Blockchain-based AI-Generated Content (AIGC) Zero Knowledge Dataset Regulation System

Jiaxiang Sun, Rong Zhao, Lehao Lin, Yuanfang Chi, *Graduate Student Member, IEEE*, Victor C.M. Leung, *Life Fellow, IEEE*, Wei Cai, *Senior Member, IEEE*

***Abstract*—The popularity of Artificial Intelligence-Generated Content (AIGC) has experienced significant growth recently. Despite AIGC's potential to transform content creation in various industries, its dependence on extensive computational resources poses a challenge for widespread adoption. To address this challenge, AIGC as a service has been proposed. However, concerns related to dataset compliance have emerged as a source of apprehension among stakeholders. The complexities associated with manual supervision, apprehensions regarding data leakage, and the potential for malicious behavior by third-party supervisors collectively present formidable challenges in the regulation of datasets within the domain of AIGC service. To tackle these challenges, this paper presents a blockchain-based system for regulating AIGC datasets. Our proposed system employs AI, zero-knowledge proofs, and smart contracts as integral components for overseeing dataset compliance. To assess the feasibility and effectiveness of the proposed system, a comprehensive analysis and a series of simulations have been conducted. These evaluations offer valuable insights into the system's security, privacy, and performance.**

***Index Terms*—AIGC, Regulation, Blockchain, Smart contract**

I. Introduction

WITH the developments of Generative Adversarial Network (GAN), Diffusion, and Transformer, the popularity of Artificial Intelligence Generated Content (AIGC) has been increasing. AIGC encompasses the concept of automatically generating content using Artificial Intelligence (AI) models, such as Generative Pretrained Transformer (GPT) model [1] for text-to-text generation and the Diffusion model for text-to-image generation. AIGC, with its ability to automate content generation for text and images, is expanding the possibilities in technological and societal systems.

Despite AIGC's potential to transform content creation in various industries, its dependence on extensive computational resources poses a challenge for widespread adoption. To address this challenge, AIGC as a service has been proposed [2]. In AIGC as a service, AIGC service providers adopt a dual-step process: initially pre-training models on cloud servers and then fine-tuning them on edge servers with user-specific datasets. This approach enables users to access AIGC services with low latency and high customizability. Once the fine-tuning of the model is complete, users can submit instructions for using the fine-tuned model to achieve their desired output results. Through AIGC as a service, content generation becomes more accessible and affordable, thereby promoting its utilization in technological and societal systems.

In AIGC service, the training dataset usually has a much larger volume, and the fine-tuning dataset is generated regularly. These training and fine-tuning datasets are vital in the development and functioning of AIGC models. However, these datasets can sometimes lead to legal issues, particularly if they contain privacy-sensitive or copyrighted material. A prominent example is the lawsuit filed by comedian Sarah Silverman against OpenAI and Meta for using her writing without authorization [3]. Moreover, the necessity and techniques of sharing generated content among parallel metaverses are discussed in [4]. Yet, challenges of the regulation of AIGC datasets have only been studied until recently. For instance, Hacker et al. [5] underscored the necessity of examining training data to identify possible privacy or copyright violations. Nevertheless, the majority of current research primarily addresses legal issues, with a notable deficiency in technical solutions.

Currently, a notable research gap exists in the area of dataset regulation within AIGC service. This indicates a need for further investigation and exploration in this field. This field faces challenges in regulating fine-tuning and feedback datasets to prevent privacy breaches and copyright infringement. These challenges include the impracticality of manual supervision due to the large size of training datasets and frequent updates of fine-tuning datasets, the risk of data leaks in regulation process, and potential misconduct by third-party regulators. These challenges highlight the complex relationship between system engineering, technological systems, as well as societal systems, in regulating AIGC datasets.

To tackle these challenges, promising solutions can be found in the utilization of blockchain technology and Zero-knowledge proof (ZKP) to execute smart contracts and ensure privacy protection, respectively. Furthermore, advancements in AI technology contribute to the development of automated review processes, enhancing the efficiency and accuracy of identifying compliance issues. In this paper, We introduce a blockchain-based AIGC dataset regulation system. This innovative system uses AI models for the purpose of supervision.

Manuscript received xxx, 2024; revised xxx, 2024. This work was supported in part by the Guangdong Basic and Applied Basic Research Foundation under Grant 2024A1515012323; in part by Guangdong Pearl River Talent Recruitment Program under Grant 2019ZT08X603; and in part by Guangdong Pearl River Talent Plan under Grant 2019JC01X235. (Corresponding author: Wei Cai.)

Jiaxiang Sun, Rong Zhao, Lehao Lin and Wei Cai are with the School of Science and Engineering, The Chinese University of Hong Kong, Shenzhen 518172, China; Yuanfang Chi and Victor C.M. Leung are with The University of British Columbia, Vancouver, BC V6T 1Z4, Canada, and also Shenzhen University, Shenzhen 518060, China. Victor C.M. Leung is also with Shenzhen MSU-BIT University, Shenzhen 518000, China (e-mail: jiaxiangsun@link.cuhk.edu.cn; rongzhao@link.cuhk.edu.cn; lehaolin@link.cuhk.edu.cn; yuanchi@ece.ubc.ca; vleung@ieee.org; weicai@ieee.org).

This article has been accepted for publication in IEEE Systems, Man, and Cybernetics Magazine. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MSMC.2024.3482691

Smart contracts are deployed to verify zero-knowledge proofs and the inference results obtained from these AI models. Moreover, users and AIGC service providers can utilize regulatory AI models to generate zero-knowledge proofs for their datasets, demonstrating the security and compliance of their data. By incorporating AI models for supervision and utilizing smart contracts for verification, our system establishes an automated and efficient regulatory framework. This paper's contributions can be summarized as follows:

- We propose a blockchain-based AIGC dataset regulation system that enables the utilization of AI models for supervision. The system utilizes smart contracts to verify zero-knowledge proofs for supervision results, ensuring data security and compliance while automating the regulatory process. By bridging the gap between advanced technology and societal requirements, this solution safeguards data privacy and streamlines regulatory operations.
- We conduct a security analysis of the AIGC dataset regulation system, specifically focusing on its ability to ensure privacy. This research aspect underscores the system's strength in protecting confidential data. The analysis underscores the importance of our system in creating a privacy-conscious setting for technological activities and social interactions.
- We simulate and evaluate the efficiency and gas consumption of the system. The analysis focuses on assessing the effectiveness of the regulatory system, particularly in terms of its operational performance and resource utilization within the blockchain environment. This simulation illustrates the feasibility of the system and its potential applicability in technological and societal contexts.

II. Related Work

A. AIGC

AIGC refers to the concept of generating content automatically using AI models. In recent years, AIGC has witnessed significant development. For instance, ChatGPT [6] has advanced the field by enabling high-quality text-to-text generation. Additionally, technologies such as Diffusion Models [7] has demonstrated remarkable progress in high-quality text-to-image generation. The AIGC process consists of three stages: pre-training, fine-tuning, and inference [8]. In the pre-training phase, the model is trained using large-scale datasets. Following pre-training, fine-tuning is performed to enhance the model's knowledge in specific domains or fields. Once the fine-tuning process is completed, the model is deployed to offer AIGC services to users. Users can then utilize the model's inference capabilities to obtain AIGC results.

Due to the high resources needed for AIGC, the concept of AIGC as a service has been proposed [2]. In AIGC as a service, the service providers can pre-train their models on a cloud server and deploy them on edge servers. Subsequently, users access the AIGC service from the edge server. This methodology allows for low latency and high customizability in accessing the AIGC service. This emerging concept holds significant importance as a future development direction for the field of AIGC. In AIGC as a service, blockchain can offer a secure and reliable framework for AIGC service transactions, using smart contracts to match AIGC service providers with users and streamline payments for AIGC services [9].

B. Dataset Regulation

With the growing controversies surrounding AI datasets, there is a rising focus on dataset regulation [5], [10]. Dataset regulation involves ensuring that datasets comply with regulations to prevent privacy, copyright, and other related issues. Hartmann et al. [11] suggest expanding data access rights to facilitate thorough third-party audits of AI systems while emphasizing the importance of safeguarding personal data during auditing processes. The European Union's Artificial Intelligence Act (EU AI Act) mandates the provision of detailed documentation on the datasets used. Additionally, it states that the utilization and handling of datasets must adhere to current EU data protection laws, specifically the General Data Protection Regulation (GDPR) [12], [13]. Currently, dataset regulation is a topic in AI regulation. However, there is a lack of dedicated research focusing on dataset regulation.

C. Zero Knowledge Proof

Zero-knowledge proofs (ZKPs) are cryptographic protocols that enable a prover to demonstrate the correctness of a statement to a verifier, without disclosing any additional information apart from the statement's correctness [14]. They are utilized in different fields such as set membership [15], training model proofs [16], and smart contracts to guarantee privacy and security [17]. Within the realm of ZKPs, Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) represents a particular form of zero-knowledge proof characterized by its compact proof size and efficient verification [18]. zk-SNARKs offer a concise and effective method for validating computation accuracy, thereby lessening the computational load on verification entities [19].

ZKP and zk-SNARK are widely used in verifiable machine learning. Verifiable machine learning refers to the application of cryptography to offer evidence regarding the accuracy and inference outcomes of machine learning models, while keeping the models or the input undisclosed [20]. ZKP can guarantee the integrity of model training in machine learning, while preserving the privacy of the server's intellectual property and maintaining the integrity of the training process [21]. ZKP can also facilitate the verification of decision tree model predictions and their accuracy on datasets without disclosing any proprietary information about the models themselves [22].

III. Preliminaries

A. Zero Knowledge Proof

A ZKP compiler called ZEN [23] has been developed to optimize the generation of efficient and verifiable zero-knowledge neural network inference schemes. Specifically, ZEN comprises two components: ZEN$_{acc}$ and ZEN$_{infer}$. The ZEN$_{acc}$ component is designed to furnish zero-knowledge proofs for the accuracy of a model, while simultaneously preserving the privacy of the model itself. Meanwhile, the ZEN$_{infer}$ component is responsible for providing zero-

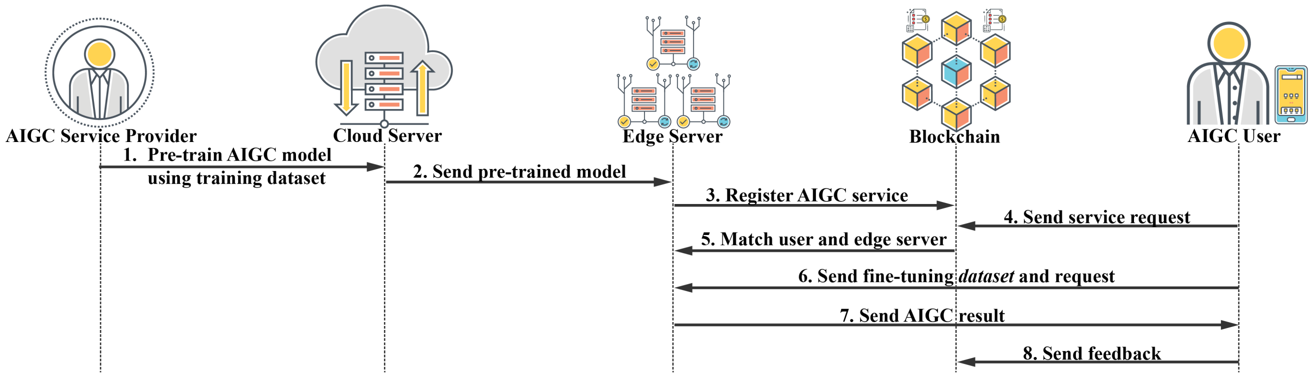

Fig. 1. Overview of Blockchain-based AIGC System

knowledge proofs for the outcomes generated by the verified model, ensuring the confidentiality of the input data throughout the process.

ZEN$_{acc}$ includes four functions:

- ZEN$_{acc}$.GEN generates proving and verification keys using a neural network model and a security parameter.
- ZEN$_{acc}$.Commit creates a commitment to the model.
- ZEN$_{acc}$.Prove produces a proof of the model's accuracy using the model, test dataset, and proving key.
- ZEN$_{acc}$.Verify uses the commitment, proof, verification key, and the accuracy to confirm the model's accuracy while protecting privacy.

ZEN$_{infer}$ consists of three functions:

- ZEN$_{infer}$.GEN, which generates proving and verification keys using a neural network model and a security parameter.
- ZEN$_{infer}$.Prove, which produces a proof of the model's result utilizing the model, input data, and proving key
- ZEN$_{infer}$.Verify, which employs the proof, verification key, and the result to validate the model's output while ensuring the privacy of the input data.

IV. Challenges in AIGC dataset regulation

In this section, we first review the blockchain-based AIGC service system. Then, we analyze the problems and challenges of AIGC dataset regulation in AIGC service.

A. Overview of Blockchain-Based AIGC Service System

The overview of blockchain-based AIGC service system is shown in Fig. 1. The system comprises the following entities: AIGC service provider, AIGC user, edge server, and cloud server. We will first introduce the complete process of blockchain-based AIGC system.

The AIGC service system initiates with the AIGC service provider conducting pre-training of AIGC base models on the cloud server using training datasets. Following the pre-training phase, the AIGC service provider proceeds to deliver the base model to edge servers via network. Consequently, the edge server is equipped to deliver AIGC services to users within the respective region.

Before offering AIGC services to users, the AIGC service provider must register their services on the blockchain using smart contracts to showcase their ability to provide AIGC services. A user requiring AIGC service will submit a service request to the smart contract on the blockchain. The smart contract will then match the service request with the corresponding service and send the matching result to both the AIGC service provider and the user. The transactions between AIGC users and AIGC service providers will utilize tokens on the blockchain. Leveraging the distributed ledger capability of blockchain enables the establishment of secure transactions, thereby ensuring trust and integrity in the interactions between AIGC users and AIGC service providers.

AIGC users often have diverse requirements for AIGC services, often providing domain-specific datasets for fine-tuning the AIGC model to achieve their desired output. The edge server will use these fine-tuning datasets to fine-tune AIGC models. This fine-tuning involves adjusting the model's parameters to better suit these identified tasks using provided fune-tuning dataset. Once the fine-tuning of the model is complete, AIGC users are able to submit instructions for utilizing the fine-tuned model to obtain their desired output results. This iterative process may encompass multiple rounds of refinement, each aimed at improving the model's performance and output quality for the specific applications envisaged by AIGC users.

After completing the AIGC service, users are encouraged to submit brief feedback on the service. The feedback information will be recorded on the blockchain, which can help improve the quality of AIGC services and assist others in choosing appropriate AIGC services.

B. Challenges of AIGC Dataset Regulation

In this AIGC service system, regulators often raise concerns regarding the usage of datasets. Improper handling of datasets can give rise to various issues. For instance, if a dataset contains data related to privacy or copyright, it could potentially lead to legal disputes. Similarly, if the dataset contains inappropriate information, it may result in the generation of inaccurate or improper results by AIGC models. Consequently, the implementation of an AIGC dataset supervision system becomes imperative. However, challenges such as manual supervision difficulty, data leakage concerns, and third-party regulatory misconduct impede research advancement.

Firstly, in AIGC service system, the fine-tuning datasets

This article has been accepted for publication in IEEE Systems, Man, and Cybernetics Magazine. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MSMC.2024.3482691

are often comprised of numerous smaller subsets, rendering manual supervision impractical due to their substantial volume and high frequency of updates. Similarly, the training datasets are typically large-scale, making manual oversight ineffective. Consequently, the exploration of automated methods for dataset supervision is indispensable. Recent advancements in AI have made it feasible to employ algorithms for automatic data inspection. Utilizing these AI algorithms can facilitate automated supervision, aiding in adherence to privacy regulations and copyright protection within AIGC service system.

Secondly, there exists a risk of data leaks in the regulation process of AIGC dataset, where datasets may contain critical information for their owners. Such leaks could infringe upon the owners' rights. This risk may deter dataset holders from engaging in regulation. Thus, a regulatory method that ensures data privacy is necessary. Zero-knowledge proof (ZKP), renowned for providing verification while maintaining data confidentiality, emerges as a viable solution. Implementing ZKP in the regulation of AIGC datasets could offer a robust method for privacy-protective regulation.

Thirdly, employing third-party supervision in AIGC service can lead to potential misconduct by these external supervisors. These parties might engage in biased behavior, such as applying different regulatory standards to various individuals, thus impeding fair regulation. A method to mitigate third-party misconduct is essential. Blockchain technology, known for its transparency and immutability, offers a promising approach. Additionally, the capability of blockchain to automate smart contracts presents an opportunity to develop an automated regulatory verification system, potentially enhancing the efficiency and integrity of the regulatory process. To address these issues, we propose a blockchain-based AIGC service system employing zero-knowledge proofs for dataset regulation.

V. Blockchain-based Dataset Regulation System

Leveraging the transparent characteristics of blockchain and its ability to execute smart contracts, we have designed a blockchain-based AIGC dataset regulation system. This system integrates AI functionalities to automate the dataset review process. To maintain privacy throughout the regulatory procedure, ZKP technology is utilized. Fig. 2 provides an overview of the regulation system.

A. System Components in Dataset Regulation System

The system comprises the following components.

Data Regulator: The data regulator plays a pivotal role in formulating regulatory rules for governing datasets. This involves creating and providing distinct example regulatory datasets tailored for different types of regulatory subjects, such as separate sets for training and fine-tuning datasets. The regulatory rules and information of these datasets are securely stored on the blockchain. Additionally, the data regulator is responsible for deploying smart contracts on the blockchain, which are designed to facilitate the verification process for a AI model for regulation.

AIGC Service Provider: The AIGC service provider offers AI-generated content services within edge networks. They utilize cloud servers for the pre-training of AIGC models and edge servers to deliver AIGC services to users. To ensure that their training dataset adheres to regulatory standards, AIGC service providers employ AI models and ZKP to generate proofs for datasets on cloud server. These proofs are then verified using smart contracts to demonstrate compliance with the established regulatory requirements.

AIGC User: The AIGC users access AIGC services via the edge server. They provide a fine-tuning dataset to the edge server for the purpose of fine-tuning the AIGC model and subsequently receive results from this tailored model. After the AIGC service, users are encouraged to offer feedback about their experience. To demonstrate that their fine-tuning dataset meets regulatory standards, users will employ the edge server to generate a proof for the dataset using AI models and ZKP. This proof is then verified through smart contracts, ensuring and indicating compliance with the established regulatory requirements.

Cloud Server: The cloud server has a dual role in the AIGC system. Firstly, it is used for the pre-training of AIGC models and for training AI models to meet regulatory compliance standards. Additionally, the cloud server computes a zero-knowledge proof for the training dataset to ensure compliance with regulatory standards. This proof is then forwarded to the AIGC service provider.

Edge Server: Edge servers are used to deploy AIGC models, offering users model fine-tuning and inference services. These servers, upon receiving fine-tuning datasets from users, fine-tune the model accordingly. Subsequently, they provide inference outputs based on these personalized models. Additionally, edge servers are instrumental in training regulation models. These models are used to generating zero-knowledge proofs associated with users' fine-tuning datasets. These proofs validate the compliance of datasets with regulatory requirements before being returned to the users.

Key Management System (KMS): The Key Management System is a trusted setup place that plays a vital role in generating proving keys and verification keys for AI models for regulatory purposes. KMS can be a trusted third party, or it can be achieved through multi-party computation. When it receives a model from an edge or cloud server, the system is responsible for creating proving keys and verification keys for ZEN$_{acc}$ and ZEN$_{infer}$. These keys are then distributed to the relevant parties as needed, facilitating the regulatory processes.

AI Models for Regulation: AI models are used to supervise dataset compliance. They are trained by cloud servers and edge servers according to regulatory rules and example regulatory datasets provided by the data regulator. The cloud server trains AI models to regulate training datasets, while edge servers train models to regulate fine-tuning datasets. The regulation models take a dataset as input and output whether the dataset complies with regulatory standards.

ZKP for Regulation: The system uses the ZEN [23] scheme, which includes ZEN$_{acc}$ and ZEN$_{infer}$ components, to implement ZKP. ZEN$_{acc}$ is used to demonstrate the accuracy of the regulation AI model on example regulatory datasets, without revealing the model itself. ZEN$_{infer}$ is used to prove that a dataset complies with regulatory rules, without revealing

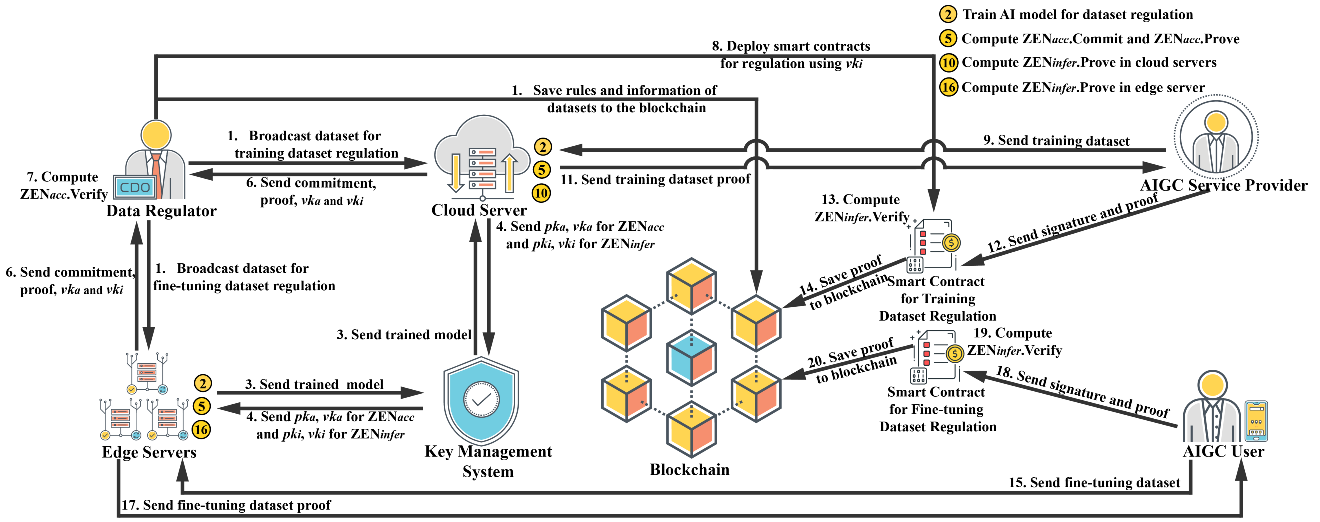
2 Train AI model for dataset regulation
5 Compute ZENacc.Commit and ZENacc.Prove
10 Compute ZENinfer.Prove in cloud servers
16 Compute ZENinfer.Prove in edge server
8. Deploy smart contracts for regulation using vki
1. Save rules and information of datasets to the blockchain
1. Broadcast dataset for training dataset regulation
6. Send commitment, proof, vka and vki
7. Compute ZENacc.Verify
CDO
Data Regulator
Cloud Server
2
5
10
11. Send training dataset proof
9. Send training dataset
AIGC Service Provider
4. Send pka, vka for ZENacc and pki, vki for ZENinfer
6. Send commitment, proof, vka and vki
1. Broadcast dataset for fine-tuning dataset regulation
3. Send trained model
13. Compute ZENinfer.Verify
12. Send signature and proof
14. Save proof to blockchain
Smart Contract for Training Dataset Regulation
19. Compute ZENinfer.Verify
20. Save proof to blockchain
18. Send signature and proof
Smart Contract for Fine-tuning Dataset Regulation
2
5
16
3. Send trained model
4. Send pka, vka for ZENacc and pki, vki for ZENinfer
Edge Servers
Key Management System
Blockchain
AIGC User
15. Send fine-tuning dataset
17. Send fine-tuning dataset proof

Fig. 2. Blockchain-Based AIGC Zero Knowledge Dataset Regulation System

the contents of the dataset. The application of ZKP guarantees the privacy of both the regulatory AI model and datasets.

Blockchain: The blockchain in this context serves three critical functions. First, it offers a decentralized platform for executing smart contracts, which are utilized to supervise datasets. Second, the blockchain acts as an immutable storage medium for information about regulatory datasets, ensuring transparent regulatory standards. Finally, it stores both the details and the proof of dataset regulation outcomes, facilitating regulatory inquiries and the preservation of this information.

Smart Contract: Smart contracts in this framework are specifically deployed for dataset regulation. Each smart contract associated with an AI regulation model is deployed using its inference verification key. These contracts are designed to receive users' signature, commitments and proofs for datasets as inputs. Their primary function is to verify the compliance of these datasets with predefined regulatory rules. Upon successful verification, the smart contract records key information about the dataset regulation on the blockchain. The process of smart contracts is shown in Algorithm 1.

Algorithm 1: Smart Contract for Dataset Regulation

```
Input: Signature $s$, Dataset commitment $cm_d$, Model
       commitment $cm_m$, Output $y$, Proof $\pi$
Output: Verification Result (True/False)
Function createVerifyingKey():
    Create verifying key $vk$ from stored constant
      variables;
    return $vk$
return
Function saveInformation($s, cm_d, cm_m, y, \pi$):
    Emit event($s, cm_d, cm_m, y, \pi$);
return
Function verifyProof($s, cm_d, cm_m, y, \pi$):
    $vk \leftarrow$ createVerifyingKey() ;
    if $ZEN_{infer}.Verify(vk, cm_d, cm_m, y, \pi)$ == $True$
      then
        saveInformation($s, cm_d, cm_m, y, \pi$);
        return True;
    else
        return False;
    end
return
```

B. Blockchain-based Dataset Regulation System

The process of the blockchain-based AIGC dataset regulation system is depicted in Fig. 2. The system consists of two stages: the initialization stage and the regulation stage.

In the initialization stage of this AIGC system, the data regulator begins by providing regulatory rules and example regulatory datasets. These are essential for the regulation for training and fine-tuning datasets datasets. The information pertaining to these rules and datasets is stored on the blockchain, ensuring transparency and consistency in regulatory standards, thereby preventing the application of different standards to different entities. Following this, both the cloud server and edge servers engage in training AI models in accordance with the established regulation rules. Post-training, these servers interact with a KMS to obtain a set of keys: the proving key pk_a and verification key vk_a for ZEN$_{acc}$, and similarly, a proving key pk_i and verification key vk_i for ZEN$_{infer}$. These regulation models will be kept secret afterwards. Then the cloud server is responsible for computing the accuracy of the regulation model on example regulatory datasets for training dataset regulation, while the edge server performs a similar task for fine-tuning datasets regulation. Both servers utilize ZEN$_{acc}$.Commit and ZEN$_{acc}$.Prove to create a commitment for the model alongside a zero-knowledge proof of the model's accuracy on these datasets, which serves to protect the privacy of the trained model. Subsequently, the servers transmit the commitment, proof, and both vk_a and vk_i to the regulator. The data regulator uses vk_a to verify the model's accuracy. If this verification is successful, vk_i is then employed to deploy a smart contract. This contract is designed for verifying inference result proofs from the AI regulation model. Once the smart contract is deployed, the initialization stage concludes.

In the regulation phase, the AIGC service provider sends training datasets to the cloud server. Then the cloud server generates a zero-knowledge proof for this dataset using the regulation model via ZEN$_{infer}$.Prove, which is sent to the AIGC service provider. This provider then sends signature and the proof to the smart contract for regulation of the specific training dataset. The smart contract performs verification using ZEN$_{infer}$.Verify and, post-verification, stores the proof information for the training dataset on the blockchain for subsequent regulation queries. Similarly, AIGC user initially transmits the fine-tuning dataset to the edge server to fine-tune the model. Prior to this fine-tuning, the edge server employs ZEN$_{infer}$.Prove to create a zero-knowledge proof for the fine-tuning dataset using a regulation model, which is then returned to the AIGC user. This user subsequently sends signature and the proof to a smart contract designated for regulating the specific fine-tuning dataset. The smart contract validates the proof through ZEN$_{infer}$.Verify. Upon successful verification, it records the proof details for the fine-tuning dataset on the blockchain, enabling future regulation inquiries.

C. Design of Zero Knowledge Proof

The ZEN scheme [23] is employed in the regulation system to conceal the regulation model and the content of the dataset during the data supervision process. The accuracy of the regulation model on the datasets can be verified using ZEN$_{acc}$. The compliance of the dataset can be verified using ZEN$_{infer}$. The utilization of the ZEN scheme ensures the preservation of model privacy and dataset privacy during the supervision process. The system includes two proof and verification processes: one to prove the accuracy of the regulation model on example regulatory datasets, and another to prove the dataset's compliance with regulation rules.

In the accuracy proof process, the roles of prover and verifier are assigned to the cloud and edge servers, and the data regulator, respectively. The process initiates with the prover sending the model to the KMS. The KMS then employs ZEN$_{acc}$.Gen to generate the proving key pk_a and verification key vk_a for the accuracy proof. Additionally, it uses ZEN$_{infer}$.Gen to produce the proving key pk_i and verification key vk_i for the inference proof. Once the KMS dispatches these keys to the prover, the prover, having received pk_a, utilizes ZEN$_{acc}$.Commit to create a commitment for the model. Following this, the prover uses ZEN$_{acc}$.Prove to generate a proof that prove the model's accuracy on the example regulatory dataset. Subsequently, the prover forwards the commitment, proof, vk_a, and vk_i to the verifier. The verifier then applies ZEN$_{acc}$.Verify to authenticate the proof. After verification, the verifier will deploy a smart contract for this model using vk_i. This systematic process ensures that the accuracy of the model is validated in a secure and reliable manner, adhering to the established regulatory standards.

In the inference proof process, the cloud and edge servers act as the prover, while the smart contract serves as the verifier. The prover begins by utilizing pk_i and ZEN$_{infer}$.Prove to generate a proof for either the training or the fine-tuning dataset dataset. Following the generation of this proof, it is sent to the specific smart contract designated for this purpose. Upon receiving the proof, the smart contract employs its built-in verification key vk_i to verify the proof's authenticity using ZEN$_{infer}$.Verify. This methodical approach guarantees that the verification of the inference results is conducted securely, ensuring that no additional information is disclosed.

D. Discussion

1) Regulation Flexibility

The proposed system utilizes AI models to supervise datasets in the AIGC service system. To comply with regulatory requirements set by a data regulator, multiple cloud servers can be utilized to train various regulation AI models for these rules. In practical scenarios, different countries and regions have distinct data requirements and limitations. The proposed framework addresses this diversity by depicting it through multiple data regulators. Each data regulator represents a regulation standard within a specific jurisdiction, and corresponding smart contracts can be implemented on the blockchain to support the regulation. This method offers a flexible mechanism for varied regional regulation rules.

2) Scalability

The scalability of the proposed system is influenced by several factors, such as servers and the blockchain. Server-side scalability depends on the infrastructure, where the number of servers impacts the system's ability to generate proofs concurrently, and each server's computational capacity determines the speed of proof generation. Blockchain-side scalability relies on smart contracts' efficiency on the blockchain and choosing an appropriate blockchain platform is crucial due to varying transaction processing speeds and smart contract execution capabilities offered by different platforms.

3) Potential for Cross-Domain Application

The proposed system shows great potential for application in different domains beyond its initial scope. This system utilizes AI to manage datasets, which can be adjusted to oversee and guarantee compliance of datasets in various fields. For instance, in the healthcare industry, the system could be used to ensure compliance and protect privacy. With growing focus on data compliance, the capability to supervise these datasets effectively and accurately is crucial. Hence, this system becomes a valuable tool for maintaining data integrity and compliance across diverse areas.

VI. Analysis

A. Security Analysis

The system is designed to safeguard both the privacy of the regulation model and the input dataset. Regarding the regulation model's privacy, the servers generate a commitment using the model and a random factor. This commitment, made available to others, reveals nothing about the model itself, thereby maintaining its confidentiality. For the dataset's privacy, the system only discloses the inference result, along with the associated commitment and proof. This limited disclosure ensures that no information about the datasets can be inferred by external parties. As a result, the privacy of the datasets is effectively protected. This dual-layered approach to privacy protection is integral to the system's design, ensuring secure and confidential data handling.

B. Performance Analysis

The system was evaluated on a MacBook Air M2 with 8GB RAM using simulations that focused on performance and resource usage. The assessment included measuring the time taken for zero-knowledge proof processes and the gas used during smart contract execution.

In this simulation, we hypothesize a scenario mandated by a data regulator to exclude facial information from the image dataset. Utilizing the CIFAR-10 [24] and ORL [25] datasets, we developed a facial classification model based on the LeNet [26] architecture. The model comprises three convolutional layers with ReLU activations and average pooling, followed by two fully connected layers to generate a binary classification output. This model takes a dataset as input and outputs a result list identifying whether the dataset contains facial information. Subsequently, we used subsets of 10,000 to 50,000 images from CIFAR-10 for evaluation. Upon completion of the model's execution, we employed the ZEN$_{infer}$ framework to generate and verify zero-knowledge proofs. The supervision process includes the following steps: 1) The model receives the dataset as input and produces the supervision result. While executing the model, quantization is performed to store quantitative intermediate weight and result. 2) The ZEN$_{infer}$ framework utilizes the quantitative intermediate weight and result to create proof for the supervision process. 3) The proof is sent to a smart contract for verification.

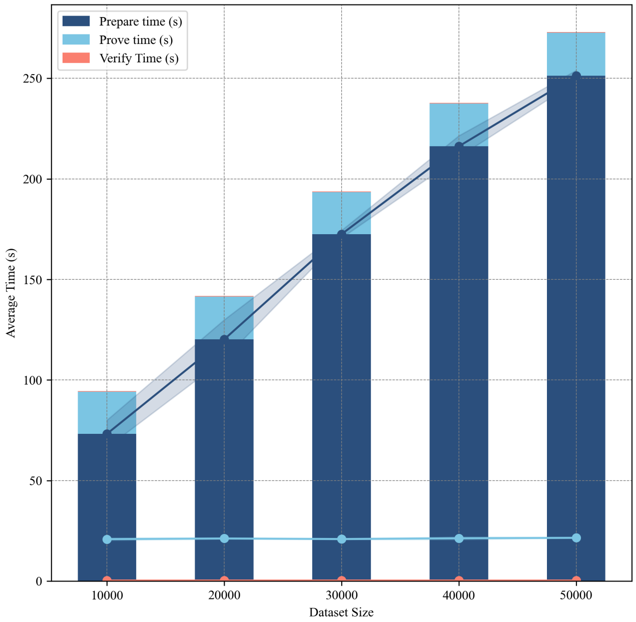

Fig. 3. Time vs Different dataset size

In zero-knowledge proof systems, the time expenditure is categorized into three distinct phases: preparation, proof generation, and verification. The preparation phase encompasses tasks such as data acquisition, model execution, and model quantization, which involves transforming the model's floating-point values into integers. The proof generation phase is dedicated to creating zero-knowledge proofs based on the quantized models. Finally, the verification phase involves the authentication of the zero-knowledge proofs. Fig. 3 depicts the relationship between dataset size and the time required for zero-knowledge proof processing. The graph reveals a roughly proportional correlation between preparation time and dataset size. Conversely, because the model used is the same, both proof generation and verification time remain constant, exhibiting no variation in response to changes in dataset size.

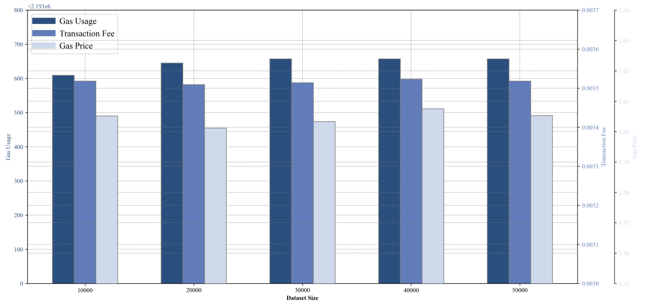

Fig. 4. Gas usage vs Different dataset size

To analyze the gas consumption in smart contract validation, we deployed a validator-specific smart contract on the Ethereum Sepolia testnet. This enabled the measurement of gas usage during the verification of five unique zero-knowledge proofs in the smart contract. Data presented in Fig. 4 encompasses the gas usage, gas fee, and transaction fee for different verifications. Insights from this figure reveal minimal variation in gas consumption for verifying diverse zero-knowledge proofs. This uniformity in gas requirements for proof verification is likely due to the similar sizes of the generated proofs, implying a consistent gas demand for verifying smart contract proofs.

These experiments successfully showcase the performance and resource utilization of the proposed system, emphasizing two key aspects: time spent across various stages and the gas consumption in smart contract verification. The results provide crucial insights into the efficiency and performance of zero-knowledge proof systems within blockchain applications.

VII. Future Research Directions

A. ZKP Improvement

The usage of ZKP may introduce certain issues. Current ZKP algorithm introduces computational overhead. The efficiency of ZKP is crucial for the practical implementation of our proposed system. Future research should focus on developing high-efficiency ZKP algorithms, which involves optimizing algorithms to reduce computational overhead. Research efforts should also focus on ensuring the post-quantum security of the ZKP algorithm against quantum computing threats. Furthermore, current ZKP needs specialized knowledge to implement and verify the proofs. Establishing standards for ZKP in dataset regulation is necessary to enhance interoperability and increase adoption rates.

B. Scalability

To ensure the system can handle increasing volumes of data and users, future work should focus on enhancing overall system scalability. Improving server infrastructure by investigating distributed computing architectures and load balancing techniques could greatly enhance the system's ability to generate proofs. Investigating options like layer-2 scaling or alternative consensus mechanisms may assist the blockchain component in managing a higher volume of smart contract interactions.

C. Real-world Deployment

To transition from theoretical model to practical application, future research should focus on deploying the system in real-world scenarios. Conducting comprehensive testing in real-world conditions will help identify potential issues and areas for improvement that may not be apparent in simulated environments. Gathering and analyzing data on the system's performance, user experience, and regulatory effectiveness will be crucial for refining the system and demonstrating its value to potential adopters.

VIII. Conclusion

In this study, we initially explore AIGC and AIGC service, underscoring the necessity for dataset regulation. We delve into the complexities associated with dataset governance in AIGC service system, and introduce a novel solution: a blockchain-based AIGC zero knowledge dataset regulation system. Our proposed system leverages AI for automated regulation, employs ZKP for data privacy, and integrates blockchain and smart contracts to mitigate third-party misconduct. The paper further presents a security analysis and performance simulation of our system. This includes an assessment of privacy safeguards, efficiency metrics like proof generation and verification time, and the resource consumption for smart contract verification proofs. This approach ensures that the system is not only private but also practical for AIGC service system.

References

[1] T. Brown, B. Mann, N. Ryder, M. Subbiah, J. D. Kaplan, P. Dhariwal, A. Neelakantan, P. Shyam, G. Sastry, A. Askell, *et al.*, "Language models are few-shot learners," *Advances in neural information processing systems*, vol. 33, pp. 1877–1901, 2020.

[2] H. Du, Z. Li, D. Niyato, J. Kang, Z. Xiong, D. I. Kim, *et al.*, "Enabling ai-generated content (aigc) services in wireless edge networks," *arXiv preprint arXiv:2301.03220*, 2023.

[3] C. Geiger and V. Iaia, "The forgotten creator: Towards a statutory remuneration right for machine learning of generative ai," *Computer Law & Security Review*, vol. 52, p. 105925, 2024.

[4] Y. Chi, H. Duan, W. Cai, Z. J. Wang, and V. C. Leung, "Networking parallel web3 metaverses for interoperability," *IEEE Network*, 2023.

[5] P. Hacker, A. Engel, and M. Mauer, "Regulating chatgpt and other large generative ai models," in *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*, pp. 1112–1123, 2023.

[6] T. Wu, S. He, J. Liu, S. Sun, K. Liu, Q.-L. Han, and Y. Tang, "A brief overview of chatgpt: The history, status quo and potential future development," *IEEE/CAA Journal of Automatica Sinica*, vol. 10, no. 5, pp. 1122–1136, 2023.

[7] J. Ho, A. Jain, and P. Abbeel, "Denoising diffusion probabilistic models," *Advances in neural information processing systems*, vol. 33, pp. 6840–6851, 2020.

[8] Y. Cao, S. Li, Y. Liu, Z. Yan, Y. Dai, P. S. Yu, and L. Sun, "A comprehensive survey of ai-generated content (aigc): A history of generative ai from gan to chatgpt," *arXiv preprint arXiv:2303.04226*, 2023.

[9] M. Xu, H. Du, D. Niyato, J. Kang, Z. Xiong, S. Mao, Z. Han, A. Jamalipour, D. I. Kim, X. Shen, *et al.*, "Unleashing the power of edge-cloud generative ai in mobile networks: A survey of aigc services," *IEEE Communications Surveys & Tutorials*, 2024.

[10] D. Zhang, B. Xia, Y. Liu, X. Xu, T. Hoang, Z. Xing, M. Staples, Q. Lu, and L. Zhu, "Privacy and copyright protection in generative ai: A lifecycle perspective," in *Proceedings of the IEEE/ACM 3rd International Conference on AI Engineering-Software Engineering for AI*, pp. 92–97, 2024.

[11] D. Hartmann, J. R. L. de Pereira, C. Streitbörger, and B. Berendt, "Addressing the regulatory gap: moving towards an eu ai audit ecosystem beyond the aia by including civil society," *arXiv preprint arXiv:2403.07904*, 2024.

[12] D. Mügge, "Eu ai sovereignty: for whom, to what end, and to whose benefit?," *Journal of European Public Policy*, pp. 1–26, 2024.

[13] J. Laux, S. Wachter, and B. Mittelstadt, "Trustworthy artificial intelligence and the european union ai act: On the conflation of trustworthiness and acceptability of risk," *Regulation & Governance*, vol. 18, no. 1, pp. 3–32, 2024.

[14] S. Goldwasser, S. Micali, and C. Rackoff, *The knowledge complexity of interactive proof-systems*, p. 203–225. New York, NY, USA: Association for Computing Machinery, 2019.

[15] D. Benarroch, M. Campanelli, D. Fiore, K. Gurkan, and D. Kolonelos, "Zero-knowledge proofs for set membership: Efficient, succinct, modular," in *International Conference on Financial Cryptography and Data Security*, pp. 393–414, Springer, 2021.

[16] S. Garg, A. Goel, S. Jha, S. Mahloujifar, M. Mahmoody, G.-V. Policharla, and M. Wang, "Experimenting with zero-knowledge proofs of training," in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1880–1894, 2023.

[17] S. Steffen, B. Bichsel, R. Baumgartner, and M. Vechev, "Zeestar: Private smart contracts by homomorphic encryption and zero-knowledge proofs," in *2022 IEEE Symposium on Security and Privacy (SP)*, pp. 179–197, IEEE, 2022.

[18] N. Bitansky, R. Canetti, A. Chiesa, and E. Tromer, "From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again," in *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, pp. 326–349, 2012.

[19] K. Baghery, Z. Pindado, and C. Ràfols, "Simulation extractable versions of groth's zk-snark revisited," in *International Conference on Cryptology and Network Security*, pp. 453–461, Springer, 2020.

[20] Z. Xing, Z. Zhang, J. Liu, Z. Zhang, M. Li, L. Zhu, and G. Russello, "Zero-knowledge proof meets machine learning in verifiability: A survey," *arXiv preprint arXiv:2310.14848*, 2023.

[21] C. Huang, J. Wang, H. Chen, S. Si, Z. Huang, and J. Xiao, "zkmlaas: a verifiable scheme for machine learning as a service," in *GLOBECOM 2022-2022 IEEE Global Communications Conference*, pp. 5475–5480, IEEE, 2022.

[22] J. Zhang, Z. Fang, Y. Zhang, and D. Song, "Zero knowledge proofs for decision tree predictions and accuracy," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2039–2053, 2020.

[23] B. Feng, L. Qin, Z. Zhang, Y. Ding, and S. Chu, "Zen: An optimizing compiler for verifiable, zero-knowledge neural network inferences," *Cryptology ePrint Archive*, 2021.

[24] A. Krizhevsky, "Learning multiple layers of features from tiny images," Master's thesis, University of Toronto, 2009.

[25] F. S. Samaria and A. C. Harter, "Parameterisation of a stochastic model for human face identification," in *Proceedings of 1994 IEEE workshop on applications of computer vision*, pp. 138–142, IEEE, 1994.

[26] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proceedings of the IEEE*, vol. 86, no. 11, pp. 2278–2324, 1998.

Jiaxiang Sun received a B.Sc. degree in Environmental Science and a B.Sc. degree in Computer Science and Technology from Peking University, China in 2022. He is currently pursuing an M.Phil. in Computer and Information Engineering in the School of Science and Engineering at the Chinese University of Hong Kong in Shenzhen, China, under the supervision of Prof. Wei Cai. He is working in Human-Crypto Society Laboratory. His current research interests include blockchain and game theory.

Rong Zhao received the B.Eng. degree in Communication Engineering from The Southern University of Science and Technology, China in 2018. He is currently working towards Ph.D. in Computer and Information Engineering in the School of Science and Engineering at The Chinese University of Hong Kong, Shenzhen, China. He is working as an Research Assistant in Human-Crypto Society Laboratory. His current research interests include blockchain, game theory and digital twin.

Lehao Lin received the BEng degree in Computer Science and Engineering from The Chinese University of Hong kong, Shenzhen, China, in 2021. He is currently working towards the PhD degree in Computer and Information Engineering with The Chinese University of Hong Kong, Shenzhen, China. He is working as a research assistant with Human-Crypto Society Laboratory. His current research interests include blockchain, human-centered computing and multimedia.

Yuanfang Chi received her B.Eng. and M.A.Sc. degree in Electrical and Computer Engineering from The University of British Columbia (UBC) in 2011 and 2015, respectively. She is currently a Ph.D. candidate at UBC and is visiting Shenzhen University, China. Her research interests include distributed computing and networking. She is a student member of IEEE.

Victor C.M. Leung is the Dean of the AI Research Institute and a Professor of Engineering at Shenzhen MSU-BIT University, China. He is also a Distinguished Professor of Computer Science and Software Engineering at Shenzhen University, China, and an Emeritus Professor of Electrical and Computer Engineering at the University of British Columbia, Canada. He has published widely in the broad areas of wireless networks and mobile systems, and is a Clarivate Analytics “Highly Cited Researcher”. He is a Life Fellow of IEEE, and a Fellow of the Royal Society of Canada, Canadian Academy of Engineering, and Engineering Institute of Canada.

Wei Cai is an Assistant Professor of Computer Science and Systems at the University of Washington, Tacoma, WA, USA. Prior to joining UW, He was an Assistant Professor of Electrical and Computer Engineering at The Chinese University of Hong Kong, Shenzhen, China. He holds a Ph.D. from the University of British Columbia, Vancouver, BC, Canada. Dr. Cai has published over 100 peer-reviewed papers, winning six Best Paper Awards. His research focuses on decentralized computing, with emphasis on mechanism design, social computing, multimedia, and applications. He is a Senior Member of IEEE and an ACM member.