Towards Trustworthy Governance of AI-Generated Content (AIGC): A Blockchain-Driven Regulatory Framework for Secure Digital Ecosystems

Fan Yang, Mohammad Zoynul Abedin, Yanan Qiao, Lvyang Ye

***Abstract*—Digital platforms are experiencing a growing presence of generative artificial intelligence (AI) content, raising concerns due to the prevalence of misinformation that disrupts market integrity. Consequently, the development of effective regulatory measures for overseeing generative AI content becomes imperative. This necessitates the establishment of mechanisms to detect and filter out inaccuracies, ensuring compliance with regulatory requirements. In addition, collaboration among experts, regulators, and AI developers is essential to encourage responsible AI deployment on digital platforms. Successful governance hinges on principles of transparency, accountability, and proactive risk management to navigate the evolving generative AI on digital platforms. Therefore, in order to address the security issues currently faced by Artificial Intelligence Generated Content (AIGC), this article first proposes a method of efficient cache mechanism for AIGC content. The secure method of determining the identity of AIGC content owners is proposed based on blockchain technology. Subsequently, it suggests mechanisms for access control and data encryption for generated content within a blockchain environment. Finally, it presents an efficient data supervision mechanism tailored to the AIGC environment. The methods outlined in this article aim to enhance security from three perspectives: protection of content creators' identities, safeguarding data security, and ensuring effective data supervision within the AIGC framework. The experimental results further confirm that our proposed method not only ensures the security of the AIGC framework but also provides an efficient data analysis and supervision solution for digital platforms.**

***Index Terms*—AIGC regulation, Blockchain governance, Data traceability, Consensus mechanism, Data security.**

Manuscript received 2 May 2024; revised 1 August 2024; accepted 28 September 2024. Date of publication XX XX 2024; date of current version XX XX 2024. This research is supported by the Natural Science Basic Research Program of Shaanxi [Program No. 2023-JC-YB-490]. This research is also supported by the Research Fund of Guangxi Key Lab of Multisource Information Mining & Security [Program No.MIMS24-06]. This research is also supported by "the Fundamental Research Funds for the Central Universities, JLU" [Program No.93K172024K12].(Corresponding author: Mohammad Zoynul Abedin and Yanan Qiao.)

F. Yang is with the School of Computer Science and Technology, Xi'an Jiaotong University, Xi'an 710049, China; F. Yang is also with Guangxi Key Lab of Multi-source Information Mining Security, Guangxi Normal University, Guilin 541004, PR China; F. Yang is also with Key Laboratory of Symbolic Computation and Knowledge Engineering of Ministry of Education, Jilin University, Changchun, Jilin, 130012, PR China. (e-mail: f.yangcs@xjtu.edu.cn)

M.Z.Abedin is with Department of Accounting and Finance, School of Management, Swansea University, Bay Campus, Fabian Way, Swansea SA1 8EN, Wales, the United Kingdom (e-mail: m.z.abedin@swansea.ac.uk).

Y. Qiao is with the School of Computer Science and Technology, Xi'an Jiaotong University, Xi'an 710049, China. (e-mail: qiaoyanan@mail.xjtu.edu.cn)

L. Ye is with Xi'an Institute of Electromechanical Information Technology, Xi' an, Shaanxi, 710065, China. Besides, he also jointly researched with Science and Technology on Electromechanical Dynamic Control Laboratory, Xi'an, Shaanxi, 710065, China (e-mail: lvyangye2016@163.com).

I. Introduction

In the domain of digital platforms, the prevalence of AIGC is steadily increasing [1]–[3]. However, this proliferation is accompanied by a significant challenge: a plethora of inaccuracies and misinformation within such content. AIGC is content produced by AI for text, images, audio, etc., while Generative AI specifically mimics human creativity in generating natural language text and images. AIGC can be viewed as a practical application of Generative AI, highlighting its role in content creation. The content generated by Generative AI contains a significant amount of erroneous and unsupervised information, posing new challenges to the security of digital platforms. The rapid advancement of Generative AI technology allows for the easy generation of various types of content, including text, images, and audio, but it also increases the risks of misinformation, fraudulent content, and privacy violations. Therefore, regulation of Generative AI technology on digital platforms has become crucial. Regulating Generative AI technology helps ensure the quality and security of content on digital platforms [4]–[6]. The regulation can include establishing stringent algorithm and model review standards to ensure that the generated content complies with ethical principles and legal requirements. Moreover, implementing transparent data usage policies is also necessary to protect user privacy and data security. By strengthening regulation, the risks of spreading misinformation and harmful content can be reduced, thereby safeguarding the healthy development of digital platforms and user trust. Therefore, regulating Generative AI technology on digital platforms is of significant importance as it can effectively address the security challenges it poses, safeguard user rights, and promote the healthy development of the digital ecosystem.

The swift development of generative artificial intelligence technology has ignited a transformation across multiple industries, notably within digital platforms and risk management. As a result, this innovative technology has emerged as a versatile and powerful tool, revolutionizing the way businesses operate and manage risks. For example, by analyzing patterns in transactional data using generative AI models, companies can identify potential fraudulent activities more accurately and efficiently. These AI systems can continuously learn and adapt to new data, enabling proactive risk mitigation strategies and enhancing overall security measures. Leveraging advanced algorithms and machine learning techniques, generative artificial intelligence systems can efficiently analyze vast datasets to

accurately evaluate content, offering valuable insights within digital platforms [7]. The increasing integration of AIGC within the digital platforms sphere underscores its transformative potential and emphasizes the growing reliance on AI-driven solutions to drive innovation and competitiveness in the digital landscape. The advancement of Internet of Things (IoT) technology has laid the foundation for the dissemination and widespread user adoption of AIGC. With an increasing number of users engaging in AIGC on digital platforms, issues related to user identity verification security and data content access security have gradually surfaced [8], [9]. As the landscape of digital content creation continues to evolve, ensuring robust mechanisms for safeguarding user identities and data privacy becomes increasingly imperative.

With numerous applications in so many different industries, artificial intelligence generated content has shown to be a potent tool for creating content, especially in the digital platform space [10], [11]. AIGC has completely changed the way content is made by allowing businesses to produce tailored and interesting content at scale. It does this by utilizing sophisticated algorithms and machine learning approaches. It has become an invaluable tool for businesses looking to improve their online presence and establish more effective connections with their target audience because of its capacity to analyze data, recognize trends, and adjust to user preferences. AIGC is expected to become more and more important in determining the direction of content creation in a variety of industries as it develops and gets better.

AIGC can increase productivity when building digital systems [12]–[14]. When building a digital platform, AIGC can increase productivity by automating the processing of complicated computational processes and vast volumes of data. It has the ability to evaluate data fast and precisely, find hidden patterns and trends, and offer solid assistance in making decisions. Additionally, data platforms can become more intelligent and adaptable by using AIGC technology, assisting companies in making better use of data resources to meet their goals. For instance, AIGC models can analyze vast amounts of diverse data sources, generate realistic synthetic data sets, and uncover valuable insights that traditional methods may overlook. By harnessing the power of AIGC, organizations can optimize decision-making processes, improve data-driven strategies, and drive innovation by unlocking the hidden potential within their data resources, ultimately propelling them towards successful goal attainment [15], [16].

However, despite its benefits, there are significant challenges that need to be addressed. One critical issue is the difficulty in tracing the sources and origins of data generated by AIGC systems [17]. This lack of transparency raises concerns about data integrity, reliability, and accountability, especially in sensitive areas such as credit evaluation where decision-making is heavily reliant on accurate and trustworthy information. Moreover, the inadequate security measures in place for safeguarding AIGC-generated data pose a significant risk of unauthorized access, manipulation, or leakage of sensitive financial information. These vulnerabilities not only compromise data privacy but also expose corresponding institutions to potential regulatory violations and reputational damage. Addressing these challenges through robust data traceability mechanisms, enhanced cybersecurity protocols, and regulatory frameworks is essential to ensure the responsible and secure deployment of AIGC in the credit domain and maintain trust in AI-driven digital platforms.

However, several challenges still exist concerning the security of AIGC on digital platforms. Firstly, one significant difficulty is in identifying the sources or origins of the data generated by AIGC. This lack of transparency can lead to uncertainties about the authenticity and reliability of the content produced. Secondly, there is a challenge in effectively tracking and tracing the dissemination of AIGC-generated data, making it more susceptible to unauthorized access and potential information leaks. This aspect raises concerns regarding data privacy and security breaches. Lastly, ensuring the overall security of AIGC systems poses a notable challenge, particularly in distributed environments where data may be stored and processed across multiple locations and networks. Addressing these challenges is crucial to enhancing the trustworthiness and integrity of AI-generated content and maintaining data security in AIGC systems.

Therefore, in order to address the current challenges of AIGC regulatory issues in digital platforms, this study focuses on a blockchain-based approach to AIGC regulation. The main contributions of this study are 1) we propose an efficient cache mechanism for AIGC content, thus guaranteeing that the efficiency of AIGC content storage meets the requirements of the regulatory mechanism; 2) we propose a blockchain-based approach to AIGC owner identification and assurance approach to AIGC owner, thus guaranteeing the security of AIGC content owner's identity; 3) finally, we propose a blockchain-based AIGC whole process regulation and data encryption method, which ensures that the AIGC content and data transaction processes are always in the state of security regulation, thus guaranteeing the security of AIGC digital platform and reliability of the AIGC digital platform.

The subsequent sections of the paper are structured as follows. In Section 2, we will introduce the current research on AIGC regulatory frameworks and the methods that have been adopted, in addition to a summary of the existing methods. In Section 3, we will comprehensively describe the specific approach of our proposed blockchain-driven regulatory framework. In the 4th section, we will present the experimental data and information on the configuration of the experimental settings. In Section 5, we will analyse the contribution of a blockchain-based approach to AIGC regulation in balancing data security and AIGC generation efficiency. In Section 6, we will analyse future research directions on blockchain-based AIGC regulation, as well as critical trends and contributions to research on digital platforms. In section 7, we will summarise the paper's contribution to AIGC safety regulation in digital platforms and the present study's commitment to engineering management.

II. Related Work

In this section, we will provide a comprehensive overview of recent works on AIGC regulatory frameworks in three

closely related aspects: 1) AIGC and its application, 2) AIGC data privacy protection, and 3) blockchain governance and regulation.

A. Generative AI and its application to digital platforms

In recent years, the contribution of generative artificial intelligence to digital platforms has been steadily increasing. An increasing number of researchers are focusing on utilizing generative AI technologies to tackle challenges such as low model efficiency and insufficient AI capabilities in digital platforms and large-scale models.

Of the relevant studies on Generative AI and its application to digital platforms, Du et al. [18] propose an innovative architecture for collaborative distributed diffusion-based AIGC, aiming to expedite the development of widespread AIGC services. By leveraging device cooperation in wireless networks, their framework streamlines AIGC tasks and optimizes edge computing resource utilization. Furthermore, they explore the practical implementation of denoising processes on mobile devices, assess the impact of their approach on wireless network-enabled AIGC, and outline future integration prospects into real-world applications. Chen et al. [19] propose the concept of Large Language Model Systems Engineering (LLM-SE) and delve into the foundational principles driving the development of LLM industry applications. They outline the functional and feature requirements essential for LLM industry applications, culminating in the creation of an AI-assisted clinical risk prediction system for amyloidosis disease, employing the LLM-SE architecture. This system integrates quality engineering, knowledge engineering, and other methodologies, while also exploring the expansion architecture and methodology of LLM-SE. Guo et al. [20] provide a comprehensive technical overview and historical context of ChatGPT, while also examining the potential security threats encompassing political, military, economic, cultural, social, ethical, and legal dimensions, along with concerns regarding machine escape and information leakage. Additionally, they explore the prospective benefits that AIGC brings to public safety education, politics, military applications, cybersecurity, and societal advancements. Du et al. [21] develop a novel deep learning-based AIGC system specifically designed for spatiotemporal sketch extraction. This system capitalizes on the structural and temporal attributes of videos, enabling sparse coding and sketch extraction at the sender's end. Upon reception, the original videos can be generatively reconstructed or utilized for various machine vision tasks. Through these research endeavors, it is evident that prevalent investigations on Generative Artificial Intelligence systems primarily center on augmenting model precision and devising strategies to alleviate ethical dilemmas and prejudices embedded in AI-generated content. Consequently, in this process, effective regulatory oversight of AI-generated content emerges as imperative.

B. AIGC data privacy protection

Currently, ensuring data privacy protection is crucial for Generative AI. As Generative AI technology generates content using advanced artificial intelligence algorithms, there is a growing concern about safeguarding the privacy of the data involved in this process [22], [23]. Protecting sensitive information such as personal data, intellectual property, and confidential business data is essential to prevent privacy breaches and maintain trust with users. By implementing robust data encryption, access controls, data anonymization techniques, and compliance measures, organizations can effectively protect data privacy within AIGC applications and mitigate the risks associated with handling sensitive information.

In the realm of AIGC data privacy protection research, effective regulation and safeguarding of data, particularly with regards to platform interaction data, are crucial. Wang et al. [24] conduct a systematic examination of the security and privacy implications surrounding generative data in AIGC, approaching the subject through the lens of information security features for the first time. Klaine et al. [25] propose a pioneering blockchain framework tailored to safeguard privacy within data exchange marketplaces. Leveraging blockchain technology, the framework records transactions pertaining to data exchanges and enables access control through the generation of access sequences post-trade execution. Notably, data-generating entities, such as sensors and devices, are afforded the option to store their data on alternate servers. The authors advocate a fresh outlook on data ownership, emphasizing that blockchain transactions merely grant temporary data access while affirming absolute ownership and control to the original data creators. Furthermore, the envisioned blockchain framework supports various data types and ensures data quality, timeliness, and similarity control within the marketplace, capitalizing on its decentralized and transparent attributes. Xu et al. [26] and colleagues delve into the challenges of edge pretrained foundation model (PFM) concerning mobile AIGC services in the metaverse. They initiate by elucidating the fundamentals of PFM, highlighting their distinctive edge intelligence inference and fine-tuning methodologies. Proposing a fresh paradigm for efficient model management and resource allocation to meet user demands, they advocate for strategies combining model caching and inference. Moreover, they introduce the novel metric, the Age of Context (AoC), tailored to gauge the relevance and freshness of examples in tasks and demonstrations, aligning with PFMs' contextual learning capabilities. Lastly, they endorse a least-context (LC) approach, aimed at striking a balance between accuracy, latency, and energy consumption for governing cached models on edge servers.

C. Blockchain Governance and Regulation

Blockchain governance plays a critical role in ensuring data security. Blockchain technology offers a decentralized and transparent way to store data, making it resistant to tampering and unauthorized access [27]–[31]. Proper governance frameworks help establish rules and protocols for managing blockchain networks, including access control, data validation, and consensus mechanisms. By implementing effective governance practices, organizations can enhance the security of their data stored on the blockchain, maintain the integrity of transactions, and ensure that sensitive information remains secure

from cyber threats and malicious actors. Overall, blockchain governance is essential for maintaining trust, transparency, and data security within blockchain ecosystems.

Of the relevant studies on blockchain governance and regulation, Yusuf et al. [26] propose leveraging blockchain's inherent structure to ensure the security, anonymity, and integrity of financial transactions in the Metaverse. They introduce a novel consensus mechanism merging Proof of Stake (PoS) and Proof of Authority (PoA) to enhance network security and scalability. Additionally, they advocate for a user-centric decentralized identity management system to protect personal information. Their approach includes a smart contract-based method for securely managing Metaverse transactions, ensuring reliable transactional proof, recording, and validation. Furthermore, they outline a reputation system aimed at incentivizing compliance and discouraging misconduct within the virtual environment. Li et al. [32] propose a collaborative framework named "Value–Standard–Process" for blockchain-based enterprise data governance, focusing on robust data security, dependable task execution, and transparent value translation. They introduce a novel collaborative mode for blockchain-based manufacturing in the sharing economy, incorporating a trusted data governance mechanism, a smart contract generation mechanism for value-driven collaboration, and a nonlinear dynamic evaluation and value balancing mechanism for multi-attribute data. The subsequent elaboration and implementation details of these elements validate the feasibility and effectiveness of the proposed framework through experimentation. Ultimately, this value-driven, multi-level blockchain-based cooperation mode enhances trust and streamlines production component flow. Ullah and colleagues [33] seek to clarify blockchain's role in governance processes, explore blockchain-specific governance, and propose a robust governance structure for the blockchain-driven Internet of Things (IoT) ecosystem. They offer a case study in smart logistics to exemplify the practical application of their governance system. Anticipating enhanced reliability and security for the Internet of Things, their envisioned governance framework aims to foster seamless integration of blockchain technology with IoT across diverse application domains. Chatterjee and co-authors [34] propose a framework utilizing blockchain smart contracts for managing transactions among parties within a blockchain-powered supply chain network. The framework ensures transparency and traceability throughout the supply chain ecosystem by documenting all transactions. In case of abuse, a group signature technique is employed. The system's overall performance is evaluated using three metrics: transaction efficiency, system risk reduction, and participant trust. Gas cost, average execution time, throughput, and latency are utilized post-framework implementation to assess transaction efficiency, demonstrating satisfactory system performance.

Through analysis of existing research, it can be concluded that recent advancements in AIGC have demonstrated promising applications across various sectors. Table.I presents a summary of technologies used in existing blockchain and regulatory mechanism. As can be seen from Table.I, our blockchain-based regulatory approach will comprehensively consider the characteristics of AIGC data sharing security, regulatory reliability, traceability, etc., so as to enhance the regulatory capability of the AIGC system. Nevertheless, challenges concerning data security, content ownership verification, traceability, and privacy persist. The governance and regulation of blockchain present efficient traceability and robust data privacy protection mechanisms, potentially offering effective regulatory solutions for AIGC governance.

TABLE I
SUMMARY OF TECHNOLOGIES USED IN EXISTING BLOCKCHAIN AND REGULATORY MECHANISM ON DIGITAL PLATFORMS

Study	Traceability	Data sharing	Regulation scheme	Privacy protection
[21]	✓			
[24]		✓		
[25]	✓	✓		
[26]	✓	✓		
[32]		✓		
[33]	✓	✓		
[34]	✓			
This study	✓	✓	✓	✓

III. THE APPROACH

Blockchain technology is well-suited for regulatory oversight in generative artificial intelligence platforms due to its immutable and decentralized ledger, ensuring transparency and traceability of data transactions. Its cryptographic security features also help safeguard user privacy and uphold ethical and legal standards within the platform's ecosystem. The blockchain-based AIGC regulation method for digital platforms proposed in this paper will be investigated in three aspects: efficient caching mechanism of AIGC content, blockchain-based AIGC owner identification and assurance method, blockchain-based AIGC full-process regulation and data encryption method, and blockchain-based AIGC full-process regulation and data encryption method, respectively. Fig.1 illustrates the overall workflow of the proposed blockchain-based AIGC regulation method. Each of the following subsections will be structured around each of the proposed research points for the blockchain-based AIGC regulatory framework.

As shown in Fig.1, the Blockchain-based AIGC regulatory system is a platform that leverages blockchain technology to facilitate oversight and governance of content produced by artificial intelligence algorithms.The system serves as a decentralized and transparent ledger that meticulously records the entire life cycle of AI-generated content. Each piece of content is chronologically stamped and securely stored on the blockchain, ensuring its integrity and preventing any unauthorized alterations. To uphold regulatory standards, smart contracts are employed to automate compliance verifications, ensuring that all content complies with the stipulated guidelines before dissemination. This automated validation process guarantees that content creators adhere to established regulations and mitigates the dissemination of harmful or deceptive information. Key components of the system encompass a distributed ledger for content data storage, smart contracts for regulatory compliance enforcement, and a user-friendly

interface for regulatory bodies to efficiently monitor and audit the content creation process. By seamlessly interfacing blockchain technology with artificial intelligence, the AIGC regulatory system provides a robust, streamlined, and transparent framework for overseeing the generation of AI-produced content.

A. Efficient cache mechanism for AIGC content

In this subsection, we will introduce the key ideas of efficient cache mechanism for AIGC content approach in the AIGC regulatory framework. In the proposed efficient cache mechanism for AIGC conten, the importance of generated content at different times in the AIGC digital platform can be expressed as follows.

$$u_t = \sqrt{\alpha_t} u_{t-1} + \sqrt{1-\alpha_t} z_t,$$

where u_t is the digital content after adding noise z_t at the t step, and $\alpha_t = 1-\beta_t$. Besides, z_t is sampled from the standard normal distribution $\mathcal{N}(0,1)$. If β_t increases, $1-\alpha_t$ increases. It means that the proportion of the adding noise z_t increases, while the importance of digital content u_{t-1} reduces, which can lose its distinguishable features in the forward process. (1) can be utilized to derive the relationship of u_t and u_0 as

$$\begin{aligned} u_t &= \sqrt{\alpha_t \alpha_{t-1} \cdots \alpha_2 \alpha_1} u_0 + \sqrt{1-\alpha_t \alpha_{t-1} \cdots \alpha_2 \alpha_1} z \\ &= \sqrt{\bar{\alpha}_t} u_0 + \sqrt{\overline{\alpha_t + 1}} z \end{aligned}$$

where $\bar{\alpha}_t = \prod_{t=1}^{T} \alpha_t$. Since $z_1, \ldots, z_t, \ldots, z_T$ are sampled from Gaussian noises $\mathcal{N}(0,1)$, they can be merged with different variance $\left\{\mathcal{N}\left(0,\sigma_1^2\right), \ldots, \mathcal{N}\left(0,\sigma_t^2\right), \ldots, \mathcal{N}\left(0,\sigma_T^2\right)\right\}$ as the new distribution as $\mathcal{N}\left(0, \sigma_1^2 + \cdots + \sigma_t^2 + \cdots + \sigma_T^2\right)$. Therefore, $1 - \sqrt{\alpha_t \alpha_{t-1} \cdots \alpha_2 \alpha_1}$ represents the combined standard deviation calculated from the updated distribution. Hence, the training process in the forward phase can be conducted as follows: 1) randomly select an image from the dataset; 2) randomly pick a step t from 1 to T; then determine u_t; 3) feed u_t into the model and acquire the output into the model and obtain the output out $= \operatorname{model}(u_t, t)$; 4) evaluate the loss by introducing additional variations and adjust the model's gradient through the loss function = loss_func (out,z).

There is a need to decrease AIGC service latency for recurring complex requests from users in the regulation framework. However, there is a dearth of metrics to gauge service excellence. Additionally, as content caching necessitates participants to contribute resources to sustain digital content availability, caching devices might act selfishly by manipulating AIGC digital platform object to maximize their profits. In this segment, leveraging the quality of validated content as delineated in prior sections, we introduce a Stackelberg game-inspired content caching mechanism. This mechanism considers the interactions between each AIGC digital platform object and caching devices as a two-stage hierarchical game to determine the optimal strategies.

A group of AIGC digital platform objects on edge devices has the option to participate as caching entities (participants) for the primary AIGC digital platform objects to deliver a collection of digital contents $\mathcal{C} = \{1, 2, \ldots, n$ generated by AIGC request tasks on blockchain, which can be represented as $\mathcal{I} = \{1, 2, \ldots, i, \ldots, I\}$. The payment schemes $\mathbf{p}$ can be represented as $\mathbf{m} = [\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_i]$, where m_{ic} signifies the compensation that each AIGC digital platform object offers to caching entities i for content c.

Since caching services necessitate participants to expend resources to deliver content, participants might prioritize higher profits over the quality of caching services. Digital content verification can be achieved using the regulation framework, while assessing caching service quality entails determining the similarity between u_t' and u_t. For instance, if there are $T = 15$ steps involved in generating and caching digital content, participants may opt to execute only a subset of steps to conserve resources. AIGC regulation user can randomly define a step interval $[u_c, u_c+$ step] to assess the quality correct/step, where "correct" denotes the steps verified. Evaluating service quality mirrors the methodology of Truebit, extensively utilized for verifying computational tasks in Ethereum. Consequently, the quality n_{ic} of caching services furnished by participant i for content c is akin to evaluating computation tasks.

In addressing the different AIGC scenario concerning caching devices, the evaluation of the utility function occurs when $n_{ic} = -1$. We initially examine $q_{ic} = -1$ to simplify the determination of u_{ic}. By calculating $P_{ic}(0,-1) = P_{ic}(0,0) = 0$ and $R_{ic}(-1) = r_i > R_{ic}(0) = 0$, resulting in the utility $u_{ic}(0,-1) = -r_i < u_{ic}(0,0) = 0$ for caching device i. Thus, if caching device i relies on chance outcomes when retrieving digital content, its utility is inferior compared to scenarios where $q_{ic} \in [0,1]$. Consequently, the equations are as follows.

$$u_{ic}(m_{ic}, n_{ic}) = -d_i v^2 n q_{ic}^2 + \tau m_{ic} n_{ic}, \quad n_{ic} \in [0,1]. \tag{1}$$

The first-order and second-order derivatives of the utility function $u_{ic}(m_{ic}, n_{ic})$ with respect to q_{ic} are given by:

$$\frac{\partial u_{ic}(m_{ic}, n_{ic})}{\partial n_{ic}} = -d_i v^2 n_{ic} + \tau m_{ic}, \quad n_{ic} \in [0,1], \tag{2}$$

$$\frac{\partial^2 u_{ic}(m_{ic}, n_{ic})}{\partial n_{ic}^2} = -d_i v^2 < 0, \quad n_{ic} \in [0,1]. \tag{3}$$

Given that the second derivative is negative, we can determine that the first derivative is a monotonically decreasing function. It can be expressed as:

$$\lim_{m_{ic} \to 0} \frac{\partial u_{ic}(m_{ic}, n_{ic})}{\partial q_{ic}} = \tau m_{ic} > 0 \tag{4}$$

$$\lim_{n_{ic} \to 1} \frac{\partial u_{ic}(m_{ic}, n_{ic})}{\partial n_{ic}} = -d_i v^2 + \tau m_{ic} \tag{5}$$

The sign of $\frac{\partial u_{ic}(m_{ic}, n_{ic})}{\partial_{,ic}}$ determines the monotonicity of $u_{ic}(m_{ic}, q_{ic})$. When $\tau m_{ic} \geq d_i v^2$, we have $\lim_{n_{ic} \to 1} \frac{\partial u_{ic}(m_{ic}, n_{ic})}{\partial n_{ic}} \geq 0$, indicating that $u_{ic}(m_{ic}, n_{ic})$ is a monotonically increasing function. Therefore, when $q_{ic}^* = 1$, the maximum utility of caching device i is given by:

$$u_{ic}^*(m_{ic}, n_{ic}) = -d_i v^2 + \tau m_{ic}, \quad d_i v^2 \leq \tau p_{ic}. \tag{6}$$

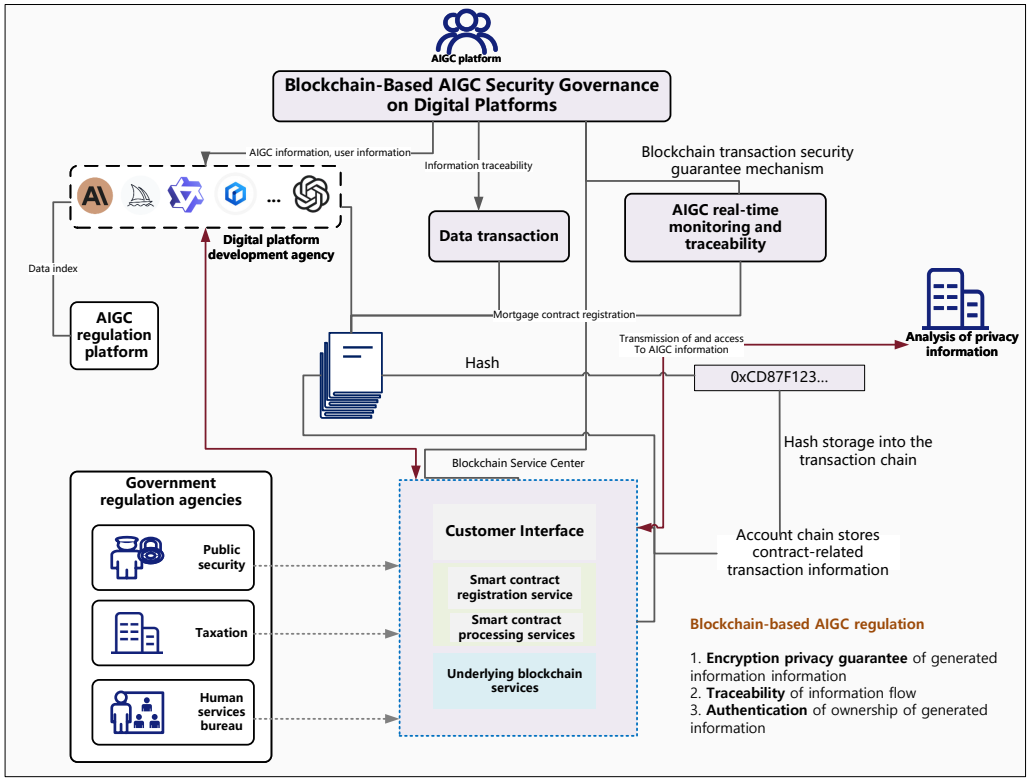

Fig. 1. The overview workflow of blockchain based AIGC regulation. Through smart contracts, participants can execute various transactions and agreements securely and transparently. Through blockchain technology, personal data is encrypted and stored on an immutable distributed ledger, ensuring data confidentiality and integrity. The framework utilizes multiple security measures, including encryption techniques, access control, and identity verification.

B. Blockchain-based approach to AIGC owner identification and assurance

1) Mechanisms for securing AIGC information: As a decentralized and tamper-proof distributed ledger technology, blockchain plays a crucial role in the identification and assurance of ownership for AI-generated content (AIGC). Through blockchain technology, ownership information of AIGC can be securely stored and cannot be altered, thereby preventing data forgery and infringement. Additionally, blockchain technology can provide traceability and transparency for content creators of AIGC, ensuring that their legal rights are protected. In conclusion, blockchain-based approaches are vital for the identification and assurance of AIGC ownership, providing a safer, fairer, and more trustworthy environment for the development of digital content industry.

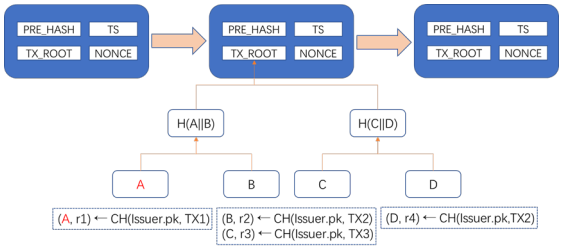

Fig. 2. Block structure in the blockchain-based AIGC content regulation mechanism

The block structure of the blockchain-based AIGC regulation mechanism is shown in Fig.2. The traceability and transparency of AIGC content can be guaranteed by the links formed between blocks. An unchangeable chain-like structure is formed by each block containing the hash value of the one before it. This architecture improves the security and reliability of the material by guaranteeing that any changes made to AIGC content will be detected and reported along the whole chain. Each block also contains transaction timestamps, transaction IDs, and other information that makes regulatory supervision and auditing easier. All things considered, the blockchain-based AIGC content regulation system provides a dependable and effective approach to content governance.

Fig. 3 presents the blockchain-based AIGC identity encryption mechanism. As data on the blockchain is transparent and publicly accessible, any node that joins the blockchain can view the data on the chain. Adding authorization information directly in plaintext to the blockchain may result in user information leakage.

To address this concern, our AIGC regulation scheme employs an Identity-Based Encryption (IBE) system to encrypt upstream information and attach the corresponding decryption key to downstream users. This approach allows upstream information to be visible to downstream users while preventing unauthorized users from decrypting the information. However, the repeated IBE encryption and decryption on the chain lead to an increase in system response time. Fig.4 presets the secure transaction mechanism for AIGC content in IoT environments in our method.

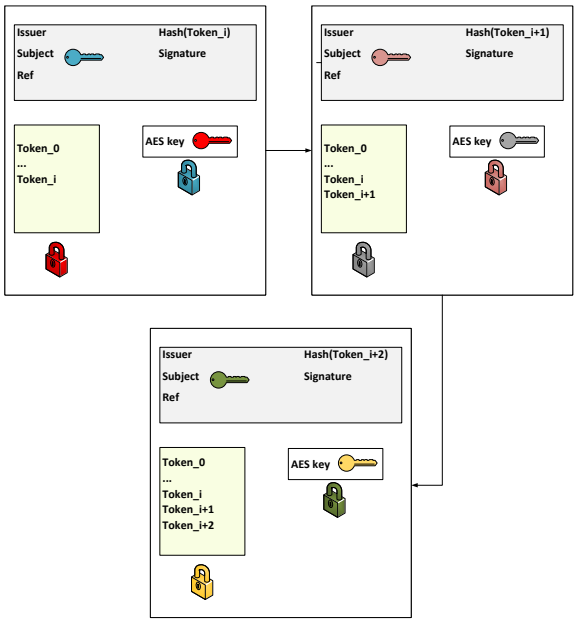

Fig. 3. Blockchain-based AIGC identity encryption mechanism

In Fig.4, Alice, as the AIGC digital platform content owner, registers the new device on the blockchain through transaction $tx1$. Since this transaction is a registration transaction, there is no reference transaction upstream. Then, Alice generates token2 and grants a permission to Bob through transaction $tx2$. Bob then publishes transaction $tx3$ to grant token3 to Carol. When Carol requests service from the device, the device checks the legitimacy of the authorization chain to determine whether to provide the service.

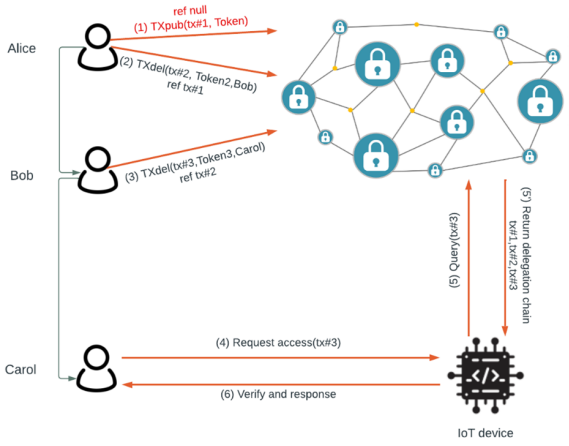

Fig. 4. Blockchain-based secure transaction mechanism for AIGC content in IoT environments

In Traditional blockchain applications transfer homogeneous tokens (such as BTC, ETH) in transactions, while our access control chain transfers permissions, which we represent as tokens. 1) Transaction In order to grant permissions to other entities, the sender constructs a transaction signed by the grantee, which includes the specific information of the permissions to be transferred. A transaction includes the following:

- Issuer: the AIGC owner entity that wishes to grant permissions to another entity.
- Subject: the entity receiving the permissions.
- Token: the expression of regulaiton permissions.
- Ref: reference for the previous transaction.

In our method, data transactions are divided into two types. The first type is TXregister, which is used for registration. When a new IoT device wishes to join the access control chain, a transaction TXregister is published with the address of the device, and the recipient of this transaction is the owner of the device. After the transaction is successfully published, the subject is registered as the owner of the device and obtains all permissions related to the device. All permissions related to the device are granted either directly or indirectly by the owner. The second type of transaction is TXdelegate, which is used to transfer permissions. The issuer publishes this transaction to grant permissions to other entities. In order to trace the permissions and form a delegation chain, the issuer needs to indicate the transaction in which they obtained the relevant permissions.

In our regulation framework, Token indicates a license certificate that is transmitted during the authorization process, used to describe permissions. To achieve fine-grained management of permissions, our designed token contains the following fields. Object is the resource entity that provides the regulation service; Valid time is the time during which the permission is valid; Delegation Policy(DP) is the authorization policy expressed as an integer;

In our scheme, we use Delegation Policy (DP) to control the depth of authorization. When DP is 0, the subject can only use the token and cannot delegate it. When DP is greater than 0, the subject can use and delegate the token to a depth no greater than DP. When DP is less than 0, the subject cannot use the token, but can pass the permission to others with a delegation depth no greater than the absolute value of DP. This is a necessary design in practical scenarios and, to the best of our knowledge, no other distributed scheme can support this requirement.

It should be noted that when an Issuer creates a new token and issues a transaction TX granting a permission to a subject, the Issuer does not lose its original permission due to the authorization. Instead, the Issuer only needs to attach the transaction TX, which grants the Issuer the permission, as a dependency to TX. When the subject of TX needs Object to provide a service, the subject sends TX to Object for verification. To avoid security issues during the authorization process, the granted permission must meet certain conditions: 1). the issuer has the corresponding permission, 2). the subject satisfies all restrictions in the authorization rule, and 3). the authorization itself does not violate any general constraints). To improve the readability of this paper, additional authorization restrictions are not discussed herein.

Specifically, each field of the token (Tokento) authorized by the issuer must be a subset of the issuer's own token (Tokenfrom). To prevent privilege escalation, when the Object receives a new request, it will follow the Ref field of the

transaction and verify whether each downstream token is a subset of the adjacent upstream token. If all are valid and the TXregister transaction is reached, the transaction TX1 is considered legitimate and the device returns acceptance and provides the service.

C. Blockchain-based approach to full-process regulation of AIGC-generated content

1) AIGC information security guarantee mechanism: Firstly, in order to preserve the security of the content in the process AIGC blockchain regulation, we designed the AIGC message encryption guarantee mechanism. We employed an encryption scheme by using AES encryption and the AES symmetric key encrypted by RSA. AES is a symmetric encryption algorithm used for data encryption and protection. It is currently one of the most commonly used encryption standards, widely applied in various fields such as network communication, database storage, digital platforms, etc., to ensure the security and confidentiality of data [35]. In our regulation framework, each authorization transaction generated contains both the old authorization chain information from the upstream and the newly authorized permissions granted in this transmission. These two parts are combined into a new authorization chain and encrypted with AES. In this way, downstream users can easily obtain the specific information of the upstream authorization chain without the upstream keys.

To enhance the security of AIGC supervision, our proposed system adopts a redefined blockchain that extends traditional blockchain systems to ledger systems, incorporating smart contract systems and oracle systems. The system can have many-to-many relationships. For example, a ledger system can have multiple smart contract (SC) systems, an SC system can collaborate with multiple ledger systems, and an oracle machine (OM) can connect to multiple SC systems. To simplify the system, code and data are separated. For supervision, embedded supervision mechanisms are introduced at the protocol layer. The system proposes to decouple the ledger system, oracle system, and contract system of LSO (Ledgers, Smart Contracts, Oracles) to make the system more stable, leading to a more engineering and scientific development, ultimately bringing significant changes in standardization, networking, and service. Fig.5 presents AIGC's full-process regulatory guarantee mechanism incorporating multi-layer smart contracts.

In the AIGC regulatory model, data transactions and consensus mechanisms are not required to be tied together. Transactions are transactions, and consensus is consensus. Consensus is simply about consistency, while transactions not only require consistency but also transaction ordering. Therefore, consistency should come first, while transactionality should come later. The core structure and system of blockchain have been revolutionized, marking a significant breakthrough in the next generation of blockchain systems.

The model adopts an improved Practical Byzantine Fault Tolerance (PBFT) consensus mechanism based on a reputation-based mechanism. It integrates the advantages of Proof of Authority (POA) consensus into the new PBFT

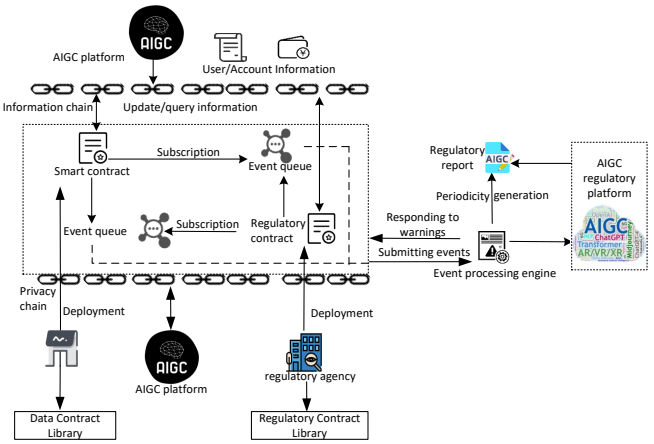

Fig. 5. AIGC's regulatory guarantee mechanism incorporating multiple smart contrac smart contracts

algorithm, leveraging organizational authority to reduce the likelihood of malicious attacks or tampering, thus enhancing the efficiency of traditional PBFT consensus. Following the PBFT consensus algorithm, each node is considered equal with the same level of trust, and accounting is conducted sequentially according to certain rules. In the new consensus mechanism, authoritative departments from real-world functions and other highly reputable institutions are prioritized as accounting nodes. These organizations are not only trustworthy themselves but also operate physical machines capable of withstanding network attacks. Therefore, the likelihood of these trusted organizations engaging in malicious behavior and requiring re-election is reduced. This approach saves time spent on re-elections, leading to improved algorithm efficiency. Moreover, in cases where accounting nodes act maliciously, the network can promptly address the situation and decrease the credibility of these malicious organizations within the system.

In order to enable the separation of private and generation-critical information in AIGC messages, we propose the dual-chain structure and smart contracts. We use the integration of AIGC Information chain and privacy chain in a Dual-Chain Structure: The dual-chain structure combines the AIGC information chain and privacy chain. Based on the analysis of requirements, two separate chains are constructed: the AIGC information chain is used to maintain primary AIGC content, while the privacy chain handles sensitive identity authentication information. All AIGC data generated throughout the business process is uploaded to different blockchains based on the distinction between AIGC content and privacy information. This dual-chain concept, where account content information and privacy information are separated, enhances the overall system scalability.

Furthermore, the segregated dual-chain structure facilitates regulatory transactions while preserving the privacy of AIGC owners. Strict monitoring of data transactions on the privacy chain is enforced, and homomorphic encryption technology effectively protects users' AIGC content information. Upon receiving identity information query requests from AIGC con-

tent owners, the privacy chain retrieves user information from the information chain, encrypts and sends the information in ciphertext form, and then performs homomorphic encryption calculations on the retrieved information before returning the results in ciphertext form to both the information chain providing the data and the requesting institution. After the transaction is completed, the privacy chain does not retain any account-related data but stores the calculation records on the chain.

In the regulation framework, by utilizing oracles, the system links the data chains within the dual-chain structure with smart contracts. AIGC regulation information is written into five smart contracts and evaluated based on the rules required by applications such as the AIGC regulatory authentication platform or commonly recognized rules, allowing reactions to uncertain external dynamics. This enables interoperability between blockchain data and real-world data, enhancing transparency and providing reliable references for AIGC regulation.

In our regulation method, interactions between systems involve complex exchanges but do not equate to cross-chain transactions. The essence of interactions lies in merging and computing data obtained from multiple chains, multiple oracle machines (OMs), or multiple smart contracts. This differs from traditional cross-chain concepts where value exchange occurs between two or more chains, which may have different or similar structures, requiring consensus from both sides during transactions. Cross-chain transactions necessitate multiple consensuses, thereby impacting speed. Some cross-chain technologies sacrifice transactional and supervisory capabilities for speed, making them challenging to use in compliant financial markets.

2) Full process AIGC regulation: Compared to traditional regulatory model, we proposed the blockchain-based full process regulation scheme to offer higher efficiency by automatically placing transactions within the appropriate regulatory framework, enabling a close integration of regulation and transactions. With the introduction of immersive supervision, the entire transaction process is subject to efficient and comprehensive supervision. Simultaneously, the regulatory process enhances the security and effectiveness of transactions. Algorithm 1 and Algorithm 2 present the regulatory equity allocation algorithm and regulatory incentive algorithm in the proposed AIGC regulation framework. Two algorithms ensure the efficiency and stability of the entire AIGC regulation process from the aspects of regulatory requests and regulatory incentives.

In the full process regulation, firstly, all data is uniformly and instantly recorded on the chain, making it difficult for any organization or individual to alter the on-chain data, thus achieving real-time self-certification of on-chain data. Secondly, regulatory agencies are no longer detached from the regulated system; all responsible entities (AIGC subjects, AIGC institutions, regulatory bodies, etc.) are in a constant state of regulation and being regulated. They no longer need to specially collect, store, coordinate, and summarize data. Real-time regulation eliminates falsification, money laundering, fraud, and other malpractices. Algorithm 3 proposed the regulatory default penalty algorithm to penalize violations during the regulatory process. Throughout the entire monitoring process, real-time AIGC risk monitoring is achieved by calculating the AIGC regulatory risk index.

When working within a scenario where the AIGC has a very large number of supervisory tasks, multiple supervisory entities collectively form an exclusive alliance chain, granting them access rights to transaction information for investigating money laundering clues. Through the combination of ”smart contracts + network-wide broadcasting,” these entities can participate in internal industry rule agreements, leveraging the immutability, distributed ledger, and traceability advantages of blockchain technology. This significantly enhances internal compliance and audit convenience, promoting sustainable and healthy development within the industry.

In our blockchain based regulation scheme, we propose the construction of editable blockchains. Specifically, the AIGC publisher (Issuer) can revoke the token granted in the current transaction, which refers to the last token in the token list. Revocation may be caused by various reasons, and in the long-term operation of the system, downstream of an authorized transaction may contain many authorized branches, forming a large authorized directed acyclic graph. In some cases, downstream authorizations can be directly discarded, but there are also situations where the complexity of the system makes it impossible to discard them. These two cases are classified as non-cascading revocation and cascading revocation, respectively. Cascading revocation not only revokes the current authorization but also indirectly revokes all other authorization transactions that depend on this authorization. Non-cascading revocation only revokes the current authorization transaction without affecting the normal use of downstream authorizations[20]. When the Issuer needs to revoke an authorized transaction, the Issuer needs to mark the Hash of Token as cascading revocation or non-cascading revocation (at this point, the Hash of Token has lost its original meaning) and use the Adapt function of the Chameleon Hash algorithm to rewrite the hash value of the transaction. Due to the constant changes of data on the blockchain, even if an Entity has passed the validation of Object, Object still needs to recheck the authorization chain on the blockchain when a new request arrives. If there is a cascading revocation in the authorization chain, the service will be denied, and if there is a non-cascading revocation in the authorization chain, the validity of the entire authorization chain will continue to be checked.

Fig.6 depicts the timing state chart of the blockchain-based AIGC framework. It can be observed that blockchain supervision throughout the entire process can provide crucial AIGC status information to regulatory entities at each stage, thereby ensuring a reliable regulatory process over time.

IV. Experiment results and analysis

This study proposes an efficient and secure blockchain-based regulatory framework for AIGC information, thereby safeguarding the needs for owner security, content delivery security, and real-time content regulation of AI-generated information in digital platforms. Since the primary focus of the paper is on establishing an efficient and secure regulatory mechanism between AI-generated content (AIGC) and

Algorithm 1 AIGC regulatory equity allocation algorithm

Input: Data conversion value of user's AIGC content S_u^0, regulatory risk score C_u^0, size of data transactions Am, regulatory risk conversion factor μ, grade decay rate η

Output: AIGC content risk indicators after n-level guarantee credit enhancement C_u^i,$C_g^{k,i}$,$P_{k,i}$

if $C_u^0 < C_u^b$ **then**
  for k in n **do**
    $\alpha_k \leftarrow \frac{S_g^k + C_g^k/\mu}{\sum_{k=1}^{m}\left(S_g^k + C_g^k/\mu\right)}$
  end for
  for i in n **do**
    $C_u^i \leftarrow C_u^{i-1} + \alpha_k * (1-\eta)^{i-1} * \mu * \frac{\sum_{k=1}^{n} S_g^k}{Am}$
    $C_g^{k,i} \leftarrow C_g^{k,i-1} - \alpha_k * (1-\eta)^{i-1} * \mu * \frac{S_g^k}{Am}$
    $P_{k,i} \leftarrow \frac{\alpha_k * (1-\eta)^{i-1}}{\sum_{i=1}^{n} \alpha_k * (1-\eta)^{i-1}}$
  end for
end if

Algorithm 2 AIGC regulatory incentive algorithm

Input: Data conversion value of user's AIGC content S_u^0, regulatory risk score C_u^0, size of data transactions Am, regulatory risk conversion factor μ, grade decay rate η

Output: AIGC regulatory incentives after incentivised metrics C_g^k, C_u^n

if repayment is done **then**
  for i in n **do**
    $C_g^k \leftarrow C_g^k + \alpha_k * (1-\eta)^{i-1} * \mu * \frac{S_g^k}{Am}$
    $C_g^k \leftarrow C_g^k * \left(1 + \frac{Am * P_k}{S_g^k}\right)^{-i}$
    $C_u^n \leftarrow C_u^0 * \sum_{i=1}^{n} \left(1 + \frac{Am * P_{k,i}}{S_g^k}\right)^{-i}$
  end for
end if

Algorithm 3 AIGC regulatory default penalty algorithm

Input: Data conversion value of user's AIGC content S_u^0, regulatory risk score C_u^0, size of data transactions Am, regulatory risk conversion factor μ, grade decay rate η,Scale of data to be regulated $OutAm$

Output: AIGC regulatory incentives after incentivised metrics C_g^k, C_u^n

if regulation is overdue **then**
  $S_u \leftarrow S_u^0 -$ OutAm
  if $S_u < 0$ **then**
    $S_g^k \leftarrow P_k * \left(\text{OutAm} - S_u^0\right)$
  for i in n **do**
    $C_g^k \leftarrow C_g^k * \left(1 - \theta * \frac{Am * P_k}{S_g^k}\right)^{-i}$
    $C_u^n \leftarrow C_u^0 * \sum_{i=1}^{n} \left(1 - \theta * \frac{Am^* P_{k,i}}{S_g^k}\right)^{-i}$
  end for
  end if
end if

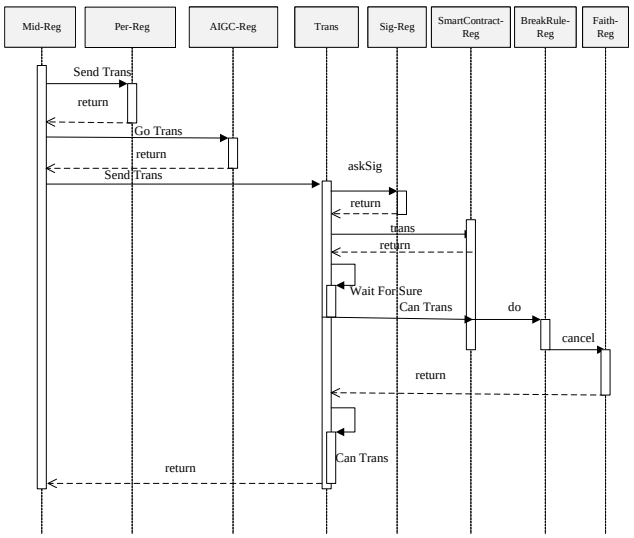

Fig. 6. The timing state chart of blockchain-based AIGC framework.

blockchain technology on digital platforms, our goal is to address the following research questions through experiments:

RQ 1) Whether our blockchain-based AIGC regulatory platform has satisfactory AIGC data processing performance, especially with high data volumes?

RQ 2) How do the different performance metrics of our blockchain-based AIGC regulatory platform change as the participating regulatory nodes change?

The dataset used in this article is the dialogue response generation dataset PhotoChat [36], which is the first dataset to reveal photo sharing behavior in online message exchanges. PhotoChat comprises 12,000 conversations from the AIGC digital platform, each conversation accompanied by information shared by users during the conversation and the generated content. Based on this dataset, we will conduct performance testing and experiments on the blockchain-based digital platform AIGC for governance. We will focus on testing the performance of key features such as AIGC identity security verification and content moderation. We will begin by presenting analytical results, offering quantitative insights into the effectiveness and performance of the proposed framework. Finally, we will delve into a comprehensive discussion, analyzing the implications and potential applications of our findings within the realm of AIGC regulation and blockchain integration on digital platforms.

A. Experimental results regarding RQ1

We first conduct experimental results for RQ1, thus demonstrating whether the performance of our proposed blockchain-based AIGC regulatory platform is within reasonable limits.

Table.II shows the results of the time consumption at different stages in blockchain-based AIGC regulation in case of different block sizes. As can be seen in Table.III, the time consumption of the different metrics for AIGC regulation is within a reasonable range as the block sizes change.

Fig.7 presents the variation of validation time in RDE with the authorization depth. shows the variation of validation time

TABLE II
TIME CONSUMPTION AT DIFFERENT STAGES IN BLOCKCHAIN-BASED AIGC REGULATION IN CASE OF DIFFERENT BLOCK SIZES

Block Size	Agency Registration	AIGC Reugulation Application	Guarantee Voucher Generation	Guarantee	Enquiry
10	38.9	36.8	30.5	35.3	1224.6
20	78.6	75.3	65.2	71.6	1254.3
50	189.7	183.2	162.7	174.9	1243.5
100	350.1	338.6	306.4	319.5	1278.7
1000	432.2	420.3	361.2	384.8	1231.6
2000	434.3	421.7	363.5	385.4	1237.4

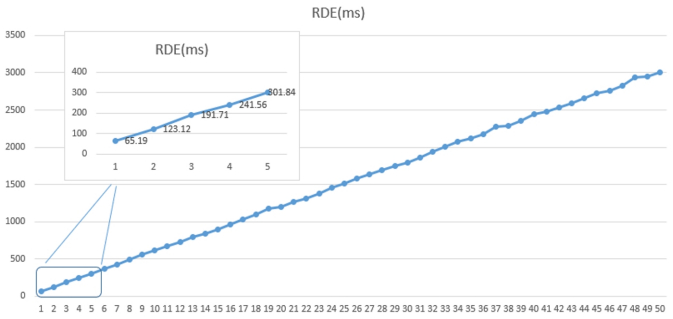

Fig. 7. The variation of validation time in our regulation framework with the authorization depth

in AIGC regulating scheme (validation time = n × IBE decryption time + 2 × n × AES decryption time + token legality check time) with the AIGC authorization depth. It can be observed that the time required to validate the entire authorization chain in regulation framework is linearly related to the authorization depth. When the authorization depth is only 1, it takes $65ms$ to validate an authorization transaction. Fig.7 illustrates the variation of validation time in I-RDE (validation time = 1 * RSA decryption time + 1 * AES decryption time + token legality check time + time to compare token hash value with the hash value saved in the corresponding transaction) with the authorization depth. In our method, since the device only needs to decrypt the transaction that the service requester obtained permission (i.e., the credential transaction) once, the device decrypts the token list and compares the hash value of each token in the token list with the corresponding hash value saved in the transaction one by one. The validation time in our method shows a stable trend and remains below 0.25ms.

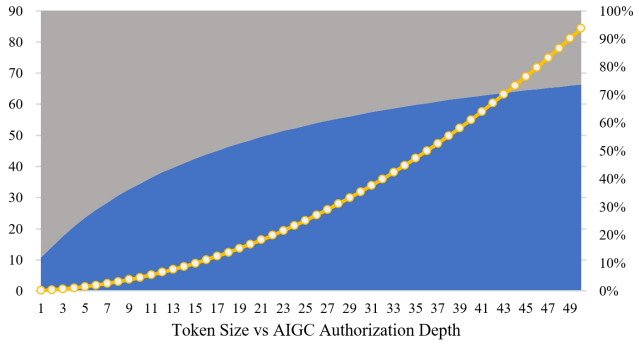

Fig. 8. Relationship between AIGC authentication depth and different block token sizes

Our proposed regulation method, only needs to store n specific tokens on the blockchain under an authorization chain with depth n, while the framework needs to store $(n+1)*n/2$ specific tokens. Therefore, we conducted an analysis and comparison of the storage space of the system. As our regulation scheme does not store duplicates, each token is encrypted and stored in a single transaction. The size of tokens included in an authorization chain increases linearly from $0.125kb$ to $6.25kb$ (yellow line in Fig.8) as the authorization depth increases. The proportion of storage space occupied by tokens stored in transactions at different depths of the authorization chain remains approximately constant at 10.3% (blue area ratio).

Fig.9 shows the changes in regulatory efficiency ratios under different regulatory unit times. It can be observed that with more regulatory unit time, the regulatory efficiency ratio is larger in regulatory frameworks with more nodes. This indicates that with the participation of more nodes, regulatory capabilities have been further enhanced.

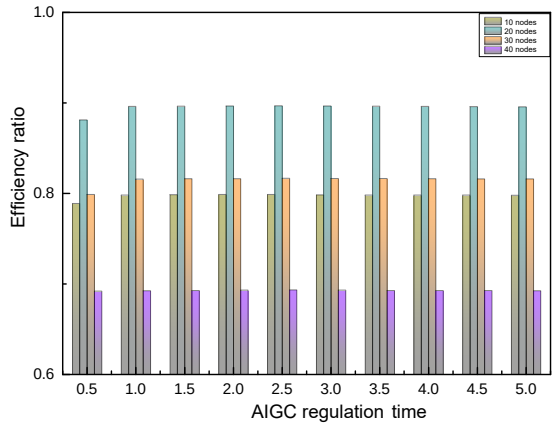

Fig. 9. Effect of different running times on efficency ratio

With the increase in participating nodes, the phenomenon of steady improvement in the efficiency of regulating AIGC is deeply influenced by blockchain technology. The increase in the number of nodes leads to an overall increase in the computational power of the blockchain network, making the data verification and storage of AIGC more efficient. Furthermore, the increase in nodes can enhance the decentralization of the network, reduce the risk of single points of failure, and further ensure the security and reliability of AIGC. Moreover, as the number of participating nodes increases, the consensus mechanism in the blockchain network becomes more robust and reliable. The increased frequency and immediacy of in-

TABLE III
RESULTS OF DIFFERENT CREDIT SCORING METHODS

Number of AIGC Regulation Requests	Throughput (s)	Average User Request Wait Time (ms)	System Operation
50	24.51	2040.259	Normal
100	47.98	1042.055	Normal
200	93.19	536.551	Normal
500	214.46	233.148	Normal
1000	378.94	131.949	Normal

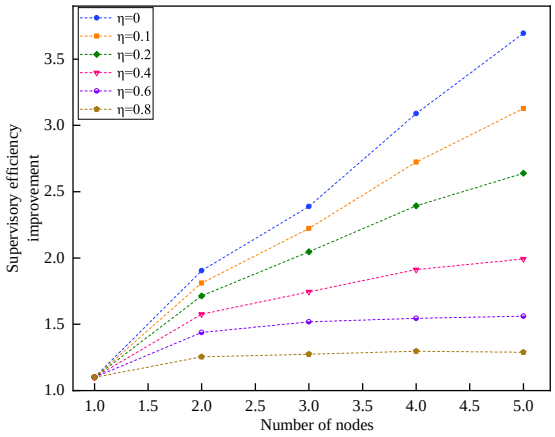

Fig. 10. Line graph of the change in the multiplier of supervisory efficiency improvement as the number of nodes increases

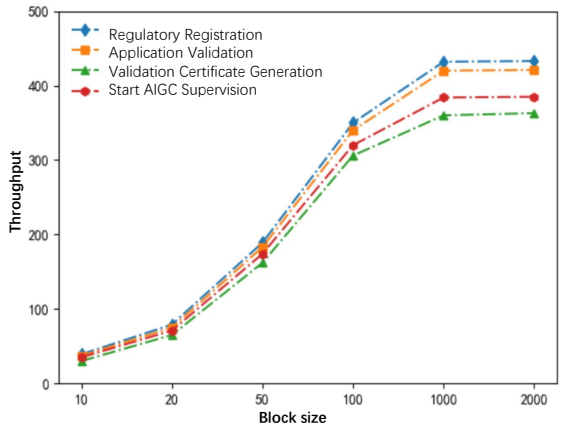

Fig. 11. Line graph of throughout versus block size for AIGC regulatory data

formation exchange between nodes help in quickly detecting and correcting errors or anomalies, thereby improving the efficiency of regulating AIGC. Additionally, the increase in the number of nodes promotes the scalability of the blockchain network, allowing the network to better adapt to the growing data traffic of AIGC, which is beneficial for enhancing overall performance. Based on the experimental results, it is evident that increasing participating nodes has a significantly positive impact on the efficiency improvement of regulating AIGC. In future research and practice, further exploration can be done on optimizing node selection strategies, improving consensus mechanisms, and strengthening network security protection to better leverage the potential application of blockchain technology in the regulation of AIGC.

B. Experimental results regarding RQ2

Next, we will further test how the performance of our blockchain regulatory platform changes under different conditions of node participation, different consensus rounds, etc. Fig.11 presents the line graph of throughout versus block size for AIGC regulatory data.

In Fig.11, with the increase in the number of nodes, the throughput of supervisory blocks for AIGC-generated content gradually increases and tends to stabilize. The main reason is that the addition of nodes enables the blockchain network to have higher processing capacity and capability. As the number of nodes grows, the overall computational power also strengthens, thereby enhancing the processing speed and throughput of supervisory blocks. This means that more AIGC-generated content can be effectively verified, stored, and processed, making the supervisory process more efficient. Furthermore, with the growth in the number of nodes, the data transmission speed and efficiency within the blockchain network are also improved. The increased number of nodes implies more network bandwidth and resources available for utilization, accelerating the information transmission speed between supervisory blocks. This helps ensure real-time and timely supervision, further enhancing the throughput of supervisory blocks. In conclusion, based on the experimental results, it can be observed that the throughput of supervisory blocks for AIGC-generated content gradually increases and stabilizes with the increase in the number of nodes. The increase in node numbers plays a crucial role in enhancing the processing capacity and data transmission efficiency of the blockchain network, effectively promoting an improvement in the throughput of supervisory blocks. Future research could further explore optimizing network architecture, enhancing inter-node communication efficiency, and improving data processing algorithms to further elevate the throughput and performance of supervisory blocks.

Fig.12 presents the graph of the efficiency of block generation as it varies with different consensus rounds. The experimental results demonstrate that as the consensus rounds increase, the efficiency of our method in block generation gradually improves and stabilizes. This improvement can be attributed primarily to the efficient consensus mechanism embedded in our blockchain regulation framework. The increased consensus rounds lead to a more refined and optimized process for block generation, resulting in enhanced efficiency over time. This improvement is crucial for ensuring the smooth operation of the blockchain network and the timely processing

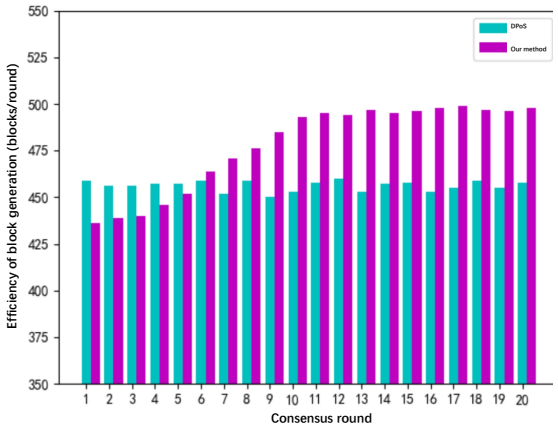

Fig. 12. Graph of the efficiency of block generation as it varies with different consensus rounds

of transactions. Furthermore, the stability observed in the efficiency of block generation indicates the robustness and reliability of our method under varying conditions. This stability is essential for maintaining consistent performance and preventing disruptions in the blockchain network's operations. Overall, our experiment results underscore the effectiveness of our approach in enhancing block generation efficiency over successive consensus rounds. This improvement contributes to the overall performance and reliability of the blockchain network, making it better equipped to meet the demands of various applications and scenarios. Moving forward, further research can delve into optimizing additional aspects of our method to continue improving the efficiency and effectiveness of blockchain regulation and operation.

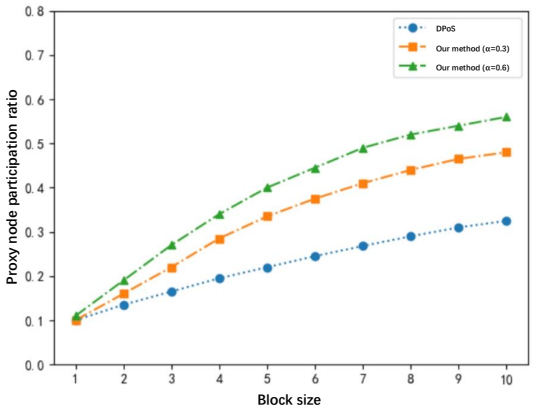

Fig. 13. Graph of the percentage of participation of agent nodes with different block sizes

Fig.13 presents the graph of the percentage of participation of agent nodes with different block sizes. In Fig.13, with the increase in the number of experiments, the participation ratio of supervisory nodes for AIGC-generated content is gradually increasing. The main reason is that as more AIGC is generated, maintaining the security and reliability of the data requires the involvement of more blockchain supervisory nodes for monitoring and verification. The gradual increase in the participation ratio of these supervisory nodes means that more nodes are involved in the monitoring and verification process during AIGC generation, thereby enhancing the security and trustworthiness of the data.

Moreover, the increased participation ratio of supervisory nodes also contributes to improving the efficiency of data verification and supervision. More supervisory nodes participating means more verification and supervision resources available, speeding up the process of data verification and supervision, thereby enhancing the efficiency and timeliness of the monitoring process. In conclusion, with the increase in the number of experiments, the participation ratio of supervisory nodes for AIGC-generated content is gradually increasing. Increasing the participation ratio of supervisory nodes plays a crucial role in enhancing data security, tamper resistance, and monitoring efficiency. Future research could further explore optimizing the selection mechanism of supervisory nodes, strengthening collaboration among supervisory nodes, and increasing the automation level of the monitoring process to further enhance the security and trustworthiness of AIGC-generated content.

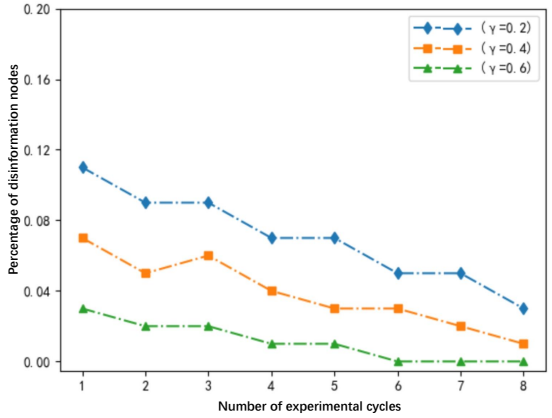

Fig. 14. Line graph of the change in the proportion of disinformation nodes with different experimental rounds

Fig.14 presents the line graph of the change in the proportion of disinformation nodes with different experimental rounds. In Fig.14, as the number of experiments increases, the proportion of highly untrustworthy nodes in the content generated by AIGC is gradually decreasing. The main reason for this trend is that with more experiment repetitions, more regulatory blockchain nodes are participating in the regulation of AIGC. The involvement of these nodes effectively expands the coverage of regulation, enhancing its comprehensiveness and credibility, while reducing the proportion of highly untrustworthy content nodes. The increased participation of regulatory nodes also contributes to improving the security and stability of the blockchain network. The decrease in highly untrustworthy nodes signifies a lower likelihood of malicious activities and attacks within the network, thereby strengthening its resilience against potential attacks. In addition, we tested the running time of the blockchain-based AIGC security regulatory mechanism under different operations, including the comparison of the time consumption of the three phases of AIGC's information generation, regulatory operation, and regulatory status confirmation with other methods, and the

experimental results are demonstrated in Tab.IV. It can be seen that our proposed blockchain-based regulatory mechanism with AES+RSA encryption is able to complete all the regulatory processes in a shorter period of time.

C. Case study and analysis

In order to address the scenario of a large number of users engaging in different transaction volumes simultaneously in an actual blockchain regulatory framework, we conducted case study using a generative artificial intelligence platform in a real-world environment. We conducted performance tests on throughput and average user request waiting time. The number of blockchain network nodes was set to the default value of 10. We utilized Apache Bench for stress testing, setting the total request execution numbers at 50, 100, 200, 500, and 1000, with a concurrent request number of 50. The monitored system throughput results are shown in Table.V. Among them, the unit of Throughput is requests per second, and the unit of Average User Request Waiting Time is milliseconds.

From the test results in Table.V, it can be observed that as the total request execution number increases, the throughput of the blockchain-based regulatory system also increases relatively, while the average user request waiting time decreases accordingly. Additionally, the system can handle a large number of requests from users at the same time, demonstrating that it can operate normally and meet the requirements of real-world scenarios. This further indicates that the blockchain-based AIGC regulatory system exhibits high efficiency and stability, making it suitable for practical AIGC regulatory tasks.

The results of the case study further illustrate that the advantages of utilizing blockchain technology for regulating AIGC lie in its stability in distributed environments. Blockchain's decentralized nature ensures that regulatory oversight is not dependent on a single point of control, reducing the risk of censorship or manipulation. The use of distributed ledger technology enhances transparency, accountability, and resilience in monitoring AIGC activities across diverse networks.

D. Discussion

1) Performacne: From the experimental results, we can see that the blockchain-based AIGC regulatory framework demonstrates exceptional performance through its innovative design and architecture. Leveraging the decentralized nature of blockchain technology, the framework effectively distributes computational tasks across a network of nodes, ensuring high availability and fault tolerance. This decentralized approach minimizes the risk of a single point of failure, enhancing system reliability and robustness. Furthermore, the implementation of consensus mechanisms, such as proof of stake or proof of work, facilitates efficient transaction processing and validation, maintaining the integrity of the regulatory process. Moreover, the transparent and immutable nature of blockchain enables real-time auditing and tracking of regulatory activities. This feature allows for immediate identification and resolution of any regulatory issues or discrepancies, enhancing the overall effectiveness of regulatory oversight. By providing a tamper-proof record of transactions and activities, blockchain technology plays a crucial role in ensuring data integrity and fostering trust within the regulatory framework. The seamless integration of blockchain into AIGC regulation significantly enhances overall performance by facilitating swift, secure, and transparent transactions. This integration sets a new standard for regulatory efficiency in the digital age, offering numerous benefits such as real-time monitoring, increased security, reduced costs, and improved compliance management. Incorporating blockchain into AIGC regulations not only simplifies processes but also opens the door for more creative ways to governance and compliance in an ever-evolving technology environment.

2) Efficiency: The proposed blockchain-based AIGC regulatory framework excels in efficiency by revolutionizing traditional regulatory processes through automation and transparency. By adopting a decentralized architecture, the framework eliminates the need for intermediaries, reducing bureaucratic complexities and streamlining regulatory procedures. This streamlined approach not only accelerates compliance processes but also significantly decreases administrative overhead, making regulation more cost-effective and accessible to a wider range of stakeholders. Furthermore, the utilization of smart contracts within the framework automates regulatory enforcement, ensuring compliance with predefined rules and regulations. Smart contracts execute automatically when specified conditions are met, minimizing the potential for human error or bias in regulatory decision-making. Additionally, the immutability of blockchain records enhances auditability and transparency, simplifying regulatory reporting and compliance verification processes. In conclusion, the efficiency of the blockchain-based AIGC regulatory framework lies in its ability to automate processes, reduce bureaucracy, and enhance transparency. By leveraging blockchain technology, the framework optimizes regulatory performance, improves operational efficiency, and strengthens compliance mechanisms, positioning itself as a superior solution for AIGC regulation in the modern era.

V. Can blockchain-based approach to AIGC regulation balance data security and content generation efficiency? Analysing the contribution and policy implications of this study from the engineering management perspective

Blockchain-based regulatory frameworks can significantly enhance the safety of Generative AI on digital platforms. By leveraging blockchain technology, these frameworks offer enhanced data integrity, traceability, compliance enforcement, and transparency. This approach not only mitigates risks associated with data manipulation and fraud but also promotes accountability and fairness in AI-driven credit decisions, ultimately fostering a more secure and trustworthy environment for financial transactions and credit evaluations.

- Blockchain governance ensures traceability and security of AIGC data: Blockchain governance plays a crucial role in ensuring the traceability and security of AIGC data without impeding the efficiency of data generation and

TABLE IV
COMPARISON OF TIME CONSUMPTION OF DIFFERENT COMPARISON METHODS IN THE THREE PHASES OF AIGC REGULATION

Methods of comparison	Generation	Operation	Verification
Our AIGC blockchain based regulation method (AES+RSA encryption)	0.07	1.35	2.04
Blockchain with CH.hash encryption	0.21	2.33	4.76
Blockchain with SIGN.sign encryption	0.16	2.81	5.16
Blockchain with Diffie-Hellman encryption	3.22	4.39	4.96

TABLE V
SYSTEM PERFORMANCE TEST RESULTS

Request Count	Throughput	Average User Request Waiting Time
50	24.51	2040.259
100	47.98	1042.055
200	93.19	536.551
500	214.46	233.148
1000	378.94	131.949

transmission. Specifically within AIGC financial credit markets, the implementation of blockchain governance measures enhances the overall security and stability of the ecosystem. By utilizing blockchain technology, AIGC data can be securely stored in decentralized ledgers, providing robust protection against unauthorized access and tampering attempts. This approach not only safeguards the confidentiality of sensitive information but also facilitates transparent tracking of data transactions, thereby fostering trust among stakeholders. The transparency and immutability inherent in blockchain technology contribute to an environment where data security is prioritized while allowing for seamless content generation processes within the AIGC framework.

- Blockchain governance can securely tag owners of AIGC data: Blockchain governance empowers the secure tagging of AIGC data owners, establishing a robust framework to uphold data ownership rights. Through the utilization of cryptographic techniques and smart contracts integrated into blockchain technology, ownership of AIGC data can be unequivocally assigned to the appropriate entities, ensuring accountability and transparency within the data ecosystem. This not only fosters trust among stakeholders but also safeguards against unauthorized data manipulation or disputes over ownership. The implementation of secure data labeling through blockchain governance not only enhances data security but also promotes the efficient generation of content in AIGC applications. By preserving data integrity and ownership rights throughout the data lifecycle, blockchain governance plays a pivotal role in maintaining a harmonious balance between data security and operational efficiency within the AIGC landscape.
- The encryption provided by blockchain governance ensures the privacy and security of data: The encryption mechanisms implemented through blockchain governance play a pivotal role in safeguarding the privacy and security of AIGC data. By leveraging strong encryption algorithms and decentralized storage solutions, blockchain governance effectively shields data from unauthorized access, tampering, and disclosure. This robust encryption framework acts as a barrier against identity theft and various security vulnerabilities, thereby ensuring the integrity and confidentiality of sensitive information stored within the AIGC ecosystem. The integration of encryption techniques within blockchain governance not only fortifies data security but also enables a delicate balance between protecting data privacy and promoting efficient content generation in AIGC applications. By prioritizing data protection measures, blockchain governance fosters a secure environment where data integrity is upheld without compromising the productivity and effectiveness of content creation processes in the AIGC domain.
- Data integrity and ethical-legal safeguards in AIGC: Blockchain technology plays a pivotal role in ensuring the integrity and traceability of data utilized in Generative AI systems within the financial credit domain. In the regulatory framework of a generative artificial intelligence platform based on blockchain technology, ethical, legal, and societal impacts are paramount considerations, with a particular emphasis on safeguarding user data security and privacy. Smart contracts play a pivotal role in ensuring transparency and security by enabling automated compliance with predefined rules and conditions. Through the use of blockchain's decentralized and immutable nature, sensitive user data is encrypted, stored securely, and accessed only through authorized protocols, thereby upholding ethical standards, complying with legal requirements, and aligning with societal expectations concerning data protection and privacy within the platform's ecosystem. One prominent example of blockchain's application in ensuring data integrity and traceability in the financial credit domain is demonstrated by TrustChain, a collaborative initiative involving IBM, jewelry companies, and financial institutions. TrustChain utilizes blockchain technology to trace the journey of diamonds from mines to consumers, ensuring transparency and authenticity in the diamond supply chain. Similarly, in the context of financial credit, blockchain can be employed to track the lineage of credit-related data, including borrower information, transaction records, and credit scores. This ensures that AI-generated credit assessments are based on verifiable and trustworthy data sources, minimizing the risk of fraud or manipulation.
- Compliance and transparency: Blockchain-based regulatory frameworks offer a robust mechanism for enforcing compliance with data privacy regulations and industry standards in the financial credit sector. Through the

use of smart contracts, these frameworks automate the verification and enforcement of rules governing the utilization and sharing of sensitive credit information. This automation not only streamlines compliance processes but also enhances transparency by providing stakeholders with real-time visibility into data usage and access permissions. As a result, stakeholders can have greater confidence in the integrity of credit-related operations, fostering trust and cooperation among industry participants. A pertinent example of blockchain enhancing compliance and transparency in the financial sector is demonstrated by the Australian Securities Exchange (ASX). ASX has embarked on a project to replace its existing clearing and settlement system with a blockchain-based platform known as CHESS (Clearing House Electronic Subregister System). By leveraging blockchain technology, ASX aims to improve the efficiency and transparency of post-trade processes, ensuring compliance with regulatory requirements and reducing operational risks. Similarly, in the realm of financial credit, blockchain-based solutions can automate compliance checks and provide stakeholders with real-time insights into data usage, enhancing transparency and regulatory adherence.

- Application scenarios of blockchain-based AIGC regulatory framework: The Blockchain-based AIGC (Artificial Intelligence Generated Content) regulatory system can also be implemented across various domains, including online advertising, website content creation, and other engineering management fields. In online advertising, the system can be utilized to authenticate the origin and compliance of AI-generated ads, ensuring transparency and adherence to advertising standards. For website content creation, the framework can validate the accuracy of AI-generated content, enhancing the credibility and reliability of information published online. In engineering management fields, the system could be used to verify the compliance of AI-generated technical documentation and project reports, streamlining regulatory processes and improving quality control measures. By extending the application of this framework to these key domains, the integration of blockchain technology in monitoring and regulating AI-generated content brings about significant advancements in transparency, accuracy, and regulatory compliance within digital ecosystems.

In conclusion, blockchain governance emerges as a promising approach to regulate the efficient and secure utilization of AIGC on digital platforms. By leveraging blockchain technology, regulatory frameworks can address key safety concerns associated with AI-generated content, particularly in ensuring data integrity, traceability, compliance, transparency, risk mitigation, and accountability. The implementation of blockchain-based solutions offers a pathway towards establishing trust and transparency within the digital ecosystem by creating immutable records of data sources and AI-generated content. Through smart contracts and real-time monitoring capabilities, blockchain enhances the credibility and fairness of AI-driven processes, laying the groundwork for a more secure environment for digital transactions and content creation.

VI. Challenges and future directions for AIGC regulation

A. AIGC privacy on digital platforms

Privacy preservation in AIGC is pivotal in safeguarding sensitive information from inadvertent exposure. Existing methods predominantly focus on removing potentially sensitive content from generative data through techniques such as machine unlearning or concept forgetting. However, despite these efforts, the provability of privacy protection remains a significant challenge. The inherent parameters of generative models might still retain sensitive information, leaving them vulnerable to exploitation through hidden backdoors. While approaches like differential privacy offer provable guarantees, they often necessitate extensive model retraining, introducing practical challenges and overhead.

Addressing this challenge requires a multifaceted approach that combines rigorous algorithmic scrutiny with innovative privacy-enhancing techniques. Research efforts should delve into developing sophisticated privacy verification mechanisms that can rigorously assess the efficacy of privacy protection schemes across various AIGC applications. Additionally, novel cryptographic tools and protocols can be explored to fortify privacy guarantees without imposing substantial overhead on model performance or requiring extensive retraining. Collaborative endeavors between academia, industry, and regulatory bodies can foster the development of standardized privacy benchmarks and evaluation frameworks, facilitating the adoption of best practices in AIGC privacy protection.

Furthermore, proactive measures should be taken to raise awareness about the potential privacy risks associated with AIGC applications and promote responsible data handling practices among stakeholders. Initiatives aimed at enhancing transparency and accountability in data processing pipelines can help mitigate privacy concerns and build trust among users. Ultimately, the pursuit of robust privacy protection mechanisms in AIGC necessitates a concerted effort to innovate, collaborate, and prioritize user privacy in the evolving landscape of artificial intelligence.

B. Robustness of blockchain based AIGC regulatory framework

As the intersection of blockchain technology and AIGC gains prominence on digital platforms, ensuring the robustness of regulatory frameworks becomes paramount for fostering trust, transparency, and accountability. Future research endeavors in this domain are poised to address several key trends and challenges to enhance the efficacy and resilience of blockchain-based AIGC regulatory mechanisms. One significant trend involves exploring innovative approaches for integrating blockchain technology into AIGC regulatory frameworks. Blockchain's inherent characteristics, such as immutability, transparency, and decentralized consensus, offer promising avenues for enhancing regulatory compliance, data integrity, and auditability in AIGC ecosystems. Future research will focus on leveraging smart contracts, cryptographic

techniques, and decentralized governance models to design resilient regulatory frameworks capable of mitigating risks and ensuring compliance across digital platforms.

Furthermore, future research will emphasize the development of interoperable and scalable regulatory solutions that can accommodate the diverse needs and complexities of AIGC applications on digital platforms. Interdisciplinary collaborations between blockchain experts, AI researchers, legal scholars, and policymakers will be essential in formulating comprehensive regulatory frameworks that strike a balance between innovation and regulatory compliance. Additionally, addressing emerging challenges related to data privacy, security, and ethical considerations will be a focal point of future research in blockchain-based AIGC regulatory frameworks. Researchers will explore novel cryptographic primitives, privacy-preserving techniques, and ethical guidelines to safeguard user rights, mitigate algorithmic biases, and promote responsible AI development and deployment on digital platforms.

Therefore, future research trends in blockchain-based AIGC regulatory framework on digital platforms will revolve around integrating blockchain technology, ensuring interoperability and scalability, addressing privacy and ethical concerns, and fostering interdisciplinary collaborations. By addressing these key trends, researchers can contribute to the development of robust regulatory frameworks that support the responsible and sustainable growth of AIGC technologies in the digital age.

VII. Conclusion

Against the backdrop of the prevalent prevalence of Artificial Intelligence Generated Content (AIGC), the imperative of advocating regulatory frameworks for AIGC governance via blockchain technology is paramount. Despite the pronounced attention garnered by AIGC, particularly within domains such as credit finance, persistent challenges revolve around insufficiencies in data confidentiality and safeguarding protocols, complexities in ascertaining the provenance of generated content, and the susceptibility of AIGC to fraudulent manipulation. Hence, pivotal to ensuring the security, integrity, and transparency of AIGC is the adoption of blockchain-driven governance mechanisms, imparting substantial underpinning for the enduring progression of AIGC technologies across diverse sectors. The primary contribution of this discourse lies in presenting a blockchain-oriented AIGC regulatory framework that proffers efficacious strategies for data security enhancement, fortification of data owner identities, and the auditability of AIGC.

This research makes significant contributions to the security and regulatory aspects of AIGC within digital platforms. By introducing a blockchain-based monitoring method, it effectively enhances data security, safeguards data owner identities, and ensures the traceability and oversight of AIGC information. In addition, this research provides valuable insights and contributions to the field of engineering management. By incorporating a blockchain-based approach for AIGC supervision, it sets a precedent for enhancing data security, protecting data owner identities, and ensuring regulatory compliance in various engineering management applications. In future research, we aim to enhance the performance of the framework, such as diversity and personalization [37], [38] of blockchain-based supervision to ensure that AIGC regulation within digital platforms evolves towards a more efficient direction.

References

[1] M. Anwar, M. A. Scheffler, and T. Clauss, "Digital capabilities, their role in business model innovativeness, and the internationalization of smes," *IEEE Transactions on Engineering Management*, 2022.

[2] J. Frishammar, A. Essén, C. Simms, R. Edblad, and V. Hardebro, "Older individuals and digital healthcare platforms: Usage motivations and the impact of age on postadoption usage patterns," *IEEE Transactions on Engineering Management*, 2022.

[3] N. Lakemond, G. Holmberg, and A. Pettersson, "Digital transformation in complex systems," *IEEE Transactions on Engineering Management*, vol. 71, pp. 192–204, 2021.

[4] A. Caporuscio, P. Moran, and M. Simoni, "Complexity induced risks posed by upcoming digital ultra-platforms: An agent-based simulation model," *IEEE Transactions on Engineering Management*, 2021.

[5] A. La Sala, F. Iandolo, M. Mohiya, N. Farronato, and F. Caputo, "Unfolding resilience in digital platforms from a microfoundations perspective," *IEEE Transactions on Engineering Management*, 2023.

[6] S. N. G. Gourisetti, M. Mylrea, and H. Patangia, "Evaluation and demonstration of blockchain applicability framework," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1142–1156, 2019.

[7] X. Zhao, L. Xue, P. Song, and E. Karahanna, "Direct communication and two-sided matching quality on a digital platform: A perspective of choice based on consideration set," *Information Systems Research*, 2023.

[8] A. R. Doshi and W. Schmidt, "Soft governance across digital platforms using transparency," *Strategy Science*, 2024.

[9] D. Fürstenau, A. Baiyere, K. Schewina, M. Schulte-Althoff, and H. Rothe, "Extended generativity theory on digital platforms," *Information Systems Research*, vol. 34, no. 4, pp. 1686–1710, 2023.

[10] P. zur Heiden, J. Priefer, and D. Beverungen, "Predictive maintenance on the energy distribution grid—design and evaluation of a digital industrial platform in the context of a smart service system," *IEEE Transactions on Engineering Management*, 2024.

[11] D. Cetindamar and R. Phaal, "Technology management in the age of digital technologies," *IEEE Transactions on Engineering Management*, 2021.

[12] J. Mo, X. Kang, Z. Hu, H. ZHou, T. Li, and X. GU, "Towards trustworthy digital media in the aigc era: An introduction to the upcoming isojpegtrust standard," *IEEE Communications Standards Magazine*, vol. 7, no. 4, pp. 2–5, 2023.

[13] F. Yang, "Aigc enables digital transformation of fashion exhibitions," *Electronics Science Technology and Application*, vol. 10, no. 6, 2023.

[14] J. Chen, C. Yi, H. Du, D. Niyato, J. Kang, J. Cai, and X. Shen, "A revolution of personalized healthcare: Enabling human digital twin with mobile aigc," *IEEE Network*, 2024.

[15] Z. Li, W. Zhang, H. Zhang, R. Gao, and X. Fang, "Global digital compact: A mechanism for the governance of online discriminatory and misleading content generation," *International Journal of Human–Computer Interaction*, pp. 1–16, 2024.

[16] Y. Zhao, L. Li, H. Jia, and S. Wu, "Opportunities and challenges of artificial intelligence generated content on the development of new digital economy in metaverse," in *2023 2nd International Conference on Artificial Intelligence, Internet and Digital Economy (ICAID 2023)*. Atlantis Press, 2023, pp. 473–480.

[17] R. Osorno and N. Medrano, "Open innovation platforms: A conceptual design framework," *IEEE Transactions on Engineering Management*, vol. 69, no. 2, pp. 438–450, 2020.

[18] H. Du, R. Zhang, D. Niyato, J. Kang, Z. Xiong, D. I. Kim, X. S. Shen, and H. V. Poor, "Exploring collaborative distributed diffusion-based ai-generated content (aigc) in wireless networks," *IEEE Network*, 2023.

[19] W. Chen, L. Yan-yi, G. Tie-zheng, L. Da-peng, H. Tao, L. Zhi, Y. Qing-wen, W. Hui-han, and W. Ying-you, "Systems engineering issues for industry applications of large language model," *Applied Soft Computing*, vol. 151, p. 111165, 2024.

[20] D. Guo, H. Chen, R. Wu, and Y. Wang, "Aigc challenges and opportunities related to public safety: a case study of chatgpt," *Journal of Safety Science and Resilience*, vol. 4, no. 4, pp. 329–339, 2023.

[21] Q. Du, Y. Duan, Z. Xie, X. Tao, L. Shi, and Z. Jin, "Optical flow-based spatiotemporal sketch for video representation: A novel framework," *IEEE Transactions on Circuits and Systems for Video Technology*, 2024.

[22] K.-B. Ooi, G. W.-H. Tan, M. Al-Emran, M. A. Al-Sharafi, A. Capatina, A. Chakraborty, Y. K. Dwivedi, T.-L. Huang, A. K. Kar, V.-H. Lee *et al.*, "The potential of generative artificial intelligence across disciplines: Perspectives and future directions," *Journal of Computer Information Systems*, pp. 1–32, 2023.
[23] S. Noy and W. Zhang, "Experimental evidence on the productivity effects of generative artificial intelligence," *Science*, vol. 381, no. 6654, pp. 187–192, 2023.
[24] T. Wang, Y. Zhang, S. Qi, R. Zhao, Z. Xia, and J. Weng, "Security and privacy on generative data in aigc: A survey," *arXiv preprint arXiv:2309.09435*, 2023.
[25] P. V. Klaine, H. Xu, L. Zhang, M. Imran, and Z. Zhu, "A privacy-preserving blockchain platform for a data marketplace," *Distributed Ledger Technologies: Research and Practice*, vol. 2, no. 1, pp. 1–16, 2023.
[26] M. Xu, D. Niyato, H. Zhang, J. Kang, Z. Xiong, S. Mao, and Z. Han, "Sparks of generative pretrained transformers in edge intelligence for the metaverse: Caching and inference for mobile artificial intelligence-generated content services," *IEEE Vehicular Technology Magazine*, 2023.
[27] A. Monti, A. P. Giuliani, A. C. Scapolan, and F. Montanari, "From physical to digital: Investigating the offline drivers of the online use and quality of knowledge exchange of an intraorganizational digital collaborative technology," *IEEE Transactions on Engineering Management*, 2023.
[28] M. Kuperberg, "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1008–1027, 2019.
[29] C. Baliker, M. Baza, A. Alourani, A. Alshehri, H. Alshahrani, and K.-K. R. Choo, "On the applications of blockchain in fintech: advancements and opportunities," *IEEE Transactions on Engineering Management*, 2023.
[30] Y. Cui, V. Gaur, and J. Liu, "Supply chain transparency and blockchain design," *Management Science*, 2023.
[31] Y. Cui, M. Hu, and J. Liu, "Value and design of traceability-driven blockchains," *Manufacturing & Service Operations Management*, vol. 25, no. 3, pp. 1099–1116, 2023.
[32] Z. Li, F. Liang, and H. Hu, "Blockchain-based and value-driven enterprise data governance: A collaborative framework," *Sustainability*, vol. 15, no. 11, p. 8578, 2023.
[33] I. Ullah and P. J. Havinga, "Governance of a blockchain-enabled iot ecosystem: A variable geometry approach," *Sensors*, vol. 23, no. 22, p. 9031, 2023.
[34] K. Chatterjee, A. Singh *et al.*, "A blockchain-enabled security framework for smart agriculture," *Computers and Electrical Engineering*, vol. 106, p. 108594, 2023.
[35] A. M. Abdullah *et al.*, "Advanced encryption standard (aes) algorithm to encrypt and decrypt data," *Cryptography and Network Security*, vol. 16, no. 1, p. 11, 2017.
[36] X. Zang, L. Liu, M. Wang, Y. Song, H. Zhang, and J. Chen, "Photochat: A human-human dialogue dataset with photo sharing behavior for joint image-text modeling," *arXiv preprint arXiv:2108.01453*, 2021.
[37] L. Schelenz, A. Segal, O. Adelio, and K. Gal, "Transparency-check: An instrument for the study and design of transparency in ai-based personalization systems," *ACM Journal on Responsible Computing*, vol. 1, no. 1, pp. 1–18, 2024.
[38] R. Alkurd, I. Abualhaol, and H. Yanikomeroglu, "Big-data-driven and ai-based framework to enable personalization in wireless networks," *IEEE Communications Magazine*, vol. 58, no. 3, pp. 18–24, 2020.

Fan Yang received the Ph.D. degree in computer science and technology from Xi'an Jiaotong University, Xi'an, China, in 2023. He is currently an Assistant Professor with the school of computer science and technology, Xi'an Jiaotong University.

Dr. Yang is intensively immersed in research activities centered around blockchain, AIGC security, and associated domains, actively engaging in the dissemination of projects at both national and international levels. Dr. Yang's research has been published in leading computer science and operational research journals such as *IEEE Transactions on Industrial Informatics, IEEE Transactions on Engineering Management, IEEE Transactions on Network Science and Engineering, European Journal of Operational Research, Annals of Operations Research, Expert Systems with Applications, Knowledge-Based Systems, Information Sciences, Applied Soft Computing, Computer Communications.*

Mohammad Zoynul Abedin received the Ph.D. degree in investment theory from Dalian University of Technology, Dalian, China, in 2018. He is a Senior Lecturer in Finance (FinTech) with the School of Management, Swansea University, United Kingdom. His current research interests include fintech, data mining, and big data analytics.

Dr. Abedin is actively engaged in research activities and project dissemination across various disciplines nationally and internationally. His research works appeared on the leading journals, including *IEEE Transactions on Industrial Informatics, IEEE Transactions on Engineering Management, European Journal of Operational Research, Annals of Operations Research, International Journal of Production Research, International Journal of Finance and Economics, Research in International Business and Finance, Complex & Intelligent Systems.*

Yanan Qiao received the Ph.D. degree in computer science and technology from Xi'an Jiaotong University, Xi'an, China, in 2010. He is currently a Professor with the school of computer science and technology, Xi'an Jiaotong University. Dr. Qiao leads a research team affiliated with the Intelligent Blockchain Technology Research Laboratory at Xi'an Jiaotong University, focusing on cutting-edge interdisciplinary research spanning AIGC security, blockchain technology, smart finance, cross-chain interoperability, and beyond.

Dr. Qiao's research has been published in leading computer science and information system journals such as *IEEE Transactions on Industrial Informatics, IEEE Transactions on Engineering Management, IEEE Transactions on Network Science and Engineering, Future Generation Computer Systems, Expert Systems with Applications, Annals of Operations Research, Knowledge-Based Systems, Information Sciences, Applied Soft Computing, Computer Networks, Computer Communications.*

Lvyang Ye obtained his D.Eng. degree in electronics and information from Xi'an Jiaotong University, China, in 2023. Currently, he serves as an engineer at the Xi'an Institute of Electromechanical Information Technology, where he actively contributes to technological advancements and innovations. His research pursuits encompass a broad spectrum of interests, ranging from information processing and communication to telemetry, tracking, and command (TT&C). With a robust academic background and practical experience, he is well-positioned to make significant contributions to the development and implementation of cutting-edge technologies in his areas of expertise.