put FL into actual practice and to have decent performance, there still needs some further investigation to solve these problems and get improvement. The workflow of the federated learning is illustrated in Fig. 1.

The major benefit of FL is that framework can deploy all the clients' data without actually acquiring them, which can save the communication cost and protect privacy. Below we will provide some introduction on some fundamental and important algorithms and concepts in FL.

- *FedAvg:* This is the most fundamental algorithm in FL [60]. The framework is simple (distribute, train locally and aggregate globally by averaging the parameters of the uploaded models). When there's no threats or special occasion in reality situation, FedAvg is powerful. Yet, the reality is not perfect, therefore we need to make some improvement.
- *FedProx:* A novel modification on FedAvg. A brief introduction of FedProx is that during the client local training, the cost function has an additional penalty regularization term to punish those models which deviate too much from the initial global model [50]. This method is to make some restrictions on the statistic heterogeneity of clients.
- *Federated Dropout:* This is applicable in federated training a massive neural network. For some limited-resource clients which doesn't process strong calculation and communication capabilities, it's wise to train a model that is only a fraction of the global (such as a smaller hidden layer) to reduce the burden and boost the efficiency [11]. There are also similar methods like HeteroFL and FedRolex.
- *FedBN:* One major kind of clients' statistic heterogeneity is feature shift, which means different client's dataset has different distribution of feature. Simply using FedAvg framework will cause poor performance of the final global model. FedBN could be a solution to this. The main content of FedBN is leaving the Batch Normalization layer trained in the local clients and don't participate in global aggregation [51].
- *FedAsync:* The major characteristic of FedAsync is asynchronous, meaning that the global update is not synchronous, the update can take place whenever there's a new local model sent from the client and we don't have to wait for those slow-functioning clients [91]. This has much speed advantage compared to FedAvg, but its drawback is that it might ignore the contribution of small clients.

B. BLOCKCHAIN

Blockchain is basically a kind of linked list, where the transaction information is stored in sequential blocks. The functionality of blockchain is based on its rich technology stack.

1) HASHING DIGITAL SIGNATURES

Since blockchains, especially public chains, are deployed on the Internet, participants are assumed to be mutually distrusting by default. This requires the use of cryptographic methods to achieve proof of trustworthiness between users. Hashing and digital signatures can achieve this. A hash function is a one-way function that maps input information of arbitrary length to output information of fixed length. One-way means that it is difficult for anyone to infer the input value from the output value, and thus hashing is generally used to verify the integrity of information [17]. The timestamp server in the Bitcoin protocol uses hashing to verify whether a block is truly the child block of the block which it claims to be the parent block. Digital signature technology is based on hashing and public key cryptography [18]. In addition to hashing, it can also verify whether the source of a message is consistent with expectations. In blockchain protocols, digital signatures are generally used to verify transaction information.

2) CONSENSUS MECHANISM

Blockchain is a distributed system, so it requires a consensus mechanism to coordinate each participant in the system and ensure their data consistency. It also has a certain degree of fault tolerance to address potential Byzantine general problems [46]. The common consensus mechanisms in blockchain are as follows. *Proof-of-Work (PoW)* is used in Bitcoin [62]. Each node in the network calculates the hash value of the block header, and the values calculated by each node are usually different. Only nodes whose calculated values are less than or equal to a given value have the right to append their blocks to the chain. Nodes participating in the calculation are called miners, and the calculation process is called mining.

Most of the computing power in PoW is wasted, resulting in a huge waste of energy. *Proof-of-Stake (PoS)* improves this deficiency [45]. It refers to the cryptocurrency pledged by nodes as stake and uses it as a condition for obtaining the right to verify new blocks on the chain. *Partial Byzantine Fault Tolerant (PFBT)* can maintain system consensus when less than 1/3 of the nodes are Byzantine [13]. With additional features such as hashing [6], it can also serve as an efficient and environment-friendly blockchain consensus mechanism. The consensus mechanism can also be modified according to the specific purpose of the blockchain, such as proof-of-learning mentioned earlier in the article.

3) DISTRIBUTED LEDGER

Distributed ledger is the fundamental technology for cryptocurrencies. The working principle of a distributed ledger can be described as follows: Within the system, there are multiple ledgers. Whenever a record in one ledger undergoes a change, this action follows a set of rules to propagate to all other ledgers [69]. In other words, a distributed ledger ensures the consistency of records. Therefore, this technology requires the implementation of a consensus mechanism. One major challenge of distributed ledgers is network attacks, particularly during the data synchronization process. In practice, the hash technology used in blockchain can help mitigate such attacks [23]. This technology is applicable to decentralized transactions, avoiding system crashes caused by the failure of central nodes in centralized storage. It also greatly reduces the cost of trust. Therefore, distributed ledger serves as a key application of blockchain technology.

4) SMART CONTRACT

In essence, a smart contract is code stored on a blockchain that is triggered and executed under specific conditions. Simultaneously, the intermediate variables and outcomes generated by the code are also stored on the blockchain. Smart contracts were initially proposed by Nick Szabo in 1997 [82], but at that time there was no corresponding technology available to realize this concept. It was not until Ethereum implemented smart contracts as its core functionality [10] that smart contracts began to be applied in practical scenarios. By utilizing smart contracts, blockchain technology can be extended to various aspects such as peer-to-peer (P2P) transactions, the Internet of Things (IoT), data provenance and the sharing economy, significantly broadening its application scope [101].

The secure and decentralized bottom stack gives the blockchain the ability to combine with the machine learning system to provide a secure environment. Shafay et al. [76] reviews applications of blockchains for machine learning, including healthcare [5], which demonstrate blockchain technology's complementary role in privacy protection for AI. Shayan et al. [79] proposed a large-scale multi-party machine learning scheme which exhibits the capability to maintain model performance even in the presence of 30% adversarial participants. Furthermore, blockchain technology can also incentivize users to contribute their computing power to participate in deep learning model training through cryptocurrency-based rewards, thereby effectively utilizing redundant computational resources. Currently, there exist federated learning protocols that utilize the Shapley Value (SV) [78] as a metric for measuring the contribution level of users during training. Blockchain entities release the computation of SV as a puzzle and provide rewards to users participating in the training process through the blockchain [55].

C. MODEL WATERMARK TECHNOLOGY

As a valuable information resource on the Internet, multimedia resources are the main carriers of information in the web 2.0 era [14]. Due to the arbitrary copying nature of the Internet, it is difficult to identify the real owners and copyright holders of these resources, which leads to many attackers to gain benefits from malicious and unauthorized copying of these resources. Some may even launch cyber attack through changing a reliable resource. Digital watermarking technology has long been used to verify the copyright and the integrity of multimedia resources [67]. With the coming of deep learning and the era of big models, deep learning models are also served as a network resource with intellectual property rights. Digital watermarking techniques have also inspired researchers to use watermarking techniques to prevent serial attacks, illegal use, and other problems towards the models. By introducing traditional watermarking techniques and then turn to the model watermarking techniques applied to deep learning models, we give a development route on the protection of the digital assets.

Traditional resources such as images, multimedia audio and video face the threat of illegal use, content tampering and other attacks, causing both security and economic threats to both parties distributing and using the resources [84].

Different with the multimedia resources, it is hard to predict the changing of performance of the deep learning models by applying the traditional watermark embedding methods to change the parameters directly. To face the above challenge, most of the current watermark embedding methods use optimization or deep learning strategy to make the watermark participate in the model training process. These methods aim to inject watermark which can be identified by some designed mechanism to the model without changing the original function of the model. The common models can be divided into discriminative and generative models, and for these two different models, several different watermark embedding methods are introduced below.

- *Fingerprint-based methods [77], [48], [25]:* This approach is inspired by traditional watermark embedding methods, where the layer parameters of a neural network are treated as traditional data and embedded directly into the watermark. As mentioned earlier, since it is not clear how changing model-specific parameters will affect the neural network, some optimization or deep learning methods are still needed to assist the embedding

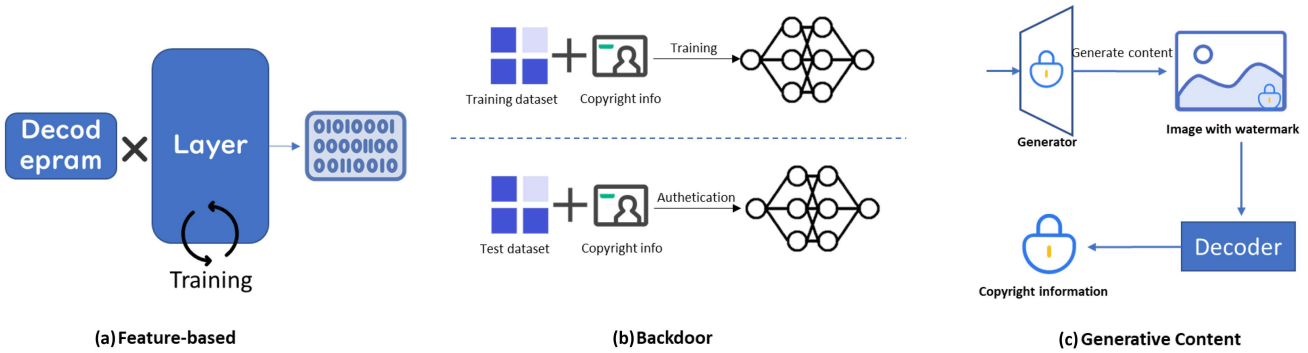
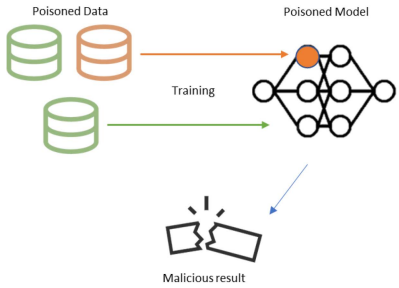
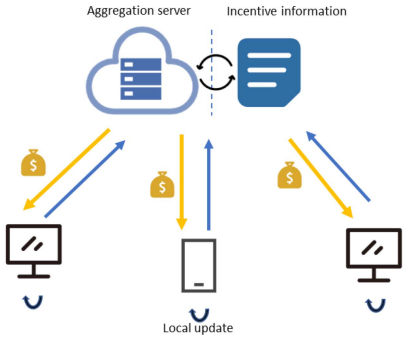
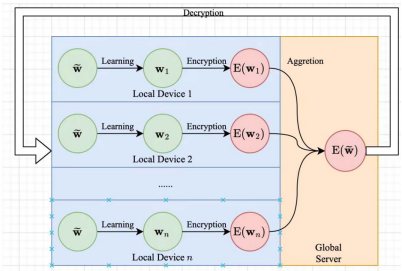


FIGURE 2. Model watermarking technology.

TABLE 1. Challenging Problems in AIGC Systems

Model Attack	Incentive Mechanism	Data Privacy
		
• Poison attack [40] • Free-rider attack [27], [54] • Leakage attack [77] • Inference attack [61]	• Game theory based [74], [43] • Reinforcement learning based [86], [98] • Shapley Value based [81]	• Differential privacy [22], [83] • Homomorphic encryption [71], [24]

process to ensure that the functionality of the model is not affected by the watermark embedding. The advantage of this approach is that the detection and robustness of the watermark are more stable.

- *Backdoor-based methods [3], [57], [66]:* Backdoor attacks were originally studied as a model attack method [35], where the attacker inserts a specially designed trigger into the training set data and identifies the samples containing the specific trigger as a specific label during the model training process. in the model watermarking method, this trigger can then be used as a non-visible watermark of the model by observing In the model watermarking approach, this trigger can be used as a non-visible watermark for the model, and by observing the model's output for the samples containing the trigger, we can know whether the model contains a watermark or not.
- *Watermark insertion into generators [26]:* This is a watermark embedding method designed for generative models, and the generative modules (VAE, GAN) of generative models can be designed so that the generators contain special watermarks that can be detected by decoders. At a time when AIGC has made significant progress, attention is being paid to designing watermark embedding methods applicable to AIGC models.

In summary, the model watermarking technology use a specific binary data series and some designed method to insert directly or indirectly into the parameters which can be detected in the model or the output of the model. In Fig. 2, we summarize the main technology for model watermarking with 1) embeds the watermark into the parameter into the parameters, 2) use backdoor sample and 3) embeds the watermark into the generative contents for generative models.

III. ADVANCED RESEARCH AND CHALLENGES IN AIGC SYSTEM

In this section, we will introduce the risk and challenge faced by the machine learning system (Table I) and introduce the role in which the ownership verification mechanism can play to help solve these problems.

A. MODEL ATTACK

During the training process of an AIGC models, especially the federated training process, the mission is completed by massive number of individuals. Under this circumstance, there may involve some participants who has the evil goal to attack the FL process diminish the benefit of FL group or to leak the training process to gain some profit. The malicious participant may execute kinds of attack to disrupt the system. Judging by the attacking behavior and the target, We categorize the attack method as follows: *poison attack*, *leakage attack*, *free-riding attack* and *inference attack*.

1) POISON ATTACK

Poison attack means a byzantine client will use poisoned data or model to sabotage the training process. Depending on the attack goal, there are two kinds of poison attack [40].

- *Untargeted:* The malicious client is training model with random data or just sending random model to the server, therefore its goal is just to create chaos and worsen the model performance.
- *Targeted:* The malicious client is trying to change some small function in the model like misclassifying some labels while behaving well in other aspects.

When a Byzantine Client is acting poison attack, the model (or gradient) it sends is different from the other honest models, which is a breakthrough of defending methods, finding the difference among the models can help detect the poison model. Many novel and powerful defending mechanisms has been put forward under this point, such as Krum [8], Bulyan [34] and FLTrust [12].

2) LEAKAGE ATTACK

In some cases, the malicious clients don't have a specific goal to sabotage the FL training process, nor do they want to reduce the model performance. Instead, they want to improve it to the best level, in this occasion they want to steal the model to the external parties for some benefit, that is also a kind of attack. Although it doesn't damage the model property, it does harm the intellectual property of other FL group members.

An effective way to prevent leakage attack is planting a backdoor watermark in the model [77] or planting the fingerprint into the parameters of the model, training the global model with some specific trigger set, making it be able to react to these set with a specific action. When there's a suspicious model on the outside, in this way we can recognize our model by the watermarks.

3) FREE-RIDING ATTACK

Some participants may want to join in the federated learning system and benefit from the incentive mechanism without paying cost to train, and thus they just download the global model and fine-tune the parameters. We call this type of attack the free-riding attack [27], [54]. This attack doesn't have an obvious damage on training side but is unfair to other participants who have paid lot of calculation power on training process. It is difficult to distinguish the attacker and the model owner since the free-rider model is similar to the original model [68].

4) INFERENCE ATTACK

Another kind of attack which doesn't harm the global model named inference attack. In the inference attack, attackers infer the information of other clients and the privacy of the latter is leaked, this could be a severe problem since the initial purpose of FL is to protect the privacy. There are some methods of inference attack, like collecting the snapshots of training global model [61] or constructing some generative network like GAN to infer information about the data distribution of other clients. There are also some countermeasure to defend [40]. First one is Differential Privacy, which, in simple word, is adding some random noise in the local model before sending to the server, keeping the adversary to deduct the real local model of other clients. Another one is Homomorphic Encryption, where the data is firstly encrypted and then encounter calculation of global model, then decrypted in local client, protecting the privacy to leak from the server.

For general model training, we analyze various model attack methods during the training period. While for AIGC in particular, the model will be published on the internet for the commercial or academic propose. Thus, the attacker beyond the training process will also threaten the utilization of the AIGC. Here the tampering of ownership and the plagiarizing of AIGC will be simply described: The middle man attack which third-party malicious client will just simply pretend to be an AIGC website providing the service, but in fact they only forward the user's requests to the real platform providing the service and return the results they return to the user. The third-party malicious client will simply pretend to be an AIGC website providing a service. However in the reality, they just forward the user's request to the real platform providing the service and return the results they return to the user. On the one hand, users may not get the best quality AIGC resources, and on the other hand, the interests of the original AIGC providers will be threatened by these intermediaries.

The uselessness of these attacks during the training period or during the use of the model makes the use of AIGC threatened, and the better methods proposed by the academic community for these attacks will also be described in detail later.

B. INCENTIVE MECHANISM

Apart from preventing the malicious node from destroying the normal function of the whole system. The incentive mechanism is also a crucial key to the better utilization of the AIGC system. The incentive mechanism in federated learning means to give the participant a reasonable profit according to their contribution to the whole systems. For AIGC, in addition to the incentives of each participant under the federated learning paradigm need to be allocated, the allocation of incentives

for subsequent generator content [20] is also an issue worth considering.

The survey [96] gives us an overview of the incentive mechanism of the federated learning to better allocate the resource in the entire training system. Some of classic and widely-used incentive algorithms will be described below. During the training process, the contribution of each client will be quantified as a number by some specific algorithm. Shapley Value is a classic value designed to calculate the contribution to a system [81]. Because its nature, the combination with the federated learning is widely researched to better predicted a value according to the accuracy of the model and to other strategies [85]. Also, for the high calculation power needed by Shapley Value in FL, many approximation algorithm are also proposed to accelerate the incentive evaluation progress [38], [95]. Other methods using the Game theory like Stackelberg Game [74], [43] problems or using reinforcement learning [86], [98] to automatically decided which client deserves better profit also have a good performance on this problem. Many incentive mechanisms in federated learning is proposed, and what we will discuss in the next section is to provide the incentive mechanism a good platform to execute and the ownership verification mechanism to mark the unique contributors.

In summary, incentive mechanisms play an important role in federated learning. It can stimulate cooperation among participants, protect data privacy, and ensure the fairness and credibility of federated learning. Through reward mechanisms, consensus algorithms, smart contracts, and penalty mechanisms, blockchain provides a secure, transparent, and trustworthy environment for federated learning, promoting its application and development in various field.

C. DATA PRIVACY

1) DIFFERENTIAL PRIVACY

Differential privacy is a method in database security that defends against differential attacks. Its objective is to protect individual data from being disclosed or inferred without altering the overall statistical properties of the database [21].

It is demonstrated that incorporating specific Gaussian noise into a deterministic function can satisfy differential privacy [22], which forms the foundation for the application of differential privacy in machine learning, and even deep learning. In deep learning, it is sufficient to impose a threshold constraint on the gradients of the objective function during each iteration of the SGD algorithm and incorporate Gaussian noise related to the threshold, to ensure that the model satisfies differential privacy [1].

Due to the frequent utilization of the SGD optimization algorithm in federated learning, several differential privacy federated learning frameworks have been proposed at present. Kim et al. conducted a comprehensive theoretical analysis of local differential privacy in federated learning and proposed metrics for balancing privacy and efficiency [44]. Wei et al. [89], on the other hand, introduced and analyzed a global differential privacy algorithm for model aggregation, demonstrating its efficiency and convergence properties.

Federated learning empowered by differential privacy presents numerous opportunities for further research and expansion. Triastcyn and Faltings [83] applied the relaxed version of differential privacy, namely Bayesian differential privacy, to federated learning in order to enhance its performance. Hu et al. [37] introduced differential privacy into personalized federated learning, allowing models to be personalized based on user preferences while preserving the privacy of individual data. Additionally, Meta AI has released an open-source differential privacy library [94] to facilitate the convenient integration of differential privacy mechanisms into a wider range of machine learning or federated learning projects. Differential privacy, which effectively balances efficiency and privacy, has emerged as the mainstream privacy protection mechanism in federated learning.

2) HOMOMORPHIC ENCRYPTION

Homomorphic encryption (HE) is an effective method for protecting federated learning models. The ciphertext after HE can obtain the ciphertext corresponding to the addition or multiplication result between the plaintexts through specific operations [2]. That is to say, the aggregation server of federated learning can complete the aggregation process by only knowing the ciphertext and avoid the risk of data leakage accompanied by directly reading gradient information.

PHE schemes appeared earlier. The famous public key encryption schemes RSA [71] and Elgamal [24] both have multiplicative homomorphism, but this property is not useful for federated learning. However, Paillier cryptosystem [65] is in line with federated learning with its additive homomorphism, since only the average of the local gradients needs to be calculated in the aggregation stage then only addition is needed. Given that the gradient data is represented by floating-point numbers, a scheme is needed to convert floating-point numbers into integers to meet the input requirements of Paillier encryption. Zhang et al. [97] used this idea to propose a scheme for batch encoding gradients for encryption and designed a cross-silo federated learning framework with PHE based on this. PHE has an acceptable computational overhead, and its applications have reached a mature stage.

The concept of FHE was proposed early on, but the first practical implementation was introduced by Gentry [29] in 2009. Current FHE schemes typically share common characteristics: performing addition or multiplication operations on ciphertext introduces noise into the resulting output, and excessive noise can render the ciphertext infeasible to decrypt. To address this limitation, *bootstrapping* is commonly employed in the schemes to reduce the noise and obtain "fresh" ciphertexts [30]. Cryptographers have proposed numerous FHE algorithms based on Gentry's research, among which BGV [9] scheme and GSW [31] scheme, both designed for encrypting integers, have landmark significance. However, since gradient information is typically represented

(a) Malicious Behavior Track (b) Incentive Mechanism (c) Copyright Protection

FIG. 3. Application of the model ownership verification.

using floating-point numbers, it is more suitable to introduce the CKKS scheme [16], designed specifically for encrypting real numbers, into federated learning. Certainly, these encryption schemes need to be modified to accommodate the characteristics of federated learning when applied in practice. For instance, in the xMK-CKKS federated learning framework [58], each local model has its own key. All the local keys are combined to form a global key for model aggregation. This approach ensures the protection of both user information and local model information. While possesses excellent properties, computational requirements of FHE are still too demanding given the current level of computing power, especially in the context of bootstrapping. Hence, reducing the complexity of FHE algorithms is a crucial challenge.

IV. BLOCKCHAIN-EMPOWERED RELIABLE AIGC TRAINING SYSTEM

Blockchain, as a distributed database, has long been the basis of research in building a secure and reliable machine learning system. For the problem of single point of server failure in federation learning, blockchain introduces decentralized training architecture to make federation learning free from this problem and so on. This section will discuss about how blockchain provides a secure and reliable platform for AIGC in the following three aspects. As we summarized in Fig. 3, with the embedding of the watermark, many applications based on this mechanism can be created such as 1) the track of the malicious client or model and 2) as the record for conducting incentive mechanism and for the model copyright protection with the embedded model.

A. SECURE AND PRIVACY MACHINE LEARNING SYSTEM

For a secure machine learning system, the primary goal is to prevent potential malicious client attacks. A secure machine learning system provides with the participant an environment to make sure they will train a clean model without any latent backdoor and make sure the profit of all participant get well protected. As mentioned in the previous section, such potentially malicious nodes may compromise the whole system by lurking in the system and by some covert means. Shuo Shao et al. [77] designed the FedTracker model by adding a watermark to the federated learning model through a backdoor watermarking method to record the ownership information of the federated learning parties for the copyright by returning to each model by inserting a detectable watermark into each returned model to find out the malicious client who leaks the privacy model. And WAFFLE [7] watermark model is the first federated leaning watermark mechanism for the server to prevent the free-rider attacks. Blockchain has already been used in preventing the attack in the federated learning. The Muhammad Shayan et al. presented Biscotti [79] to prevent the poison attack and other node failure problem which could influence the final performance of the system. Biscotti is the first system to provide the privacy-preserving by designing a secure distributed blockchain ledger.

Flock [19] propose to use smart contract technology to achieve a secure and reliable decentralized FL system which guarantee model quality by designing a novel P2P review and reward mechanism to detect and deter malicious clients. Y Li et al. [52] designs an committee mechanism to elect some good-behavior node as the supervisor of the whole system to detect the malicious models in the federated learning system. And Truc Nguyen et al. [63] design an mechanism by designing a secure client selection to prevent the possible attack lies in the client. While BlockDFL [99] designs a integrate system through a voting mechanism to defend poisoning attacks while achieving efficiency and scalability. Many of these mechanism needs the cooperation among many clients which are of the equals levels. And the traditional centralized mechanism FL system cannot satisfy these form of cooperation. And HBFL [73], Block Hunter [93] and secure aggregation [41] aim to do some invasion detection on the blockchain which deploys on the IoT.

B. INCENTIVE MECHANISM FOR PARTICIPANTS

Another important function of AIGC system is a reasonable incentive mechanism. The incentive mechanism contains not only the training process but also the AIGC trading process. During the generative content providing process, some attackers will apply middle man attack by simply copying the

generative content of other generative models and provide them to the user for profit. The malicious trading behavior should be recognized and apply punishment mechanism for the malicious clients. These malicious nodes need mechanisms to punish them while also making it more reasonable for nodes which are training normally to gain the profit they deserved. We call this kind of algorithm that rewards good nodes and punishes malicious nodes the incentive mechanism. Since the general incentive mechanism is first done on centralized nodes, this centralized paradigm makes it difficult to accept the incentive algorithm even for good design by the training parties involved in the learning. Therefore, designing an automatically executed decentralized incentive algorithm on the blockchain becomes particularly important in a practical system.

As with early blockchain design concepts, the incentive distribution mechanism has long been built into the blockchain's entire algorithm. Miner rewards refer to the PoW consensus mechanism where miners receive a certain amount of digital currency as compensation after completing the excavation of a block [32]. This reward mechanism can motivate miners to participate in mining competitions and improve the overall system security. And to the PoS [45] consensus mechanism where nodes holding a certain amount of digital currency receive interest income. This reward mechanism can make the consensus process more decentralized, further improving the security and stability of the entire system. For the other application, a proper incentive mechanism is also a crucial key to a more active system.

To federated learning, Kang Jiawen et al. [42] propose a reputation based worker selection scheme to achieve reliable federated learning by using a multi weighted subjective logic model. Also, an effective incentive mechanism combines reputation with contract theory to encourage high reputation mobile devices with high-quality data to participate. Martinez Ismael et al. [59] propose to record the contributions to make an accurate payment of high-quality data contributions.

Article [15] reviewed the research on the combination of blockchain and machine learning technologies and demonstrated that they can collaborate efficiently. And for the ownership verification, the blockchain has adopted the concept of tokens to mark the ownership of a digital assets. The application of token has risen the emergence of NFT and other ownership. What we want to point out is that like all the digital assets, the blockchain can also tokenize the model ownership information for a better execution of the incentive mechanism, while using smart contract to better supervised for the benign distribution of a incentive mechanism. In the article [100], the author collected and processed the latest Ethereum data on the chain and named the dataset XBlock ETH, which mainly includes blockchain transactions, smart contracts and virtual currencies, and also provides basic statistical use of these datasets.

The proper model ownership verification mechanism is also also a key part of the profit distribution. Blockchain technology can provide the following functions in model authentication: The decentralized and tamper resistant nature of blockchain enables the ownership records of the model to be reliably preserved on the blockchain. This means that the owner of the model can confirm ownership on the blockchain and prove their ownership of the model. Paper [90] employ the payment channel techniques to design and implement EdgeToll, a blockchain-based toll collection system for heterogeneous public edge sharing. Test-bed has been developed to validate the proposal and preliminary experiments have been conducted to demonstrate the time and cost efficiency of the system. Other field has already combined the blockchain with the ownership to achieve a more accurate result [80], [49].

Model ownership refers to the process of assigning intellectual property and ownership to machine learning models. In traditional machine learning environments, ownership of the model usually belongs to the data owner or model developer. However, in distributed learning environments such as Federated learning, the training of models involves multiple participants, so the determination of model weights becomes more complex. The blockchain still need a more robust technology to record the ownership information.

C. COPYRIGHT AND OWNERSHIP

With the emergence of the large generative model and its application, the copyright issue of the model comes into view, while for the application on this issues, blockchain has been in place for many years [39]. Since the creation of blockchain, copyright recording for digital assets has been one of its most important applications. Recording the ownership of the cryptocurrency is the basic function of blockchain. The advanced application such as NFT [28], which records and determines the attribution of digital art collections through meta-information, also aims to record the information of copyrights and ownership permanently on the chain. With the increasing research of the applications of blockchain, more and more digital assets have been designed to be managed with the help of blockchain platform. Through the immutable nature of blockchain, it can implement the authentication of the owner of these resources to protect the rights and interests of the owner, and make the circulation of these digital assets faster and more convenient. Many studies are already focus on blockchain networks designed for many different forms of digital assets to manage these resources. The article [56] designs a blockchain-based management platform for multimedia resources. Since it is difficult for a centralized platform to ensure the integrity of data and the fulfillment of listed obligations, the article designs a multi-level access control mechanism. Again, the attribution of visitors and media resources is verified and different access levels are assigned. The article [4] provides an Internet database platform for music creation through a blockchain platform, using the decentralized and tamper-proof features of the Ethereum blockchain to store music works and protect the copyright information of music albums. The design and implementation of the system model and data storage are proposed, and the process of

storing data through Ethernet smart contracts is flowed out in detail.

For deep learning models which are also one kind of digital assets producing contents and profits for the internet, it is difficult to use a centralized strategy for copyright recording and verification of models, especially in scenarios that are sensitive to single point failure and untrust central nodes. The blockchain has a long history of research for copyright verification of various digital assets, and thus we can study how to establish a suitable mechanism to achieve copyright verification for deep learning models by combining existing algorithms. This can be considered as a direction which can be applied for model copyright verification at present. The paper [47] accomplishes the authentication and transaction of both sides of AIGC generators transaction through blockchain. By recording the information of the generative model provider on the blockchain to realize the authentication and confirmation of the model.

V. CONCLUSION

This survey explores the existing problem in the AIGC machine learning system and the necessity of introducing the ownership verification to give these problem a new mechanism to be solved. Also, we summarize the success achieved by the blockchain in the copyright domain and analyze the potential of blockchain playing a key role in managing the ownership verification and provide AIGC and other model a reliable environment to be trained, deployed and traded without illegal use or other copyright problems. All these aims to provide the AIGC a safe and fair environment to be trained, distributed and exploited and make the formalization of the market of the AIGC a possible future. Still the research on the watermark technology is under developing to provide a more robust and accurate algorithm for us to record the true owner of a specific model and give a new way to solve the improper behavior laying under the whole system of AIGC.

REFERENCES

[1] M. Abadi et al., "Deep learning with differential privacy," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 308–318.

[2] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," *ACM Comput. Surveys (Csur)*, vol. 51, no. 4, pp. 1–35, 2018.

[3] Y. Adi, C. Baum, M. Cisse, B. Pinkas, and J. Keshet, "Turning your weakness into a strength: Watermarking deep neural networks by backdooring," in *Proc. 27th USENIX Symp.*, 2018, pp. 1615–1631.

[4] I. Adjei-Mensah, I. O. Agyemang, C. Sey, L. D. Fiasam, and A. A. Salako, "Securing music sharing platforms: A blockchain-based approach," 2021, *arXiv:2110.05949*.

[5] R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, S. Ellahham, and M. Omar, "The role of blockchain technology in telehealth and telemedicine," *Int. J. Med. Inform.*, vol. 148, 2021, Art. no. 104399.

[6] E. Androulaki et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, 2018, pp. 1–15.

[7] B. G. A. Tekgul, Y. Xia, S. Marchal, and N. Asokan, "Waffle: Watermarking in federated learning," in *Proc. IEEE 40th Int. Symp. Reliable Distrib. Syst.*, 2021, pp. 310–320.

[8] P. Blanchard, E. M. El Mhamdi, R. Guerraoui, and J. Stainer, "Machine learning with adversaries: Byzantine tolerant gradient descent," in *Proc. Adv. Neural Inf. Process. Syst.*, 2017, pp. 118–128.

[9] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "Fully homomorphic encryption without bootstrapping," in *Cryptology Eprint Archive*, 2011.

[10] V. Buterin, "A next-generation smart contract and decentralized application platform," in *Ethereum White Paper*, 2014.

[11] X. Cao et al., "FLTrust: Byzantine-robust federated learning via trust bootstrapping," in *Proc. ISOC Netw. Distrib. Syst. Secur. Symp.*, 2021.

[12] X. Cao, M. Fang, J. Liu, and N. Z. Gong, "Fltrust: Byzantine-robust federated learning via trust bootstrapping," *arXiv:2012.13995*, 2020.

[13] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," *OsDI*, vol. 99, pp. 173–186, 1999.

[14] C. Chen et al., "When digital economy meets web3.0: Applications and challenges," *IEEE Open J. Comput. Soc.*, vol. 3, pp. 233–245, 2022.

[15] F. Chen, H. Wan, H. Cai, and G. Cheng, "Machine learning in/for blockchain: Future and challenges," *Can. J. Statist.*, vol. 49, no. 4, pp. 1364–1382, 2021.

[16] J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic encryption for arithmetic of approximate numbers," in *Proc. 23rd Adv. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*,, 2017, pp. 409–437.

[17] I. B. Damgård, "A design principle for hash functions," in *Proc. Conf. Theory Appl. Cryptol.* 1990, pp. 416–427.

[18] W. Diffie and M. E. Hellman, "New directions in cryptography," in *Democratizing Cryptography : The Work of Whitfield Diffie and Martin Hellman*, 2022, pp. 365–390.

[19] N. Dong, J. Sun, Z. Wang, S. Zhang, and S. Zheng, "Flock: Defending malicious behaviors in federated learning with blockchain," 2022, *arXiv:2211.04344*.

[20] H. Du, J. Wang, D. Niyato, J. Kang, Z. Xiong, and D. I. Kim, "AI-generated incentive mechanism and full-duplex semantic communications for information sharing," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 9, pp. 2981–2997, Sep. 2023.

[21] C. Dwork, "Differential privacy," in *Proc. 33rd Int. Colloq. Automata, Languages Program.*, 2006, pp. 1–12.

[22] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Foundations Trends Theor. Comput. Sci.*, vol. 9, no. 3, pp. 211–407, 2014.

[23] N. El Ioini and C. Pahl, "A review of distributed ledger technologies," in *Proc. On Move Meaningful Internet Syst. Conf.: Confederated Int. Conf.: CoopIS, C&TC, ODBASE*, 2018, pp. 277–288.

[24] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469–472, Jul. 1985.

[25] L. Fan, K. W. Ng, and C. S. Chan, "Rethinking deep neural network ownership verification: Embedding passports to defeat ambiguity attacks," in *Proc. Adv. Neural Inf. Process. Syst.*, 2019.

[26] P. Fernandez, G. Couairon, H. Jégou, M. Douze, and T. Furon, "The stable signature: Rooting watermarks in latent diffusion models," 2023, *arXiv:2303.15435*.

[27] N. Dong et al., "FLock: Defending malicious behaviors in federated learning with blockchain," in *Proc. 37th Conf. Neural Inf. Process. Syst.*, 2022.

[28] R. García, A. Cediel, M. Teixidó, and R. Gil, "Semantics and non-fungible tokens for copyright management on the metaverse and beyond," 2022, *arXiv:2208.14174*.

[29] C. Gentry, *A Fully Homomorphic Encryption Scheme*. Stanford, CA, USA: Stanford Univ., 2009.

[30] C. Gentry, "Computing arbitrary functions of encrypted data," in *Commun. ACM*, vol. 53, no. 3, pp. 97–105, 2010.

[31] C. Gentry, A. Sahai, and B. Waters, "Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based," in *Proc. 33rd Adv. Cryptol.–CRYPTO: Annu. Cryptol. Conf.*, 2013, pp. 75–92.

[32] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 3–16.

[33] A. Guadamuz, "The treachery of images: Non-fungible tokens and copyright," *J. Intellectual Property Law Pract.*, vol. 16, no. 12, pp. 1367–1385, 2021.

[34] R. Guerraoui et al., "The hidden vulnerability of distributed learning in Byzantium," in *Proc. Int. Conf. Mach. Learn.*, 2018, pp. 3521–3530.

[35] W. Guo, B. Tondi, and M. Barni, "An overview of backdoor attacks against deep neural networks and possible defences," *IEEE Open J. Signal Process.*, vol. 3, pp. 261–287, 2022.

[36] C. He et al., "FedML: A research library and benchmark for federated machine learning," in *Proc. Adv. Neural Inf. Process. Syst.*, 2020.

[37] R. Hu, Y. Guo, H. Li, Q. Pei, and Y. Gong, "Personalized federated learning with differential privacy," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9530–9539, Oct. 2020.

[38] R. Jia et al., "Towards efficient data valuation based on the shapley value," in *Proc. 22nd Int. Conf. Artif. Intell. Statist.*, 2019, pp. 1167–1176.

[39] N. Jing, Q. Liu, and V. Sugumaran, "A. blockchain-based code copyright management system," *Inf. Process. Manage.*, vol. 58, no. 3, 2021, Art. no. 102518.

[40] P. Kairouz et al., "Advances and open problems in federated learning," *Foundations Trends Mach. Learn.*, vol. 14, no. 1/2, pp. 1–210, 2021.

[41] A. P. Kalapaaking, I. Khalil, M. S. Rahman, M. Atiquzzaman, X. Yi, and M. Almashor, "Blockchain-based federated learning with secure aggregation in trusted execution environment for internet-of-things," *IEEE Trans. Ind. Inform.*, vol. 19, no. 2, pp. 1703–1714, Feb. 2023.

[42] J. Kang, Z. Xiong, D. Niyato, S. Xie, and J. Zhang, "Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10700–10714, Dec. 2019.

[43] L. U. Khan et al., "Federated learning for edge networks: Resource optimization and incentive mechanism," *IEEE Commun. Mag.*, vol. 58, no. 10, pp. 88–93, Oct. 2020.

[44] H. Kim, J. Park, M. Bennis, and S.-L. Kim, "Blockchained on-device federated learning," *IEEE Commun. Lett.*, vol. 24, no. 6, pp. 1279–1283, Jun. 2020.

[45] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," in *Self-Published Paper*, 2012.

[46] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," in *Concurrency: The Works of Leslie Lamport*, 2019, pp. 203–226.

[47] B. Li, L. Fan, H. Gu, J. Li, and Q. Yang, "FedIPR: Ownership verification for federated deep neural network models," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 45, no. 4, pp. 4521–4536, Apr. 2023.

[48] G. Li, S. Li, Z. Qian, and X. Zhang, "Encryption resistant deep neural network watermarking," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, 2022, pp. 3064–3068.

[49] L. Li et al., "Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2204–2220, Jul. 2018.

[50] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, "Federated optimization in heterogeneous networks," *Proc. Mach. Learn. Syst.*, vol. 2, pp. 429–450, 2020.

[51] X. Li, M. Jiang, X. Zhang, M. Kamp, and Q. Dou, "Fedbn: Federated learning on non-IId features via local batch normalization," 2021, *arXiv:2102.07623*.

[52] Y. Li, C. Chen, N. Liu, H. Huang, Z. Zheng, and Q. Yan, "A blockchain-based decentralized federated learning framework with committee consensus," *IEEE Netw.*, vol. 35, no. 1, pp. 234–241, Jan./Feb. 2021.

[53] W. Liang, D. Zhang, X. Lei, M. Tang, K.-C. Li, and A. Y. Zomaya, "Circuit copyright blockchain: Blockchain-based homomorphic encryption for IP circuit protection," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 3, pp. 1410–1420, Jul.–Sep. 2021.

[54] J. Lin, M. Du, and J. Liu, "Free-riders in federated learning: Attacks and defenses," 2019, *arXiv:1911.12560*.

[55] Y. Liu, Z. Ai, S. Sun, S. Zhang, Z. Liu, and H. Yu, "Fedcoin: A Peer-to-peer payment system for federated learning," in *Federated Learning: Privacy Incentive*, Cham, Switzerland: Springer, 2020, pp. 125–138.

[56] Y. Liu, Q. Lu, C. Zhu, and Q. Yu, "A blockchain-based platform architecture for multimedia data management," *Multimedia Tools Appl.*, pp. 1–17, 2021.

[57] N. Lukas, Y. Zhang, and F. Kerschbaum, "Deep neural network fingerprinting by conferrable adversarial examples," 2019, *arXiv:1912.00888*.

[58] J. Ma, S.-A. Naas, S. Sigg, and X. Lyu, "Privacy-preserving federated learning based on multi-key homomorphic encryption," *Int. J. Intell. Syst.*, vol. 37, no. 9, pp. 5880–5901, 2022.

[59] I. Martinez, S. Francis, and A. S. Hafid, "Record and reward federated learning contributions with blockchain," in *Proc. IEEE Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov.*, 2019, pp. 50–57.

[60] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y. Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. Artif. Intell. Statist.*, 2017, pp. 1273–1282.

[61] L. Melis, C. Song, E. De Cristofaro, and V. Shmatikov, "Exploiting unintended feature leakage in collaborative learning," in *Proc. IEEE Symp. Secur. Privacy*, 2019, pp. 691–706.

[62] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," in *Decentralized Business Review*, 2008, Art. no. 21260.

[63] T. Nguyen, P. Thai, T. R. Jeter, T. N. Dinh, and M. T. Thai, "Blockchain-based secure client selection in federated learning," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency*, 2022, pp. 1–9.

[64] OpenAI, "Gpt-4 technical report," 2023, *arXiv:2303.08774*.

[65] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Adv. Int. Conf. Theory Appl. Cryptographic Techn.*, 1999, pp. 223–238.

[66] W. Peng et al., "Are you copying my model? protecting the copyright of large language models for EAAS via backdoor watermark," 2023, *arXiv:2305.10036*.

[67] C. I. Podilchuk and E. J. Delp, "Digital watermarking: Algorithms and applications," *IEEE signal Process. Mag.*, vol. 18, no. 4, pp. 33–46, Jul. 2001.

[68] A. Qammar, A. Karim, H. Ning, and J. Ding, "Securing federated learning with blockchain: A systematic literature review," *Artif. Intell. Rev.*, vol. 56, no. 5, pp. 3951–3985, 2023.

[69] M. Rauchs et al., "Distributed ledger technology systems: A conceptual framework," 2018.

[70] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You only look once: Unified, real-time object detection," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2016, pp. 779–788.

[71] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[72] R. Rombach, A. Blattmann, D. Lorenz, P. Esser, and B. Ommer, "High-resolution image synthesis with latent diffusion models," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, 2022, pp. 10684–10695.

[73] M. Sarhan, W. W. Lo, S. Layeghy, and M. Portmann, "HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection," *Comput. Elect. Eng.*, vol. 103, 2022, Art. no. 108379.

[74] Y. Sarikaya and O. Ercetin, "Motivating workers in federated learning: A stackelberg game perspective," *IEEE Netw. Lett.*, vol. 2, no. 1, pp. 23–27, Mar. 2020.

[75] A. Savelyev, "Copyright in the blockchain ERA: Promises and challenges," *Comput. Law Secur. Rev.*, vol. 34, no. 3, pp. 550–561, 2018.

[76] M. Shafay, R. W. Ahmad, K. Salah, I. Yaqoob, R. Jayaraman, and M. Omar, "Blockchain for deep learning: Review and open challenges," *Cluster Comput.*, vol. 26, no. 1, pp. 197–221, 2023.

[77] S. Shao et al., "Fedtracker: Furnishing ownership verification and traceability for federated learning model," 2022, *arXiv:2211.07160*.

[78] L. S. Shapley et al., *A Value for N-Person Games*. 1953.

[79] M. Shayan, C. Fung, C. J. Yoon, and I. Beschastnikh, "Biscotti: A blockchain system for private and secure federated learning," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 7, pp. 1513–1525, 2020.

[80] A. K. Shrestha and J. Vassileva, "User data sharing frameworks: A blockchain-based incentive solution," in *Proc. IEEE 10th Annu. Inf. Technol., Electron. Mobile Commun. Conf.*, 2019, pp. 0360–0366.

[81] T. Song, Y. Tong, and S. Wei, "Profit allocation for federated learning," in *Proc. IEEE Int. Conf. Big Data*, 2019, pp. 2577–2586.

[82] N. Szabo, "Formalizing and securing relationships on public networks," First Monday, 1997.

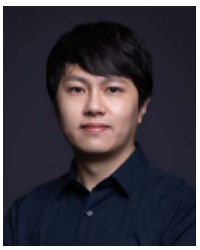
[83] A. Triastcyn and B. Faltings, "Federated learning with bayesian differential privacy," in *Proc. IEEE Int. Conf. Big Data*, 2019, pp. 2587–2596.

[84] G. Voyatzis, N. Nikolaidis, and I. Pitas, "Digital watermarking: An overview," in *Proc. IEEE 9th Eur. Signal Process. Conf.*, 1998, pp. 1–4.

[85] G. Wang, C. X. Dang, and Z. Zhou, "Measure contribution of participants in federated learning," in *Proc. IEEE Int. Conf. Big Data*, 2019, pp. 2597–2604.

[86] H. Wang, Z. Kaplan, D. Niu, and B. Li, "Optimizing federated learning on non-iid data with reinforcement learning," in *Proc. IEEE Conf. Comput. Commun.*, 2020, pp. 1698–1707.

[87] Q. Wang, R. Li, Q. Wang, and S. Chen, "Non-fungible token (NFT): Overview, evaluation, opportunities and challenges," 2021, *arXiv:2105.07447*.
[88] Y. Wang, Y. Pan, M. Yan, Z. Su, and T. H. Luan, "A survey on chatGPT: AI-generated contents, challenges, and solutions," 2023, *arXiv:2305.18339*.
[89] K. Wei et al., "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 3454–3469, 2020.
[90] B. Xiao, X. Fan, S. Gao, and W. Cai, "Edgetoll: A blockchain-based toll collection system for public sharing of heterogeneous edges," in *Proc. IEEE Conf. Comput. Commun. Workshops*, 2019, pp. 1–6.
[91] C. Xie, S. Koyejo, and I. Gupta, "Asynchronous federated optimization," 2019, *arXiv:1903.03934*.
[92] M. Xu et al., "Unleashing the power of edge-cloud generative AI in mobile networks: A survey of AIGC services," 2023, *arXiv:2303.16129*.
[93] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, M. Hammoudeh, H. Karimipour, and G. Srivastava, "Block hunter: Federated learning for cyber threat hunting in blockchain-based IIoT networks," *IEEE Trans. Ind. Informat.*, vol. 18, no. 11, pp. 8356–8366, Nov. 2022.
[94] A. Yousefpour et al., "Opacus: User-friendly differential privacy library in PyTorch," 2022, *arXiv:2109.12298*.
[95] H. Yu, G. Iosifidis, B. Shou, and J. Huang, "Market your venue with mobile applications: Collaboration of online and offline businesses," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, 2018, pp. 1934–1942.
[96] R. Zeng, C. Zeng, X. Wang, B. Li, and X. Chu, "A comprehensive survey of incentive mechanism for federated learning," 2021, *arXiv:2106.15406*.
[97] C. Zhang, S. Li, J. Xia, W. Wang, F. Yan, and Y. Liu, "BatchCrypt: Efficient homomorphic encryption for cross-silo federated learning," in *Proc. USENIX Annu. Tech. Conf.*, 2020, pp. 493–506.
[98] S. Q. Zhang, J. Lin, and Q. Zhang, "A. multi-agent reinforcement learning approach for efficient client selection in federated learning," in *Proc. AAAI Conf. Artif. Intell.*, 2022, pp. 9091–9099.
[99] Q. Zhen, Y. Xueqiang, Z. Mengchu, Z. Peng, and D. Shuiguang, "Blockdfl: A blockchain-based fully decentralized federated learning framework," 2022, *arXiv:2205.10568*.
[100] P. Zheng, Z. Zheng, J. Wu, and H. N. Dai, "Xblock-ETH: Extracting and exploring blockchain data from ethereum," *IEEE Open J. Comput. Soc.*, vol. 1, pp. 95–106, 2020.
[101] Z. Zheng et al., "An overview on smart contracts: Challenges, advances and platforms," *Future Gener. Comput. Syst.*, vol. 105, pp. 475–491, 2020.



CHUAN CHEN (Member, IEEE) received the Ph.D. degree from Hong Kong Baptist University, Hong Kong, in 2016. He is currently an Associate Professor with the School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou, China. He has authored or coauthored more than 80 international journal and conference papers. His research interests include federated learning, robust machine learning, and graph neural networks. He was an Associate Editor for journal *Software Impacts*.

YIHAO LI received the B.S. degree in information engineering from Sun Yat-sen University, Guangzhou, China, in 2022, where he is currently working toward the Graduate degree in computer technology. His research focuses on federated learning.

ZIHOU WU is currently working toward the undergraduate degree with the School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou, China.

MINGFENG XU received the B.S. degree in mathematics and applied mathematics from Shenzhen University, Shenzhen, China, in 2023, and the graduation degree in applied statistic from Sun Yat-Sen University, Guangzhou, China. His research focuses on federated learning.

RUI WANG is currently working toward the undergraduate degree in computer science and technology with Sun Yat-sen University, Guangzhou, China. His research focuses on federated learning.

ZIBIN ZHENG (Fellow, IEEE) received the Ph.D. degree from the Chinese University of Hong Kong, Hong Kong, in 2011. He is currently a Professor with the School of Software Engineering, Sun Yat-sen University, Guangzhou, China. He has authored or coauthored more than 300 international journal and conference papers, including 9 ESI highly cited papers. His research interests include blockchain, artificial intelligence, and software reliability. He was the recipient of several awards, including the Top 50 Influential Papers in blockchain of 2018 and ACM SIGSOFT Distinguished Paper Award at ICSE2010.