PDF Download
3657284.pdf
17 February 2026
Total Citations: 24
Total Downloads: 2080

Published: 14 May 2024
Online AM: 11 April 2024
Accepted: 31 March 2024
Revised: 28 January 2024
Received: 26 March 2023

Citation in BibTeX format

SURVEY

Artificial Intelligence for Web 3.0: A Comprehensive Survey

MENG SHEN, Beijing Institute of Technology, Beijing, China

ZHEHUI TAN, Beijing Institute of Technology, Beijing, China

DUSIT (TAO) NIYATO, Nanyang Technological University, Singapore City, Singapore

YUZHI LIU, Beijing Institute of Technology, Beijing, China

JIAWEN KANG, Guangdong University of Technology, Guangzhou, Guangdong, China

ZEHUI XIONG, Singapore University of Technology and Design, Singapore City, Singapore

View all

Open Access Support provided by:

Beijing Institute of Technology

Singapore University of Technology and Design

Beijing Jiaotong University

Guangdong University of Technology

University of Waterloo

Nanyang Technological University

ACM Computing Surveys, Volume 56, Issue 10 (October 2024)
https://doi.org/10.1145/3657284
EISSN: 1557-7341

Artificial Intelligence for Web 3.0: A Comprehensive Survey

MENG SHEN, Beijing Institute of Technology, Beijing, China
ZHEHUI TAN, Beijing Institute of Technology, Beijing, China
DUSIT NIYATO, Nanyang Technological University, Singapore, Singapore
YUZHI LIU, Beijing Institute of Technology, Beijing, China
JIAWEN KANG, Guangdong University of Technology, Guangzhou, China
ZEHUI XIONG, Singapore University of Technology and Design, Singapore, Singapore
LIEHUANG ZHU, Beijing Institute of Technology, Beijing, China
WEI WANG, Beijing Jiaotong University, Beijing, China
XUEMIN (SHERMAN) SHEN, University of Waterloo, Waterloo, Canada

Web 3.0 is the next generation of the Internet built on decentralized technologies such as blockchain and cryptography. It is born to solve the problems faced by the previous generation of the Internet such as imbalanced distribution of interests, monopoly of platform resources, and leakage of personal privacy. In this survey, we discuss the latest development status of Web 3.0 and the application of emerging AI technologies in it. First, we investigate the current successful practices of Web 3.0 and various components in the current Web 3.0 ecosystem and thus propose the hierarchical architecture of the Web 3.0 ecosystem from the perspective of application scenarios. The architecture we proposed contains four layers: data management, value circulation, ecological governance, and application scenarios. We dive into the current state of development and the main challenges and issues present in each layer. In this context, we find that AI technology will have great potential. We first briefly introduce the role that artificial intelligence technology may play in the development of Web 3.0. Then, we conduct an in-depth analysis of the current application status of artificial intelligence technology in the four layers of Web 3.0 and provide some insights into its potential future development directions.

This work is partially supported by the National Key R&D Program of China with No. 2023YFB2703800; NSFC Projects with Nos. 62222201 and U23A20304; Beijing Nova Program with No. 20220484174; Beijing Natural Science Foundation with No. M23020; National Research Foundation, Singapore, and Infocomm Media Development Authority under its Future Communications Research & Development Programme; Defence Science Organisation (DSO) National Laboratories under the AI Singapore Programme (AISG Award No: AISG2-RP-2020-019 and FCP-ASTAR-TG-2022-003); and Singapore Ministry of Education (MOE) Tier 1 (RG87/22).

Authors' Contact Information: Meng Shen, School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing, China; e-mail: shenmeng@bit.edu.cn; Zhehui Tan, School of Computer Science, Beijing Institute of Technology, Beijing, China; e-mail: zhehuitan@bit.edu.cn; Dusit Niyato, College of Computing and Data Science, Nanyang Technological University, Singapore, Singapore, Singapore; e-mail: niyato@ntu.edu.sg; Yuzhi Liu, School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing, China; e-mail: liuyuzhi@bit.edu.cn; Jiawen Kang, School of Automation, Guangdong University of Technology, Guangzhou, Guangdong, China; e-mail: kavinkang@gdut.edu.cn; Zehui Xiong, Pillar of Information Systems Technology and Design, Singapore University of Technology and Design, Singapore, Singapore; e-mail: zehui_xiong@sutd.edu.sg; Liehuang Zhu, School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing, China; e-mail: liehuangz@bit.edu.cn; Wei Wang, School of Computer and Information Technology, Beijing Jiaotong University, Beijing, China; e-mail: wangwei1@bjtu.edu.cn; Xuemin (Sherman) Shen, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada: e-mail: sshen@uwaterloo.ca.

ACM 0360-0300/2024/05-ART247
https://doi.org/10.1145/3657284

CCS Concepts: • **General and reference → Surveys and overviews**; • **Security and privacy → Network security**; • **Computing methodologies → Machine learning;**

Additional Key Words and Phrases: Web 3.0, artificial intelligence, blockchain, computing network

ACM Reference Format:
Meng Shen, Zhehui Tan, Dusit Niyato, Yuzhi Liu, Jiawen Kang, Zehui Xiong, Liehuang Zhu, Wei Wang, and Xuemin (Sherman) Shen. 2024. Artificial Intelligence for Web 3.0: A Comprehensive Survey. *ACM Comput. Surv.* 56, 10, Article 247 (May 2024), 39 pages. https://doi.org/10.1145/3657284

1 INTRODUCTION

In recent years, the rapid development of the Internet has brought many problems, including the concentration of interests in a few people, the monopoly of platform resources, and the loss of personal privacy. In this context, the concept of Web 3.0 emerges, trying to reconstruct the future development of the Internet by introducing technologies such as blockchain and cryptography. Web 3.0 focuses on value expression, decentralization, and data ownership to solve the above major challenges encountered by the current Internet.

The concept of Web 3.0 was first proposed by Gavin Wood, co-founder of Ethereum, in 2014. He believes that Web 3.0 is the blockchain-based Internet and the goal of Web 3.0 is to reduce the reliance on centralized institutions. With the enrichment of Web 3.0 concepts, Web 3.0 can reconstruct the contemporary Internet from two aspects. From the perspective of data ownership, Web 3.0 not only is a readable and writable network but also enables users to own their data and assets [1]. From the perspective of data management, Web 3.0 is a new economic system that is jointly built and shared by users and builders [2].

Web 3.0 has seen significant growth and development, driven largely by the increasing interest in cryptocurrencies and blockchain technology. We can see a clear trail of Web 3.0 evolution, from the beginning with Bitcoin [3], a decentralized electronic cash system; to Ethereum [4], a decentralized application platform; to EOS [5], a decentralized public chain operating system; to Nostr [6], decentralization Internet; to the recently popular concept of the Metaverse. However, with the continuous expansion of the scope of applications and the increase in the number of users, the development of Web 3.0 has encountered some new challenges. It is currently facing major difficulties in terms of data management, value circulation, and ecological governance.

(1) In the Web 3.0 scenario, data is diverse and plentiful and stored across a distributed network, making it more challenging to manage compared to traditional centralized databases.
(2) In the value circulation system of Web 3.0, the user's identity system is complicated to use and is easily attacked by hackers. Also, the transaction efficiency and pricing accuracy of the circulation system need to be further improved.
(3) The Web 3.0 ecosystem is susceptible to various operational abnormalities, such as the spread of inappropriate content by users [7], leading to a deterioration of the ecosystem's overall quality. Considering the increased autonomy and anonymity of Web 3.0's users, it can be costly and resource-intensive to detect and address.

Driven by these problems, we find that the advancements in **Artificial Intelligence (AI)** technology in recent years have provided new and powerful solutions to various obstacles in the development of Web 3.0. The powerful capabilities of AI in optimization can refine the strategies of the system to maximize the overall system performance to address the problem faced by the infrastructure layer. The abilities of AI large-scale models in content generation can help solve the challenges faced in the interface layer in generating a wide range of unique digital assets. The superior performance of AI algorithms in detection and classification can help identify abnormal

Table 1. The Differences between Other Existing Works and Our Survey

Survey Paper	Year	Description
Wang et al. [13]	2022	Discussing the security and privacy threats to the metaverse and the state-of-the-art countermeasures
Yang et al. [14]	2022	Surveying how blockchain and artificial intelligence (AI) fuse with the metaverse
Huynh-The et al. [15]	2023	Exploring the role of AI in the foundation and development of the metaverse
Mukhopadhyay et al. [16]	2016	Evaluating the strengths, weaknesses, and possible threats to the incentive mechanism of each cryptocurrency
Zarrin et al. [17]	2020	Investigating two aspects in the decentralized Internet: consensus algorithms and other cutting-edge technology
Yang et al. [18]	2019	Introducing the blockchain-based Internet with decentralized processing and traceable trustworthiness
Gilani et al. [19]	2020	Providing the identity proofing and authentication solutions for different self-sovereign identity solutions
Our Survey	2023	Proposing a hierarchical architecture of the Web 3.0 ecosystem from a significant amount of concrete research and providing a comprehensive overview of the current state of AI in Web 3.0

content and track malicious users to solve the challenges faced by management. Specific solutions include utilizing AI for big data analysis [8], AI-generated content [9–11], and detecting and classifying various forms of content such as text and video [12]. These AI-powered technologies can be applied across different aspects and stages of Web 3.0, improving the overall functionality and user experience. Through in-depth research, we give a hierarchical architecture of the Web 3.0 ecosystem and then discuss how AI can play an essential role in the current challenges encountered by Web 3.0 in each layer.

Although a comprehensive survey of Web 3.0 has not yet been conducted, there have been some reviews of some components and applications of Web 3.0, as shown in Table 1. For example, some surveys investigate the metaverse, an important application of Web 3.0 [13–15], focusing on its integration with blockchain and virtual reality. Other surveys focus on digital assets [16], an important component of Web 3.0, and mainly on the architecture, consensus mechanism, privacy, and security of cryptocurrency. There are also surveys of decentralized networks [17, 18] and decentralized identities [19]. Compared with the articles published on Web 3.0, we systematically introduce the development history of Web 3.0, the framework structure of the Web 3.0 system, and the current application of AI in the Web 3.0 ecosystem. The main contributions of this investigation are summarized as follows:

- To the best of our knowledge, we are the first to conduct a survey of the existing literature on the use of AI in Web 3.0. Through our survey, we provide a comprehensive overview of the current state of AI in Web 3.0, including the types of AI algorithms that have been applied, the results and outcomes achieved by different studies, and the key technical challenges and limitations that have been encountered.
- We abstract the architecture of Web 3.0 from a great amount of concrete AI research, which presents an overview from four aspects: data management, value circulation, application scenarios, and ecological governance. We provide a comprehensive overview of the current research and challenges of the Web 3.0 ecosystem.
- We not only present an overview of the existing studies in the field of AI for Web 3.0 but also provide further insights into the defects of existing studies and discuss in detail the future research challenges and directions on AI for Web 3.0, which provides readers with possible directions for developing innovative solutions.

The rest of this article is organized as follows. We commence with the evolution of Web technology and the classification of AI used in Web 3.0 in Section 2. We present the architectural layers of the Web 3.0 ecosystem we define and formulate a case to aid understanding in Section 3. In Sections 4 through 7, we respectively introduce the issues and existing AI solutions in the four layers of Web 3.0: infrastructure, interface, management, and application. In Section 8, we introduce the technical challenges faced by Web 3.0 and prospects for the future research direction of Web 3.0 technology. In Section 9, we summarize the full literature.

2 BACKGROUND

In this section, we introduce the history of the World Wide Web. Since the World Wide Web was invented in 1989, it has experienced three generations, namely Web 1.0, Web 2.0, and Web 3.0. We summarize the development process and characteristics of these three generations and guide the logic behind the development of the World Wide Web. Then, we investigate the classification of AI technology and focus on what might be used in Web 3.0.

2.1 The Evolution of the Web

Web 1.0. In 1989, Tim Berners Lee invented the World Wide Web at CERN in Switzerland, marking the beginning of the era of the Internet as an application. He then, with his team, created the first website, http://info.cern.ch/, in the next year [20]. In the following years, the important components that make up the web page were invented, including HTML [21], HTTP [22], and Browser. Web 1.0 implements the Internet application in the era of personal computers, but most users can only use access and search functions to obtain information, rather than edit content.

Web 2.0. In 2014, the first Web 2.0 conference was hosted by O'Reilly Media and MediaLive, at which the concept of web as platform was proposed [23]. In the same year, Mark Zuckerberg founded Facebook. In the following years, companies in different fields, including Amazon and Google, were established, which enabled users to publish, comment, like, and upload content on the network. Web 2.0 realizes the network for users to edit content, making the network a huge social circle covering the whole world. However, it has spawned electronic giants, such as Facebook and Google, causing serious privacy problems.

The conception of Web 3.0. The conception of Web 3.0 is proposed to address the limitations of the current centralized web. To solve the problems of privacy leakage and monopoly of large companies, Tim Berners-Lee proposes a system called Solid [24], which is considered the prototype of Web 3.0 now. It is a decentralized platform for social applications, which ensures that the user's data is managed independently of the application accessing this data. Users store their data in pods, and the application needs to comply with certain protocols for access. At the same time, distributed authentication and access control mechanisms ensure data privacy. Users' data is no longer fragmented across different platforms. They can freely migrate between different platforms and determine the access rights of services to their data.

Later, Gavin Wood formalizes the concept of Web 3.0, a system combining the World Wide Web with distributed technology, like blockchains and smart contracts [25]. It is generally accepted that the most important characteristic of Web 3.0 is decentralization [26]. In conclusion, we summarize the key characteristics of the web through the ages as shown in Table 2 and propose our definition of Web 3.0. It is the new generation of the Internet that is reconstructed with distributed technology, which focuses on data ownership and value expression. And it operates under the principle that data and digital assets should be owned and controlled by users rather than large corporations. The key features of Web 3.0 include decentralized, blockchain based, privacy protected, and AI empowered.

2.2 The Categorization of AI in Web 3.0

The rapid development of AI technology in recent years has brought new solutions to many challenges encountered in the development of Web 3.0. After our research and summary, we find that AI can play a unique role in Web 3.0. It can be divided into four categories, namely detection of malicious content and behavior, generation of digital entities, optimization of network architecture,

Table 2. The Evolution of Key Features of the Web

The Evolution of Web	Web 1.0 (1980s–)	Web 2.0 (2000s–)	Web 3.0 (2020s–)
Entrance	Browser	App	Wallet
Back-end computing center	Server	Clouds	Peer-to-peer network, blockchain
Interactive mode	Read-only	Read & write	Read & write & own
Economic model	Advertising economy	Platform economy, advertising economy	Ownership/creator economics
Network form	Centralized	Centralized	Decentralized
Data/content publisher	Web portals	PGC, UGC	PGC, UGC, DAO, AIGC
Data/content ownership	Institution	Company and platform	Individuals and organizations, portable
Digital identity system	Username & password	Platform-based identity	Decentralized digital identity

and prediction of digital asset price. In terms of detection, machine learning and deep learning methods can be employed to identify malicious addresses and abnormal behaviors, as well as to ensure the integrity and security of smart contracts. Graph neural networks are naturally suitable for representing transaction behaviors in Web 3.0. In terms of generation, Generative Adversarial Networks and large-scale models have showcased impressive capabilities in generating various forms of content, such as images, text, videos, and more. In terms of prediction, neural networks capable of processing temporal information can predict the future price of digital assets based on a large amount of relevant data. In terms of optimization, AI algorithms can assist in optimizing the network architecture [27] to enhance operational efficiency.

We evaluate the algorithms based on their model complexity. Based on this criterion, machine learning can be broadly categorized into two groups: traditional machine learning techniques and deep learning techniques. The main distinction between the two is the use of cascaded neural network layers in the algorithm.

(1) Traditional machine learning: Traditional machine learning refers to the earlier methods and algorithms of machine learning that are based on statistical and mathematical principles, including **Support Vector Machine (SVM)**, Decision Trees, K-Nearest Neighbors, and Naive Bayes. These methods require fewer computational resources and are easier to interpret.

SVM [28] works by finding the best boundaries called hyperplanes to separate data into classes or predict output values. To handle non-linear relationships in the data, SVM uses the kernel trick, which maps the input data into a higher-dimensional space. Common kernel functions used in SVMs include linear kernels, polynomial kernels, Gaussian kernels, and sigmoid kernels. For example, SVM can be used to improve the security of the Web 3.0 identity management system by detecting user behavior and identifying malicious users [29].

Naïve Bayes [30] is a statistical learning algorithm. It is based on Bayes' theorem, which provides a way to calculate the probability of an event based on prior knowledge of the conditions likely to be associated with the event. The algorithm assumes that the features of a given data point are independent of each other. Naive Bayes can be used for data pricing [31].

Decision tree [32] works by building a tree model of decisions and their potential consequences. The tree consists of nodes representing tests on features and edges representing test results. The root node represents the first decision, internal nodes represent subsequent decisions, and leaf nodes represent the final prediction. The path from the root node to the leaf nodes represents a sequence of decisions based on the input feature values. Decision tree can be used to predict the price of digital assets [8].

Random Forest [33] is an ensemble learning algorithm that combines multiple decision trees to make predictions for classification and regression tasks in machine learning. The algorithm trains multiple decision trees on random subsets of the training data and combines their predictions through voting or averaging to produce a final prediction. Random forest algorithm can be used for network behavior perception [34] in Web 3.0.

(2) Deep learning techniques: It is a subfield of machine learning that is inspired by the structure of the brain, specifically the neural networks. It involves training artificial neural networks, which are composed of layers of interconnected nodes or artificial neurons, on a large dataset. Each layer processes the input and passes it on to the next layer until the final output is produced. The layers between the input and output layers are known as the hidden layers.

Convolutional neural network [35] is a specific type of deep learning. It uses convolutional layers to learn local features and pooling layers to reduce spatial resolution. Also, CNNs have a relatively small number of parameters, making them efficient for tasks with scarce labeled data. CNN has a wide range of applications in Web 3.0, which can be used to transform the image style [36, 37], improve the blockchain incentive mechanism [38], and detect bad content [7, 39, 40].

Recurrent Neural Networks (RNNs) [41] are a type of neural network that specializes in processing sequential data, such as time series, text, and speech by maintaining a hidden state that allows the network to learn and maintain context from previous time steps. They are well suited for tasks that require understanding the context of the input. There are also variants of RNNs such as **Long Short-Term Memory (LSTM)** and **Gated Recurrent Unit (GRU)** that have been developed to further improve the ability of RNNs to handle long-term dependencies. RNN is used in Web 3.0 to generate content [11], predict the price of encrypted assets [42, 43], and detect unhealthy content [44].

Graph Convolutional Network (GCN) [45] is a deep learning architecture designed for graph-structured data. In GCN, the nodes in the graph represent entities, and the edges represent the relationships between them. The core component of GCN is the graph convolution operation, which aggregates information from neighboring nodes to generate a new representation for the current node. GCN is widely used in the protection of privacy and security in Web 3.0, such as the transaction entity recognition [46], malicious transaction identification [47], and the perception of network behavior [48].

3 ARCHITECTURE OF WEB 3.0

In this section, we introduce a new Web 3.0 architecture from the perspective of application scenarios and ecosystems, as shown in Figure 1. In the past, the framework of Web 3.0 was often from a technical perspective, such as the Web 3.0 technology stack proposed by Gavin Wood [25]. We will illustrate the rationale for dividing Web 3.0 into distinct layers and the function of each layer as well as the crucial role of AI within this context. The list of common abbreviations and explanations of the article are summarized in Table 3.

3.1 The Hierarchical Architecture of Web 3.0

As illustrated in Figure 1, Web 3.0 can be divided into four layers: infrastructure layer, interface layer, management layer, and application layer. The infrastructure layer primarily handles data management. The interface layer is responsible for mapping physical world data to the digital space. The management layer governs the ecosystem of Web 3.0. And the application layer is where actual use cases for Web 3.0 are designed and implemented. In the following section, we will explain each layer in detail.

Infrastructure layer. It is responsible for collecting, storing, transmitting, and processing data. With the adoption of Web 3.0 technologies, which emphasize decentralization and co-governance [38, 49–51], the sources of data have been greatly expanded, including the use of terminal devices from the Internet of Things and real-time feedback from users. This data is transmitted to edge devices or nodes for analysis and may be stored using an on-chain or combination of on-chain and off-chain methods to ensure the transparency and effectiveness of the data. In the whole process, AI technology can be integrated into all aspects to optimize strategies, improve storage computing efficiency, improve system security, and protect privacy.

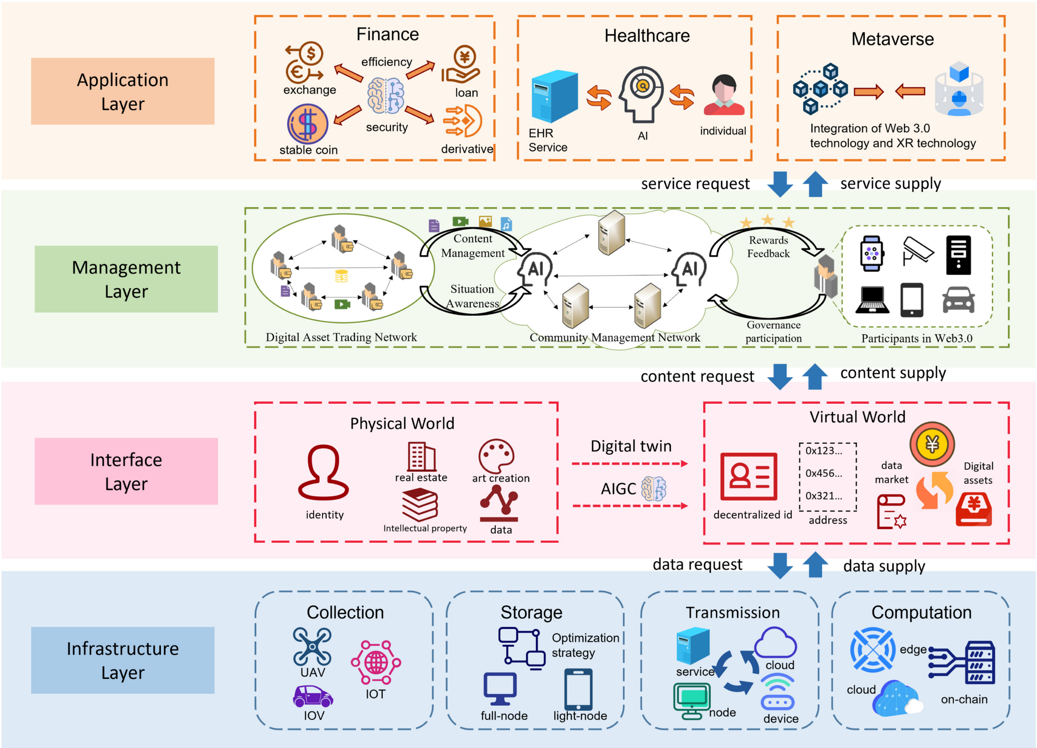

Fig. 1. The hierarchical architecture of Web 3.0.

Interface layer. It serves as a connection between the physical world and the digital world, transforming data collected from the infrastructure layer into valuable digital assets. This layer also establishes a value circulation system to optimize the utilization of data and motivate user participation. The value of this data is determined by supply and demand, allowing users to benefit from their contributions. Unlike the Web 2.0 architecture, where private data is controlled by centralized institutions, Web 3.0 grants individuals ownership of their data, with decentralized identities responsible for protecting privacy and access control. AI can assist in the decentralization of identity systems [29, 52] and the creation of a more intelligent data market [53], while also safeguarding the privacy of individuals [48, 54–56].

Management layer. It is responsible for the overall governance of the lower layers, including the implementation of incentives that encourage user participation [57–60] and the review of user-generated content [61]. In the case of a smart city, the management layer may correct or remove erroneous or outdated traffic information uploaded by users and detect and defend against malicious traffic attacks on the system. AI can also assist in identifying abnormal trading behavior and detecting false or inappropriate information.

Application layer. It is the application system built upon the previous three layers. As an example, in the context of a smart city, this layer may include navigation apps that adjust routes in real time based on traffic conditions. Beyond the realm of smart cities, the application layer of Web 3.0 has seen significant progress in finance [62–64], medicine [65, 66], the metaverse [67, 68], and healthcare [69]. AI technology is also heavily integrated at this level, improving user experience, enhancing privacy protection, and increasing efficiency.

Table 3. Common Abbreviations and Explanations Used in This Article

Abbreviation	Explanation	Abbreviation	Explanation	Abbreviation	Explanation
ADS	Authenticated Data Structure	FCN	Fully Convolutional Neural Network	NLP	Natural Language Processing
ANN	Artificial Neural Network	FL	Federated Learning	PUL	Positive and Unlabeled Learning
AoI	Age of Information	GA	Genetic Algorithm	QoS	Quality of Service
BI	Bayesian Inference	GAN	Generative Adversarial Networks	RBFNN	Radial Basis Function Neural Network
CLIP	Contrastive Language-Image Pre-Training	GBDT	Gradient Boosting Decision Trees	RF	Random Forest
CNN	Convolutional Neural Network	GCN	Graph Convolutional Network	RL	Reinforcement Learning
CNNs	Capsule Neural Network	GNN	Graph Neural Network	RNN	Recurrent Neural Network
DAG	Directed Acyclic Graph	HAN	Hierarchical Attention Network	SL	Supervised Learning
DBN	Deep Belief Network	HMM	Hidden Markov Model	SNN	Siamese Neural Network
DCNN	Deep Convolutional Neural Network	IoT	Internet of Things	SVD	Singular Value Decomposition
DDPG	Depth Deterministic Policy Gradient	LBF	Learning-based Bloom Filter	SVM	Support Vector Machine
DL	Deep Learning	LSTM	Long Short-term Memory	TPS	Transactions per Second
DNN	Deep Neural Network	MBP	Multi-armed Bandit Problem	UAV	Unmanned Aerial Vehicles
DQN	Deep Q-Network	MC	Markov Chain	VGGNet	Visual Geometry Group Network
DRFNet	Dilated Residual Feature Net	MDP	Markov Decision Process	WCN	Wireless Communication Network
DRL	Deep Reinforcement Learning	MEC	Moblie Edge Computing	WSN	Wireless Sensor Network

3.2 Case Study

In this section, we explore how a smart city project would function within the Web 3.0 scenario, providing a deeper understanding of the architecture of Web 3.0 that we design. Smart city is a city that uses technology and data to improve the quality of life for its citizens. One important function is using sensors and information technologies to monitor and optimize traffic flow. In the context of Web 3.0, this function will be implemented by the following steps.

The initial layer that plays a role is the infrastructure layer, which mainly deals with data collection, analysis, storage, and other functions. To achieve real-time navigation route adjustments, it is imperative to gather current road condition information as the first step. There are two methods of obtaining this information: the first involves edge device sensors, such as cameras and **Unmanned Aerial Vehicles (UAVs)** [70], while the second method acquires traffic information from users and drivers. After data is collected, it will be transmitted to computing nodes and the cloud for analysis.

The interface layer receives data from the infrastructure layer, and its major function is to add value to the raw data, ensuring that it can be utilized to its fullest potential at the most relevant locations, while also incentivizing the providers of such data, thus keeping them engaged over an extended period of time [57]. Once these data are mapped to the Web 3.0 system, their ownership will be secured by blockchain and data confirmation technologies. Subsequently, they will be priced and circulated in the digital asset market [53].

Then the management layer will come into play, and due to the permissionless nature of Web 3.0, censorship of content will be crucial. The content review mechanism includes verifying the credibility and timeliness of transaction information, while also identifying any illegal material [61], such as pornography and violence, that may be uploaded by users.

Finally, the application layer is built on the above system. Based on the services and data provided by the lower layer, developers can realize a wide range of commercial applications. In the context of smart cities, there is navigation software that can adjust routes according to real-time traffic conditions and recommendation software that can provide local service (catering, entertainment, etc.) information according to user preferences.

4 INFRASTRUCTURE LAYER

The infrastructure layer of Web 3.0 is primarily responsible for data processing, which is like the foundation of a building. In Web 3.0, data is stored in a decentralized blockchain system and has various types, large quantities, and distributed storage, which is more difficult to manage than traditional databases, as shown in Figure 2. Compared with traditional centralized systems, Web 3.0 systems have higher requirements for performance due to their transaction latency, and more evaluation indicators such as decentralization, scalability, and resource cost of blockchain-related

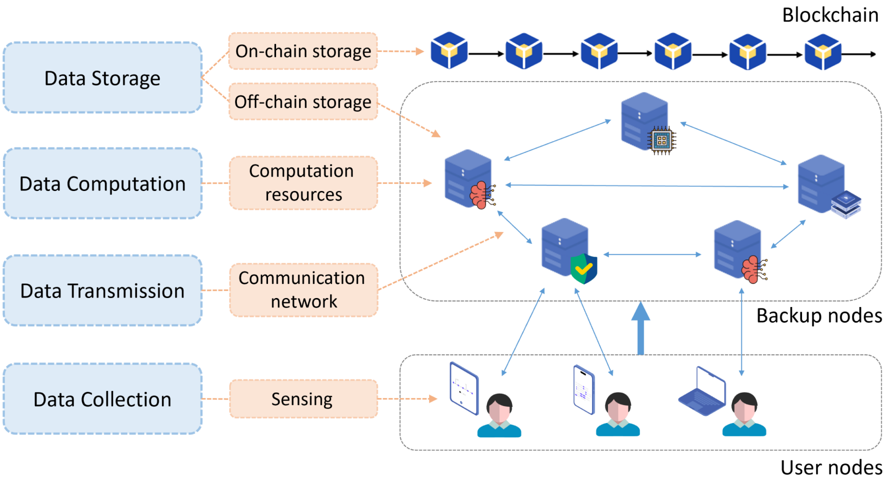

Fig. 2. A common structure of the infrastructure layer.

operations that require consideration. Therefore, a specific data management solution for Web 3.0 scenarios is needed.

AI can help in enhancing the Web 3.0 infrastructure layer in various ways. AI is capable of optimizing strategies for data collection, data distribution, and computing resource allocation, which helps reduce energy costs and improve the throughput of Web 3.0 systems. Also, AI has the capacity to build a collaboration-enabled intelligent Internet architecture to enable the intelligence of the Web 3.0 network, which can overcome resource limitations and improve performance in complex scenarios [27]. Simultaneously, AI effectively avoids abnormal situations and automatically adapts to changes by detecting and predicting potential threats to the systems.

4.1 Data Collection

The data volume in the Web 3.0 system is huge and requires many nodes and validation, which brings challenges for related studies. In Web 3.0, **Internet of Things (IoT)** devices play a crucial role as they provide reliable data support for web applications and services by integrating digital information between things. Therefore, Web 3.0 applications often require the support of UAVs [71], the Internet of Vehicles [72], abd so forth, in which AI optimizes the behavior of peers to maximize the overall system performance. At the same time, for Web 3.0 problems such as scalability and edge intelligence, the policies of the system or each node can also be optimized by AI.

The data collected by the Web 3.0 system has the characteristics of large quantity and diversity. Collection strategies should be adopted in the system to avoid unreasonable allocation of resources. AI can be used to optimize the data collection strategy, with **deep reinforcement learning (DRL)** being a common approach. Liu et al. [70] propose an efficient data collection and secure sharing scheme based on blockchain. This scheme, based on distributed DRL, is adapted to allow each mobile terminal to move to a certain location for data acquisition, maximizing the collecting rate. And according to the article, by introducing AI, energy consumption decreases from 64% to 78%.

The convergence of IoT and Web 3.0 provides security and reliability for data collection. IoT in Web 3.0 is typically blockchain based, and there are extra factors to be considered (e.g., blockchain-related operations) in terms of strategy optimization. The authors in [73] propose an adaptive linear prediction algorithm. In this work, the sensed value to be uploaded is predicted and by which the actual value is replaced, thus reducing the transmission overhead. After that, Tang et al. [71]

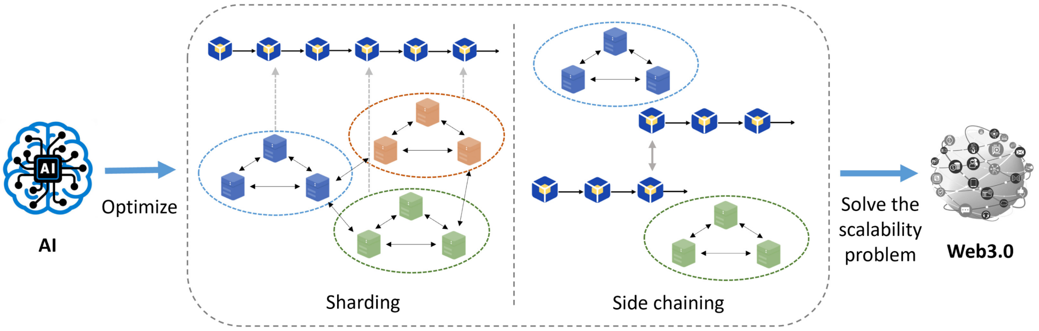

Fig. 3. The role of AI in addressing the scalability problem.

use reinforcement learning to judge the optimal solution of each node under the PoS consensus mechanism. Compared with traditional IoT, the determination of the optimal solution needs to consider the fairness mechanism of the blockchain.

4.2 Data Storage

Data storage in Web 3.0 is decentralized and based on blockchain. Common blockchain systems have full nodes, which store the full blockchain, and light nodes, which store only the block headers. In order to improve the scalability of the Web 3.0 storage system, recent studies have proposed operation modes for Web 3.0 such as collaborative storage and blockchain sharding, in which AI can participate in the formulation of storage strategies. Due to the high requirements of Web 3.0 for system throughput, the storage strategy has become an important aspect, such as block generation strategy, sharding strategy, and chain update strategy, which provide solutions to the scalability problem, as shown in Figure 3.

Determining the generation strategy of storage structure. According to the blockchain trilemma, it is impossible for any blockchain system to take into account the following three points: scalability, decentralization, and security. Therefore, the problem of storage strategy optimization is an issue worth studying. A method of determining the sharding strategy of the blockchain and identifying the optimal parameters of the system is highlighted by Yun et al. [74]. With this method, the sharding strategy and optimal parameters are successfully derived. DRL is also employed to analyze the network state, facilitating adaptive optimization of the system's throughput and security level. Also, for formulating block generation policies, the problem of quantifying the degree of decentralization in blockchain is addressed by Bai et al. [75]. By introducing an AI-based system optimization model utilizing DRL, this method dynamically adjusts the system parameters, improving the degree of decentralization and enhancing the system throughput.

Additionally, sidechain is also a common solution for scalability issues, and AI can help optimize the construction and update of the sidechain, which enables sidechains to handle a higher volume of data and more complex computational tasks, enhancing the scalability of the Web 3.0 ecosystem. We will further introduce the role of AI in the sidechain at the Management Layer.

Developing the edge storage strategies. Recent research has proposed the concept of Web 3.0 collaborative storage, in which nodes with more resources can offload part of their data to nodes with fewer resources to collaboratively use their storage resources. The data offloading technology in edge computing provides an idea for this scenario, and the technology can be transferred to this scenario. For instance, a task offloading method based on meta-reinforcement learning is proposed by Wang et al. [84]. This method exhibits the ability to swiftly adjust to new environments with only a few gradient updates and samples. By employing this AI-driven approach, a reduction in latency by 25% can be achieved, making it highly adaptable to varying system conditions.

As a common infrastructure for Web 3.0, IoT systems need to cache files to edge nodes to meet the requirements of large throughput. Cui et al. [76] propose a system combining IoT devices, edge nodes, and blockchain. The algorithm they design applies the federated learning compression algorithm to the content cache to predict cached files. Each edge node uses local data to train a model, predicting popular files and improving the cache hit ratio.

As the explosion of on-chain recorded contents and the fast-growing number of users cause increasingly unaffordable resource consumption in storage in Web 3.0, Lin et al. [85] propose a unified blockchain-semantic ecosystems framework. This framework can convey precisely the desired meanings without consuming many resources by utilizing dynamic sharding mechanisms to classify the same semantic demands. This dynamic sharding mechanism used in the proposed framework is adaptive and based on DRL, which can adjust the number of shards and their sizes based on the current workload and semantic demand patterns.

4.3 Data Transmission

The Web 3.0 network is a peer-to-peer structure, which is decentralized and relies on user groups to exchange information. For data transmission in the network structure of Web 3.0, AI can help solve the problem of path optimization of data transmission and formulate transmission strategies.

AI can be used to determine the transmission strategy optimization model, which helps design routing algorithms or identify the traffic changes in the network environment to dynamically adjust the data transmission volume. IoT requires better communication networks for data transfer between heterogeneous devices and an optimally **Wireless Sensor Network (WSN)** [86]. In the Web 3.0 system, edge nodes tend to use the distributed data transmission strategy [87]. Farquhar et al. [77] study transmission control in distributed wireless communication networks from the perspective of multi-agent reinforcement learning. Each node acts as an independent reinforcement learning agent without knowledge of actions taken by other agents. Considering the special uncertainty in the Web 3.0 scenario, Luong et al. [78] use blockchain and mining pools to support IoT services based on cognitive radio networks. In their method, a DRL algorithm is proposed to derive the optimal transaction transport strategy for secondary users. Also, the **Double Deep Q Network (DDQN)** is used, which allows secondary users to learn the optimal strategy.

From the view of data transmission, data availability is an important aspect. Typically, the edge devices need to connect to a reliable Web 3.0 node for efficient data synchronization as they complete data collection. Therefore, reliability prediction is needed, in which AI can be used. For instance, Zheng et al. [88] develop a framework using **machine learning (ML)** methods to predict reliable peers in blockchain systems. Moreover, considering the privacy issues, a personalized reliability prediction model for privacy protection is proposed by Xu et al. [79]. This model utilizes the **Federated Learning Neural Collaborative Filtering (FNCF)** technique to improve the accuracy of predictions while ensuring privacy preservation. By adopting this approach, users can receive personalized predictions without the risk of privacy leakage.

4.4 Data Computation

Web 3.0 uses distributed computing, eliminating the need for a central authority to manage and allocate resources. Resources are aggregated and optimized by the network itself, thus improving the efficiency and cost-effectiveness of resource use. Web 3.0 obtains computing capability by connecting with cloud servers, which also causes a series of challenges, such as system scalability, efficiency of computing resource integration, and privacy issues of user data. Web 3.0 data computing covers a wide range of fields, including common computing scenarios like **federated**

learning (FL), migration learning, computing resource allocation, and related operations on the database, such as data retrieval.

ML is a common data computing scenario in Web 3.0. In Web 3.0 systems, distributed ML is a more common mode, which solves the problem that traditional centralized FL is susceptible to a single point of failure and external attacks. A DFL framework is proposed by Lu et al. [89]. This framework takes into account resource consumption and models the task of resource sharing in FL as a combinatorial optimization problem. Furthermore, it employs DRL-based algorithms to optimize the solution for this problem. After that, Li et al. [83] aim at the problem that previous work does not consider the mining overhead. They model the time of training and mining in the blockchain and propose an optimized scheme for ML computing resource allocation.

Blockchain sharding is the solution to the scalability problem. However, the current throughput of sharded blockchains remains limited in terms of a high proportion of Cross-shard Transactions. Yang et al. [80] propose a cluster-based sharding strategy for collaborative computing of the IoT. This sharding strategy is based on the user grouping of K-means clustering and the allocation of consensus nodes, improving the scalability of sharded blockchain. As another common scenario of data computation in decentralized systems, **Collaborative Edge Computing (CEC)** transfers tasks from busy edge servers to idle servers. Yet different **Mobile Edge Computing (MEC)** service providers have no incentive to help others. He et al. [81] propose a collaborative mechanism. This mechanism can obtain additional profits by sharing idle computing resources, describes the social welfare maximization problem as a **Markov Decision Process (MDP),** and breaks it down into the allocation and execution of unloading tasks.

Verifiability is the key advantage of Web 3.0 from the point of data retrieval. In the Web 3.0 verifiable query scenario, users need to verify the correctness and completeness of query results. To ensure the completeness of Boolean queries, a Bloom filter may be required as a tool for constructing proof of the nonexistence of data elements. Dai et al. [82] propose a **learning-based Bloom Filter (LBF)**. In this method, different machine learning models are used to construct multiple LBFs, and the LBF with the lowest false-positive rate is selected. After that, Chang et al. [90] propose a learning-based index for the construction of an authenticated index, which improves the efficiency of verifiable query.

4.5 Summary and Lessons Learned

The problems in the infrastructure layer can be summarized in two points, namely the scalability problem and the security problem. In the scalability problem, the main role of AI is optimization, with RL being a common approach. In the security problem, the main role of AI is detection and prediction. AI technology can make Web 3.0 systems intelligent and significantly improve the efficiency of Web 3.0 data management in various scenarios. We have summarized the references mentioned in this chapter in Table 4, and illustrate the significance of AI through the above discussion. However, despite the work that has been done, the scalability problem and security challenges still exist in Web 3.0, which are the inherent challenges of decentralization. The current research does not completely solve these problems, and further optimization is needed.

5 INTERFACE LAYER

The second layer of Web 3.0 is the interface layer, which serves as a bridge between the physical and digital worlds, as shown in Figure 4. This layer consists of two components: digital identity and digital assets. In Web 2.0, each person's digital identity on different platforms is fragmented and interoperable. At the same time, users do not have their own identities and affiliated data assets, which are monopolized by large companies. In order to solve these problems, Web 3.0 adopts a decentralized identity scheme, which ensures the user's ownership of their identity and data by

Table 4. Research of Infrastructure Layer Based on AI

Subjects	Refs	AI Methods	Specific Scenarios	Web 3.0 Tasks
Data Collection	[70]	DRL	Industrial IoT	Optimize collecting strategies using distributed DRL in blockchain systems
	[73]	Linear Model	UAV-assisted IoT	Develop prediction algorithm to save the overhead of transaction
	[71]	DRL	UAV-assisted IoT	Determine the optimal strategy of edge nodes under the PoS consensus
Data Storage	[74]	DRL	IoT	Determine the sharding strategy to adjust the system parameters
	[75]	DRL	IoT	Incorporate the degree of decentralization for DRL training
	[76]	FL	IoT	Enable edge intelligence for decentralized systems
Data Transmission	[77]	Multi-agent RL	WCN	Determine the distributed data transport policy
	[78]	DDQN	IoT	Derive an optimal transaction transport strategy for secondary users
	[79]	FNCF	IoT	Predict reliable nodes for data transmission in decentralized systems
Data Computation	[80]	DRL	Collaborative computing	Determine blockchain sharding policy for the allocation of computing resources
	[81]	DRL	MEC	Create incentives using ML techniques for task offloading
	[82]	SVM,DNN	Verifiable searching	Construct high-performance ADS for verifiable query in blockchain
	[83]	FL	Decentralized FL	Optimize the resource allocation between training and mining

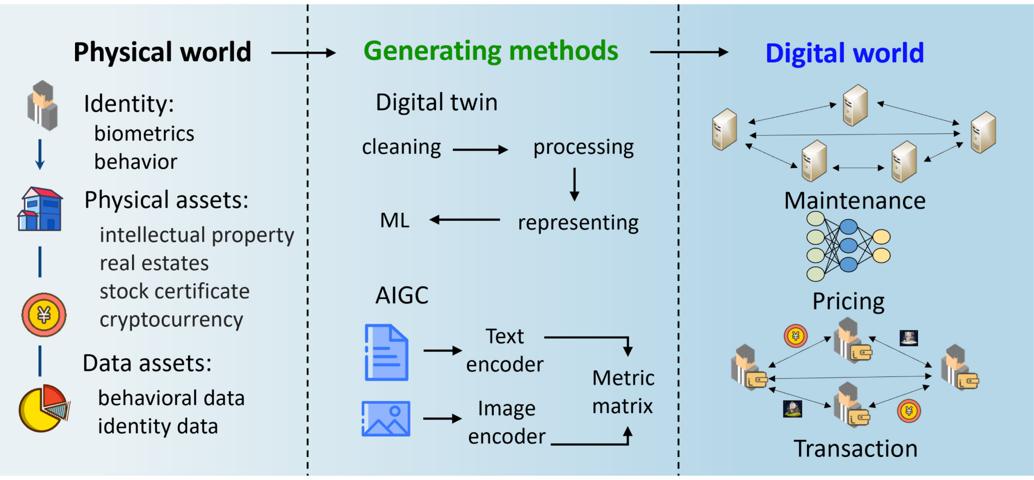

Fig. 4. A common mapping model from the physical world to the digital world in the interface layer.

storing identities on a distributed system (such as blockchain). Digital assets refer to valuable goods in the virtual world, including data generated by user behavior, property rights, and securities that users map from the physical world to the digital world. The introduction of digital assets means that an endogenous new equity trading market has been established in Web 3.0. This platform provides users with a value circulation system for creating, pricing, trading, and consuming digital assets. Through this value circulation system, digital assets can be utilized to their fullest potential by the people who need them most, and the providers can also obtain corresponding value returns. As a result, this digital property economy will completely change the development mode of the digital economy.

However, Web 3.0 systems are currently facing some serious challenges. Traditional digital identity management methods incur significant overhead and pose high security risks due to the involvement of key management processes. The capabilities of AI algorithms in classification and detection can provide new solutions for digital identity systems. For instance, AI recognition algorithms based on biometrics can greatly improve the usability and security of digital ID [91, 92]. In terms of digital assets, the system for the generation and pricing of digital assets is still not

Table 5. Research of Digital Assets Based on AI

Subject	Ref.	AI Methods	Specific Scenarios	Web 3.0 Task
Generate Digital Assets through Digital Twin	[98]	CNN	Digital avatar	Generating high-fidelity 3D avatar from a single image
	[99]	DNN	Digital city	Transforming 3D spatial data and city models to a virtual world
	[100]	SVD DNN	Digital avatar	Formalize personality as digital twin models by observing users' posting content
Generate Digital Assets through AIGC	[36]	CNN	Style transfer	Produce a rather psychedelic and hallucinatory stylistic effect
	[37]	CNN		Rendering the semantic content of an image in different styles
	[101]	GAN	Generate content	Stochastic variation in the generated images
	[102]	GAN		Generate images from text descriptions
	[9]	CLIP		Maximize the similarity between real image–text pairs
	[10]	VAE		Generate texts with better discourse structure and narrative flow
	[11]	LSTM		Solve the gradient disappearance and gradient explosion in text generation
The Circulation of Digital Assets	[103]	MBP	Data pricing	Price of privacy in personal data market
	[31]	BI		Pricing when few data points are available
	[104]	MBP		Decide on prices with incomplete demand information
	[53]	DNN	Transaction matching	A market mechanism to price training data and match buyers to sellers
	[42]	LSTM	Assets pricing	High-performance model prediction in the case of insufficient data samples
	[8]	GBDT		Comparison of trading strategies based on different neural network methods
	[43]	LSTM		Price prediction using user behavior data

established. AI models excel in generation, enabling the creation of rich and distinctive digital assets in Web 3.0 [9–11]. The strong performance of AI in prediction and big data analysis can enhance the efficiency of digital asset trading and pricing [8, 43]. We will explore these topics in the following sections. The main articles mentioned in this Section 5 are listed in Table 5.

5.1 Digital ID

Digital identity allows individuals to verify their identity and access online services in the digital environment. It is the mapping of a human's real identity in the physical world to the virtual world. The decentralized identity scheme is adopted in Web 3.0. At present, there are mainly two ways to realize decentralized identity: **World Wide Web Consortium (W3C) Decentralized Identifiers (DID)** and Ethereum **Non-Fungible Token (NFT)**. On the one hand, the W3C has developed a set of DID standards and protocols for creating, managing, and using DIDs [93]. It includes guidelines for creating and managing DIDs and rules for using DIDs to represent and verify identity information in a decentralized manner. It can be used not only for people but also for anything, including cars, machines, and even algorithms. On the other hand, NFT can also be used as an expression of digital identity on the chain. Vitalik [94] demonstrates how to use the **soul binding token (SBT)** to code the trusted network in the economy and establish the reputation. These tokens represent commitments, vouchers, and affiliations of individuals or entities and are non-transferable.

Although the decentralized identity system has a bright future, it is currently facing challenges in identity authentication. One problem is that the system may be very complex for users and needs to manage complex private keys, which may be stolen or lost. However, AI technology can help solve these challenges by assisting with biometric authentication and behavioral authentication. By using AI in these areas, the threshold of using a decentralized identity system can be lowered, and the risk of key loss and identity theft can be reduced.

Biometrics authentication is less prone to forgetfulness compared to knowledge-based authentication and is difficult to lose compared to token-based authentication [95]. Fingerprint recognition is commonly used in practice, with one typical example being the work of Svoboda et al. [91]. The method they propose uses generative convolutional networks to denoise visible details and predict missing parts of fingerprint ridge patterns. Iris recognition is generally considered to be a secure method of biometric identification because the iris is an internal body part that is protected by the eyelid. Wang and Kumar [92] implement the use of dilated convolutional kernels and residual learning in their deep learning framework. This method not only improves the accuracy of iris matching but also simplifies the network structure.

However, biometric authentication has been criticized because it is vulnerable to attacks that happen after the initial authentication, while behavior recognition can provide continuous recognition. Screen touch gestures are typically used in behavior recognition. Debard et al. [96] propose a method that utilizes deep neural networks and features a dynamic sampling and temporal normalization component. Their approach can be adapted to different gestures, user styles, and hardware variations. Mahbub et al. [52] innovatively use the user's habit of using the application to implement identification. This innovative approach collects data from participants using smartphones, including information on device location; install, remove, or update applications; and the currently running foreground application, to implement identity authentication.

Some methods have been used in virtual systems to achieve accurate identification and access control in the virtual world. Bader and Amada [97] use a combination of 3D tools and the Unreal Engine, a comprehensive collection of tools for creating 3D games and virtual spaces, to create a virtual world. This platform utilizes a centralized biometric authentication module that uses fingerprint technology to achieve access control. However, this method cannot match the real identity with the virtual identity. Yampolskiy et al. [29] propose a set of algorithms for accurately verifying and recognizing avatar faces. These algorithms aim to authenticate avatars within virtual worlds and enable tracking of individuals across both the real and virtual realms in inter-reality scenarios.

To conclude, we discuss the challenges in identity authentication and suggest leveraging AI technology for biometric and behavioral authentication. We highlight the use of fingerprint and iris recognition for secure biometric identification, as well as screen touch gestures and user habits for behavior recognition. We also mention the application of virtual world authentication methods for accurate identification and access control in virtual environments.

5.2 Digital Asset

Web 3.0 is a new generation of the Internet that focuses on the circulation of value. The digital asset is its core object. Web 3.0 uses algorithms to create and distribute these assets, enabling the flow of value at a minimal cost. By utilizing blockchain technology and smart contracts, Web 3.0 allows users to create, own, and trade digital property rights on the Internet and gives users personal data ownership and the right to participate in the governance of Internet platforms and applications.

There are two main types of digital assets in Web 3.0. One is the assets owned or controlled by individuals and enterprises in the form of electronic data, including digital intellectual property rights, emerging cryptocurrencies, and real-world physical assets mapped to digital assets like cars, real estate, and lands. The second category is data assets, which are mainly a series of behavioral data generated by the operation of users in the digital world. It can directly or indirectly create economic and social benefits. Web 3.0 provides a value circulation system to help digital assets circulate freely and maximize their value where they are most needed. We divide the entire life cycle of digital assets into two stages, namely the generation of digital assets and the transaction circulation of digital assets. AI technologies all play a huge role throughout the lifecycle of digital assets. Each of these will be described below.

The generation of digital assets. The generation of digital assets includes the mapping from the physical world to the virtual space and the generation of native virtual assets. Two technologies used for this process are Digital Twin and **AI-generated content (AIGC)**. Digital twin technology can be used in Web 3.0 to build smart cities, virtual avatars, and virtual world infrastructure [105].

AI technology can help improve the efficiency and accuracy of digital twins. At present, the original digital assets are mainly digital collections and NFT, and the forms are pictures, texts, music, and so forth. The traditional generation method is costly and inefficient. AIGC can help creators try out the inspirational scheme more efficiently and directly in the early stage, and it saves manpower to complete the details in the later stage.

Digital twin is a method of generating digital assets, which refers to mapping objects in the physical world to the digital world. Digital twin can help build users' digital avatars in the virtual world. Wang et al. [98] develop a method for creating high-quality 3D face avatars with detailed texture maps from a single 2D image. This method utilizes a deep neural network to predict the vertex coordinates of the 3D face model from the input image. To create more lifelike and engaging digital avatars, we should focus on not just physical characteristics but also developing unique personalities and preferences. Sun et al. [100] propose a method for creating digital twin models of personalities by analyzing a user's posting content and liking behavior. The technique involves the use of a multitask learning deep neural network model to predict personality based on two types of data representation.

AIGC is another method of generating digital assets. It can be utilized as a tool for creating variations of images by altering their style. The first approach to receive significant attention in this field is DeepDream [36], a pioneering method developed by Mordvintsev. It can create a distinctive, psychedelic visual style, leading to its use as a form of digital art. The separation between content and style is one of the most iconic milestones in the field of style transfer. Gatys et al. [37] first propose this idea. Their algorithm can manipulate natural images by separating and recombining their content and style. With this algorithm, users can generate new, high-quality images that incorporate the content of any photograph with the style of various famous artworks.

One of the most significant technological advancements driving the current AI art movement is the use of **Generative Adversarial Networks (GANs)**. The use of GANs has resulted in the generation of realistic, vivid images for various types of content, such as StyleGAN [101] and BigGAN [106]. Most GAN models will only learn how to generate images that look like art that already exists, and in a similar way to the NST method, this will not produce anything truly artistic or novel.

However, significant advancements have been made in the field of image generation from text recently. Radford et al. [9] introduce the CLIP model, which is a pre-trained model that has been trained on a large number of image–text pairs from the Internet using contrastive learning. This means that it maximizes the similarity between real image–text pairs and minimizes the similarity between mispairs. In January 2021, based on the CLIP model, DALL-E [102] was proposed by OpenAI, which is a 12-billion-parameter neural-network-based image generation system developed by OpenAI. It is trained on a dataset of text–image pairs and can generate images from textual descriptions. DALL-E can generate a wide range of images, from photorealistic to highly stylized, and can even generate images of objects and scenes that do not exist in the real world.

AI technology has also made breakthroughs in other forms of content generation in recent years, such as **natural language generation (NLG)**. With the rapid development of the deep learning neural network, the current NLG models are mainly based on deep learning neural networks and utilize a vast corpus of human-written text. Graves et al. [107] use recursive neural networks. However, RNNs has the problem of gradient explosion and gradient disappearance. To overcome these challenges, Pavade et al. [11] propose a text generation model based on LSTM. Another option is GRU, which is another extension of the standard RNN and is simpler than LSTM. Many deep generation architectures use GRU to generate text [108]. After that, the wide application of encoder–decoder architecture opened a new chapter. Although the sequence-to-sequence model is originally developed for machine translation, it soon proved that it could improve the performance of NLG tasks. Bowman et al. [109] propose an attempt at the **Variational AutoEncoder (VAE)** text generation model. They use RNNs to capture the general characteristics of sentences in continuous variables, such as theme and style. Later, Dathathri et al. [10] use VAE to learn and generate texts with better discourse structure and narrative flow.

Recently, ChatGPT [110] has achieved great success in large-scale NLP models, which is a typical application of **Pretrained Foundation Models (PFMs)**. ChatGPT is fine-tuned by the Generation Pre-training Transformer model GPT-3.5. It applies convolution and recursion modules to feature extraction based on PFMs and uses autoregressive paradigms to train on large datasets mixed with text and code. It also innovatively combines **reinforcement learning from human feedback (RLHF)**. Due to its exceptional performance, ChatGPT has become a milestone in **Natural Language Generation (NLG)**, moving toward artificial general intelligence.

The pricing of digital assets. The second stage of the life cycle of digital assets involves the pricing and exchange of these assets. AI technology is being used to create sophisticated and accurate models of digital asset prices and develop algorithms that match buyers and sellers. The increasing value of personal data in the era of big data has brought about a significant conflict between the exploitation of this data and the protection of individual privacy. One potential solution to this issue is the development of a personal data market, but determining the appropriate price for an individual's privacy remains a challenging problem. Bauer and Jannach [31] suggest an effective data pricing method. It uses a combination of kernel regression and Bayesian inference, along with a confidence interval estimation algorithm based on the Bootstrap method. This approach is suitable for use with sparse and noisy data. However, this method is not suitable for the scenario of rapid demand change and high price sensitivity.

In a price-sensitive scenario, another approach is proposed by Xu et al. [103], which views data pricing as a reinforcement learning problem for multi-armed bandit machines. However, this method faces a unique challenge with incomplete demand information. To solve this problem, Misra et al. [104] propose a dynamic price experimentation policy based on the extension of multiarmed bandit algorithms with microeconomic choice theory. The proposed approach uses a scalable, distribution-free algorithm to solve the resulting multiarmed bandit problem. Since the data is freely replicable, the current conventional market model is not feasible for data transactions. Agarwal et al. [53] propose a new data marketplace for efficiently buying and selling training data for machine learning tasks. They make two technical contributions to this marketplace: a new concept of fairness for cooperative games involving easily replicable goods and a mechanism for auctioning combinatorial goods that is truthful and regret-free, using Myerson's payment function and the Multiplicative Weights Algorithm.

When it comes to pricing narrowly defined assets in the Web 3.0 world, there is a lot of relevant AI-based research. Zhao [42] present a deep learning framework based on LSTM networks to predict short-term price movements of all cryptocurrencies. While the models presented in this study can accurately predict the movement of Bitcoin prices, they do not provide information on the extent of the price movement. To evaluate the performance of different existing neural-network-based trading strategies, Alessandretti et al. [8] examine the effectiveness of three models in predicting daily cryptocurrency prices for more than 1,000 currencies. Two models employed gradient-boosting decision trees, while the third utilized LSTM RNNs. The results revealed that all three models outperformed a baseline model using simple moving averages, with the LSTM model consistently yielding the highest return on investment.

However, those cryptocurrency price prediction methods rely on the use of past price indexes to forecast future prices and do not take into account the volatile behavior of network entities that may indirectly impact the price. Features contributing to price increases in the Bitcoin and Ethereum networks are explored by Saad et al. [43]. This method analyzes user and network activity that has a significant impact on the prices of these cryptocurrencies and uses machine learning methods to build models that predict prices.

In conclusion, the key role of AI in Web 3.0 digital assets consists of two aspects: (1) efficiently generate high-quality content and (2) accurately predict digital asset prices. We illustrate the irreplaceability of AI for Web 3.0 digital asset circulation through our analysis of existing work.

5.3 Summary and Lessons Learned

In sub-subsection entitled “The Generation of Digital Assets,” we introduce papers mainly including some milestones in the field of generative AI and practical applications of **digital twins (DTs)** in creating digital counterparts of physical objects. While many scholars have described Web 2.0 as a network of **user-generated content (UGC)**, we consider Web 3.0 as a network of both UGC and **AI-generated content (AIGC)**. Web 3.0 is not only a mapping of the real world but also needs a wealth of background information, where some approaches [102, 110] can play an important role. This is how the two methods DT and AIGC, cooperate with each other. DT is responsible for displaying the mapping of the real world, and AIGC is responsible for expanding the information in a broad sense.

Web 3.0 is also a value Internet where users can create, trade, and consume digital assets in Web 3.0. In the first subsection, we focus on the generation of digital assets. In the second subsection, seven related papers are introduced, which cover the pricing of data [31, 103, 104], the trading mechanism of data market [53], and the pricing and trading of encrypted assets [8, 43, 111]. The objective of presenting these papers is essentially to explore one question, how to establish an efficient value circulation system to maximize the use of data, assets, and other means of production.

6 MANAGEMENT LAYER

The management layer is responsible for maintaining the long-term and stable operation of the Web 3.0 ecosystem, which consists of four modules, including interoperability modules, incentive mechanisms, security services, and privacy services. The interoperability module is responsible for communication between different subsystems of the Web 3.0 ecosystem. The incentive mechanisms module incentivizes participants in the Web 3.0 ecosystem to consistently contribute and allows them to receive corresponding rewards. The security module protects the Web 3.0 ecosystem from malicious attacks. The privacy module is responsible for safeguarding user privacy.

However, the management layer also faces some new challenges. Incompatibility between different protocols brings huge obstacles to mutual communication. Also, the lack of central authority makes it challenging to enforce security measures or respond to security threats. The unique capabilities of AI can help address these issues. The optimization algorithms of AI can enhance the efficiency of interoperability between different systems by determining the strategies of transaction processing [112–114]. Moreover, AI models can assist in improving the intelligence and usability of incentive mechanisms, striking a balance between effectiveness and fairness [115, 116]. In addition, the identification and classification capabilities of AI can be used to identify malicious content [12, 61, 117] and abnormal behaviors [118, 119] in Web 3.0, which helps to maintain the credibility and reliability of the content platforms and protect Web 3.0 systems from malicious attacks.

6.1 Interoperability

In the ecosystem of Web 3.0, there are strong barriers and isolation between different blockchain networks, which makes it difficult for seamless data and value exchange across different networks. AI can help address interoperability problems by translating protocols across different systems and optimizing the strategies of side-chain generation, thus making blockchain networks communicate with each other.

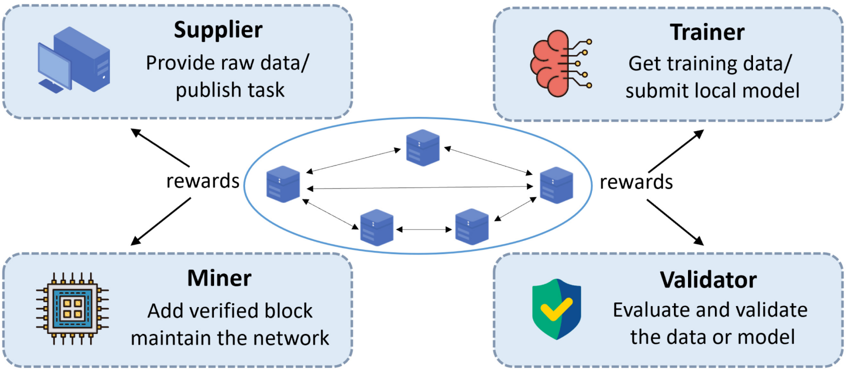
Supplier
Provide raw data/ publish task
Trainer
Get training data/ submit local model
rewards
rewards
Miner
Add verified block maintain the network
Validator
Evaluate and validate the data or model

Fig. 5. A typical AI-assisted incentive mechanism structure in the management layer.

Protocol Incompatibility poses a significant hurdle to interoperability. Each chain may have its own unique protocol, making it difficult for different networks to understand and interpret data and transactions from one another. AI can analyze the structure of various protocols, thus assisting in translating data and transactions across different blockchain systems, enabling seamless communication and interaction among different Web 3.0 networks. Tothfalusi et al. [112] introduce a generic methodology for ML-based translation of data formats and protocols, which can be adapted to the Web 3.0 scenario.

Side chain is also a significant method that enhances Web 3.0 interoperability. AI algorithms can help optimize the allocation of computational resources in sidechains to improve system throughput. For instance, Vairagade and SH [113] use the mixed delegation practical Byzantine fault-tolerant-delegated proof of equity to update the side chain, and the continuous network information analysis is used to improve the **Quality of Service (QoS)**. Using the modified genetic algorithm, this work optimizes the construction of side chains and solves the problem to a certain extent that assets can be stolen by malicious nodes.

It is difficult to directly share data in different Web 3.0 systems. AI can analyze data from various Web 3.0 networks and enable cross-chain data interoperability, in which FL is a popular technology. Kang et al. [114] propose an efficient cross-chain empowered FL framework. This framework realizes cross-chain information communication and heterogeneous blockchain interoperability to meet particularly the scalability and diversity requirements in FL scenarios, which enables intelligence for multi-chain systems.

To conclude, AI has a great impact in terms of interoperability issues in Web 3.0. AI can translate protocols across systems and assist in the generation of side chains, making it efficient to interact across different Web 3.0 systems.

6.2 Incentive Mechanism

The Web 3.0 ecosystem needs to encourage users to participate in community affairs, such as encouraging users to participate in community governance, community decision-making, encouraging blockchain node consensus, node computing, and so forth. Incentive mechanisms involve many aspects. We focus on the incentive of the blockchain consensus mechanism and FL scenario. As shown in Figure 5, it is a scenario diagram of a common incentive mechanism. And the main articles mentioned in Section 6.2 are listed in Table 6.

Blockchain consensus mechanism. The consensus mechanism is an incentive mechanism to encourage nodes to calculate and reach data consensus. Chen et al. [38] propose a novel node selection algorithm based on AI technology, which uses almost complementary information of

Table 6. Research of Incentive Mechanism on AI

Subjects	Refs.	AI Methods	Scenario Oriented	Web 3.0 Tasks
Blockchain Consensus Mechanism	[38]	CNN	Blockchain	An AI-based super node selection algorithm in blockchain networks
	[50]	DL	Blockchain	Consensus mechanism based on machine learning competitions
	[51]	SL	Blockchain-based IoT networks	An outlier-aware consensus protocol
	[120]	FL	Sustainable blockchains	A platform-free proof of FL consensus mechanism
Federated Learning	[121]	DRL and GNN	Wireless federated learning	Toward an automated auction framework for wireless FL services market
	[115]	DRL	Edge ML	An incentive mechanism design-based DRL for efficient edge learning
	[122]	DRL	/	A learning-based incentive mechanism for federated learning
	[116]	Clustering	BFL	A flexible and incentive redesign for BFL

each node and relies on a specially designed convolutional neural network to reach a consensus. To ensure the decentralization and security of the network, the dynamic threshold method is used to obtain super nodes and random nodes.

To reduce the computational waste involved in hash-based problems, several papers discuss the possible solutions that miners' computing power will be used for relatively useful work, such as solving machine learning tasks. Bravo-Marquez et al. [50] introduce WekaCoin, which is a point-to-point cryptocurrency based on a new distributed consensus protocol called **Proof-of-Learning (POLE)**. POLE realizes distributed consensus by ranking machine learning systems for a given task. Miners' computing ability can also be used to solve deep learning training tasks, such as Proof of Federated Learning [120]. To reach a secure and robust consensus in the blockchain-based IoT networks, Salimitari et al. [51] use machine learning to propose a new framework. They introduce an **AI-enabled blockchain (AIBC)** with a two-step consensus protocol, which uses an outlier detection algorithm to reach consensus in the IoT network implemented on the hyper ledger fabric platform.

Federated learning. Incentive mechanism is the key design element of the new FL system, because (1) participating in the FL will lead to the consumption of computing resources and use of network bandwidth and shorten the battery life of customers, and enough rewards can encourage them to tolerate these costs and make contributions, and (2) the worker thread in the FL is independent, and only its owner can determine when, where, and how to participate in the FL. Through different incentive mechanisms, customers will implement different training strategies, which will affect the performance of the final ML model. AI technology can help address the two main challenges in the FL system's incentive mechanism: evaluating the contribution of each customer and recruiting and retaining more customers.

For trading FL services in wireless environments to encourage data owners to participate in FL, Jiao et al. [121] novelly develop an automated DRL-based auction mechanism that is integrated with the **Graph Neural Network (GNN)**. The proposed auction mechanisms can help the FL platform make practical trading strategies to efficiently coordinate data owners to invest their data and computing resources in FL while optimizing the social welfare of the FL services market. In Edge Learning, the existing work mainly focuses on the design of efficient learning algorithms, and few works focus on the design of incentive mechanisms with heterogeneous **edge nodes (ENs)** and network bandwidth uncertainty. An edge learning incentive mechanism based on DRL is proposed by Zhan and Zhang [115]. This mechanism enables the effective learning of optimal pricing strategies by aggregators in dynamic networks, even without prior information about the ENs.

In FL, it is important to measure the contribution of each federal participant fairly and accurately [116, 123]. Such quantification provides a reasonable metric for allocating rewards among federated clients and helps to find malicious participants who may poison the global model. The previous contribution measurement method is based on the enumeration of possible combinations

Table 7. Research of Content Management on AI

Subjects	Refs.	AI Methods	Web 3.0 Tasks	Limits
Malicious Content Detection	[12]	GAN	Movie review spam detection	Poor generality: set feature words manually
	[61]	CNN	Pornography image detection	Model depends on training dataset
	[124]	DL		Not applicable to pictures with low resolution
	[7]	CNN	Child sex abuse detection	The age group detection technology is not mature
Deepfake Detection	[125]	CNN	Detect the deepfake image and video	Compression level and resolution are ignored
	[126]	CNN and CL	Detect the deepfake image	The model ignores low-quality data
	[127]	CNN and SNN	Detect the deepfake video	Not applicable to multi-person video
	[128]	CNN		Poor versatility and low-quality video data is ignored

of federated participants. Their calculation cost increases sharply with the increase in the number of participants or feature dimensions, making them unsuitable for the actual situation. Zhao et al. [123] propose an integrated contribution evaluation method, F-RCCE. This method is based on reinforcement learning, which can accurately evaluate the contribution of each customer's gradient. As the number of clients increases, its time cost almost remains the same.

In summary, considering the establishment of an efficient and robust intelligent incentive mechanism, AI makes a significant contribution. Regarding consensus mechanisms, AI can optimize the node selection process in consensus algorithms, reducing computational costs. In the context of FL, AI algorithms can assist in evaluating the contributions of each participant, enhancing model performance, and incentivizing greater participation.

6.3 Security

Security is one of the key issues for the Web 3.0 system that is more vulnerable to attacks due to its permissionless nature. AI plays a crucial role in security, which is mainly reflected in two aspects: content management and situation awareness. In this section, we will discuss how to apply AI technology to maintain the stable operation of Web 3.0 in these two fields.

Content management. The Web 3.0 ecosystem encourages users to create content, including text, images, and videos. However, malicious content will have a serious impact on the Web 3.0 ecosystem, and AI is of great significance in the content management of the Web 3.0 ecosystem. We divide the content management of Web 3.0 into two fields: malicious content detection (real but illegal) and deepfake content detection (fake). The main articles on content management are listed in Table 7.

The first field of content management is malicious content detection. We divide it into malicious text, malicious images, and malicious videos according to the form of content. AI technology can provide great help in malicious content detection. Junk comment is a kind of malicious text that can mislead users in online comments. Researchers use methods based on AI technology to detect junk comments [12, 117]. A multimodal fake review detection model called BAM (BERT + Attention + MLP) is proposed by Jian et al. [117]. This model utilizes neural networks and multimodal fusion technology to effectively recognize and detect fake reviews.

In terms of malicious image and video detection, Moreira et al. [61] contribute a pornographic dataset (PEDA 376K) and propose a deep learning architecture for training on this dataset, which has excellent performance. A deep learning solution ensemble is proposed by Pandey et al. [124]. The framework consists of a MobileNetV3 classifier and SSD with a MobileNetV3 feature extractor. This ensemble not only detects unsafe body parts but also provides localized information about the human body. To detect child sexual abuse images, Gangwar et al. [7] propose a deep CNN architecture with a novel attention mechanism and metric learning, denoted as AttM-CNN. For malicious video detection, Wu et al. [129] first release a large-scale multi-scene dataset called XD

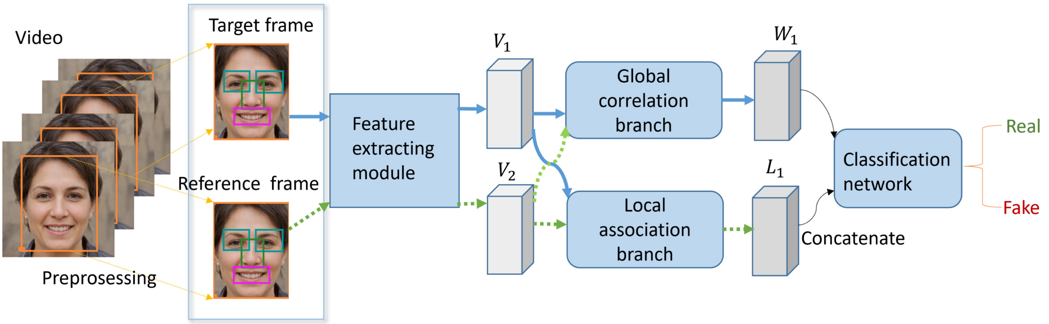

Fig. 6. Technology roadmap of deepfake video detection. Utilizing the inconsistency information between adjacent frames to detect deepfake video [128] .

Violence and propose a neural network with three parallel branches to capture different relationships between video clips and integrate features.

The second field of content management is deepfake detection. Deepfake content mainly includes images and videos. AI technology plays an important role in deepfake detection. An effective solution is to use image inconsistency to detect deepfake images. Li et al. [125] creatively propose a new **Patch and Pair Convolutional Neural Network (PPCNN)** architecture to detect deepfakes. This dual-branch learning framework is the first to learn the difference between real and false face patches and the second to capture the inconsistency between the facial and the nonfacial regions. Zhao et al. [126] propose a new representation learning approach, called **Pair-wise Self-consistency Learning (PCL)**. This approach leverages the cue of source feature inconsistency within the forged image to accurately identify deepfake content.

Deepfake video detection is also a concern for researchers. Audiovisual joint detection is a popular method of deepfake video detection. Mittal et al. [127] propose a new method for detecting forgery or alterations in input videos. This method incorporates audio (speech) and video (face) modes, along with perceptible emotional features extracted from these modes. To simulate these multimodal features and perceived emotions, Siamese network-based architecture is employed as part of the learning method.

Hu et al. [128] propose a new **Dynamic Inconsistency-aware Network (DIANet)** for DeepFake video detection by utilizing the inconsistency information between adjacent frames. As shown in Figure 6, DIANet consists of three modules: Feature Extraction Module, **Cross-Reference Module (CRM)**, and Classification Network. DIANet takes a pair of frames as input and obtains their feature representation through the Feature Extraction module. Then the proposed CRM is used to capture the global and local inconsistencies between adjacent frames. Finally, the global and local inter-frame inconsistencies are combined and sent to the classification network. The model generalizes well on videos of low quality and unseen manipulation techniques. At present, most algorithms are trained to detect specific fake methods. Therefore, these methods show poor generalization in different types of face operations, from face swapping to facial reenactment. A new method is proposed by Cozzolino et al. [130] to learn the temporal facial features associated with a person's speech movements. This is achieved through the combination of measurement learning and antagonistic training strategies. One of the key advantages of this method is its reliance on real video training alone. Furthermore, the incorporation of advanced semantic features enhances its robustness against various forms of extensive and destructive post-processing.

Situation awareness. The operation of Web 3.0 depends on the safe and stable cyberspace security environment, so situation awareness of network security is essential. Artificial intelligence

Table 8. Research of Situation Awareness Works in Web 3.0

Subjects	Refs.	AI Methods	Utilized Feature	Web 3.0 Tasks
Transaction Entity Recognition	[142]	Clustering	Transaction inputs, amount, and time	Transaction address association analysis
	[46]	GCN	Relationship between account and contract	Transaction account type identification
	[143]	GNN	Transaction amount and time	Transaction account identification
	[144]	PUL	Transaction order and amount	Transaction data labeling
Malicious Transaction Identification	[47]	GCN	Transactions between accounts	Phishing scams detection
	[119]	SVM	Transaction amount and timestamp	Phishing scams detection
	[118]	XGBoost	Operation codes of the smart contracts	Ponzi contract identification
Network Behavior Perception	[48]	GCN	Graph representation of traffic interaction features	Dapp access behavior identification
	[34]	RF	Cumulative downlink packet length	Web page access behavior recognition
	[134]	MC	State transition in SSL/TLS handshake	Web 3.0 application classification
	[133]	CNN	Sequence of unidirectional burst lengths	Web 3.0 website identification
	[135]	CNN	Packet round-trip time	Video quality detection for network users

plays a crucial role in network situation awareness, which is mainly reflected in two aspects: malicious transaction identification and network behavior recognition. The main articles on situation awareness are listed in Table 8.

The first part of security services is malicious transaction identification. Malicious asset trading behavior will have a bad impact on the Web 3.0 ecosystem, and AI technology can effectively improve the accuracy of identifying malicious trading behavior. Common malicious transactions in Web 3.0 include Ponzi schemes, phishing websites, and money laundering. In research on identifying Ponzi schemes, Chen et al. [118] extract features from user accounts and operation codes of the smart contracts and then build a classification model through the XGBoost algorithm to detect Ponzi schemes implemented as smart contracts. For phishing website detection, researchers extract features from the labeled transaction dataset that can mark phishing addresses and then use ML [119] or GCN [47] to transform the phishing site detection task into a classification problem based on the specific structure of the transaction features. In terms of identifying money laundering transactions, GNNs have a significant advantage in analyzing graph-structure-based transaction data [131]. And by enhancing the edge features of the trading graph [132], GCN can also be used to identify money laundering accounts.

The second part of security services is network behavior recognition. Since many Web 3.0 applications use encrypted communication protocols such as SSL/TLS, most of the behavior traffic in the network appears in the form of ciphertext, which makes the key information contained in the plaintext invisible to regulators. AI has been widely used in network behavior perception of Web 3.0, including website fingerprinting [34, 133], application traffic classification [48, 134], and video traffic classification [135].

In constructing web page fingerprints, Shen et al. [34] construct a web fingerprint classifier using the random forest algorithm to identify web traffic by extracting packet length features. To fully extract the traffic features, Shen et al. [133] train a fine-grained website fingerprint classifier with CNN to achieve better results. In addition to being used to train website fingerprint classifiers, CNNs are also used to train video traffic classifiers to detect network video quality [135]. In terms of application traffic classification, Shen et al. [134] use a second-order Markov model to construct a web application classifier to achieve the classification of encrypted web application traffic. Based on this, GNNs are used to train classifiers based on traffic interaction graphs.

In conclusion, AI plays a crucial role in establishing a secure and stable Web 3.0 system. Regarding content management, AI can detect various forms of malicious and illegal content, as well as identify false and fabricated information. In terms of situational awareness, AI can assist in recognizing abnormal and malicious behavior within the Web 3.0 ecosystem, identifying malicious traffic, and tracking and tracing anomalous activities to maintain cybersecurity.

6.4 Privacy

Privacy is one of the most significant concerns of Web 3.0 itself. However, with the widespread application of AI technology in the Web 3.0 ecosystem, privacy has become an increasingly important issue. The introduction of AI in Web 3.0 brings challenges to privacy, particularly in scenarios involving distributed data collection, distributed machine learning, and collaborative learning. In these scenarios, AI models inevitably require sensitive data from organizations or individuals as learning samples, which raises concerns about privacy attacks during this process. Current privacy attacks on a distributed learning system include membership inference attacks, attribute inference attacks, and data reconstruction attacks.

Membership inference attacks occur when the attacker aims to predict whether a data sample is used to train the target machine learning model. By querying the model and collecting a sufficient number of high-confidence records, the attacker constructs their own dataset to train a set of shadow models. These shadow models are then used to determine whether a given data record is part of the training data used by the target model. In terms of defending against membership inference attacks, there are several robust privacy-preserving measures such as differential privacy and secure multi-party computation. Here we focus on how to apply them in Web 3.0 scenarios. FedServing, designed by Weng et al. [136], is a federated prediction service framework. This framework aggregates the predictions inside the **Trusted Execution Environment (TEE)** to solve the problem of privacy leakage and propose an incentive mechanism to improve the accuracy of the prediction. However, privacy risks in neural network pruning have not been considered in previous works. The method proposed by Yuan and Zhang [137] is the first-ever defending method against self-attention membership inference attacks focusing on pruning neural networks. This new defense mechanism protects the pruning process by mitigating the prediction divergence based on KL divergence distance.

Attribute inference attacks refer to the attackers using machine learning classifiers to infer the target user's private attributes from the target user's public dataset. In terms of defending against attribute inference attacks, there are already several reliable solutions. In distributed data collection scenarios, most existing systems are based on third-party platforms, which cannot guarantee that the center server is completely trustworthy, secure, and private. An et al. [138] integrate blockchain into this scenario and design a privacy-protection quality control mechanism. This mechanism can achieve verification without any third-party arbiter so that various information and true values of participants will not be exposed. Simultaneously, in recommendation systems, user privacy has become the hardest-hit area of attribute inference attacks. Liu et al. [139] design GERAI, which combines the information perturbation mechanism of differential privacy and the recommendation capability of graph convolutional networks. This method is a two-stage privacy-preserving paradigm through local differential privacy to protect the privacy of users' sensitive features and the model optimization process.

Data reconstruction attacks mean that the attackers reconstruct the original training data by analyzing the output of the model or other information. In terms of defending against data reconstruction attacks, there are several works that can be used in distributed systems. Regarding the scenario of jointly completing a certain task by leveraging distributed learning, a defense called Soteria [140] is proposed, which perturbs data representation to severely degrade the quality of reconstructed data while maintaining FL performance, significantly improving the privacy of the FL system. However, it has not yet been systematically evaluated how robust FL-based NIDSs are against attacks. For the application of deep learning in anomaly-based network intrusion detection systems, a new privacy evaluation indicator is proposed by Chen et al. [141], and a new defense strategy named FedDef is also introduced. It achieves a higher degree of privacy protection and model accuracy than ever before by minimizing gradient distance and maximizing input distance.

As AI and Web 3.0 become more deeply integrated, privacy becomes an increasingly serious challenge. Scenarios involving distributed data collection, distributed machine learning, and collaborative learning are particularly vulnerable to privacy attacks, including member inference attacks, attribute inference attacks, and data reconstruction attacks. Researchers have proposed defense mechanisms such as differential privacy, secure multi-party computation, blockchain integration, and perturbation techniques to mitigate these attacks and protect user privacy in Web 3.0 scenarios.

6.5 Summary and Lessons Learned

In this section, we introduce existing studies focusing on AI technology applied in Web 3.0 ecological management, including interoperability, incentive mechanisms, and security and privacy services. The Web 3.0 ecosystem is subject to various anomalies in its operation. For example, users may create vulgar digital works to circulate, leading to ecosystem pollution. Due to the greater autonomy and anonymity of Web 3.0 users, it is costly and inefficient to detect these user anomalies manually. AI technology plays a huge role in assisting community administrators with anomaly detection and decision-making. However, because of the variety of unforeseen anomalies that can occur in the ecosystem, it is relatively rudimentary to train AI models to deal with these anomalies using labeled data.

We summarize that data privacy breaches, poor model generalization, and lack of labeled data are three main dilemmas of Web 3.0 ecological management based on AI technology. First, using privacy-preserving techniques such as FL, homomorphic encryption, and differential privacy can effectively avoid the privacy leakage problem in joint data training. Second, due to the dynamics and diversity of abnormal community behavior, the model should be lightly trained based on a small amount of anomalous behavior data, allowing the features and parameters of the model to be optimized and fine-tuned promptly. Lastly, combining unsupervised learning and reinforcement learning, which are less dependent on label data, can effectively improve the performance of the auxiliary management model.

7 APPLICATION LAYER

Web 3.0 is widely applied in finance, healthcare, and game entertainment, demonstrating numerous successful cases in industry, business, or academia. In this section, we illustrate some applications and discuss the current situation of these applications and how to integrate with AI technology to provide more solid support for Web 3.0. The main articles mentioned in Section 7 are listed in Table 9.

7.1 Finance

Web 3.0 has a wide range of applications in the financial field. The integration of AI is mainly used to predict the price of digital assets and improve the efficiency and security of Defi, or smart contracts. We have already discussed digital asset price forecasting in Section 5.2. In this section, we will focus on vulnerability detection and efficiency improvement of Defi, or smart contracts.

Defi and smart contract. Over the years, more and more projects have focused on this field and gradually evolved the concept of Defi. Defi, in short, is to make full use of blockchain technology

Table 9. Research on AI-based Applications in Web 3.0

Subject	Ref.	AI Methods	Solutions	Web 3.0 tasks
Finance	[62]	DL	AI-based systematic modular framework	Detecting smart contract vulnerabilities
	[63]	LSTM	Applying short- and long-term memory model	Learning vulnerabilities in sequence
	[64]	GNNs	Using graph neural networks for detection	Smart contract vulnerability analysis
Metaverse	[67]	DRL	Visual deep learning	Novel virtual environment establishment
	[68]	FL	Federated-learning-based mobile edge computing	Proving computational efficiency of AR applications
	[147]	RL	Training virtual characters to move participants	Precomputing avatar behavior
	[148]	CNNs	Overlay food segmentation image inferred by CNNs	Improving the presence of users eating in metaverse
Healthcare	[65]	ANN	AI enabled and blockchain driven	Medical healthcare system for COVID-19
	[149]	DCNNs	An intermediate fusion framework	Physical activity recognition

(including smart contracts, decentralized asset custody, etc.) to replace all the intermediary roles in traditional financial services by code, to maximize the efficiency of financial services and minimize the cost. We will discuss the current situation of existing applications and focus on some smart contracts based on AI technology.

There are already many successful practices in the business world that apply AI to the Defi field. Chainalysis [145] focuses on applying deep learning to detect and prevent fraud or illegal activities on the blockchain. It collects data from public blockchain networks and uses some deep learning techniques to detect potential fraudulent news and abnormal transactions and provide early warning to individuals or organizations when they may be exposed to fraud. Augur [146] is a decentralized prediction market platform that uses AI techniques to predict the trend of events based on social media, news articles, and historical data and give relevant investment suggestions to its users.

In academia, there are many studies focusing on using AI technology to improve the security and efficiency of Defi. Some researchers have applied it to the detection of smart contract vulnerabilities. For instance, Tann et al. [63] apply the LSTM model to learn vulnerabilities in sequence. However, these methods do not consider the impact of local code vulnerabilities on the overall code, which reduces the interpretability of these methods. To solve the problem of interpretation, Zhuang et al. [64] explore the use of graph neural networks for smart contract vulnerability detection. They construct a contract graph to represent the syntax and semantic structure of smart contract functions and propose a **Time Message Propagation (TMP)** network to detect vulnerabilities. Yu et al. [62] propose *DeeSCVHounter*. This method is the first systematic modular framework for detecting smart contract vulnerabilities based on deep learning, which focuses on two types of smart contract vulnerabilities: reentry and time dependence. Their main innovation is to propose a novel **Vulnerability Candidate Slice (VCS)** concept to help the model capture the key points of vulnerabilities.

7.2 Metaverse

The metaverse is one of the important applications of Web 3.0 in the field of games and entertainment. It is the integration of Web 3.0 and technologies from other fields such as **virtual reality (VR)** and **augmented reality (AR)**. There are already several successful implementations in business and industry that integrate AI technology with the metaverse. AI Arena [150] is a game that combines Web 3.0 and AI technology. Players can purchase and train NFTs that support AI and compete with other users. Coincidentally, Chaos Box [151] is an AI engine based on DRL technology. The Chaos Box algorithm can analyze real-time input from players and dynamically generate NPC interactive responses and new stories. Without any scripts, players can control the behavioral logic of NPCs in the game, allowing them to spontaneously produce very intelligent behaviors. AI supports the metaverse mainly in two aspects: environment establishment and character's behavior. Above we talk about some examples of applications in the business world. In the following, we will focus on how AI plays a role in technology.

Environment establishment. The users of the metaverse, objects, or transactions in the physical world interact with the metaverse, constantly developing and persistently representing the structure, behavior, and context of unique physical assets in the virtual world. With the breakthrough of digital transformation, the latest trend in each industry is to build digital twins, and the ultimate goal is to use them throughout the asset life cycle through real-time data.

The virtual world of the metaverse has produced a large number of data, which makes the digital twin based on deep learning crucial. Aiming at the shortcomings of existing works such as small scenes or limited interaction with objects, Lai et al. [67] propose a novel visual depth learning virtual environment to provide large-scale and diversified indoor and outdoor scenes. AR devices can provide people with an immersive interactive experience, and their applications are sensitive to latency. Therefore, Chen et al. [68] solve the computational efficiency of AR applications, low-latency object recognition, and classification problems by combining the mobile edge computing paradigm with FL. In addition to the above, AI can help make virtual characters more intelligent. Kastanis and Slater [147] propose a reinforcement learning method used to train virtual characters to move participants to the designated position.

Character's behavior. The character's behavior in the metaverse can be the behavior characteristics in the game or the simulation behavior in VR. In the early stage, Lugrin and Cavazza [152] propose a method for the AI-based simulation of object behavior so that interactive narrative can feature the physical environment inhabited by the player character as an actor. The prototype based on the top of the Unreal Tournament game engine relies on a causal engine, which essentially bypasses the native physics engine to generate alternative consequences to player interventions. Then, to allow users to eat naturally in the **Virtual Environment (VE)**, Nakano et al. [148] propose Ukemochi to improve the presence of users eating in the metaverse. Ukemochi seamlessly overlays a food segmentation image inferred by deep neural networks on a VE. Ukemochi can be used simultaneously as a VE created with the OpenVR API and can be easily deployed for the metaverse. Recently, some users protect their identities by arbitrarily changing their avatars. However, Meng et al. [153] come up with a way to de-anonymize fake VR avatars called AvatarHunter. It achieves de-anonymization attacks by recording videos of multiple views in a VR scene, collecting the gait information of the victim's avatar and preserving the avatar's motion characteristics.

7.3 Healthcare

The applications of Web 3.0 in healthcare are mainly in the field of **Electronic Health Record (EHR)** management. The EHR management in Web 3.0 integrates blockchain technology and AI and better protects the privacy and security of patient data in medical services than before.

EHR management. The records in the traditional EHR management system are stored on a cloud server through the wireless communication channel, and there are risks of replay attacks, man-in-the-middle attacks, information leakage, and other security threats. Blockchain stores the data as a transaction with characteristics such as trust and immutability, which also eliminates the intermediaries and a centralized dependence on transaction control. Fusing blockchain and EHR management is a better solution for the security threats and the framework of EHR management system based on blockchain as shown in Figure 7. In the business world, there have been some early attempts to combine AI with Web 3.0. Medibloc [154] provides decentralized medical data services. On the one hand, it uses blockchain to ensure data security. On the other hand, it uses AI technology to provide early high-risk warnings for some diseases based on data.

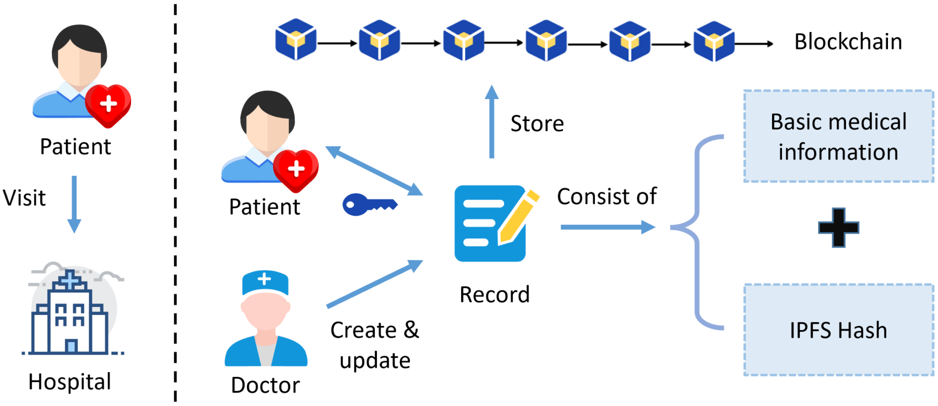

Fig. 7. The framework of EHR management system based on blockchain.

In academia, one of the solutions given by Vora et al. [69] is called BHEEM, which is a blockchain-based solution to store and efficiently transfer EHRs. The above-described approaches in the literature failed to realize the significance of AI technology for EHR security, privacy, and accessibility. Mamoshina et al. [155] propose a blockchain-based decentralized model that enables users to access their data in an AI-moderated healthcare data exchange. Another study is conducted by Krittanawong et al. [156] on AI and blockchain integration can accelerate by greatly increasing the availability of data for AI training and development, being able to share proprietary AI algorithms for generalization, decentralizing databases of different vendors or health systems, and incentivizing solutions that improve outcomes over those that do not. The integration of blockchain with AI could advance the goal of personalized cardiovascular medicine. Then, Witowski et al. [157] propose MarkIt, a blockchain and AI-based platform for collaborative annotation of medical imaging datasets. The platform enables radiologists to collaboratively annotate **Digital Imaging and Communications in Medicine (DICOM)** and non-DICOM images in order to create ML datasets and annotate them for classification and object detection tasks in an efficient manner.

7.4 Summary and Lessons Learned

As mentioned earlier, we have discussed the details of AI and Web 3.0 applications in the fields of finance, the metaverse, and healthcare and the impact of AI on the performance of these applications. Although AI technology has not been fully integrated with these Web 3.0 applications, researchers have also tried to study AI blockchain technology and given some inspiring examples. The integration of AI and blockchain, namely blockchain intelligence and intelligent blockchain, is worth exploring due to their close interaction. With the integration of AI and blockchain, distributed AI can process and execute the analysis or decision of trusted data without any support from a trusted third party. We believe that blockchain encourages AI to reach an unprecedented level in the context of various fields in Web 3.0.

8 CHALLENGES AND FUTURE RESEARCH DIRECTIONS

In this section, we discuss the impact that the introduction of AI will have on Web 3.0, as well as the challenges this field may face and the future development direction. The relationship between AI and Web 3.0 can be summarized by two keywords, namely efficiency and fairness. AI can play a significant role in the efficiency issues faced by Web 3.0, and the rapid growth brought about by AI requires Web 3.0 to ensure fairness. AI and Web 3.0 jointly create a world with rapid economic growth and equal opportunities for all individuals. We will then explain in detail the impacts, possible challenges, and future development directions of AI at each layer.

8.1 Infrastructure layer

The challenges at the infrastructure layer can be summarized in two aspects. One is the performance challenge, namely the scalability problem, and the other is the challenge of security. AI brings intelligence to the infrastructure layer. The details are introduced as follows.

Scalability. Scalability in Web 3.0 refers to the ability of a public blockchain system to process transactions, which is the key challenge faced by the Web 3.0 infrastructure layer and the primary obstacle that today's public blockchain systems are difficult to apply to practical scenarios. The specifics of the scalability problem are as follows. (1) transactions involve blockchain-related operations, which brings large processing costs; (2) on-chain data needs to be backed up at each node, which brings huge storage overhead, and a considerable number of nodes cannot afford this overhead; and (3) due to the excessive amount of data in the network, Web 3.0 applications have certain data congestion and transmission delay compared to centralized applications, which is difficult to apply to real-time systems.

As mentioned above, AI can make the system intelligent through learning algorithms and minimize the system overhead by optimizing node behavior, system resource allocation, and other strategies. AI also plays a role in assisting optimization in scenarios such as blockchain sharding and cross-chain, effectively alleviating scalability problems. It also predicts the status of nodes to improve the security and availability of the system.

Security. In Web 3.0, the security problem is also worth attention. The security problems of the infrastructure layer mainly include (1) intrusion and attack by malicious entities and (2) privacy of user data. (Other aspects like contract security, content security, etc., are outside the scope of this section.) This poses some challenges to the design of the infrastructure layer. AI can solve the above problems to a large extent. The learning algorithm can be used to predict reliable nodes in the network, detect abnormal behaviors, and identify intrusion behaviors of malicious entities. However, the model needs to use the user's data when training and the current technology cannot provide strong privacy protection under the condition of guaranteeing performance. This requires the maturity of related privacy protection technologies, such as differential privacy, secure multiparty computation, and so forth.

8.2 Interface Layer

The challenges of the interface layer can be illustrated from two aspects, digital identity and digital assets. The main problem in digital identity is the usability of the identity system. The main problem in digital assets is that the quality of AI-generated content still needs to be improved. AI can bring efficiency and personalized services to the interface layer.

Digital ID. At present, the high threshold of the identity system is one of the major problems. The public–private key system is currently the most widely used. Users need to remember the long and complex private key. Once forgotten, it cannot be retrieved. And users may also manage multiple addresses at the same time, which greatly increases the management cost. At present, the possible development direction is the private key recovery technology based on social relations and non-password technology. These methods will greatly reduce the cost of user identity management.

AI-based biometric authentication and behavioral authentication have shown their prospects as a means of identity verification. However, these methods are vulnerable to various types of attacks, including malware, imitation, simulation, deception, replay, statistics, algorithms, and robot attacks. The combination of multiple types of biometrics (i.e., multi-mode authentication) can improve security and provide more reliable authentication. Many studies have shown that multi-modal biometric methods have advantages over single biometric methods.

Digital assets. In terms of content generation, the main challenges currently focus on the field of image generation. It is difficult for AI to correctly depict spatial and physical relationships in generating images. For example, almost all AI can't draw a mirror well, because the image inside and outside the mirror needs optical knowledge, and the AI model is based on statistics and does not understand optics. Similarly, the geometry of AI painting is relatively bad. A typical example is that you will find that the wheels painted by AI are not too round. Another example is that the details of transparent-glass glasses painted by AI are not correct. AI painting is independent of each other. It is difficult for AI to draw a complete set of works, such as a storytelling comic book with complex character relationships. However, content generation based on large-scale models is developing very rapidly, and these challenges are expected to be solved in the near future.

8.3 Management Layer

Although AI technologies can help Web 3.0 administrators better maintain order in their communities, there are still significant challenges as the Web 3.0 ecosystem matures and evolves. These challenges are specific to dataset construction, personalized incentive mechanisms, and the performance of AI algorithms. Meanwhile, these challenges also point the way for the development of management technologies.

Interoperability. In terms of interoperability, although there have been many attempts at cross-chain bridges and middleware in the existing Web 3.0 ecosystem, there are still issues of efficiency and usability. Web 3.0 still lacks a unified and highly available interoperable operating system. Meanwhile, cross-chain bridges are currently the places with the highest security risks in Web 3.0, where code vulnerabilities can cause huge property losses. The combination of AI will be the visible future development direction. First of all, it can establish intelligent middleware and API management systems, while helping to establish adaptive systems and improve the robustness of the system. In addition, AI plays a huge role in automated security and privacy protection, helping to detect the security and integrity of code and reducing the risk of property damage.

Incentive mechanism. The incentive mechanism should unite benefit-sharing members in the blockchain-based trustless environment and encourage them to effectively interact and collaborate around common goals according to their information, resources, goals, and risk appetite. The incentives in Web 3.0 can be divided into transferable incentives and non-transferable incentives. Transferable incentives are mainly economic incentives in the form of fungible tokens or NFTs. Nontransferable incentives mainly refer to noneconomic incentives, including reputation, belief, and knowledge [94]. How to combine various incentive measures with AI techniques and design appropriate mechanisms to meet the specific needs of each type of member and the common goal of cooperation is a major challenge for incentive mechanisms in Web 3.0. When designing an appropriate incentive mechanism for users, measurability and personalization are particularly important, because the user's personal needs and optimization objectives largely affect the effectiveness of the incentive mechanism, and the needs and objectives vary from person to person. Therefore, the mixed incentive mechanism, which is mainly based on transferable incentives and supplemented by non-transferable incentives, can be used to quantify human contributions to the cooperation task and then allocate reputation, certificates, tokens, governance rights, and so forth. AI plays an important role in this process, which can implement more effective and personalized incentive models by analyzing user behavior, preferences, and interactions.

Security. The discussion of security can be divided into two parts. The first part is content management. The introduction of AI provides strong support for Web 3.0 content security, but it also brings impacts and challenges. The common seesaw nature between the generation method and the forensics method makes the deepfake detection face many problems. The booming media manipulation techniques such as deepfake can generate more and more authentic and diversified forged data, and the potential forged types are usually unknown in real scenes. So a media forensics algorithm should have good generalization ability. The multimedia data such as images and videos spread on the network often undergo some post-processing, which makes the performance of the forensics model decline, bringing serious challenges to forgery detection. In addition, malicious users may deliberately impose invisible disturbance on forged data to deceive detection tools. Therefore, manipulation detectors should be robust to common distortion algorithms. Although DNN has strong discrimination ability, it lacks interpretability, so the judgment based on the neural network is difficult to accept in court and other serious occasions. However, the popular trend of deepfake detection methods is still based on deep learning, so it is important to improve the interpretability and credibility of these methods.

The second part is situation awareness. The digital asset transaction dataset is a crucial component for situation awareness, as high-quality datasets can play an essential role in training. The construction of digital asset transaction datasets is a significant challenge in the current supervision of digital asset transactions. It is difficult to obtain digital asset transaction datasets with undisputed ground truth. Currently, two main methods are used in the literature to construct ground truth. We refer to a straightforward way to use an interface provided by a third-party service website to obtain the labeled data directly. This method is relatively simple, but it is often limited by the access restrictions of the third-party website, making it inefficient to obtain. Meanwhile, the labeled data provided by the third-party website has an intense lag time, and thus the researchers cannot access the latest labeled data promptly. Another method is for researchers to create digital asset transactions directly, allowing direct access to the data tags, but this method is extremely costly.

Privacy. The nature of Web 3.0 emphasizes the privacy protection of ordinary users, but it is not a place outside the law. The behavior of criminals who take advantage of the anonymity feature still needs to be cracked down on, which brings about how to strike a balance between privacy protection and regulatory friendliness in Web 3.0. In addition, as AI becomes more and more widely used in the Web 3.0 ecosystem, data leakage will also become an important privacy challenge. These are the two major challenges currently facing the Web 3.0 privacy field. Zero-knowledge-proof technology has huge potential in this field. On the one hand, it can ensure the credibility and traceability of data, and on the other hand, it cannot leak critical private information. For the introduction of AI, differential privacy, homomorphic encryption, and integrated blockchain are also very promising solutions at present.

8.4 Application Layer

We have described some frontier applications of Web 3.0, covering the fields of finance, the metaverse, and healthcare, and given some examples of the combination of Web 3.0 and AI. We will continue to describe the technical challenges and future research directions in these three fields.

Finance. Although blockchain and smart contract research have made significant progress, blockchain research also faces a well-known trilemma, which makes it difficult to create a decentralized, scalable, and secure blockchain. Meanwhile, smart contracts at this stage are usually simple and automated contracts, which can only passively respond to predefined rules but cannot actively adapt to complex and dynamic environments. At present, AI technology has not been widely used in the financial field of Web 3.0. Because Defi itself cannot be separated from smart contracts, if its application in the financial field wants to be further improved to gain more users' attention, AI technology is a new solution to the efficiency of smart contracts and privacy protection issues. AI and blockchain are mutually beneficial. We believe that AI-powered smart contracts have the potential to optimize energy consumption, enhance mining efficiency, improve blockchain scalability, and enable fraud detection in the future.

Metaverse. AI and blockchain are the basic technologies of the metaverse. The breakthrough of AI technology, especially deep learning, has made great progress in the academic and industrial circles in the field of the metaverse. However, the existing deep learning model has a large number of parameters, which brings a heavy burden to mobile devices with limited resources to deploy learning-based applications. However, current AI technology is still limited to the stage that requires humans to instruct models to perform specific tasks, rather than being able to learn automatically. Most learning tasks are only applicable to closed static environments with poor robustness and poor interpretability.Secondly, there are blockchain-related issues, such as whether the existing real-world NFT platform can adapt to the high transaction volme in the metaverse and whether the metaverse needs a new blockchain platform and a new consensus mechanism, all of which deserve our deep consideration. In addition, a natural problem is how to ensure the security and privacy in the metaverse, which may mean the violation of their privacy, potential identity theft, and other types of fraud. In the future, solving these problems of the metaverse is crucial for its development.

Healthcare. At present, some Web 3.0 applications in the medical field combine AI technology and blockchain. The current challenges faced by Web 3.0 applications in the medical field center on two main two aspects. On the one hand, the privacy of user data in the EHR management system cannot be adequately guaranteed, especially in the case of the COVID-19 pandemic. On the other hand, medical services in the metaverse are still in the initial stage. AI technology has provided a great promotion for VR, but there are many medical services in real life that cannot be realized in the metaverse at present. We believe that in future work, researchers can pay attention to the flexible application of ML in the EHR management system (especially FL) to better protect the privacy of users' medical records. In addition, we also expect more medical services in the metaverse (such as online consultation, online surgery, etc.) to emerge in the future.

9 CONCLUSION

This article surveys the application of AI technology in Web 3.0. Before starting the introduction of the specific studies, we review the evolutionary history of the Web and the current development status of Web 3.0. Based on sufficient investigation, we give our understanding of Web 3.0 and construct an architecture of the Web 3.0 ecosystem, including the infrastructure layer, interface layer, management layer, and application layer.

Through research on the major challenges currently faced by Web 3.0, we find that AI technology provides potential solutions to solve the difficulties encountered in Web 3.0. Specifically, at the infrastructure layer, AI algorithms bring intelligent strategies to the distributed data management system in the Web 3.0 ecosystem, providing new solutions to balance between efficiency and decentralization in Web 3.0. At the interface layer, emerging content generation technology plays a huge role in generating digital assets, while traditional learning algorithms can also improve the efficiency and accuracy of asset pricing. At the management level, AI technology can help optimize incentive mechanisms and provide security and privacy guarantees for Web 3.0. At the application layer, we investigate the current successful implementation of integrating AI and Web 3.0 in the fields of finance, entertainment, and medical care in academia and business circles. Finally, we discuss challenges and future directions, providing new ideas for developing innovative approaches.

In conclusion, with the rapid development of Web 3.0 technology, the integration of AI technology will be an unstoppable trend. AI can play a major role in the efficiency issues faced by Web 3.0. The rapid growth brought about by AI requires Web 3.0 to ensure fairness and jointly create a world with rapid economic growth and full and equal opportunities for everyone. In the end, we hope that this survey can provide a comprehensive reference for scholars and industry readers who are interested in the application of AI technology in Web 3.0.

REFERENCES

[1] Messari Research. Web3: In a nutshell. [n.d.] Retrieved September 10, 2021 from https://eshita.mirror.xyz/H5bNIXATsWUv_QbbEz6lckYcgAa2rhXEPDRkecOlCOI

[2] Yao Qian. 2022. Web3. 0: A new generation of Internet that is approaching gradually. *China Finance*.

[3] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*.

[4] Vitalik Buterin. 2014. A next-generation smart contract and decentralized application platform. *White Paper* 3, 37 (2014), 2–1.

[5] Ian Grigg. 2017. Eos-an introduction. White Paper. https://whitepaperdatabase.com/eos-whitepaper

[6] nostr. [n.d.] https://nostr.com/

[7] Abhishek Gangwar, Víctor González-Castro, Enrique Alegre, and Eduardo Fidalgo. 2021. AttM-CNN: Attention and metric learning based CNN for pornography, age and Child Sexual Abuse (CSA) Detection in images. *Neurocomputing* 445 (2021), 81–104.

[8] Laura Alessandretti, Abeer ElBahrawy, Luca Maria Aiello, and Andrea Baronchelli. 2018. Anticipating cryptocurrency prices using machine learning. *Complexity* 2018 (2018), 1–16.

[9] Alec Radford, Jong Wook Kim, Chris Hallacy, Aditya Ramesh, Gabriel Goh, Sandhini Agarwal, Girish Sastry, Amanda Askell, Pamela Mishkin, Jack Clark, et al. 2021. Learning transferable visual models from natural language supervision. In *International Conference on Machine Learning*. PMLR, 8748–8763.

[10] Sumanth Dathathri, Andrea Madotto, Janice Lan, Jane Hung, Eric Frank, Piero Molino, Jason Yosinski, and Rosanne Liu. 2019. Plug and play language models: A simple approach to controlled text generation. *arXiv preprint arXiv:1912.02164* (2019).

[11] Dipti Pawade, A. Sakhapara, Mansi Jain, and Neha Jain. 2018. Story scrambler-automatic text generation using word level RNN-LSTM. *International Journal of Information Technology and Computer Science (IJITCS)* 10, 6 (2018), 44–53.

[12] Yuan Gao, Maoguo Gong, Yu Xie, and Alex Kai Qin. 2020. An attention-based unsupervised adversarial model for movie review spam detection. *IEEE Transactions on Multimedia* 23 (2020), 784–796.

[13] Yuntao Wang, Zhou Su, Ning Zhang, Rui Xing, Dongxiao Liu, Tom H. Luan, and Xuemin Shen. 2022. A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials* 25, 1 (2022), 319–352.

[14] Qinglin Yang, Yetong Zhao, Huawei Huang, Zehui Xiong, Jiawen Kang, and Zibin Zheng. 2022. Fusing blockchain and AI with metaverse: A survey. *IEEE Open Journal of the Computer Society* 3 (2022), 122–136.

[15] Thien Huynh-The, Quoc-Viet Pham, Xuan-Qui Pham, Thanh Thi Nguyen, Zhu Han, and Dong-Seong Kim. 2023. Artificial intelligence for the metaverse: A survey. *Engineering Applications of Artificial Intelligence* 117 (2023), 105581.

[16] Ujan Mukhopadhyay, Anthony Skjellum, Oluwakemi Hambolu, Jon Oakley, Lu Yu, and Richard Brooks. 2016. A brief survey of cryptocurrency systems. In *2016 14th Annual Conference on Privacy, Security and Trust (PST'16)*. IEEE, 745–752.

[17] Javad Zarrin, Hao Wen Phang, Lakshmi Babu Saheer, and Bahram Zarrin. 2021. Blockchain for decentralization of internet: prospects, trends, and challenges. *Cluster Computing* 24, 4 (2021), 2841–2866.

[18] Wenli Yang, Erfan Aghasian, Saurabh Garg, David Herbert, Leandro Disiuta, and Byeong Kang. 2019. A survey on blockchain-based internet service architecture: Requirements, challenges, trends, and future. *IEEE Access* 7 (2019), 75845–75872.

[19] Komal Gilani, Emmanuel Bertin, Julien Hatin, and Noel Crespi. 2020. A survey on blockchain-based identity management and decentralized privacy for personal data. In *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS'20)*. IEEE, 97–101.

[20] Tim Berners-Lee. 1989. Tim berners-lee. (1989).

[21] Dave Raggett, Arnaud Le Hors, Ian Jacobs, et al. 1999. HTML 4.01 Specification. *W3C Recommendation* 24 (1999).

[22] Roy Fielding, Jim Gettys, Jeffrey Mogul, Henrik Frystyk, Larry Masinter, Paul Leach, and Tim Berners-Lee. 1999. *Hypertext Transfer Protocol–HTTP/1.1*. Technical Report.

[23] Cristina Aced Toledano. 2013. Web 2.0: The origin of the word that has changed the way we understand public relations. In *Barcelona International PR Conference*.

[24] Tim Berners-Lee. [n.d.] Solid. Retrieved October 25, 2022 from https://solidproject.org/about

[25] Web3 foundation. 2022. Web3.0 technology stack. https://web3.foundation/abou

[26] Longbing Cao. 2022. Decentralized ai: Edge intelligence and smart blockchain, metaverse, web3, and desci. *IEEE Intelligent Systems* 37, 3 (2022), 6–19.

[27] Yi Zhao, Ke Xu, Jiahui Chen, and Qi Tan. 2022. Collaboration-enabled intelligent internet architecture: Opportunities and challenges. *IEEE Network* 36, 5 (2022), 98–105.

[28] William S. Noble. 2006. What is a support vector machine? *Nature Biotechnology* 24, 12 (2006), 1565–1567.

[29] Roman V. Yampolskiy, Brendan Klare, and Anil K. Jain. 2012. Face recognition in the virtual world: recognizing avatar faces. In *2012 11th International Conference on Machine Learning and Applications*, Vol. 1. IEEE, 40–45.

[30] Geoffrey I. Webb, Eamonn Keogh, and Risto Miikkulainen. 2010. Naïve Bayes. *Encyclopedia of Machine Learning* 15 (2010), 713–714.

[31] Josef Bauer and Dietmar Jannach. 2018. Optimal pricing in e-commerce based on sparse and noisy data. *Decision Support Systems* 106 (2018), 53–63.

[32] Anthony J. Myles, Robert N. Feudale, Yang Liu, Nathaniel A. Woody, and Steven D. Brown. 2004. An introduction to decision tree modeling. *Journal of Chemometrics: A Journal of the Chemometrics Society* 18, 6 (2004), 275–285.

[33] Steven J. Rigatti. 2017. Random forest. *Journal of Insurance Medicine* 47, 1 (2017), 31–39.

[34] Meng Shen, Yiting Liu, Liehuang Zhu, Xiaojiang Du, and Jiankun Hu. 2021. Fine-grained webpage fingerprinting using only packet length information of encrypted traffic. *IEEE Transactions on Information Forensics and Security* 16 (2021), 2046–2059.

[35] Phil Kim. 2017. Convolutional neural network. In *MATLAB Deep Learning*. Springer, 121–147.

[36] Alexander Mordvintsev, Christopher Olah, and Mike Tyka. 2015. Inceptionism: Going Deeper into Neural Networks. https://research.googleblog.com/2015/06/inceptionism-going-deeper-into-neural.html

[37] Leon A. Gatys, Alexander S. Ecker, and Matthias Bethge. 2016. Image style transfer using convolutional neural networks. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 2414–2423.

[38] Jianwen Chen, Kai Duan, Rumin Zhang, Liaoyuan Zeng, and Wenyi Wang. 2018. An AI based super nodes selection algorithm in blockchain networks. *arXiv preprint arXiv:1808.00216* (2018).

[39] Abdulaziz Saleh Ba Wazir, Hezerul Abdul Karim, Mohd Haris Lye Abdullah, Sarina Mansor, Nouar AlDahoul, Mohammad Faizal Ahmad Fauzi, and John See. 2020. Spectrogram-based classification of spoken foul language using deep CNN. In *2020 IEEE 22nd International Workshop on Multimedia Signal Processing (MMSP'20)*. IEEE, 1–6.

[40] Abdulaziz Saleh Ba Wazir, Hezerul Abdul Karim, Mohd Haris Lye Abdullah, Nouar AlDahoul, Sarina Mansor, Mohammad Faizal Ahmad Fauzi, John See, and Ahmad Syazwan Naim. 2021. Design and implementation of fast spoken foul language recognition with different end-to-end deep neural network architectures. *Sensors* 21, 3 (2021), 710.

[41] Stephen Grossberg. 2013. Recurrent neural networks. *Scholarpedia* 8, 2 (2013), 1888.

[42] Qi Zhao. 2020. A deep learning framework for predicting digital asset price movement from trade-by-trade data. *arXiv preprint arXiv:2010.07404* (2020).

[43] Muhammad Saad, Jinchun Choi, DaeHun Nyang, Joongheon Kim, and Aziz Mohaisen. 2019. Toward characterizing blockchain-based cryptocurrencies for highly accurate predictions. *IEEE Systems Journal* 14, 1 (2019), 321–332.

[44] Mohammad Yasser Chuttur and A. Nazurally. 2022. A multi-modal approach to detect inappropriate cartoon video contents using deep learning networks. *Multimedia Tools and Applications* 81, 12 (2022), 16881–16900.

[45] Si Zhang, Hanghang Tong, Jiejun Xu, and Ross Maciejewski. 2019. Graph convolutional networks: A comprehensive review. *Computational Social Networks* 6, 1 (2019), 1–23.

[46] Jie Shen, Jiajun Zhou, Yunyi Xie, Shanqing Yu, and Qi Xuan. 2021. Identity inference on blockchain using graph neural network. *CoRR* abs/2104.06559 (2021). https://arxiv.org/abs/2104.06559

[47] Liang Chen, Jiaying Peng, Yang Liu, Jintang Li, Fenfang Xie, and Zibin Zheng. 2021. Phishing scams detection in ethereum transaction network. *ACM Transactions on Internet Technology* 21, 1 (2021), 10:1–10:16.

[48] Meng Shen, Yiting Liu, Liehuang Zhu, Xiaojiang Du, and Jiankun Hu. 2021. Fine-grained webpage fingerprinting using only packet length information of encrypted traffic. *IEEE Transactions on Information Forensics and Security* 16 (2021), 2046–2059.

[49] Rui Qin, Wenwen Ding, et al. 2022. Web3-based decentralized autonomous organizations and operations: Architectures, models, and mechanisms. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 53, 4 (2022), 2073–2082.

[50] Felipe Bravo-Marquez, Steve Reeves, and Martin Ugarte. 2019. Proof-of-learning: A blockchain consensus mechanism based on machine learning competitions. In *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON'19)*. IEEE, 119–124.

[51] Mehrdad Salimitari, Mohsen Joneidi, and Mainak Chatterjee. 2019. Ai-enabled blockchain: An outlier-aware consensus protocol for blockchain-based IoT networks. In *2019 IEEE Global Communications Conference (GLOBECOM'19)*. IEEE, 1–6.

[52] Upal Mahbub, Jukka Komulainen, Denzil Ferreira, and Rama Chellappa. 2019. Continuous authentication of smartphones based on application usage. *IEEE Transactions on Biometrics, Behavior, and Identity Science* 1, 3 (2019), 165–180.

[53] Anish Agarwal, Munther Dahleh, and Tuhin Sarkar. 2019. A marketplace for data: An algorithmic solution. In *Proceedings of the 2019 ACM Conference on Economics and Computation*. 701–726.

[54] Xiaoshan Zhou and Pin-Chao Liao. 2022. A privacy-preserving data storage and service framework based on deep learning and blockchain for construction workers' wearable IoT sensors. *arXiv preprint arXiv:2211.10713* (2022).

[55] Aitizaz Ali, Muhammad Fermi Pasha, Jehad Ali, Ong Huey Fang, Mehedi Masud, Anca Delia Jurcut, and Mohammed A. Alzain. 2022. Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: A novel approach to cryptography. *Sensors* 22, 2 (2022), 528.

[56] Yang Liu, Hongsheng Wang, Mugen Peng, Jianfeng Guan, and Yu Wang. 2020. An incentive mechanism for privacy-preserving crowdsensing via deep reinforcement learning. *IEEE Internet of Things Journal* 8, 10 (2020), 8616–8631.

[57] Paul P. Momtaz. 2022. Some very simple economics of web3 and the metaverse. *FinTech* 1, 3 (2022), 225–234.

[58] Jia Xu, Zhengqiang Rao, Lijie Xu, Dejun Yang, and Tao Li. 2019. Incentive mechanism for multiple cooperative tasks with compatible users in mobile crowd sensing via online communities. *IEEE Transactions on Mobile Computing* 19, 7 (2019), 1618–1633.

[59] Yufeng Zhan, Chi Harold Liu, Yinuo Zhao, Jiang Zhang, and Jian Tang. 2019. Free market of multi-leader multi-follower mobile crowdsensing: An incentive mechanism design by deep reinforcement learning. *IEEE Transactions on Mobile Computing* 19, 10 (2019), 2316–2329.

[60] Ryoichi Shinkuma, Rieko Takagi, Yuichi Inagaki, Eiji Oki, and Fatos Xhafa. 2020. Incentive mechanism for mobile crowdsensing in spatial information prediction using machine learning. In *International Conference on Advanced Information Networking and Applications.* Springer, 792–803.

[61] Danilo Coura Moreira, Eanes Torres Pereira, and Marco Alvarez. 2020. PEDA 376K: A novel dataset for deep-learning based porn-detectors. In *2020 International Joint Conference on Neural Networks (IJCNN'20).* IEEE, 1–8.

[62] Xingxin Yu, Haoyue Zhao, Botao Hou, Zonghao Ying, and Bin Wu. 2021. DeeSCVHunter: A deep learning-based framework for smart contract vulnerability detection. In *2021 International Joint Conference on Neural Networks (IJCNN'21).* 1–8. DOI: http://dx.doi.org/10.1109/IJCNN52387.2021.9534324

[63] Wesley Joon-Wie Tann, Xing Jie Han, Sourav Sen Gupta, and Yew-Soon Ong. 2018. Towards safer smart contracts: A sequence learning approach to detecting vulnerabilities. *CoRR* abs/1811.06632 (2018). arXiv:1811.06632 http://arxiv.org/abs/1811.06632

[64] Yuan Zhuang, Zhenguang Liu, Peng Qian, Qi Liu, Xiang Wang, and Qinming He. 2021. Smart contract vulnerability detection using graph neural networks. In *International Joint Conference on Artificial Intelligence (IJCAI'20).* Article 454, 8 pages.

[65] Chinmay Mistry, Urvish Thakker, Rajesh Gupta, Mohammad S. Obaidat, Sudeep Tanwar, Neeraj Kumar, and Joel J. P. C. Rodrigues. 2021. MedBlock: An AI-enabled and blockchain-driven medical healthcare system for COVID-19. In *IEEE International Conference on Communications (ICC'21).* 1–6. DOI: http://dx.doi.org/10.1109/ICC42927.2021.9500397

[66] Pronaya Bhattacharya, Mohammad S. Obaidat, Darshan Savaliya, Sakshi Sanghavi, Sudeep Tanwar, and Balqies Sadaun. 2022. Metaverse assisted telesurgery in healthcare 5.0: An interplay of blockchain and explainable AI. In *2022 International Conference on Computer, Information and Telecommunication Systems (CITS'22).* 1–5. DOI: http://dx.doi.org/10.1109/CITS55221.2022.9832978

[67] Kuan-Ting Lai, Chia-Chih Lin, Chun-Yao Kang, Mei-Enn Liao, and Ming-Syan Chen. 2018. VIVID: Virtual environment for visual deep learning. In *Proceedings of the 26th ACM International Conference on Multimedia.* 1356–1359. DOI: http://dx.doi.org/10.1145/3240508.3243653

[68] Dawei Chen, Linda Jiang Xie, BaekGyu Kim, Li Wang, Choong Seon Hong, Li-Chun Wang, and Zhu Han. 2020. Federated learning based mobile edge computing for augmented reality applications. In *2020 International Conference on Computing, Networking and Communications (ICNC'20).* 767–773. DOI: http://dx.doi.org/10.1109/ICNC47757.2020.9049708

[69] Jayneel Vora, Anand Nayyar, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar, M. S. Obaidat, and Joel J. P. C. Rodrigues. 2018. BHEEM: A blockchain-based framework for securing electronic health records. In *2018 IEEE Globecom Workshops (GC Wkshps'18).* 1–6. DOI: http://dx.doi.org/10.1109/GLOCOMW.2018.8644088

[70] Chi Harold Liu, Qiuxia Lin, and Shilin Wen. 2018. Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning. *IEEE Transactions on Industrial Informatics* 15, 6 (2018), 3516–3526.

[71] Xiao Tang, Xunqiang Lan, Lixin Li, Yan Zhang, and Zhu Han. 2022. Incentivizing proof-of-stake blockchain for secured data collection in UAV-assisted IoT: A multi-agent reinforcement learning approach. *IEEE Journal on Selected Areas in Communications* 40, 12 (2022), 3470–3484.

[72] Weihua Zhuang, Qiang Ye, Feng Lyu, Nan Cheng, and Ju Ren. 2020. SDN/NFV-empowered future IoV with enhanced communication, computing, and caching. *Proceedings of the IEEE* 108, 2 (2020), 274–291.

[73] Xiaobin Xu, Hui Zhao, Haipeng Yao, and Shangguang Wang. 2021. A blockchain-enabled energy-efficient data collection system for UAV-assisted IoT. *IEEE Internet of Things Journal* 8, 4 (2021), 2431–2443. DOI: http://dx.doi.org/10.1109/JIOT.2020.3030080

[74] Jusik Yun, Yunyeong Goh, and Jong-Moon Chung. 2021. DQN-based optimization framework for secure sharded blockchain systems. *IEEE Internet of Things Journal* 8, 2 (2021), 708–722. DOI: http://dx.doi.org/10.1109/JIOT.2020.3006896

[75] Xuetao Bai, Shanshan Tu, Muhammad Waqas, Aiming Wu, Yihe Zhang, and Yongjie Yang. 2022. Blockchain enable IoT using deep reinforcement learning: A novel architecture to ensure security of data sharing and storage. In *International Conference on Artificial Intelligence and Security*. Springer, 586–597.

[76] Laizhong Cui, Xiaoxin Su, Zhongxing Ming, Ziteng Chen, Shu Yang, Yipeng Zhou, and Wei Xiao. 2022. CREAT: Blockchain-assisted compression algorithm of federated learning for content caching in edge computing. *IEEE Internet of Things Journal* 9, 16 (2022), 14151–14161.

[77] Collin Farquhar, Prem Sagar Pattanshetty Vasanth Kumar, Anu Jagannath, and Jithin Jagannath. 2022. Distributed transmission control for wireless networks using multi-agent reinforcement learning. *CoRR* abs/2205.06800 (2022).

[78] Nguyen Cong Luong, Tran The Anh, Huynh Thi Thanh Binh, Dusit Niyato, Dong In Kim, and Ying-Chang Liang. 2019. Joint transaction transmission and channel selection in cognitive radio based blockchain networks: A deep reinforcement learning approach. In *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'19)*. IEEE, 8409–8413.

[79] Jianlong Xu, Jian Lin, Wei Liang, and Kuan-Ching Li. 2022. Privacy preserving personalized blockchain reliability prediction via federated learning in IoT environments. *Cluster Computing* 25, 4 (2022), 2515–2526.

[80] Zhaoxin Yang, Ruizhe Yang, F. Richard Yu, Meng Li, Yanhua Zhang, and Yinglei Teng. 2022. Sharded blockchain for collaborative computing in the internet of things: Combined of dynamic clustering and deep reinforcement learning approach. *IEEE Internet of Things Journal* 9, 17 (2022), 16494–16509.

[81] Xingqiu He, Yuhang Shen, Hongxi Zhu, Sheng Wang, Chaoqun You, and Tony Q. S. Quek. 2022. Social welfare maximization for collaborative edge computing: A deep reinforcement learning-based approach. *CoRR* abs/2211.06861 (2022).

[82] Zhenwei Dai, Anshumali Shrivastava, Pedro Reviriego, and José Alberto Hernández. 2022. Optimizing learned Bloom filters: How much should be learned? *IEEE Embedded Systems Letters* 14, 3 (2022), 123–126.

[83] Jun Li, Yumeng Shao, Kang Wei, Ming Ding, Chuan Ma, Long Shi, Zhu Han, and H. Vincent Poor. 2021. Blockchain assisted decentralized federated learning (BLADE-FL): Performance analysis and resource allocation. *CoRR* abs/2101.06905 (2021).

[84] Jin Wang, Jia Hu, Geyong Min, Albert Y. Zomaya, and Nektarios Georgalas. 2020. Fast adaptive task offloading in edge computing based on meta reinforcement learning. *IEEE Transactions on Parallel and Distributed Systems* 32, 1 (2020), 242–253.

[85] Yijing Lin, Zhipeng Gao, Hongyang Du, Dusit Niyato, Jiawen Kang, Ruilong Deng, and Xuemin Sherman Shen. 2022. A unified blockchain-semantic framework for wireless edge intelligence enabled web 3.0. *arXiv preprint arXiv:2210.15130* (2022).

[86] Xuemin Shen, Jie Gao, Wen Wu, Kangjia Lyu, Mushu Li, Weihua Zhuang, Xu Li, and Jaya Rao. 2020. AI-assisted network-slicing based next-generation wireless networks. *IEEE Open Journal of Vehicular Technology* 1 (2020), 45–66.

[87] Wen Wu, Nan Chen, Conghao Zhou, Mushu Li, Xuemin Shen, Weihua Zhuang, and Xu Li. 2021. Dynamic RAN slicing for service-oriented vehicular networks via constrained learning. *IEEE Journal of Selected Areas in Communications* 39, 7 (2021), 2076–2089.

[88] Peilin Zheng, Zibin Zheng, and Liang Chen. 2019. Selecting reliable blockchain peers via hybrid blockchain reliability prediction. *CoRR* abs/1910.14614 (2019). arXiv:1910.14614 http://arxiv.org/abs/1910.14614

[89] Yunlong Lu, Xiaohong Huang, Ke Zhang, Sabita Maharjan, and Yan Zhang. 2021. Blockchain and federated learning for 5G beyond. *IEEE Network* 35, 1 (2021), 219–225. DOI: http://dx.doi.org/10.1109/MNET.011.1900598

[90] Jian Chang, Binhong Li, Jiang Xiao, Licheng Lin, and Hai Jin. 2023. Anole: A Lightweight and verifiable learned-based index for time range query on blockchain systems. In *Proceedings of the 28th International Conference on Database Systems for Advanced Applications (DASFAA'23), Part I (Lecture Notes in Computer Science)*, Xin Wang, Maria Luisa Sapino, Wook-Shin Han, Amr El Abbadi, Gill Dobbie, Zhiyong Feng, Yingxiao Shao, and Hongzhi Yin (Eds.). Vol. 13943. Springer, 519–534. DOI: http://dx.doi.org/10.1007/978-3-031-30637-2_34

[91] Jan Svoboda, Federico Monti, and Michael M. Bronstein. 2017. Generative convolutional networks for latent fingerprint reconstruction. In *2017 IEEE International Joint Conference on Biometrics (IJCB'17)*. IEEE, 429–436.

[92] Kuo Wang and Ajay Kumar. 2019. Toward more accurate iris recognition using dilated residual features. *IEEE Transactions on Information Forensics and Security* 14, 12 (2019), 3233–3245.

[93] The World Wide Web Consortium. [n.d.] Decentralized identifiers (DIDs) v1.0. Retrieved July 19, 2022 from https://www.w3.org/TR/did-core/

[94] E Glen Weyl, Puja Ohlhaver, and Vitalik Buterin. 2022. Decentralized society: Finding web3's soul. *Available at SSRN 4105763* (2022).

[95] David Zhang, Guangming Lu, Lei Zhang, et al. 2018. *Advanced Biometrics*. Springer.

[96] Quentin Debard, Christian Wolf, Stephane Canu, and Julien Arné. 2018. Learning to recognize touch gestures: Recurrent vs. convolutional features and dynamic sampling. In *2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG'18)*. IEEE, 114–121.

[97] Samira Bader and Najoua Essoukri Ben Amara. 2017. Design of a 3D virtual world to implement a logical access control mechanism based on fingerprints. In *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA'17)*. 1239–1246. DOI: http://dx.doi.org/10.1109/AICCSA.2017.147

[98] Ruizhe Wang, Chih-Fan Chen, Hao Peng, Xudong Liu, Oliver Liu, and Xin Li. 2019. Digital twin: Acquiring high-fidelity 3D avatar from a single image. *arXiv preprint arXiv:1912.03455* (2019).

[99] Gerhard Schrotter and Christian Hürzeler. 2020. The digital twin of the city of Zurich for urban planning. *PFG–Journal of Photogrammetry, Remote Sensing and Geoinformation Science* 88, 1 (2020), 99–112.

[100] Jianshan Sun, Zhiqiang Tian, Yelin Fu, Jie Geng, and Chunli Liu. 2021. Digital twins in human understanding: A deep learning-based method to recognize personality traits. *International Journal of Computer Integrated Manufacturing* 34, 7–8 (2021), 860–873.

[101] Tero Karras, Samuli Laine, and Timo Aila. 2019. A style-based generator architecture for generative adversarial networks. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 4401–4410.

[102] G. Goh, A. Ramesh, M. Pavlov, and S. Gray. [n.d.] DALL·E: Creating images from text. Retrieved January 25, 2021 from https://openai.com/blog/dall-e/

[103] Lei Xu, Chunxiao Jiang, Yi Qian, Youjian Zhao, Jianhua Li, and Yong Ren. 2016. Dynamic privacy pricing: A multi-armed bandit approach with time-variant rewards. *IEEE Transactions on Information Forensics and Security* 12, 2 (2016), 271–285.

[104] Kanishka Misra, Eric M. Schwartz, and Jacob Abernethy. 2019. Dynamic online pricing with incomplete information using multiarmed bandit experiments. *Marketing Science* 38, 2 (2019), 226–252.

[105] Xuemin Shen, Jie Gao, Wen Wu, Mushu Li, Conghao Zhou, and Weihua Zhuang. 2021. Holistic network virtualization and pervasive network intelligence for 6G. *IEEE Communications Surveys & Tutorials* 24, 1 (2021), 1–30.

[106] Jun-Yan Zhu, Taesung Park, Phillip Isola, and Alexei A. Efros. 2017. Unpaired image-to-image translation using cycle-consistent adversarial networks. In *Proceedings of the IEEE International Conference on Computer Vision*. 2223–2232.

[107] Alex Graves. 2013. Generating sequences with recurrent neural networks. *arXiv preprint arXiv:1308.0850* (2013).

[108] Mingbo Hong, Mantao Wang, Lixin Luo, Xuefeng Tan, Dejun Zhang, and Yike Lao. 2018. Combining gated recurrent unit and attention pooling for sentimental classification. In *Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence*. 99–104.

[109] Samuel R. Bowman, Luke Vilnis, Oriol Vinyals, Andrew M. Dai, Rafal Jozefowicz, and Samy Bengio. 2015. Generating sentences from a continuous space. *arXiv preprint arXiv:1511.06349* (2015).

[110] OpenAI. [n.d.] Introducing ChatGPT. Retrieved November 30, 2022 from https://openai.com/blog/chatgpt/

[111] Huisu Jang and Jaewook Lee. 2017. An empirical study on modeling and prediction of bitcoin prices with Bayesian neural networks based on blockchain information. *IEEE Access* 6 (2017), 5427–5437.

[112] Tamas Tothfalusi, Eszter Varga, Zoltan Csiszar, and Pál Varga. 2023. ML-based translation methods for protocols and data formats. In *19th International Conference on Network and Service Management (CNSM'23)*. IEEE, 1–5. DOI: http://dx.doi.org/10.23919/CNSM59352.2023.10327850

[113] Rupali Sachin Vairagade and Brahmananda SH. 2022. Enabling machine learning-based side-chaining for improving QoS in blockchain-powered IoT networks. *Transactions on Emerging Telecommunications Technologies* 33, 4 (2022), e4433.

[114] Jiawen Kang, Xuandi Li, Jiangtian Nie, Yi Liu, Minrui Xu, Zehui Xiong, Dusit Niyato, and Qiang Yan. 2022. Communication-efficient and cross-chain empowered federated learning for artificial intelligence of things. *IEEE Transactions on Network Science and Engineering* 9, 5 (2022), 2966–2977. DOI: http://dx.doi.org/10.1109/TNSE.2022.3178970

[115] Yufeng Zhan and Jiang Zhang. 2020. An incentive mechanism design for efficient edge learning by deep reinforcement learning approach. In *IEEE Conference on Computer Communications (IEEE INFOCOM'20)*. IEEE, 2489–2498.

[116] Rongxin Xu, Shiva Raj Pokhrel, Qiujun Lan, and Gang Li. 2022. FAIR-BFL: Flexible and incentive redesign for blockchain-based federated learning. *arXiv preprint arXiv:2206.12899* (2022).

[117] Yifei Jian, Xingshu Chen, and Haizhou Wang. 2022. Fake restaurant review detection using deep neural networks with hybrid feature fusion method. In *International Conference on Database Systems for Advanced Applications*. Springer, 133–148.

[118] Weili Chen, Zibin Zheng, Jiahui Cui, Edith C. H. Ngai, Peilin Zheng, and Yuren Zhou. 2018. Detecting ponzi schemes on ethereum: Towards healthier blockchain technology. In *Proceedings of the 2018 World Wide Web Conference on World Wide Web (WWW'18)*. ACM, 1409–1418.

[119] Jiajing Wu, Qi Yuan, Dan Lin, Wei You, Weili Chen, Chuan Chen, and Zibin Zheng. 2022. Who are the phishers? Phishing scam detection on ethereum via network embedding. *IEEE Transactions on Systems, Man, and Cybernetics Systems* 52, 2 (2022), 1156–1166.

[120] Yuntao Wang, Haixia Peng, Zhou Su, Tom H. Luan, Abderrahim Benslimane, and Yuan Wu. 2022. A platform-free proof of federated learning consensus mechanism for sustainable blockchains. *IEEE Journal on Selected Areas in Communications* 40, 12 (2022), 3305–3324.

[121] Yutao Jiao, Ping Wang, Dusit Niyato, Bin Lin, and Dong In Kim. 2020. Toward an automated auction framework for wireless federated learning services market. *IEEE Transactions on Mobile Computing* 20, 10 (2020), 3034–3048.

[122] Yufeng Zhan, Peng Li, Zhihao Qu, Deze Zeng, and Song Guo. 2020. A learning-based incentive mechanism for federated learning. *IEEE Internet of Things Journal* 7, 7 (2020), 6360–6368.

[123] Jie Zhao, Xinghua Zhu, Jianzong Wang, and Jing Xiao. 2021. Efficient client contribution evaluation for horizontal federated learning. In *2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'21)*. IEEE, 3060–3064.

[124] Anchal Pandey, Sukumar Moharana, Debi Prasanna Mohanty, Archit Panwar, Dewang Agarwal, and Siva Prasad Thota. 2021. On-device content moderation. In *2021 International Joint Conference on Neural Networks (IJCNN'21)*. IEEE, 1–7.

[125] Xurong Li, Kun Yu, Shouling Ji, Yan Wang, Chunming Wu, and Hui Xue. 2020. Fighting against deepfake: Patch&pair convolutional neural networks (PPCNN). In *Companion Proceedings of the Web Conference 2020*. 88–89.

[126] Tianchen Zhao, Xiang Xu, Mingze Xu, Hui Ding, Yuanjun Xiong, and Wei Xia. 2021. Learning self-consistency for deepfake detection. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*. 15023–15033.

[127] Trisha Mittal, Uttaran Bhattacharya, Rohan Chandra, Aniket Bera, and Dinesh Manocha. 2020. Emotions don't lie: An audio-visual deepfake detection method using affective cues. In *Proceedings of the 28th ACM International Conference on Multimedia*. 2823–2832.

[128] Ziheng Hu, Hongtao Xie, Yuxin Wang, Jiahong Li, Zhongyuan Wang, and Yongdong Zhang. 2021. Dynamic inconsistency-aware deepfake video detection. In *IJCAI*.

[129] Peng Wu, Jing Liu, Yujia Shi, Yujia Sun, Fangtao Shao, Zhaoyang Wu, and Zhiwei Yang. 2020. Not only look, but also listen: Learning multimodal violence detection under weak supervision. In *European Conference on Computer Vision*. Springer, 322–339.

[130] Davide Cozzolino, Andreas Rössler, Justus Thies, Matthias Nießner, and Luisa Verdoliva. 2021. Id-reveal: Identity-aware deepfake video detection. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*. 15108–15117.

[131] Mark Weber, Giacomo Domeniconi, Jie Chen, Daniel Karl I. Weidele, Claudio Bellei, Tom Robinson, and Charles E. Leiserson. 2019. Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics. *CoRR* abs/1908.02591 (2019). http://arxiv.org/abs/1908.02591

[132] Da Sun Handason Tam, Wing Cheong Lau, Bin Hu, Qiufang Ying, Dah Ming Chiu, and Hong Liu. 2019. Identifying illicit accounts in large scale e-payment networks: A Graph Representation Learning Approach. *CoRR* abs/1906.05546 (2019). http://arxiv.org/abs/1906.05546

[133] Meng Shen, Zhenbo Gao, Liehuang Zhu, and Ke Xu. Efficient fine-grained website fingerprinting via encrypted traffic analysis with deep learning. In *29th IEEE/ACM International Symposium on Quality of Service (IWQOS'21)*. IEEE, 1–10.

[134] Meng Shen, Mingwei Wei, Liehuang Zhu, and Mingzhong Wang. 2017. Classification of encrypted traffic with second-order Markov chains and application attribute bigrams. *IEEE Transactions on Information Forensics and Security* 12, 8 (2017), 1830–1843. DOI: http://dx.doi.org/10.1109/TIFS.2017.2692682

[135] Meng Shen, Jinpeng Zhang, Ke Xu, Liehuang Zhu, Jiangchuan Liu, and Xiaojiang Du. DeepQoE: Real-time measurement of video QoE from encrypted traffic with deep learning. In *28th IEEE/ACM International Symposium on Quality of Service (IWQoS'20)*. IEEE, 1–10.

[136] Jiasi Weng, Jian Weng, Hongwei Huang, Chengjun Cai, and Cong Wang. 2021. Fedserving: A federated prediction serving framework based on incentive mechanism. In *IEEE Conference on Computer Communications (IEEE INFOCOM'21)*. IEEE, 1–10.

[137] Xiaoyong Yuan and Lan Zhang. 2022. Membership inference attacks and defenses in neural network pruning. In *31st USENIX Security Symposium (USENIX Security'22)*. 4561–4578.

[138] Jian An, Zhenxing Wang, Xin He, Xiaolin Gui, Jindong Cheng, and Ruowei Gui. 2022. PPQC: A blockchain-based privacy-preserving quality control mechanism in crowdsensing applications. *IEEE/ACM Transactions on Networking* 30, 3 (2022), 1352–1367.

[139] Shijie Zhang, Hongzhi Yin, Tong Chen, Zi Huang, Lizhen Cui, and Xiangliang Zhang. 2021. Graph embedding for recommendation against attribute inference attacks. In *Proceedings of the Web Conference 2021*. 3002–3014.

[140] Jingwei Sun, Ang Li, Binghui Wang, Huanrui Yang, Hai Li, and Yiran Chen. 2021. Soteria: Provable defense against privacy leakage in federated learning from representation perspective. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 9311–9319.

[141] Jiahui Chen, Yi Zhao, Qi Li, Xuewei Feng, and Ke Xu. 2023. FedDef: Defense against gradient leakage in federated learning-based network intrusion detection systems. *IEEE Transactions on Information Forensics and Security* 18 (2023), 4561–4576.

[142] Fergal Reid and Martin Harrigan. An analysis of anonymity in the bitcoin system. In *2011 IEEE 3rd International Conference on Privacy, Security, Risk and Trust (PASSAT'11) and 2011 IEEE 3rd International Conference on Social Computing (SocialCom'11).* IEEE Computer Society, 1318–1326.

[143] Jiajun Zhou, Chenkai Hu, Jianlei Chi, Jiajing Wu, Meng Shen, and Qi Xuan. 2022. Behavior-aware account de-anonymization on Ethereum interaction graph. *IEEE Transactions on Information Forensics and Security* 17 (2022), 3433–3448.

[144] Jiajing Wu, Jieli Liu, Weili Chen, Huawei Huang, Zibin Zheng, and Yan Zhang. 2022. Detecting mixing services via mining bitcoin transaction network with hybrid motifs. *IEEE Transactinos on Systems, Man, and Cybernetics Systems* 52, 4 (2022), 2237–2249.

[145] chainalysis. [n.d.] https://www.chainalysis.com/

[146] augur. [n.d.] https://augur.net/

[147] Iason Kastanis and Mel Slater. 2012. Reinforcement learning utilizes proxemics: An avatar learns to manipulate the position of people in immersive virtual reality. *ACM Transactions on Applied Perception* 9, 1 (2012), 1–15. DOI: http://dx.doi.org/10.1145/2134203.2134206

[148] Kizashi Nakano, Daichi Horita, Naoya Isoyama, Hideaki Uchiyama, and Kiyoshi Kiyokawa. 2022. Ukemochi: A video see-through food overlay system for eating experience in the metaverse. In *CHI Conference on Human Factors in Computing Systems (CHI'22), Extended Abstracts*, Simone D. J. Barbosa, Cliff Lampe, Caroline Appert, and David A. Shamma (Eds.). ACM, 380:1–380:8.

[149] Thien Huynh-The, Cam-Hao Hua, Nguyen Anh Tu, and Dong-Seong Kim. 2021. Physical activity recognition with statistical-deep fusion model using multiple sensory data for smart health. *IEEE Internet of Things Journal* 8, 3 (2021), 1533–1543. DOI: http://dx.doi.org/10.1109/JIOT.2020.3013272

[150] Aiarena. 2022. https://docs.aiarena.io/

[151] Chaos box. 2022. https://rct.ai/zh-hans/

[152] Jean-Luc Lugrin and Marc Cavazza. 2006. AI-based world behaviour for emergent narratives. In *Proceedings of the 2006 ACM SIGCHI International Conference on Advances in Computer Entertainment Technology.* 25–es.

[153] Y. Meng, Y. Zhan, J. Li, S. Du, H. Zhu, and X. Shen. 2023. De-anonymization attacks on metaverse (2023).

[154] medibloc. 2023. *IEEE INFOCOM 2023-IEEE Conference on Computer Communications*. IEEE, 1–10. https://medibloc.com/

[155] Polina Mamoshina, Lucy Ojomoko, Yury Yanovich, Alex Ostrovski, Alex Botezatu, Pavel Prikhodko, Eugene Izumchenko, Alexander Aliper, Konstantin Romantsov, Alexander Zhebrak, et al. 2018. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. *Oncotarget* 9, 5 (2018), 5665.

[156] Chayakrit Krittanawong, Albert J. Rogers, Mehmet Aydar, Edward Choi, Kipp W. Johnson, Zhen Wang, and Sanjiv M. Narayan. 2020. Integrating blockchain technology with artificial intelligence for cardiovascular medicine. *Nature Reviews Cardiology* 17, 1 (2020), 1–3.

[157] Jan Witowski, Jongmun Choi, Soomin Jeon, Doyun Kim, Joowon Chung, John Conklin, Maria Gabriela Figueiro Longo, Marc D. Succi, and Synho Do. 2021. MarkIt: A collaborative artificial intelligence annotation platform leveraging blockchain for medical imaging research. *Blockchain in Healthcare Today.*

Received 26 March 2023; revised 28 January 2024; accepted 31 March 2024