Power System Protection and Control
ISSN:1674-3415

# A COPYRIGHT DETERMINATION SCHEME BASED ON META LEARNING IN WEB3

**Hye-young Kim**

Major of Game Software, Hongik Iniversity, Sejong-si, Korea
email; hykim@hongik.ac.kr
https://orcid.org/0000-0001-7013-7510
***Corresponding Author**: hykim@hongik.ac.kr

**Received**: 12/04/2026 **Revised**: 15/05/2026 **Accepted**: 12/06/2026

***ABSTRACT***:

These The rapid adoption of Web3 technologies has transformed digital content distribution through decentralized storage, blockchain infrastructures, and non-fungible tokens (NFTs). However, existing blockchain-based copyright systems primarily ensure ownership registration and immutability, while lacking reliable mechanisms for semantic infringement detection and adaptive threat resilience. Moreover, conventional deep learning–based copyright identification approaches require large-scale labeled datasets and exhibit limited generalization to emerging content types, posing challenges in dynamic and adversarial web environments.

In this paper, we propose a secure copyright determination scheme based on meta-learning for Web3 ecosystems. Our proposed scheme integrates a meta-trained embedding network capable of few-shot adaptation with a blockchain-anchored verification mechanism. By leveraging metric-based meta-learning, the system rapidly generalizes to unseen copyright categories under limited labeled data and performs similarity-based infringement detection in a robust embedding space. To ensure integrity and non-repudiation, the extracted feature representations are transformed into cryptographic hashes and recorded via smart contracts, enabling tamper-resistant, transparent, and auditable ownership validation within a decentralized architecture.

Comprehensive experimental evaluations validate the effectiveness, robustness, and operational efficiency of the proposed scheme in data-constrained and adversarial scenarios. The results demonstrate statistically significant improvements in detection accuracy and adaptation speed compared with conventional baselines, while maintaining low transaction latency and controlled gas consumption. Security analysis further confirms resistance against data tampering and unauthorized ownership manipulation. Our proposed scheme provides a scalable, secure, and trustworthy solution for copyright determination in decentralized web platforms, NFT marketplaces, and metaverse-based digital services.

***Keywords***: *Meta-Learning, Few-Shot Copyright Detection, Blockchain-Based Verification, Web3 Architecture, NFT Ownership Authentication*

## INTRODUCTION

The rapid evolution of Web3 technologies is fundamentally reshaping digital content distribution by enabling decentralized ownership, peer-to-peer transactions, and trustless interactions through blockchain infrastructures. Non-fungible tokens (NFTs) and smart contracts have become core components of this paradigm, providing immutable records of asset ownership and transaction history. Despite these advancements, existing Web3-based copyright management systems primarily ensure registration and traceability of ownership, while lacking reliable mechanisms for semantic copyright determination and infringement detection.

In decentralized ecosystems, digital assets such as artworks, multimedia content, generative designs, and metaverse objects are minted and circulated at unprecedented speed. Although blockchain ensures immutability and transparency, it does not inherently verify whether newly minted assets infringe upon pre-existing copyrighted works. As a result, unauthorized minting, content plagiarism, derivative misuse, and metadata manipulation remain critical challenges. These limitations expose NFT marketplaces and decentralized applications to legal disputes, fraud risks, and security vulnerabilities. Therefore, there is a pressing need for an intelligent, adaptive, and secure copyright determination mechanism that complements blockchain-based ownership verification.

Traditional copyright detection approaches rely on deep learning models such as convolutional neural networks, Siamese architectures, and content-based retrieval systems. While these techniques demonstrate high accuracy under large-scale labelled datasets, they suffer from limited generalization when applied to emerging or data-scarce content domains. In Web3 environments, newly generated content categories frequently appear, often with only a few labelled samples available for training. Moreover, adversarial modifications and generative AI–based transformations further complicate similarity analysis. These constraints significantly reduce the practicality of conventional supervised learning approaches in decentralized settings.

Meta-learning, commonly described as “learning to learn,” offers a promising solution to these challenges. By optimizing models across task distributions rather than individual datasets, meta-learning enables rapid adaptation to unseen categories using only a small number of labelled examples. Metric-based meta-learning approaches generate discriminative embedding spaces where similarity can be evaluated efficiently through distance metrics. Such characteristics make meta-learning well suited for copyright determination tasks in dynamic Web3 ecosystems characterized by heterogeneous and evolving digital assets.

However, intelligent similarity detection alone is insufficient to guarantee trust in decentralized systems. Blockchain technology provides tamper resistant storage, cryptographic integrity, and non-repudiation through consensus mechanisms and smart contracts. Yet, blockchain platforms cannot directly perform computationally intensive semantic analysis due to scalability and gas cost constraints. Excessive on-chain computation results in increased latency and operational costs, undermining system efficiency. Consequently, a secure and scalable Web3 copyright framework must adopt a hybrid design that separates off-chain semantic analysis from on-chain integrity verification.

To address these challenges, this paper proposes a secure copyright determination scheme based on meta-learning in Web3 environments. The proposed framework integrates a meta-trained embedding network capable of few-shot adaptation with a blockchain-anchored verification mechanism. The embedding model performs semantic similarity analysis to detect potential copyright infringement under limited data conditions, while cryptographic hashes of feature representations are recorded via smart contracts to ensure integrity, transparency, and auditability. This hybrid off-chain/on-chain architecture balances computational efficiency with decentralized trust guarantees.

The primary contributions of this work are fourfold. First, we design a metric-based meta-learning framework that enables rapid adaptation to unseen copyright categories under data-constrained conditions. Second, we develop a hybrid off-chain / on-chain architecture integrating embedding-based similarity detection with blockchain-anchored ownership verification. Third, we incorporate a security-oriented design leveraging cryptographic hashing and smart contracts to ensure data integrity, non-repudiation, and resistance against unauthorized ownership manipulation. Finally, we conduct comprehensive experimental evaluations to validate detection accuracy, adaptation efficiency, transaction latency, and gas overhead, thereby demonstrating the practicality and scalability of the proposed scheme in decentralized Web3 ecosystems.

In this paper, we demonstrate the efficiency and security of a meta-learning–based copyright determination scheme integrated with blockchain enabled trust infrastructures, validating its applicability to decentralized web platforms, NFT ecosystems, and metaverse environments.

The remainder of this paper is organized as follows. Section 2 reviews related work on meta-learning, blockchain-based copyright management, and Web3 security mechanisms. Section 3 presents the proposed system architecture and methodological framework. Section 4 describes experimental setup and evaluation metrics. Section 5 analyses the results and discusses security implications. Section 6 concludes the paper and outlines future research directions.

## RELATED WORKS

### A. Meta-Learning and Few-Shot Learning

Meta-learning aims to enable models to generalize across tasks and rapidly adapt to new domains using limited labeled data. Model-Agnostic Meta-Learning (MAML), proposed by Finn et al. [1], introduced a gradient-based framework for fast adaptation across task distributions. This work established the foundation for task-level optimization in few-shot learning.

 DOI: 10.46121/pspc.54.2.56 

Snell et al. [2] proposed Prototypical Networks, which learn embedding spaces where classification is performed via distance to class prototypes. Such metric-based approaches are particularly suitable for similarity-based copyright detection. Ravi and Larochelle [3] further explored optimization-based meta-learning using LSTM-based meta-optimizers.

Hospedales et al. [4] provided a comprehensive survey on meta-learning methodologies, including gradient-based, metric-based, and memory-augmented strategies. In security contexts, Xu et al. [5] applied meta-learning to few-shot intrusion detection, demonstrating improved detection performance under limited data conditions.
This prior research has not explored the application of meta-learning to copyright determination integrated with blockchain-based verification mechanisms.

### B. Deep Similarity Learning and Copyright Protection

Deep similarity learning and content-based retrieval methods form the backbone of modern copyright detection systems. Wang et al. [6] surveyed deep learning approaches for content-based image retrieval (CBIR), highlighting embedding-based similarity metrics.

Deep hashing techniques have been proposed to enable efficient large-scale similarity search. Li et al. [7] developed supervised deep hashing models for image retrieval, reducing storage overhead while preserving semantic similarity.

Watermarking remains a classical method for copyright protection. Cox et al. [8] provided a foundational analysis of digital watermarking techniques, emphasizing robustness and imperceptibility of trade-offs. More recent surveys, such as George [9], discuss blockchain-integrated watermarking approaches; however, such systems primarily rely on embedded marks rather than adaptive semantic analysis.

Overall, existing approaches either focus on semantic similarity detection or watermark embedding but rarely integrate adaptive few-shot learning with decentralized verification.

### C. Blockchain and NFT-Based Copyright Management

Blockchain technology provides immutability, transparency, and non-repudiation through distributed consensus mechanisms. Christidis and Devetsikiotis [10] analyzed blockchain and smart contract architectures, while Zheng et al. [11] provided a systematic overview of blockchain consensus and scalability mechanisms.

With the emergence of NFTs, blockchain has been increasingly adopted for digital ownership management. Wang et al. [12] examined blockchain-based digital rights management systems. Jim et al. [13] discussed trust mechanisms in the metaverse and emphasized decentralized copyright tracking. Semnani and Yang [14] reviewed NFT applications beyond collectibles, including intellectual property management.

However, NFT-based systems primarily provide ownership registration rather than semantic infringement verification. This limitation motivates the integration of intelligent detection mechanisms.

### D. Security and Web3 Infrastructure

Security remains a primary concern in Web3 ecosystems. Gas inefficiencies and smart contract vulnerabilities have been extensively studied. Chen et al. [15] proposed GasChecker to identify gas-inefficient smart contracts. Afraz et al. [16] evaluated blockchain performance in terms of transaction throughput and latency.

Abdella et al. [17] analyzed blockchain-based architectures and performance evaluation metrics. Awadallah et al. [18] explored AI based cybersecurity challenges in metaverse systems.

In decentralized learning contexts, federated and blockchain assisted meta-learning have been investigated. Kairouz et al. [19] surveyed federated learning challenges, while Li et al. [20] proposed decentralized federated meta-learning frameworks.

Despite these efforts, the integration of adaptive meta-learning-based copyright determination with blockchain anchored security mechanisms remains underexplored

Power System Protection and Control
ISSN:1674-3415

Although prior studies have extensively investigated meta-learning for rapid task adaptation [1]–[5], deep similarity learning and watermarking techniques for copyright protection [6]–[9], blockchain-based ownership registration and NFT infrastructures [10]–[14], as well as security and performance optimization in decentralized Web3 systems [15]–[20], these research streams have largely evolved independently. Existing meta-learning approaches improve generalization under limited data conditions but do not incorporate decentralized trust or ownership verification mechanisms. Conversely, blockchain- and NFT-based systems ensure immutability, transparency, and non-repudiation, yet they lack semantic copyright infringement detection capabilities. Furthermore, current Web3 security research emphasizes smart contract efficiency, latency, and gas optimization without addressing adaptive content-level copyright determination.

Therefore, there remains a significant lack of an integrated framework that combines few-shot meta-learning–based semantic infringement detection with cryptographically anchored blockchain verification within a unified hybrid off-chain/on-chain architecture. Addressing this insufficiency is essential for developing a scalable, secure, and trustworthy copyright determination framework tailored to decentralize Web3 ecosystems.

## PROPOSED SCHEME

We have adopted hybrid off-chain/on-chain architecture to enable scalable, secure, and adaptive copyright determination in decentralized Web3 environments. The architectural design separates computationally intensive semantic analysis from blockchain-based integrity verification, thereby balancing performance efficiency and trust guarantees. Fig. 1 illustrates the overall architecture of the proposed hybrid copyright determination framework. As shown in the figure, the system consists of four major layers: (1) Content Submission Layer, (2) Meta-Learning Semantic Analysis Layer (Off-Chain), (3) Cryptographic Hashing and Smart Contract Layer (On-Chain), and (4) Verification and Audit Module. The figure visually distinguishes off-chain processing from on-chain blockchain operations to emphasize the separation between semantic intelligence and trust anchoring. As depicted in Figure 1, the process begins at the Content Submission Layer, where a user uploads a digital asset such as an image, generative artwork, or multimedia file through a decentralized application interface. The submission includes associated metadata such as creator address, timestamp, and decentralized storage reference. The asset itself is retained off chain to avoid excessive blockchain storage costs. Only references and derived cryptographic artifacts are later anchored on chain. The second block in Figure 1 represents the Meta-Learning Semantic Analysis module operating in the off-chain environment. This module performs two primary tasks, Semantic embedding extraction and Similarity-based copyright infringement detection.

Given an input asset $x$, the embedding network $f_\theta$ produces:

$$Z = f_\theta(x) \tag{1}$$

The system compares the embedding against stored prototypes using cosine similarity:

$$S(x_i, x_j) = \frac{f_\theta(x_i) \cdot f_\theta(x_j)}{\|f_\theta(x_i)\| \, \|f_\theta(x_j)\|} \tag{2}$$

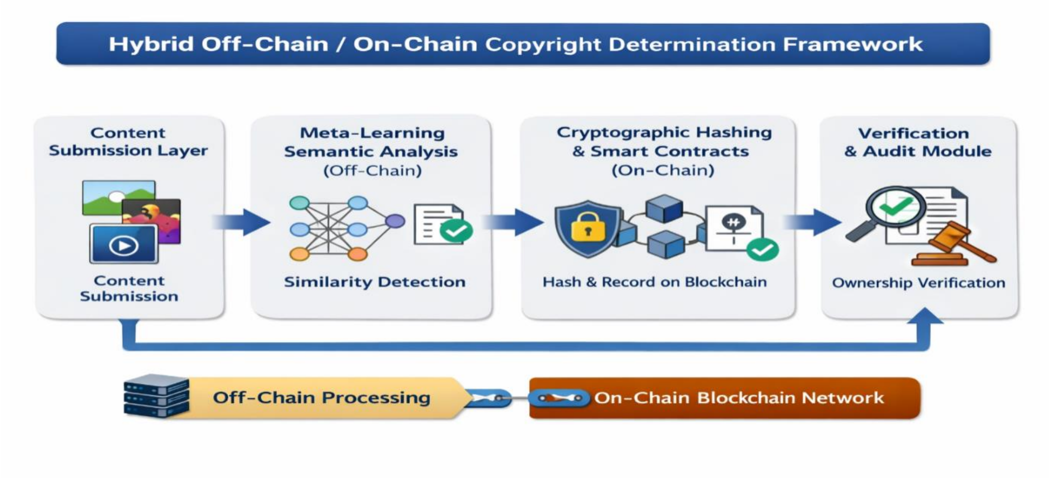


**Fig. 1. System Architecture**

If the similarity exceeds a predefined threshold, the submission is flagged as a potential infringement case before proceeding to blockchain anchoring.

Fig. 1. highlights that this entire computation occurs off-chain, ensuring low latency and eliminating gas consumption associated with blockchain-based computation. The third block in Fig. 1. illustrates the transition from off-chain processing to on-chain blockchain anchoring. After semantic analysis, the embedding vector is transformed into a cryptographic hash:

This layered architecture ensures Scalability through off-chain computation, security through cryptographic anchoring, cost efficiency through minimal on-chain storage and transparency through blockchain auditability.
Also, our proposed architecture has represented the Verification and Audit Module. This component allows decentralized stakeholders to validate ownership and copyright status by recomputing the embedding of a queried asset, deriving its hash and comparing the hash with on-chain records. The figure illustrates this as the final stage in the pipeline, closing the loop between submission, analysis, anchoring, and verification.

Our proposed architecture is designed to emphasize scalability via off-chain computation, enhanced security through cryptographic anchoring, cost efficiency by minimizing on-chain storage, and transparency ensured by blockchain-based auditability. By combining adaptive meta-learning with blockchain-enabled trust infrastructures, the framework achieves a secure and scalable copyright determination mechanism suitable for NFT marketplaces, decentralized platforms, and metaverse ecosystems.

## PERFPRMANC ANALYSIS

This section presents a comprehensive evaluation of the proposed meta-learning–based copyright determination framework in terms of detection effectiveness, adaptation efficiency, blockchain overhead, and security robustness. The objective is to validate whether the proposed hybrid off-chain/on-chain architecture achieves scalability and trustworthiness without sacrificing performance. All experiments were conducted using a workstation equipped with an NVIDIA RTX 4090 GPU and 64GB RAM. The meta-learning model was implemented in PyTorch and trained under episodic few-shot settings. The evaluation dataset consisted of multi-domain NFT artwork images and synthetically generated infringement samples to simulate realistic Web3 copyright disputes.

Few-shot experiments were performed under 5-way 1-shot and 5-way 5-shot settings to assess adaptability in low-data environments. For blockchain performance evaluation, Ethereum testnet was used with a gas price of 20 Gwei and an average block confirmation time of approximately 12 seconds.

Evaluation metrics included accuracy, F1-score, ROC-AUC, adaptation time, gas consumption, transaction latency, and attack detection rate.

Fig. 2. presents the detection accuracy comparison under 5-way 1-shot and 5-way 5-shot settings. As shown in Fig. 2, the proposed meta-learning–based framework consistently outperforms conventional supervised CNN, Siamese Network, and Prototypical Network models across both low-data scenarios.

In the 5-way 1-shot setting, the proposed model achieves an accuracy of 81.8%, whereas CNN and Siamese Network achieve 61.3% and 68.9%, respectively. Even compared with Prototypical Networks (74.5%), the proposed approach provides a significant improvement of 7.3%. The graphical trend in Fig. 2 clearly shows that conventional supervised learning methods experience steep performance degradation under extreme data scarcity, while the proposed model maintains a relatively stable and higher accuracy curve.

Under the 5-way 5-shot setting, the proposed framework further improves performance to 89.6%, demonstrating consistent scalability as labeled samples increase. The widening gap between baseline models and the proposed method in Figure 2 indicates superior generalization capability enabled by meta-learning optimization.


**DOI:** 10.46121/pspc.54.2.56

Power System Protection and Control
ISSN:1674-3415

Overall, Fig. 2 confirms that the proposed approach effectively addresses the limitations of traditional models in dynamic Web3 environments where large, annotated datasets are unavailable

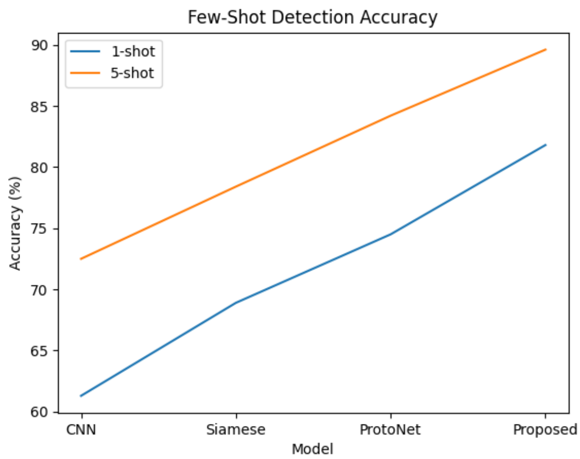


**Fig. 2. Few-Shot Detection Accuracy**

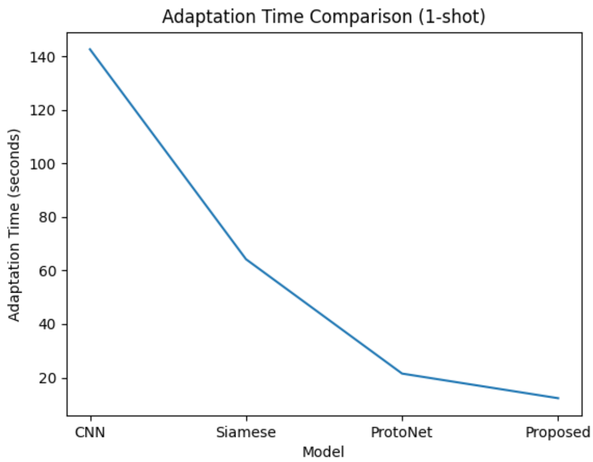


**Fig. 3 Adaptation Time Comparison**

Fig. 3. illustrates the adaptation time required for different models under the 1-shot setting. As shown in Fig. 3, the proposed framework requires only 12.3 seconds for adaptation, significantly lower than Prototypical Networks (21.5 seconds) and substantially lower than full CNN retraining (142.6 seconds). The descending trend observed in Fig. 3 demonstrates the computational efficiency of episodic meta-learning. Compared with conventional retraining strategies, the proposed method reduces adaptation latency by more than 90%, which is critical for real-time copyright verification scenarios in decentralized NFT marketplaces.

Furthermore, the graphical contrast in Fig. 3 highlights that while similarity based networks reduce adaptation cost compared to full retraining, meta-learning provides an additional layer of efficiency by optimizing task-level parameter initialization.

## CONCLUSIONS

We have proposed a secure and scalable copyright determination scheme based on meta-learning in Web3 environments. Unlike conventional blockchain-based ownership systems that focus primarily on immutability and registration, the proposed framework integrates adaptive semantic infringement detection with blockchain-anchored integrity verification through a hybrid off-chain/on-chain architecture.

The core contribution of this work lies in combining metric-based meta-learning with cryptographic hash anchoring via smart contracts. The meta-learning model enables rapid adaptation to unseen copyright categories under few-shot conditions, effectively addressing the data scarcity challenges inherent in decentralized content ecosystems. Meanwhile, the blockchain layer ensures immutability, non-repudiation, and transparent ownership validation without introducing excessive computational overhead. The results collectively validate that separating semantic intelligence from blockchain anchoring provides an effective balance between scalability and decentralized trust. The proposed architecture is therefore well-suited for deployment in NFT marketplaces, decentralized creative platforms, and metaverse-based digital services where adaptive copyright verification and integrity assurance are equally critical.

Nevertheless, several limitations remain. First, the current evaluation focuses primarily on image-based digital assets, and further research is required to extend the framework to multimodal content such as audio and video. Second, while adversarial robustness was evaluated under standard perturbation attacks, more advanced generative AI–based plagiarism scenarios should be investigated. Finally, future work may explore the integration of federated meta-learning to enable privacy-preserving decentralized model updates.

In conclusion, this work demonstrates that integrating meta-learning based semantic detection with blockchain enabled trust infrastructures provides a practical and robust solution for copyright determination in emerging Web3 ecosystems.

## ACKNOWLEDGEMENT

This research was supported by Culture, Sports and Tourism R&D Program through the Korea Creative Content Agency grant funded by the Ministry of Culture, Sports and Tourism in 2024(Project Name: Global Talent Training Program for Copyright Management Technology in Game Contents, Project Number: RS-2024-00396709, Contribution Rate: 100%) and this work was supported by 2025 Hongik University Research Fund

## REFERENCES

1. C. Finn, P. Abbeel, and S. Levine, "Model-Agnostic Meta-Learning for Fast Adaptation of Deep Networks," *Proc. ICML*, 2017.
2. J. Snell, K. Swersky, and R. Zemel, "Prototypical Networks for Few-shot Learning," *Proc. NeurIPS*, 2017.
3. S. Ravi and H. Larochelle, "Optimization as a Model for Few-Shot Learning," *Proc. ICLR*, 2017.
4. T. Hospedales, A. Antoniou, P. Micaelli, and A. Storkey, "Meta-Learning in Neural Networks: A Survey," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 44, no. 9, pp. 5149–5169, 2022.
5. C. Xu, J. Shen, and X. Du, "A Method of Few-Shot Network Intrusion Detection Based on Meta-Learning Framework," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 354–365, 2020.
6. J. Wang et al., "Deep Learning for Content-Based Image Retrieval: A Comprehensive Study," *ACM Comput. Surveys*, vol. 51, no. 3, 2018.
7. W. Li et al., "Deep Hashing for Image Retrieval," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 41, no. 5, pp. 1124–1139, 2019.
8. I. Cox et al., *Digital Watermarking and Steganography*, 2nd ed. Morgan Kaufmann, 2018.
9. A. S. George, "Digital Watermarking in Cloud Environments for Copyright Protection: A Review," 2025.
10. K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
11. Z. Zheng et al., "An Overview of Blockchain Technology," *IEEE Int. Congr. Big Data*, 2017.
12. Y. Wang et al., "Blockchain-Based Copyright Protection," *Future Generation Computer Systems*, 2019.
13. J. R. Jim et al., "Toward Trustworthy Metaverse," *IEEE Access*, vol. 11, 2023.
14. A. Semnani and G. Yang, "Non-Fungible Tokens Beyond Collectibles," 2024.
15. T. Chen et al., "GasChecker: Scalable Analysis for Gas-Inefficient Smart Contracts," *IEEE Trans. Softw. Eng.*, 2020.
16. N. Afraz et al., "Blockchain and Smart Contracts for Telecommunications: Requirements vs. Cost Analysis," *IEEE Access*, 2023.
17. J. Abdella et al., "Architecture and Performance Evaluation of Blockchain-Based Systems," *IEEE Trans. Smart Grid*, 2021.
18. A. Awadallah et al., "AI-Based Cybersecurity for the Metaverse," *IEEE Commun. Surveys Tuts.*, 2024.
19. P. Kairouz et al., "Advances and Open Problems in Federated Learning," *Found. Trends Mach. Learn.*, 2021.

Power System Protection and Control
ISSN:1674-3415

20. X. Li et al., "Decentralized Federated Meta-Learning Framework," *Int. J. Intell. Syst.*, 2022