A Survey of Blockchain, Artificial Intelligence, and Edge Computing for Web 3.0

Jianjun Zhu[a], Fan Li[a], Jinyuan Chen[a]

[a]*Louisiana Tech University, Department of Electrical Engineering, Ruston, 71270, Louisiana, USA*

Abstract

Web 3.0, as the third generation of the World Wide Web, aims to solve contemporary problems of trust, centralization, and data ownership. Driven by the latest advances in cutting-edge technologies, Web 3.0 is moving towards a more open, decentralized, intelligent, and interconnected network. Currently, increasingly widespread data breaches have raised awareness of online privacy and security of personal data. Additionally, since Web 3.0 is a complex integration, the technical details are not as clear as the characteristics it presents. In this survey, we conduct an in-depth exploration of Web 3.0 from the perspectives of blockchain, artificial intelligence, and edge computing. The methodology includes a comprehensive literature review, using specific keywords to identify relevant studies and applying strict inclusion and exclusion criteria to ensure a focus on high-quality literature. The main contributions include identifying the key challenges of Web 3.0, examining the fundamental role of each underlying technology, and surveying state-of-the-art practical applications within this ecosystem. Moreover, we introduce an innovative decentralized storage solution that facilitates secure communication and data processing without relying on centralized servers. We also introduce a novel decentralized computing solution that enhances the capabilities of Web 3.0 by enabling edge devices to perform data analysis locally, reducing dependence on traditional centralized servers. Finally, we highlight key challenges and potential research directions. Through the combination and mutual complementation of multiple technologies, Web 3.0 is expected to give users more control and ownership of data and digital assets.

Keywords: Web 3.0, Decentralization, Ownership, Blockchain, Artificial Intelligence, Edge Computing.

1. Introduction

Since the second half of 2021, Web 3.0 has become ubiquitous and gained widespread attention across various industries. Web 3.0 is a new version of the World Wide Web (also known as the Web). According to the statistical site Statista, as of April 2024, there were 5.44 billion web users worldwide, which accounts for 67.1% of the global population. Notably, social media users account for 93.2% of web users [1]. The vast online world is controlled by tech giants who collect users' data through the centralized platforms they developed. As gatekeepers and arbiters, they shape and control the content on the web while providing services. Fundamentally, entrusting personal information to third-party organizations is a flawed model. Considering that their revenue models rely on collecting as much personal information as possible, the potential for data misuse and exploitation is significant. For the current dilemma, there is an urgent need for solutions to improve web environment while returning control to users. This has laid a solid foundation for the emergence of Web 3.0.

Web 3.0 is a trustless interactive system designed to enforce predetermined processes mathematically. It has the potential to create an open, trustless, and permissionless web where users can share and exchange data without relying on centralized organizations. To explore its transformative potential, this survey will primarily explore the following research questions:

1) How can decentralized storage and computing solutions support the decentralized nature of Web 3.0 while ensuring the security and privacy of user data? The implementation and utilization of Web 3.0 relies on the development of decentralized storage and computing solutions. Despite the maturity of existing storage and computing solutions, individuals frequently relinquish control and ownership of their data to tech giants or centralized authorities. These data-driven organizations adopt a business strategy offering free services in exchange for personal data. In this scenario, an individual's digital activities, social media posts, physical location, purchasing habits, and more are tracked to build highly detailed digital profiles. However, individuals possess limited awareness and control regarding the information collected and its utilization. This data may be accessed or disclosed by unauthorized parties, or misused by the service providers. Moreover, users lack the means to communicate their unwillingness to disclose data to third parties, raising concerns about data ownership, security, and privacy. According to Statista's analysis of the number of compromised user accounts globally from the first quarter of 2020 to the fourth quarter of 2023, over eight million data records were compromised during the fourth quarter of 2023. Notably, the fourth quarter of 2020 had the highest number of exposed data records, with almost 125 million data sets compromised [2]. This points to serious issues with this pervasive data collection without transparent usage policies. Through decentralized storage and computing solutions, Web 3.0 users can maintain ownership and control of their data, ensuring privacy and security.

2) What are the current barriers to mass adoption of Web 3.0, and how can they be mitigated to enhance user accessibility and

Table 1: Literature search performed with IEEE Xplore, ACM Digital Library, and Google Scholar.

Subject	**Keywords**	**Initial literature**	**Final literature**
Blockchain for Web 3.0	"Web 3.0" AND "Blockchain"	258	22
	"Web 3.0" AND "Decentralization"	72	13
Artificial intelligence for Web 3.0	"Web 3.0" AND "Artificial intelligence"	177	19
	"Web 3.0" AND "Generative AI"	68	9
Edge computing for Web 3.0	"Web 3.0" AND "Edge computing"	94	14
	"Web 3.0" AND "Internet of Things"	46	6
Use cases of Web 3.0	"Web 3.0" AND "Non-fungible token"	180	7
	"Web 3.0" AND "Decentralized finance"	120	12
	"Web 3.0" AND "Decentralized autonomous organization"	127	11

participation? The technical barriers for using Web 3.0 remain high, making it challenging for users to migrate to Web 3.0 platforms. Users need to understand the underlying security mechanisms and complex technical documentation before they can use the Web 3.0 platform. According to an international survey conducted by Coinbase during October 2022 on the adoption of Web 3.0, 46% of respondents do not have sufficient knowledge to adopt it, while 27% do not know where to start [3]. In another global Web 3.0 perception survey conducted by Consensys, as of May 2023, 24% of respondents consider themselves familiar with the concept of Web 3.0. However, out of this percentage, only 8% described themselves as very familiar, whereas 16% said they were fairly familiar. In contrast, 37% of respondents admitted to having no understanding of Web 3.0 at all [4]. The data reveals a gap between the adoption of Web 3.0 and the transformative potential it holds. While Web 3.0 has the potential to address significant limitations in data privacy, identity management, and digital ownership prevalent in the current web, general comprehension of these concepts remains limited. It is worth noting that in its early stages, the Web 3.0 protocols focused on building the first set of solutions and made certain concessions regarding user interface and user experience. In this scenario, individuals lack the accessibility to the simplicity and convenience comparable to what Web 2.0 provides. Therefore, it is essential to eliminate the technical barriers in Web 3.0 to facilitate its widespread adoption.

Motivated by the above considerations, this paper will provide a comprehensive survey of Web 3.0, exploring the potential solutions for decentralized storage and computation, as well as strategies for achieving mass adoption. Fundamentally, Web 3.0 is the integration of emerging technologies. Among them, blockchain, artificial intelligence (AI), and edge computing are essential in this revolution, enabling users to use the Web securely and intelligently. Blockchain will allow individuals, companies, and computers to exchange data in a decentralized manner. AI will empower computers with the ability to learn and reason to provide user-centered interactions. Edge computing allows faster processing and decision-making with low latency by bringing computing and storage closer to where users consume the data.

1.1. Methodology

To thoroughly investigate the next-generation web ecosystem, this paper reviews the literature on blockchain, AI, and edge computing within the context of Web 3.0. We initiated our review with a comprehensive search across multiple databases using specific keywords to identify relevant studies. Subsequently, we applied inclusion and exclusion criteria to refine and narrow the literature set.

Initial literature search: We conducted extensive literature searches across multiple databases, such as IEEE Xplore, ACM Digital Library, and Google Scholar, to identify relevant studies. For each of the three subject areas, blockchain, AI, and edge computing, we utilized specific keywords detailed in Table 1. This approach ensured a comprehensive collection of studies relevant to Web 3.0. Our initial search obtained a total of 1142 studies across various topics.

Inclusion/exclusion criteria: Studies were included if they directly addressed blockchain, AI, or edge computing within the Web 3.0 framework, with a particular focus on surveys or applications within this context. This criterion ensured that literature providing comprehensive overviews or practical implementations of Web 3.0 was considered. While our primary focus was on peer-reviewed journal articles, conference papers, and book chapters published within the last five years to capture the most recent advancements and trends, we also included seminal works beyond this period if they were deemed crucial for understanding the development of Web 3.0 technologies. For example, we included a seminal work [13] that initially introduced and defined the concept of Web 3.0. This work laid the foundational principles and vision for the next generation of the Web. Conversely, studies were excluded if they did not align with the inclusion criteria, such as those not addressing Web 3.0, lacking focus on blockchain, AI, or edge computing, or failing to provide insights into surveys or applications within these areas. Therefore, based on the inclusion and exclusion criteria, a total of 115 articles were selected for review.

1.2. Contributions

In this work, we will explore Web 3.0 from the perspectives of blockchain, AI, and edge computing. The corresponding

Table 2: A comparison between our survey and other works on Web 3.0.

Reference	Description
[5]	Providing an integrative literature review on the development of the Web.
[6]	Conducting a review of decentralized Internet with a focus on consensus and other emerging technologies.
[7]	Exploring blockchain-based Web 3.0 from an architecture identification and evaluation perspective.
[8]	Analyzing key advances and potential impacts to emphasize the importance of Web 3.0.
[9]	Introducing the evolution, technologies, and challenges of Web 3.0.
[10]	Surveying the impact of quantum technology on the development of blockchain-based Web 3.0.
[11]	Investigating Web 3.0 application categories, popularity, challenges, and opportunities.
[12]	Conducting a comprehensive overview of the latest advances of AI in Web 3.0.
This work	Providing an in-depth analysis of Web 3.0 from the perspectives of blockchain, AI, and edge computing, discussing practical applications through a significant amount of concrete research works, and proposing solutions for decentralized storage and computation through technological integration.

technology enablers will be discussed in depth in each chapter. To the best of our knowledge, there has been no comprehensive survey on Web 3.0 from the perspective of these three technologies simultaneously. To summarize, the main contributions of our work are discussed as follows:

• Identified key challenges by exploring two research questions, focusing on data ownership for security and privacy, and enhancing user accessibility and engagement.

• Conducted a thorough study of the underlying blockchain-related technological modules for Web 3.0, demonstrating their profound impact on the development of Web 3.0.

• Elaborated on how the Web 3.0 platform can address the dual challenges of data and computing power in generative AI.

• Proposed and illustrated storage and computing solutions in decentralized scenarios by exploring the integration of blockchain, AI, and edge computing.

• Surveyed state-of-the-art Web 3.0 practical applications to explore possibilities for further integration and improvement within the Web 3.0 ecosystem.

• Highlighted critical challenges encountered in the development of Web 3.0 with concrete data and discussed future research directions.

1.3. Comparison with other surveys

To date, there have been several survey papers on different aspects of Web 3.0. Our survey is distinctive from all the other surveys as we conducted an in-depth analysis of the impact of blockchain, AI, and edge computing on the development of the Web 3.0 ecosystem. A comparison of our survey with other works on Web 3.0 is provided in Table 2.

Comparatively, Vojíř *et al.* in [5] provided an integrative literature review examining the development of the Web by analyzing its evolution from centralization to decentralization and the reactions it provoked. Zarrin *et al.* in [6] showed the potential of blockchain technology to provide a robust and secure decentralized Internet by exploring consensus algorithms and how blockchain can be combined with emerging technologies. Wang *et al.* in [7] conducted an in-depth exploration of Web 3.0 from the perspective of blockchain, identifying twelve types of architecture by decoupling existing systems into core components. Ray in [8] emphasized the importance of Web 3.0 in shaping a decentralized and democratized Internet by analyzing the key advances and impacts of Web 3.0 applications and their integration with emerging technologies. Gan *et al.* in [9] provided an overview of Web 3.0 in terms of technologies, challenges, potential, and prospects. Ren *et al.* in [10] explored the fusion of various quantum information technologies with blockchain to develop a resilient digital ecosystem based on blockchain. Huang *et al.* in [11] empirically investigated the categories of Web 3.0 applications and their popularity, as well as the potential of this emerging field. Shen *et al.* in [12] provided an overview of the latest advances of AI in Web 3.0, proposing and investigating the main challenges at each layer of the Web 3.0 architecture.

The rest of this paper is organized as follows. Section 2 provides preliminaries such as the evolution of the Web and background on technologies (i.e., blockchain, AI, and edge computing). Sections 3-5 provide an in-depth analysis of each technology regarding relevance, fundamental components, practical applications, and insights. Section 6 delves into the primary use cases of Web 3.0 and their practical applications. Additionally, major issues from both technical and non-technical aspects are discussed. Section 7 discusses key challenges and future research directions. Finally, the work is concluded in Section 8. The abbreviations used in this article are listed in Table 3.

2. Preliminaries

In this section, we introduce the fundamentals of Web 3.0 from the following aspects: evolution of the Web and enabling technologies (i.e., blockchain, AI, and edge computing).

2.1. Evolution of the Web

The Web is a hypertext document management system accessible via the Internet. In March 1989, Sir Tim Berners-Lee

Table 3: Abbreviations and explanations in alphabet order.

Abbreviation	Explanation	Abbreviation	Explanation	Abbreviation	Explanation
AI	Artificial Intelligence	DON	Decentralized Oracle Network	MEC	Mobile Edge Computing
AIGC	Artificial Intelligence Generated Content	EACs	Energy Attribute Certificates	MR	Mixed Reality
APIs	Application Programming Interfaces	EHRs	Electronic Health Records	NFT	Non-fungible Tokens
AR	Augmented Reality	ENS	Ethereum Name Service	NLP	Natural Language Processing
AVID	Asynchronous Verifiable Information Dispersal	ESP	Edge Server Placement	P2P	Peer-to-Peer
BTC	Bitcoin	ETH	Ether	PKI	Public Key Infrastructure
CNN	Convolutional Neural Network	GANs	Generative Adversarial Networks	PoS	Proof-of-Stake
CV	Computer Vision	GNNs	Graph Convolutional Networks	RNN	Recurrent Neural Network
DAO	Decentralized Autonomous Organization	IPFS	InterPlanetary File System	SC	Smart Contract
dApps	Decentralized Applications	IoT	Internet of Things	UAV	Unmanned Aerial Vehicle
DCNN	Deep Convolutional Neural Network	IT	Information Technology	VAEs	Variational Autoencoders
DeFi	Decentralized Finance	LLMs	Large Language Models	VR	Virtual Reality
DL	Deep Learning	LSTM	Long-Short-Term Memory	ZK	Zero-Knowledge

proposed an information management system that would later become the Web. He envisioned an intelligent, connected, and data-driven network in which computers could analyze all network data, including content, connections, and transactions between users and computers. He advocated for the European Council for Nuclear Research to provide the underlying code for free in April 1993, leading to today's Web [14, 15].

Web 1.0, also known as the Static Web, is described as a web of interconnected information. Tim Berners-Lee coined it a "read-only" web since a massive majority of participants were content consumers. Web 1.0 was not interactive, which made it difficult for content users to find the needed information. Additionally, proprietary web pages and browsers have led to compatibility issues.

Web 2.0, also called the Social Web, is the most familiar and widely used Web today. The focus of Web 2.0 is on enabling users to interact with web content. Users are becoming more engaged in generating and sharing web content in addition to browsing. The Web 2.0 period is also a time when mobile web access has boomed. People can utilize their phones, tablets, and almost any other web-connected devices to access web content at any time.

Web 3.0 was first coined by Gavin Wood, co-founder of Ethereum, in 2014 as a way to minimize trust in a handful of private companies [16]. It represents a decentralized and fair Internet reconstructed using distributed technology, where users can control their data and identity. Web 3.0 is characterized as a "read-write-own" web that allows users to create, trade, and collaborate directly through a peer-to-peer (P2P) network, eliminating the need for third parties. This architecture enhances privacy and security by avoiding centralized data storage, which reduces the risk of data breaches. A typical example is Solid proposed by Tim Berners-Lee in late 2020 [17]. The purpose is to propose a specification that allows users to securely store data in a decentralized manner to achieve true data ownership and improve privacy. Notably, Web 3.0 is more than just a new wave of innovation. It is an opportunity to reset and enable new benefits for ordinary users while solving some of the toughest challenges posed by disruptive technologies of the past.

2.2. What is blockchain?

A blockchain is essentially a global network of interconnected nodes that serves as a distributed database or ledger. It contains blocks of transaction records that are shared by all participants in the network. Each block carries the digest of the previous block, which is the output of the cryptographic hash function. This digest can be used to verify the validity of the previous block, such that it connects the blocks into a growing chain. Blocks cannot be changed backward without affecting all the following blocks. This assures data confidentiality and integrity, as well as the ability for blockchain participants to verify and audit transactions.

The consensus protocol is the fundamental building block of blockchain networks as well as the Web 3.0 ecosystem. According to the latest research on the priority of Web 3.0 development factors, the most important factor in the development of Web 3.0 is the consensus mechanism, with a weight of 20.0% [18]. Fundamentally, a consensus protocol is a fault-tolerant mechanism used between distributed nodes to achieve a common agreement on a single data value. From the perspective of blockchain, the consensus protocol is used by each participant to agree on the state of a distributed ledger. Consensus protocols ensure the reliability of blockchain networks by fostering trust among anonymous peers in a decentralized setting and enacting regulatory economic incentives in this way.

2.3. What is AI?

AI is an interdisciplinary science that uses computers and data to mimic the problem-solving and decision-making abilities of the human brain. Typically, humans will play a role in supervised learning, providing positive feedback for good decisions while preventing bad ones. Meanwhile, certain AI systems are designed for unsupervised learning, where they eventually figure out the rules through pattern recognition and learning using large amounts of data.

In terms of technical capabilities, there are three types of AI [19]. One type is known as Artificial Narrow Intelligence, which has been integrated to improve people's daily lives. Breakthroughs in healthcare are dependent on it, as it can greatly reduce repetitive tasks that can lead to human errors, enhance the process of developing medical materials, and improve treatment outcomes. Another type of AI is Artificial General Intelligence, in which the computer has greatly improved in intelligence compared to the level of Web 2.0. It would be self-aware, capable of problem-solving, learning, and long-term planning. If development continues, it will reach the third type of AI, i.e., Artificial Super Intelligence. With the advent of Web 3.0, the booming development of various edge technologies will propel AI into a more advanced stage.

2.4. *What is edge computing?*

Edge computing refers to offloading data storage and processing from centralized servers to the edge of the network, closer to end-user devices. This technique reduces data transfer times and device response latency while easing bandwidth congestion on the network. Localizing processing at the edge reduces data transfer costs and decentralizes computing by moving tasks away from central hubs.

The key components enabling edge computing are edge devices, edge servers, edge databases, edge nodes, and network edge [20]. Edge devices refer to the devices that process data near the data source, such as smartphones, laptops, sensors, and industrial robots. Edge servers are information technology (IT) computing devices located near edge devices for computing IT workloads and resource management. Edge databases are database systems that are deployed at the edge of the network. They are used to store the data generated by edge devices locally rather than sending it to a centralized data server. Edge nodes are nodes that hold edge devices, edge servers, and edge databases. They are connected to the network and each other, acting as intermediaries to facilitate data exchange and resource sharing. The network edge is the network infrastructure such as 5G and high-speed satellite Internet that connects edge devices and edge servers with low latency.

3. Blockchain for Web 3.0: a decentralized and trusted web

Web 3.0 is a decentralized network based on blockchain technology, collectively maintained by nodes scattered around the globe. Blockchain redefines the way data is stored and managed. It uses cryptographic techniques to provide a unique set of states that can enable true P2P transactions without third parties. With blockchain, data will be stored on a decentralized network rather than on a centralized server so that privacy and ownership will be given back to individuals [21]. Notably, blockchain combined with privacy-preserving technologies has

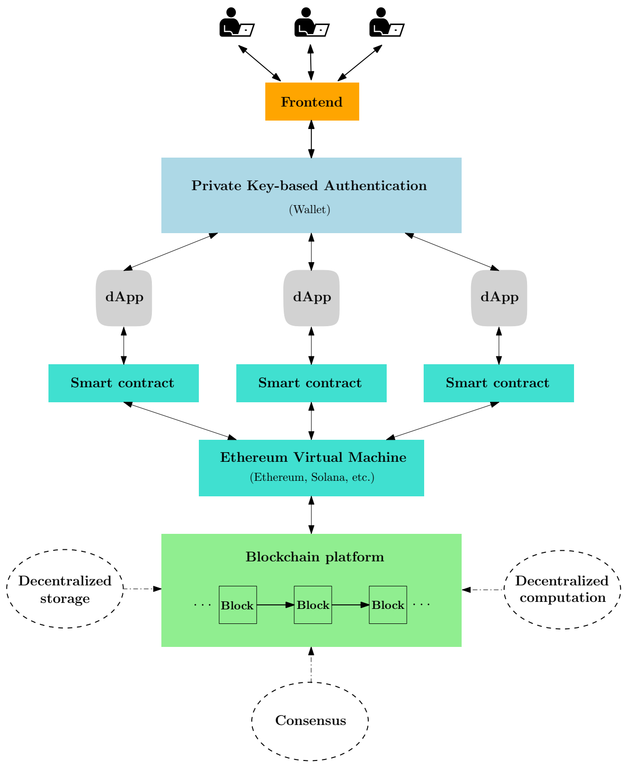

Figure 1: Web 3.0 infrastructure from the perspective of blockchain.

the potential to further enhance the protection of user privacy. Typically, website fingerprinting is a technique widely used in web browser analysis to infer sensitive information about users by examining traffic patterns. In response to such attacks, some significant improvements have been proposed for website fingerprinting-based methods. For example, a TCP/IP traffic-based defense mechanism was proposed in [22]. It is an efficient and low-overhead defense mechanism against attacks that can filter out the injected noise. A traffic splitting-based defense mechanism was proposed to limit the data that can be observed by a single entry node in [23]. By embedding these defense technologies, blockchain can provide additional layers of security on top of its inherent cryptographic protections and decentralized framework.

Due to its ability to store data in P2P networks, blockchain lays the foundation for Web 3.0. The protocol specifies the management rules, which are guaranteed by a majority vote of all members of the network. Participants are rewarded for their contributions to network security and maintenance. It enables individuals to reach a consensus while the network collectively records previous user interactions. As a result, blockchain technology is certainly a powerful force that can make the network more decentralized [24]. Web 3.0 is a backend revolution with a network architecture as shown in Fig. 1 [25, 26]. For average users, there will be no change to the interface of the Web. From a technical perspective, it is a set of blockchain-based protocols designed to transform the backend of the Web.

In this section, we will first show how blockchain technology is closely related to Web 3.0. Then, we will explain the criticality of blockchain for Web 3.0 from the perspective of specific technologies, i.e., off-chain technology, cross-chain technology, and Layer 2 solutions. We will use a case study to explore how to integrate these three technologies to contribute to decentralized finance (DeFi) in Web 3.0. Afterward, we will introduce the practical applications of blockchain in Web 3.0. Finally, the summary and insights are provided.

3.1. Relevance to Web 3.0

Web 3.0 is a decentralized and trustworthy Web, aiming to transform a centralized network platform into a decentralized, secure, and user-centric platform. Blockchain technology plays a crucial role in realizing the vision of Web 3.0. This can be demonstrated in several key aspects as shown in Fig. 2.

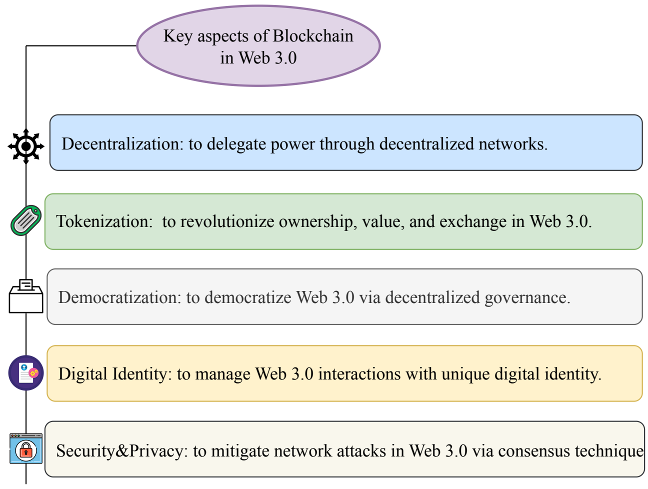

Figure 2: Relevance of blockchain to Web 3.0.

3.1.1. Decentralization

One of Web 3.0's visions is to build a decentralized system that does not depend on a single entity but operates on a distributed network of nodes. The core principle of decentralization is the delegation of power which requires the distribution of power and control outside of the central authority. The technological support comes from blockchain and its underlying P2P networks. Web 3.0 can help create more sustainable networks by decentralizing the energy consumption associated with centralized data centers. By distributing data and computing power among multiple nodes, blockchain-based systems can be more energy-efficient and environmentally friendly. For example, according to a report on the energy and carbon footprint consumption of Proof-of-Stake (PoS) blockchain protocols, the electricity consumption per Solana transaction is approximately 0.17 Wh, whereas each Visa transaction consumes around 1.49 Wh [27]. In another analysis of energy consumption and carbon footprints of cryptocurrencies, each Algorand transaction generates 0.0000004 KgCO2 compared to the 0.00045 KgCO2 of each Visa transaction [28, 29].

3.1.2. Tokenization

Token is a digital scarcity in Web 3.0, which refers to the representation of real-world assets by a string of numbers on the blockchain network. The immutability and public verifiability of blockchain guarantee the uniqueness, scarcity, and security of this digital string. Tokens can be used to represent access rights, voting rights, or other types of ownership in applications. It also enables fractional ownership, which means assets can be divided into smaller parts that can be easily bought, sold, or traded, enabling more people to participate in investment opportunities. Tokenization has great potential to revolutionize ownership, value, and exchange in the Web 3.0 ecosystem.

3.1.3. Democratization

One of the main features of Web 3.0 is the democratization enabled by blockchain technology. Web 3.0 promises to allow users to be rewarded based on their contributions to the Web. However, democratizing in an error-free and fair manner is a major challenge. Essentially, the main problem that the blockchain solves is how to transfer value and control from the platform to the community, while maintaining the prosperity of the platform. Decentralization and tokenization are two key aspects that are at the heart of the democratization of Web 3.0. Specifically, the decentralized nature of blockchain technology allows for trustless cooperation between stakeholders within the platform; then the tokenization of blockchain provides a fair way to incentivize different stakeholders to participate in the governance and use of the platform.

3.1.4. Digital universal identity

Digital identity is one of the core elements of Web 3.0. It plays a key role in managing Web 3.0 interactions. However, as data breaches and hacks expose the vulnerability of personal data, the utility and relevance of digital identities are becoming increasingly apparent. In particular, the proliferation of social media has resulted in individuals having different digital identities on different platforms. Online identity management faces serious challenges. Blockchain technology can provide a decentralized and interoperable identity system for Web 3.0 users. This ensures that each user has a secure, unique digital universal identity across multiple platforms, eliminating the need for multiple usernames and passwords.

3.1.5. Security and privacy

Ensuring the security and privacy of data and transactions is a crucial part of the rapid development of Web 3.0. Blockchain-based Web 3.0 can fundamentally eliminate the need for central institutions to manage data. Moreover, the integration of blockchain in Web 3.0 will greatly mitigate network attacks. Every data stream on the blockchain network has to be verified by different nodes. A successful network attack requires controlling the majority of nodes on the blockchain network in order to reach a consensus on its proposals. At the same time, it has to compete with potential new blocks that are added. This is impractical for hackers, as they would be trapped in an endless computational loop, making it harder for them to compromise the network and access users' personal information and transaction records.

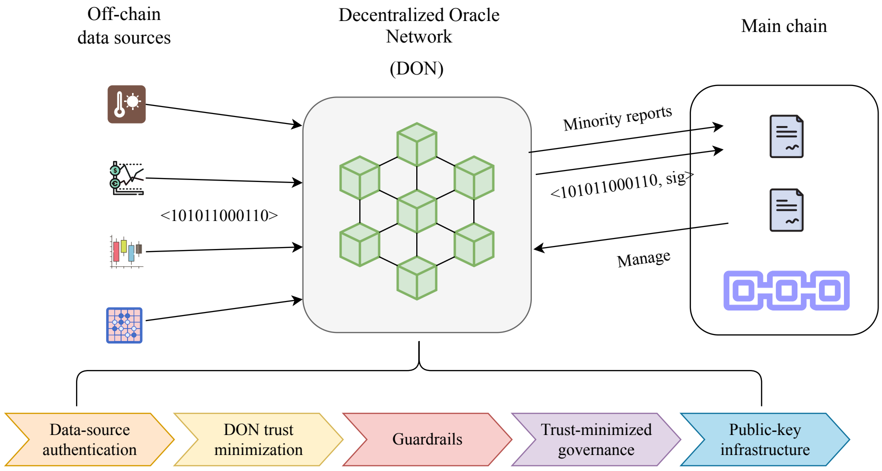

Figure 3: Interactions between off-chain and on-chain resources via DON.

3.2. *Off-chain technology*

Off-chain technologies refer to data or transactions that occur outside the main blockchain network. They play a critical role in augmenting blockchains in the Web 3.0 ecosystem. When blockchains are connected to off-chain resources, their capabilities are greatly enhanced, from incorporating real-world information into on-chain execution to reducing costs and increasing throughput by shifting computation off-chain. However, to securely and immutably connect blockchain to external resources, the oracle problem needs to be overcome. This problem refers to the inherent limitation of blockchains being unable to directly access or use external data resources due to their isolated nature. A blockchain oracle is an entity that connects blockchain to external systems, allowing smart contracts (SCs) to execute based on real-world inputs and outputs in the Web 3.0 ecosystem.

The decentralized oracle network (DON), proposed by Chainlink in [30], acts as a secure middleware to facilitate communication between on-chain and off-chain resources as shown in Fig. 3. The DON obtains data from off-chain resources and then forwards the data to the SC deployed on the main chain. Additionally, the DON incorporates a separate SC for node management. Notably, one of the goals of Web 3.0 is to minimize trust. The implementation of a DON involves integrating a variety of trust-minimized technologies.

• *Data-source authentication*: An important component of trust minimization involves strengthening data-source authentication through support for data signing tools and standards. By cryptographically signing the data they provide to SCs, a DON enables users to identify which nodes sent data and track the behaviors to determine the quality of their performance. In this way, the end-to-end integrity of the data can be guaranteed.

• *DON trust minimization*: To minimize trust in DON, there are two main methods. The first is the failover clients, which are backup clients for nodes in case of unexpected events. They do not increase the number of potential attacks and can reduce reliance on individual client security as they are not deployed on the mainline. The second is the minority report, which is a parallel report that is forwarded to SCs on the main chain. This is an important mechanism that operates in a threshold manner to maintain the integrity and reliability of the data sources provided by the DON.

• *Guardrails*: Guardrails are a collection of trust minimization mechanisms involving the implementation of monitoring and fail-safety in SCs. A circuit breaker is a guardrail where a SC may control state updates based on inputs. For example, it might be triggered if minority reports change significantly over time. Escape hatches are emergency facilities that SCs can invoke to terminate pending transactions and future transactions in adverse circumstances. Failover means that SCs can provide a failover mechanism to ensure the continuity of services even in the event of DON failure.

• *Trust-minimized governance*: Evolutionary governance and emergent governance are two types of trust-minimizing governance mechanisms. Evolutionary governance is about deploying changes gradually, ensuring the community has the opportunity to respond. Emergency governance refers to vulnerabilities in SC that require immediate intervention to avoid catastrophic consequences. Specifically, emergency governance uses a multi-signature intervention mechanism to ensure that signers dispersed across organizations are always available to authorize emergency changes.

• *Public-key infrastructure*: As decentralization continues to advance, a strong public key infrastructure (PKI) is required to reliably identify network participants, including DON nodes. The foundation of PKI in DON is the Ethereum Name Service (ENS). ENS allows human-readable Ethereum names to be mapped to blockchain addresses. Tampering with the name is inherently as difficult as tampering with the SC that governs it unless the keys are compromised.

3.3. *Cross-chain technology*

A blockchain is a decentralized system powered by distributed ledger technology. It is not a cumulative ecosystem since each blockchain is designed for a particular use. They

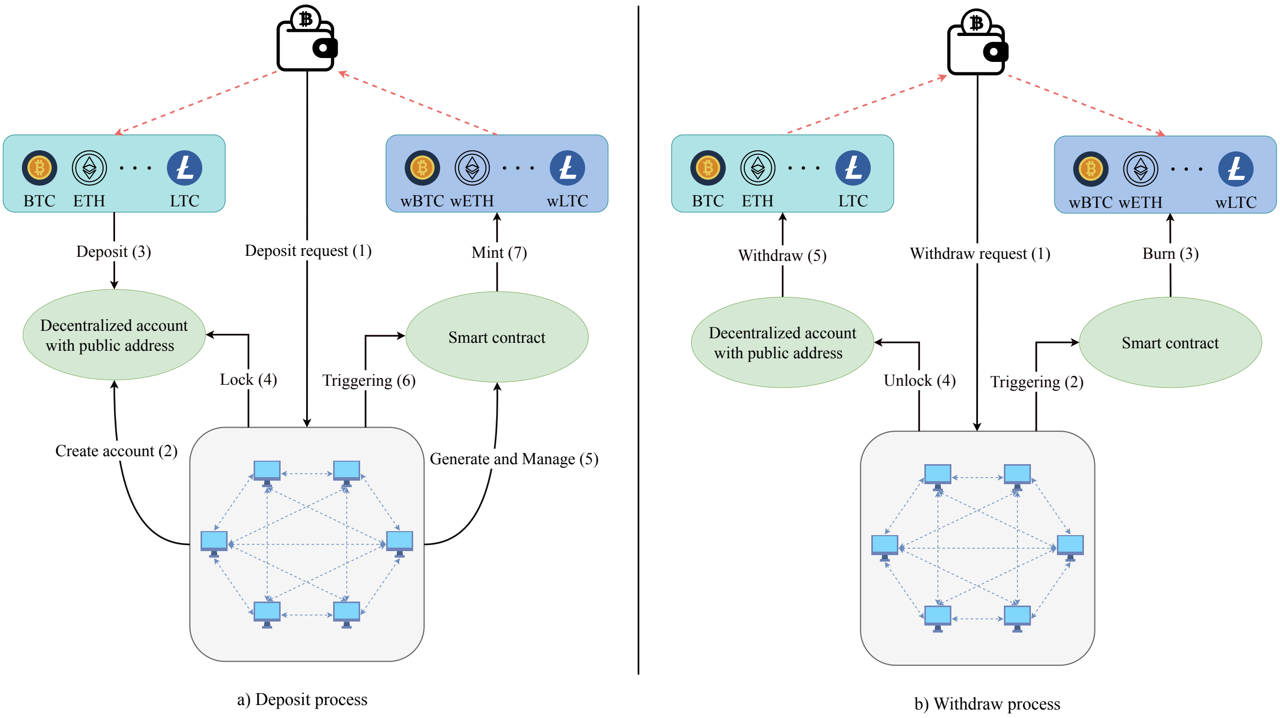

Figure 4: Cross-chain assets deposit/withdraw flowchart.

have specific advantages, limitations, and varying levels of decentralization. For example, if a blockchain aims to achieve high transaction throughput, it may be less decentralized and less secure. Since each blockchain is isolated from the others, leveraging the functionality of one blockchain cannot compensate for another. To fully take advantage of blockchain technology, cross-chain technology was developed to address interoperability which can greatly boost productivity in Web 3.0 [31–33]. Everyone involved will benefit from the increased flexibility, as users will be able to easily transfer assets and data between blockchains [34]. Given the wide variety of bridge designs, the most widely adopted bridge design is based on the lock-mint-burn method as shown in Fig. 4 [35]. This type of bridge designates a public address on the source chain for users to deposit their tokens. On the destination chain, an SC will mint the wrapped tokens 1:1 with the tokens held in the decentralized managed account and send them to the user's wallet.

Cross-chain technology enables trade-offs between two or more blockchains regarding efficiency, decentralization, and security. Additionally, cross-chain technology can improve chain efficiency, reduce fragmentation, and enable a free flow of users and features between multiple blockchains. In recent years, cross-chain platforms with different goals have been developed. For example, tBTC is a decentralized and permissionless bridge between Bitcoin and Ethereum ecosystems [36]. It enables Bitcoin (BTC) holders to gain access to the Ethereum ecosystem and DeFi applications. Parity Bridge is a cross-chain solution connecting fast and cheap Proof-of-Authority chains with the Ethereum public network and other Ethereum-like chains [37]. Wormhole is a communication bridge between Solana and other mainstream blockchains [38]. Existing projects, platforms, and communities can seamlessly transfer digital assets across blockchains by utilizing Solana's high-speed and low-cost features.

3.4. *Layer 2 scaling solutions*

Blockchain-based Web 3.0 will revolutionize the way people transact and transfer value with each other. However, with its rapid development, scalability has become a bottleneck. To solve this problem, scaling solutions developed on top of Layer 1 blockchain networks, also called Layer 2 scaling solutions, are widely adopted. The purpose is to improve the scalability, efficiency, privacy, and other characteristics of the underlying blockchain network.

3.4.1. *Types of Layer 2 solutions*

There are several types of Layer 2 solutions. For example, rollups, state channels, and sidechains. Below is an overview of Layer 2 solutions as shown in Fig. 5.

• *Rollups*: Rollups allow transactions to be executed outside the Layer 1 blockchain. When consensus is reached on the transaction data, the data will be posted back to the main chain and secured by the security mechanism of the underlying blockchain. Specifically, there are two types of rollups in terms of security models: optimistic rollups and zero-knowledge (ZK) rollups [39]. An optimistic rollup is an approach used to scale the Ethereum network by moving some computations and state storage off-chain. In ZK rollups, transactions are bundled into batches and executed outside the Layer 1 blockchain. The summary of changes will be submitted to the main blockchain,

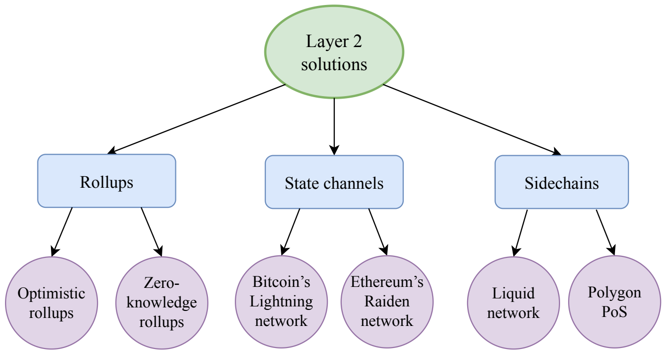

Figure 5: Layer 2 solutions with typical projects.

rather than submitting each transaction individually. To guarantee the correctness of the changes, they provide proof of validity by utilizing ZK proofs. The rollup paradigm is based on a final settlement on the Layer 1 blockchain. It requires rollups to post a copy of every transaction to the Layer 1 blockchain. To address the data availability bottleneck, it is necessary to create dedicated space for rollups. For example, Danksharding scales Ethereum for high throughput by scaling the number of binary large objects attached to blocks from 1 to 64 [40].

- *State channels*: State channels enable participants to securely transact off-chain by utilizing multi-signature contracts. Then, two on-chain transactions that can open and close the channel are submitted for final settlement with the main network [39]. State channels represent a more generalized form of payment channels. They can be utilized not only for payments but also for any state updates on the blockchain, such as changes within a SC. The most well-known examples are Bitcoin's Lightning network and Ethereum's Raiden network. The Lightning Network is a decentralized payments network that runs on top of the Bitcoin blockchain. It greatly improves the scalability of the Bitcoin blockchain by allowing users to make multiple transactions off-chain without broadcasting each transaction to the entire network. Near-instant and low-cost Bitcoin settlements can be achieved between participants. The Lightning Network uses a two-party, multi-signature Bitcoin address to store funds. It requires both parties to agree on the new balance to spend funds from the channel. In this case, the network allows dynamic participation so that payments can be made through a network of channels [41]. Similarly, the Raiden network is Ethereum's version of Bitcoin's Lightning Network. It enables the transfer of tokens that are compliant with the ERC20 standard on the Ethereum blockchain. This is achieved through the use of digital signatures and hash-lock (i.e., balance proof). Digital signatures ensure that neither party can exit any value transfers contained therein, as long as at least one participant decides to submit it to the blockchain. The Raiden balance proof is a protocol executed by the Ethereum blockchain. Since no one other than these two participants can access the tokens stored in the payment channel SC, the Raiden balance proof is as binding as on-chain transactions [42].

- *Sidechains*: A sidechain is an independent blockchain that is linked to the main chain. It allows assets to move between the sidechain and the main chain. The purpose is to solve scalability issues by offloading some of the validation and transaction processing to the sidechain [39]. Sidechains interact with Layer 1 blockchains in two primary ways: the first way is to provide a mechanism (i.e., a cross-chain bridge) for bridging assets from Layer 1 blockchain to their respective sidechain; the second method involves periodically publishing its state snapshots (i.e., highly compressed summaries of the balances of all accounts on its network) to Layer 1 blockchain network [43]. Examples of sidechains include the Liquid network and Polygon PoS. The Liquid Network is a sidechain of the Bitcoin blockchain. It facilitates fast, secure, and private settlement of digital assets. The Liquid-version BTCs are backed by an equal amount of BTCs on the main chain, ensuring verifiable 1:1 backing. This allows users to trade using the speed and confidentiality of the Liquid network [44]. Polygon PoS is a 3-layer architecture sidechain of the Ethereum blockchain to connect Ethereum-compatible blockchain networks. The Ethereum layer consists of a set of staking SCs on the main chain, allowing users to stake tokens to join the system. The Heimdall layer is a validation layer, consisting of PoS Heimdall nodes that run in parallel to the main chain. These nodes monitor the staking SCs and commit checkpoints from Polygon to the Ethereum main chain. The Bor layer is a layer for producing sidechain blocks. It is used to aggregate transactions into blocks for periodic verification by Heimdall nodes [45].

3.5. *Case study*

This section explores how off-chain, cross-chain, and Layer 2 solutions can be integrated to enhance DeFi within Web 3.0. Specifically, a customer holding BTC wants to purchase a product from an online store that only accepts Ether (ETH). This scenario can be efficiently solved using the following Layer 2 payment method.

The process starts with the customer initiating a transaction, specifying the amount of BTC to exchange for ETH. Off-chain computation will be used to search for available quotes, determine the best exchange rate, and find a counterparty willing to exchange ETH for BTC. Once the off-chain computation is complete, a cryptographic proof is generated. This proof verifies the correctness of the exchange rate, the amount of BTC to be exchanged, and the corresponding amount of ETH the customer will receive. The customer then submits this cryptographic proof along with the transaction details to the Layer 1 blockchain for the SC to verify the proof on-chain. Upon successful verification, the customer's BTC is transferred to the counterparty while the counterparty's ETH is transferred to the customer. The process is completed without relying on any central server or intermediary, ensuring decentralized and trustless transactions. With ETH, the customer can use it to pay for the products in the online store by sending the required amount of ETH to the store's wallet address.

It is worth noting that the entire process requires triggering SCs at different stages to achieve the corresponding purpose. Typically, SCs on the public chain (Layer 1) can be invoked by any user with transactions. However, the execution permissions of SCs need to be limited to a restricted set of users to

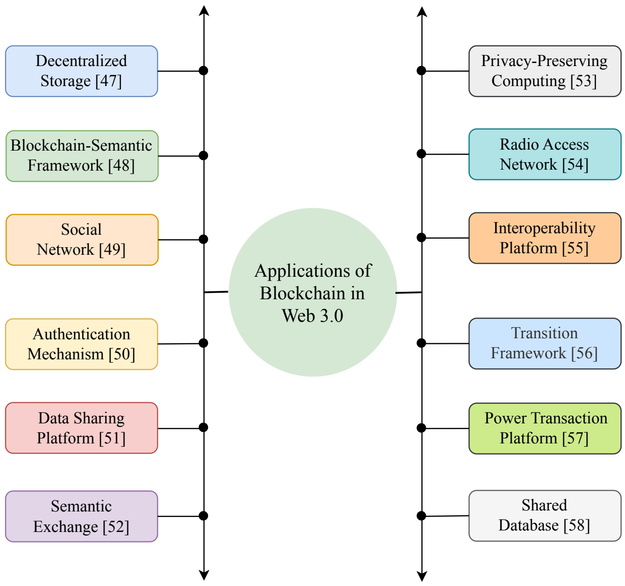

Figure 6: Applications of blockchain in Web 3.0.

ensure security. To solve this problem, the role-based trust management system has been widely studied to regulate the execution rights of SCs. L2DART is a Layer 2 DecentrAlized Role-based Trust management system that integrates on-chain and off-chain functionalities. It is designed to reduce blockchain costs while maintaining blockchain auditability, including immutability and transparency [46]. L2DART can be integrated into the above-mentioned Layer 2 payment method to regulate the execution rights of SCs in dynamic and cross-organizational scenarios. In this context, the integration of Layer 2 solutions with off-chain and cross-chain technologies, governed by sophisticated trust management systems, can facilitate secure, efficient, and cost-effective transactions within the Web 3.0 ecosystem.

3.6. Practical applications of blockchain in Web 3.0

In this section, we further explore the applications of blockchain in Web 3.0, as shown in Fig. 6, to provide intuitions on how to leverage blockchain in the Web 3.0 ecosystem. Benet in [47] designed a P2P distributed file storage system called InterPlanetary File System (IPFS). It is a modular suite of protocols for storing and sharing data, aiming to store files by connecting computing devices around the world to the same file system. It plays a crucial role as the file storage solution underlying the decentralized vision of Web 3.0. Compared to traditional centralized storage solutions, IPFS uses a global P2P network, allowing for permanent and immutable data storage without single points of failure. Its content addressing and distributed hash table technology ensures fast and reliable file retrieval. Lin *et al.* in [48] proposed a blockchain-semantic framework for Web 3.0, aiming to address the problem of unsustainable resource consumption for computation and storage due to the explosive growth of on-chain content and the growing user base. Specifically, an Oracle-based proof of semantic mechanism was introduced to facilitate on-chain and off-chain interactions while maintaining system security. Additionally, a deep learning (DL)-based sharding mechanism was designed to improve interaction efficiency. Palanikkumar *et al.* in [49] proposed a decentralized social network system implemented using the Web 3.0 library, which is a collection of Ethereum JavaScript application programming interfaces (APIs). This library provides functionalities to interact with the Ethereum blockchain. In this way, an Online Social Network service was created in a decentralized manner for democratic self-management. Petcu *et al.* [50] proposed a novel authentication mechanism utilizing Ethereum blockchain technologies, enabling the browser to interact with the user's software and hardware wallets to implement user authentication. With this approach, Web 3.0 authentication could provide enhanced security, privacy, and ownership of user data compared to existing authentication methods that rely on third-party authentication service providers. Razzaq *et al.* in [51] proposed a Web 3.0 Internet of Things (IoT) data sharing framework based on IPFS. Specifically, blockchain and SCs are used to provide data security. Hybrid storage is used to achieve secure data exchange. Additionally, access control policies are stored on-chain to ensure policy integrity and allow for public auditing of any policy changes. Lin *et al.* in [52] proposed a blockchain-based framework for semantic exchange in Web 3.0, which aims to achieve fair and efficient interactions. Specifically, it first tokenized semantic data as non-fungible tokens (NFTs). Trading strategies were then optimized via the Stackelberg game. Afterward, ZK proof was leveraged to allow the sharing of authentic semantic information. Guo *et al.* in [53] proposed a privacy-preserving computing architecture in Web 3.0. The main building blocks are state channel and computing sandbox, used to ensure secure and reliable computation. In addition, the onion routing technology was used to preserve user privacy. Qiu *et al.* in [54] proposed a framework, called FogBC-RAN, to establish a secure and decentralized communication system in Web 3.0. To this end, a cross-chain information transmission process was introduced for efficient cost-sharing. Additionally, a computational offloading strategy using matching game theory was used to minimize the system cost of computationally intensive Web 3.0 applications. Liu *et al.* in [55] proposed an interoperability platform, HyperService, that provides interoperability and programmability between blockchains to make the Web 3.0 ecosystem connected. In particular, HyperService is powered by a unified programming framework for developers and a secure cryptographic protocol for blockchain. Yu *et al.* in [56] proposed a framework called WebttCom that allows for a transition from Web 2.0 to Web 3.0. The proposed framework can build a connection between traditional Web 2.0 applications and Web 3.0 platforms, ensuring data privacy and governance while improving development efficiency. Specifically, an interpreter mechanism was used to aggregate and process requests between the Web 2.0 and Web 3.0 domains. A Web 3.0-based P2P platform, VA3, was developed by Chopra *et al.* in [57] for electricity settlement at an individual level. Specifically, VA3 automates the measurement of power consumption and production by feeding this data into a SC to modify the home router. Then, the SC could automatically manage electricity settlements. Drakato *et al.* in [58] proposed Triastore, a blockchain database system that can store and retrieve machine learning models from the blockchain. To this end, Triastore introduced Proof of Federated Learning for a global model and blockchain consensus for committing the generated model data to a blockchain database. In the context of Web 3.0, the authors claimed that Triastore has the potential for big data analytics in telecommunications and smart city applications.

3.7. Summary and insights

Off-chain, cross-chain, and Layer 2 solutions are critical in the blockchain-based Web 3.0 system. Off-chain technology greatly expands Web 3.0's ability to provide solutions to the real world by connecting on-chain and off-chain resources. Cross-chain technology provides interoperability for isolated blockchain platforms, jointly promoting the development of the Web 3.0 ecosystem. Layer 2 solutions improve the scalability of blockchain-based Web 3.0 by offloading computationally intensive operations. While these technologies demonstrate effectiveness in their respective focuses, which can collaboratively improve the performance of blockchain-based Web 3.0, they exhibit common limitations. Security is a significant and inevitable limitation of new technologies. Specialized solutions in the complex Web 3.0 ecosystem may introduce new vulnerabilities that can be exploited if not managed properly. Furthermore, the risk of centralization arises as these technologies are typically controlled by a limited number of operators, potentially undermining the decentralized vision of Web 3.0. Additionally, the interoperability issue is prevalent as different implementations may not be able to interact seamlessly with each other, resulting in a fragmented Web 3.0 ecosystem. Lastly, user experience may be impacted as the use of these solutions often requires additional steps and technical knowledge, reducing accessibility for non-technical users. Addressing these common limitations (and potentially more) is critical for blockchain-based Web 3.0 to achieve its decentralized vision and gain widespread adoption.

4. AI for Web 3.0: an intelligent and semantic web

AI plays a crucial role in realizing a more decentralized, secure, and user-centered Web 3.0. By effectively integrating AI technology into various areas of the Web 3.0 ecosystem, it is promising to bring about an era of more intelligent, efficient, and personalized digital experiences. However, the dominance of centralization has been a longstanding characteristic of AI-based solutions due to their heavy reliance on centralized massive datasets and computing resources. Traditional AI techniques typically require aggregating large amounts of data and performing computationally intensive training processes. This has inevitably led to the centralization of data and infrastructure on which advances in AI have been built. In contrast, Web 3.0 aims to build a decentralized architecture with no single point of control, raising novel challenges for integrating AI in a manner that is distributed, privacy-preserving, and aligned with

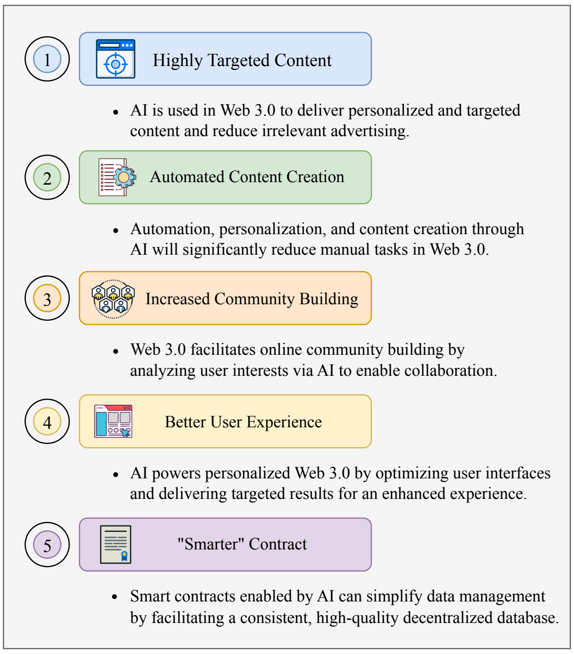

Figure 7: Relevance of AI to Web 3.0.

the vision of decentralization. As we explore the decentralized landscape of Web 3.0, it is necessary to consider how AI can adapt its centralization tendencies in order to flourish in this emerging environment.

In this section, we first show the relevance of AI and Web 3.0. Then we illustrate how generative AI and Web 3.0 complement each other through an in-depth study of generative AI. Afterward, we will introduce the practical applications of AI in Web 3.0. Finally, the summary and insights are provided.

4.1. Relevance to Web 3.0

Web 3.0 represents an intelligent and personalized Web with the goal of providing users with a more seamless experience. AI can drive the applications of Web 3.0 to handle more complex tasks due to its ability to process and analyze large amounts of data. The high correlation between AI and Web 3.0 is summarized in Fig. 7 and discussed further below.

4.1.1. Highly targeted content

Web 3.0 is powered by AI technology to provide consumers with more personalized and targeted advertising. With the ability to understand user intent and preferences, Web 3.0 allows for more effective and efficient marketing campaigns. As a result, annoying and irrelevant advertisements can be eliminated. Only the most relevant content is available to customers. For example, in e-commerce, recommender systems make personalized product recommendations by analyzing users' browsing behavior, search history, and purchase history.

4.1.2. Automated content creation

Web 3.0 allows for the creation of smarter, connected, and interactive web experiences that automate more complex tasks and reduce the need for human intervention. In Web 3.0, automated content creation will become more prevalent through the use of AI technologies. High-quality and dynamic content can be generated based on user queries and preferences. For example, ChatGPT not only helps users generate personalized product descriptions and marketing materials but also optimizes them in a real-time interactive manner.

4.1.3. Increased community building

Web 3.0 is expected to foster community building through the utilization of AI technologies. AI helps connect people with similar interests, skills, and goals by analyzing user behavior and preferences, thereby creating more meaningful discussions and collaborations in online communities to increase engagement and build a sense of community. In this way, the Web will be more interactive, intelligent, and connected.

4.1.4. Better user experiences

The integration of Web 3.0 and AI holds significant potential in enhancing the user experience. AI can deliver more precise and relevant results to Web 3.0 users, as well as personalize their interfaces to improve the usability and accessibility of Web 3.0. In order to accomplish this goal, AI-enabled websites need to classify data and present information that is deemed useful to individual users, providing a personalized and improved navigation experience. Users will search and find what they need more easily and precisely, making Web 3.0 applications more user-friendly. From this point of view, prioritizing user experience throughout the entire development of Web 3.0 applications will be more important than ever.

4.1.5. "Smarter" contract

In the era of Web 3.0, data management will be more important than ever as data becomes more complex and time-consuming to manage. Additionally, the nature of data ownership means that data will not be managed on a central server. As a decentralized solution, SCs can produce a clean version of data by connecting multiple data sources. In particular, when combined with AI, SCs have great potential to improve and simplify data management and avoid duplicate aggregation. If the underlying P2P network of Web 3.0 is regarded as a unified database, AI-powered SCs will facilitate the establishment of a consistent and high-quality database.

4.2. Generative AI

Generative AI has emerged as the most exciting technology of AI advancement over the past three years. It empowers various applications by creating new data that is similar to human-generated data. Notably, generative AI has gained significant interest in semantic communication [59–61] and edge network [62–64]. The rapid growth is attributed to the creation of large language models (LLMs) that may have billions or even trillions of parameters [65, 66]. Unlike traditional AI, which focuses on analyzing and processing existing data to accomplish tasks such as classification and clustering, generative AI creates new and original data by learning patterns and features from existing datasets.

4.2.1. Underlying technologies

Natural Language Processing (NLP) and Computer Vision (CV) are two distinct subfields of AI. The former focuses on the interaction between computers and human language. The latter focuses on enabling machines to interpret and understand visual information. Both are important components of generative AI.

• *NLP*: NLP is dedicated to empowering computers to comprehend and react to text or speech input in the same manner that humans respond to their own text or speech. NLP makes it possible for computer algorithms to effectively summarize massive volumes of information and translate text across languages and spoken commands. This is critical in Web 3.0 as natural language is ambiguous, making it difficult for algorithms to accurately recognize and process text or audio data. With the increase in computing power and a large amount of decentralized data available in Web 3.0, computers will be intelligent enough to interpret information to provide faster and more precise results, which makes machines virtually indistinguishable from human users. Imagine that a voice assistant in Web 3.0 is able to process all the unstructured data on the network. They will comprehend the meaning of anything on the web and deliver a thorough answer rather than merely replying with Wikipedia information and reading Web 2.0 articles [67–69].

• *CV*: CV aims to use computers to extract features from a large number of visual inputs and then provide recommendations. The computer will develop the ability to distinguish between images if enough data is supplied into the model. This will be greatly met in Web 3.0 with the explosive growth of decentralized data volume. Convolutional neural network (CNN)-type algorithms and recurrent neural network (RNN)-type algorithms are the pillars of computer vision [70, 71]. A CNN aids a computer's vision by breaking down an image into labeled pixels which will be further used to perform convolutional operations. Similarly, RNN techniques are applied in video applications to assist computers in understanding the connections between images within a sequence of frames. The development of self-driving cars relies on computer vision to interpret visual inputs from car cameras and other sensors, in order to understand the environment. It is crucial for distinguishing other objects on the road, such as various automobiles, traffic signs, pedestrians, and all other visual information.

4.2.2. Types of generative AI

Generative AI is a form of unsupervised learning, which means that the model learns to generate new data samples without being explicitly told what the correct output should be. Instead, the model is trained on a large dataset of examples and learns to capture the underlying patterns and structures in the data. There are four main types of generative models, including transformers, generative adversarial networks (GANs), variational autoencoders (VAEs), and autoregressive models.

• *Transformers*: A transformer model is a neural network that understands contextual meaning by analyzing relationships and patterns in sequential data [72]. It is based on an attention mechanism to selectively prioritize different parts of the input sequence to produce relevant outputs. It consists of an encoder and a decoder. The encoder processes input sequences to generate latent representations that capture semantic information. One of the key advantages is its ability to process input sequences in parallel, which makes it much faster than traditional RNNs for long sequences. This, together with its effectiveness in capturing long-range dependencies (a subtle way of detecting the interactions and interdependencies of even distant data elements in a series of data), makes the transformer model a fundamental model driving a paradigm shift in AI.

• *GANs*: One of the key breakthroughs in the development of generative AI was the introduction of GANs [73]. A GAN involves a generator and a discriminator. These two networks oppose each other, using a two-player game-like approach to generate new data. The generator generates new data based on patterns it learns from the training dataset while the discriminator evaluates the authenticity of the generated data. This adversarial training approach allows the generator to generate data that is indistinguishable from real data, while the discriminator has enhanced capabilities in identifying the generated data.

• *VAEs*: A VAE is a neural network for unsupervised learning of complex data distributions [74]. It involves two subprocesses: the encoder maps input data into a latent space; the decoder then draws samples from the data distribution in this latent space to generate the output. Unlike traditional autoencoders, VAEs introduce randomness into the encoding process, which allows them to be used in generative AI for generating new data with similar patterns to the input data. Furthermore, they could be combined with other generative models to create more advanced and powerful generative models.

• *Autoregressive models*: An autoregressive model is a statistical model used for forecasting future values in time series data based on prior observations [75]. It is assumed that there is an auto-correlated structure in the data where the current value of a time series can be modeled as a linear combination of prior values in the series. The term "autoregressive" comes from the fact that these models involve regressing a time series data to its own past values. However, autoregressive models are primarily used for stationary time series with constant mean and variance over time. Non-stationary time series may require transformation before applying an autoregressive model.

4.3. Generative AI for Web 3.0

Web 3.0 is envisioned to transform the Internet into a semantic, intelligent, and user-centric platform where information is interconnected through semantic understanding. Generative AI plays a crucial role in realizing this vision. There are four key drivers for integrating generative AI into Web 3.0, i.e., truly bringing semantics to Semantic Web 3.0, efficiently developing Web 3.0, easily performing data analysis, and proactively providing security assistance.

4.3.1. Semantic understanding

Web 3.0 proposes a digital realm where machines can interact and communicate with both other machines and human users. However, in order for machines to precisely and effectively communicate, they must first understand the meaning and subtle differences of digital information. This is why generative AI will be the cognitive layer of Web 3.0, driving machines to comprehend various types of content through DL algorithms. For instance, text, audio, images, and video. An increasing number of practical applications also highlight the advantages of incorporating semantic capabilities into the Web 3.0 ecosystem. For example, Alice is the first intelligent non-fungible token powered by GPT-3, allowing it to adjust how it interacts with people based on each new interaction [76]. Pregelj in [77] introduces a ChatGPT-based Web 3.0 plugin that enables wallet creation, on-chain queries, and on-chain operations directly from prompts. SuperCool AI is a digital marketplace based on generative AI that generates and trades NFTs via prompts [78].

4.3.2. Efficient development

To realize the decentralized and intelligent vision of Web 3.0, SCs are indispensable because most of the core applications and services in Web 3.0 are built on SCs. These include the creation and trading of NFTs, the development of decentralized applications (dApps) in the DeFi field, and the formulation of decentralized autonomous organization (DAO) rules, etc. Generative AI can revolutionize the way SCs are created as they are essentially self-executing contracts with terms and conditions programmed directly into the codes. By understanding context and expected outcomes, generative AI can advance the Web 3.0 ecosystem by efficiently developing SC code that ensures compliance with predefined rules. For example, Web3-GPT is a chat assistant based on GPT4 that combines LLMs and AI agents, aiming to revolutionize the development and deployment process of SCs [79]. ETHGPT is a development toolkit that supports semantic search to provide professional tools and assistance to support the rapid development of the Web 3.0 ecosystem [80]. FlashGPT can efficiently generate and deploy secure and reliable Solidity SCs to a variety of Layer 1 and Layer 2 solutions through simple interactions [81].

4.3.3. Data analysis

In the user-centric Web 3.0 ecosystem, generative AI will play an important role in simplifying data analysis. Through natural language interfaces, generative AI can quickly and accurately analyze complex datasets based on simple prompts from users, providing users with valuable insights. In this way, generative AI eliminates the need for Web 3.0 users to master relevant programming languages or advanced data analysis knowledge by automating data processing behind the scenes, lowering the barrier to participating in the Web 3.0 economic ecosystem. For example, TokenGPT aims to simplify complex Web 3.0 investing by using generative AI to review SCs to conduct a comprehensive analysis of the market [82]. CoinGPT is a generative AI-driven data analytics tool that allows users to connect their crypto wallets and analyze the transaction history of NFTs and other cryptocurrencies to improve transaction performance [83]. Defi-Companion is a ChatGPT-based bot that assists Web 3.0 users in querying data from endpoints, performing data analysis, and identifying DeFi opportunities [84].

4.3.4. Security assistance

Security is critical to the Web 3.0 ecosystem. The P2P architecture, consensus mechanism, and cryptographic protocol of blockchain technology provide the first level of security, preventing 51% attacks, double spends, Sybil attacks, etc. However, these guarantees are not sufficient for complex Web 3.0 systems. Various security and reliability issues may still arise. Generative AI is a promising solution that provides additional protection for Web 3.0 users and their data through continuous monitoring of SCs. For example, Aegis aims to provide an SC auditing service through generative AI, effectively responding to evolving threats and preserving the resilience of SCs over time [85]. A generative AI framework called "Lightning Cat" was proposed to enhance vulnerability detection in smart contracts, aiming to improve the overall security of smart contracts and protect against potential exploitation by malicious actors [86]. Secure Semantic Snap, a ChatGPT-based MetaMask Snap, can semantically understand the target contract to protect users from malicious SCs [87].

4.4. Web 3.0 for generative AI

Data and computing power are considered to be the two major elements that promote the development of AI. The development of these two elements has also become a booster for the explosion of AI technology. Based on the generative models, generative AI typically requires a significant amount of computing power and data. This is because generative AI models are built on complex mathematical algorithms that need to analyze large data sets to identify patterns and generate new content. In addition, training these models is computationally intensive, particularly for models that deal with high-resolution images or real-time processing. Today, LLMs are booming. However, the scale of LLMs has dramatically increased which could be a major obstacle for the majority of organizations. The high computational demands also restrict its use in computing environments with constrained resources, such as mobile devices or edge computing systems.

4.4.1. Current solution of generative AI

The current solution is cloud computing, as it provides the necessary computing resources and infrastructure required to develop and deploy chatbots at scale. Different chatbots can be deployed on different cloud computing platforms, depending on their specific needs and requirements. For example, ChatGPT is running on Microsoft Azure while Bard is executing on the Google Cloud platform. The cost of training such models is growing exponentially, which is unacceptable for many organizations. Ultimately, the tech giants will continue to dominate the market for generative AI, meaning that the value generated by this phenomenal field will be drawn by these large companies. This is still the typical way of operating in the Web 2.0 era, which is large-scale and highly centralized.

4.4.2. Web 3.0 as a solution

In the trend of decentralization, cloud computing solutions represent a compromise for the emerging industry. Web 3.0 provides a decentralized coordination platform that will facilitate unprecedented innovation and the adoption of generative AI. The enormous amount of data available for research, development, and industrial use is one of the key factors enabling the rapid development of generative AI. Accordingly, relevant solutions in this area have also received wide attention. For example, MedDAO is an innovative DAO dedicated to addressing the critical issue of the shortage of medical images in training AI models within the global healthcare field. Specifically, MedDAO creates aggregated and decentralized datasets by providing an anonymous, encrypted, and secure healthcare platform that incentivizes patients to contribute personal data [88]. A data-driven economy makes data the new gold. Correspondingly, computing power will be an important tool for contemporary "gold diggers". Under the status quo of the technological monopoly of tech giants, the Web 3.0 ecosystem will effectively promote the broader development of generative AI. Data-driven industries are no longer just limited to large technology companies. Small-scale institutions and individuals will also benefit greatly, which is consistent with the vision of Web 3.0. Generally, how Web 3.0 can solve the dual challenges of data and computing power faced by generative AI can be elaborated from several main aspects as shown in Fig. 8.

- *Decentralized storage*: Web 3.0 infrastructure can provide a more effective data storage solution. Instead of centralized servers, data can be stored on decentralized networks. In addition, there are technologies that allow for decentralized data storage such as the IPFS. In this way, generative AI models can access data from various sources, reducing the burden on individual computers and thereby assisting in solving the issues of data accessibility and availability for generative AI that the existing system confronts.

- *Data provenance*: Data provenance is a fundamental consideration in generative AI as it creates new data from existing data. Therefore, understanding the provenance of the training data is critical to assessing the quality and trustworthiness of the generated data. Web 3.0 enables the creation of a tamper-proof record of data provenance and data integrity. By ensuring that the data used to train AI models is trustworthy and comes from a reliable source, the accuracy and quality of generative language models can be improved.

- *Data sharing*: Web 3.0 can effectively facilitate data sharing as it provides accountability and transparency regarding data access. Users will have absolute control over their data, as they possess ownership of their personal data and digital identity through private keys that are exclusively under their control. Through protocols like IPFS, users can choose which data to share and with whom. Additionally, the network allows for secure data sharing through technologies such as threshold secret sharing [89, 90] and revocable data sharing [91, 92]. This means individuals and organizations can share data to jointly train generative AI models through collaborative learning and secure multi-party computing schemes without compromising their privacy.

- *Decentralized computing*: Web 3.0 enables decentralized computing through the use of blockchain networks. By lever-

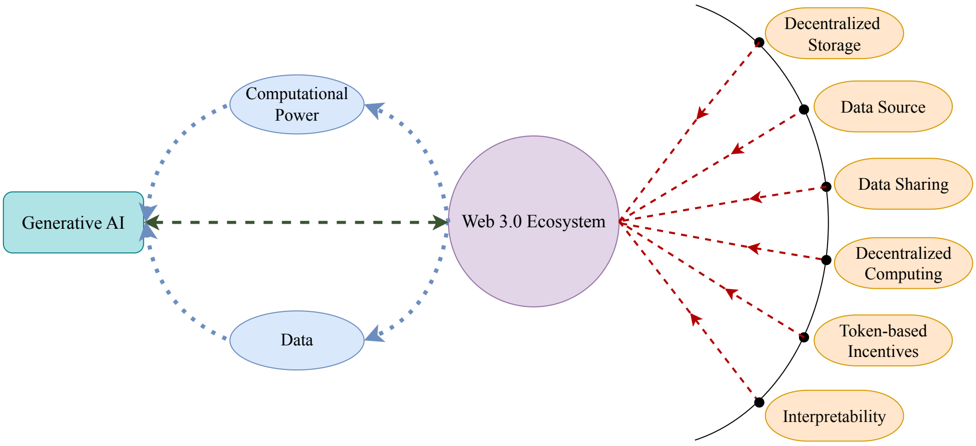

Figure 8: Web 3.0 reduces the requirements for generative AI development.

aging the computing power of a network of decentralized computers, Web 3.0 can provide a more efficient and scalable computing environment for generative AI. In this case, instead of relying on a single, centralized server or data center to perform computational tasks, blockchain-based networks can distribute computational tasks across decentralized nodes coordinated by the Web 3.0 platform.

• *Token-based incentives*: Web 3.0 allows users to monetize their data using SCs. This is a key feature of Web 3.0, where users can sell their data directly for profit without the involvement of third parties. Small companies and individuals will benefit from such a marketplace platform as it removes barriers, levels the playing field, and promotes innovation. Additionally, idle computing power could also be sold. Graphics processing units used for gaming are typically utilized only a fraction of the time. Gamers can bid and receive payment for their idle computing power using SCs. In this case, AI developers can utilize this computing power to train and deploy their models.

• *Interpretability*: The interpretability of DL has long been a bottleneck. DL-based generative AI inherits this. Due to the dramatic increase in the size of language models, interpretability has become more important than ever. Web 3.0 allows all data processing and decisions to be tracked via blockchain. In turn, the generative paradigm of the data is analyzed in depth to achieve a constant understanding of generative AI and achieve effective control over it.

4.5. Practical applications of AI in Web 3.0

In this section, we further explore the applications of AI in Web 3.0 as shown in Fig. 9, to provide intuitions on how to leverage AI in the Web 3.0 ecosystem. Yu *et al.* in [93] proposed a framework for classifying referable NFTs (rNFTs) using graph convolutional networks (GNNs). The goal was to provide an effective recommendation system for Web 3.0 assets. First, the authors converted rNFT reference relationships into direct acyclic graphs. Then, the node and edge characteristics were modeled based on rNFT metadata and token transactions. Afterward, GraphSage was modeled to contain the characteristics collected during the learning process. In this way, the model combined considerations of graph topology and attribute characteristics to enable supervised classification of existing and incoming NFT nodes. Alarab and Prakoonwit in [94] developed a classification model that utilizes a combination of long-short-term memory (LSTM) and GNN to classify illicit transactions in the Elliptic Bitcoin dataset based only on transaction features. By studying different acquisition functions under the same experimental settings, the proposed model could achieve an accuracy of 97.77%. Xu *et al.* in [95] introduced a quantum blockchain-powered Web 3.0 framework to provide information-theoretic security for decentralized data transmission and payment to cope with the situation that quantum computing subverts the conventional cryptosystems. In particular, an optimal auction for NFT transactions based on quantum DL is proposed to maximize revenue with sufficient liquidity in Web 3.0. Madhwal and Pouwelse in [96] implemented a decentralized social recommendation system, Web3Recommend, that aimed to generate balanced recommendations for trust and relevance on Web 3.0 platforms. It addressed the challenges of generating recommendations in decentralized networks that lacked central authority and were vulnerable to Sybil attacks. Web3Recommend combined MeritRank (a decentralized reputation scheme that provides Sybil resistance) and SALSA (a personalized graph algorithm). Specifically, MeritRank added decay parameters to SALSA to theoretically guarantee protection against Sybil attacks. By integrating with Music-DAO, an open-source Web 3.0 music-sharing platform, the proposed system was shown to generate personalized real-time recommendations. Unzeelah *et al.* in [97] proposed an AI-powered method to build a secure, reliable, and efficient platform in Web 3.0 to address the issues of misleading content and fake news spreading on current platforms. To this end, NLP technologies and DL models were implemented. For example, LSTM with Word2Vec and GloVe were used for word embeddings. Additionally, the combination of the Ethereum blockchain with the IPFS technique was utilized to decentralize the system and enable off-chain storage. Kim *et al.* in [98] presented a novel security mechanism using blockchain network traffic statistics as a metric for identifying malicious events. Specif-

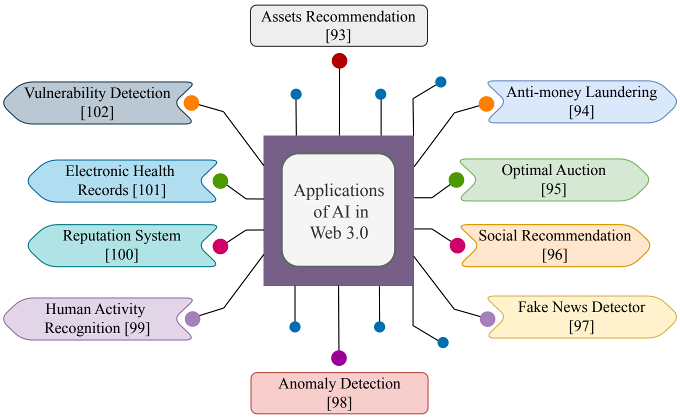

Figure 9: Applications of AI in Web 3.0.

ically, a data collection engine periodically generated multi-dimensional, real-time data streams by monitoring underlying blockchain activities. Afterward, an anomaly detection engine was used to detect anomalies from the generated data instances based on One-class Support Vector Machine or AutoEncoder. Thien Huynh-The *et al.* in [99] proposed an efficient Human Activity Recognition approach that exploited an intermediate fusion model to integrate DL with traditional feature extraction. Specifically, the proposed method transformed segmentation data from multiple sensors into activity images, which were then processed using a deep convolutional neural network (DCNN). Next, this DCNN utilized innovative residual triple convolutional blocks to extract the correlations between features. Additionally, handcrafted statistical features were combined with deep features to train a multiclass support vector machine classifier to improve the model accuracy. Keizer *et al.* in [100] introduced the need for a decentralized trust and reputation system on the Web 3.0 platform by discussing the trust issues arising from Web 3.0's distributed shared services. Specifically, this paper proposed a framework based on deep reinforcement learning that allows reputation scores to be calculated in a decentralized manner while still being personalized for each user. Mistry *et al.* in [101] proposed a novel scheme for maintaining Electronic Health Records (EHR), aiming to provide a reliable, secure, and robust storage system for EHR by integrating AI and blockchain technologies. Specifically, the system utilized artificial neural networks to classify patients as COVID-19 positive or negative based on clinical and computed tomography scan reports. The data of positive patients would be stored on the blockchain through the IPFS protocol, ensuring that authorized entities could access it safely and reliably after verification. Additionally, the system could employ advanced networking technologies to solve latency and reliability issues and facilitate real-time data transmission. Zhuang *et al.* in [102] investigated the application of graph neural networks for detecting vulnerabilities in SCs. Specifically, it involved constructing a contract graph that captures both syntactic and semantic features of the SC. An elimination phase was then employed to normalize the graph and emphasize the major nodes. Additionally, the paper introduced a degree-free graph CNN and a novel temporal message propagation network to enhance learning from the normalized graphs, improving the effectiveness of vulnerability detection.

4.6. Summary and insights

Web 3.0 is a user-centric web where users can create and trade digital assets. Generative AI and Web 3.0 have great potential to reinforce each other significantly. On one hand, Generative AI lowers the barriers that ordinary users face when entering the Web 3.0 world through its powerful API. Its semantic understanding capabilities allow users to easily create exclusive NFTs, providing a solid foundation for participating in the digital economy. On the other hand, Web 3.0 can alleviate the large demand for data and computing power of generative AI by distributing computational tasks in a decentralized network, reducing reliance on centralized servers. In this way, lightweight, personalized, and even decentralized generative AI will become possible. Despite these promising aspects, ethical considerations such as data bias and lack of model explainability must be prioritized to effectively and safely integrate generative AI into Web 3.0 environments. AI systems may perpetuate or even amplify existing biases in the training data, leading to unfair and potentially harmful outcomes. For example, if an AI system used for recruitment is trained on a biased dataset of applicant resumes, it may unconsciously exclude or marginalize certain groups in its output. Additionally, the black-box nature of AI models makes it difficult for people to understand the decision-making process. This lack of transparency can severely impact user trust and limit the adoption of AI-driven applications in Web 3.0. To create a robust and trustworthy Web 3.0 ecosystem, addressing these challenges is critical to seamlessly and ethically integrating generative AI into the decentralized web.

5. Edge computing for Web 3.0: an interconnected and ubiquitous web

Web 3.0 is expected to be an interconnected and ubiquitous web that is accessible to everyone and anywhere at any time. With the rise of IoT devices and the increasing need for low-latency and real-time data processing, edge computing has become an important part of the Web 3.0 ecosystem. Edge computing is essentially a distributed computing paradigm in which computing services occur at the edge of the network as opposed to being performed in centralized data servers. Users can benefit from faster service via edge computing by bringing computing resources and data storage closer to where users actually consume the data.

In this section, we will first illustrate the close correlation between edge computing and Web 3.0. Then we will explore the integration of edge computing and other cutting-edge technologies to promote the development of Web 3.0. Specifically, we proposed two solutions for decentralized storage and computing. Afterward, we will introduce the practical applications of edge computing in Web 3.0. Finally, the summary and insights are provided.

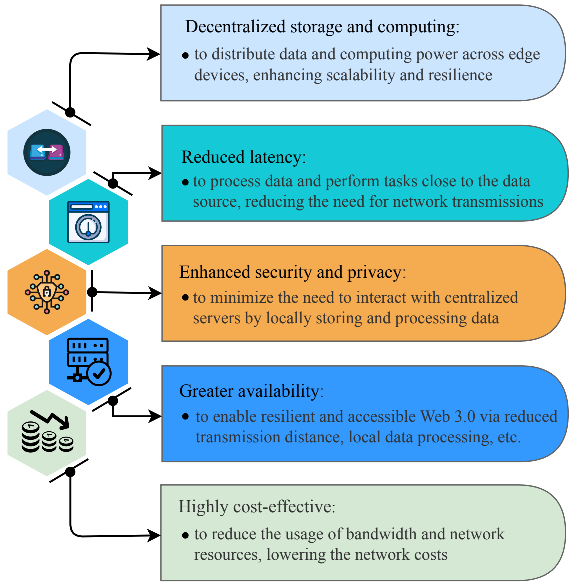

Figure 10: Relevance of edge computing to Web 3.0.

5.1. Relevance to Web 3.0

Web 3.0 is a network of ubiquitous connectivity that aims to create a collaborative platform that everyone can access anytime, anywhere. The decentralized infrastructure of edge computing is highly compatible with this vision of Web 3.0. Specifically, edge computing can support Web 3.0 in the following aspects as shown in Fig. 10.

5.1.1. Decentralized storage and computing

Edge computing plays a crucial role in facilitating decentralized storage and computation in the Web 3.0 ecosystem. With edge computing, users are able to store and process data in edge devices without relying on centralized servers. This increases users' control over their data. In addition, edge computing can distribute storage and computing tasks across edge devices, making Web 3.0 more scalable and resilient [103]. In this way, users can also share or monetize their idle storage space and computing power on the Web 3.0 platform, which contributes to the realization of data ownership and fair incentives in Web 3.0.

5.1.2. Reduced latency

Edge computing can significantly reduce the latency of Web 3.0 applications, improving the overall performance of the Web 3.0 ecosystem. Edge devices can process data and perform tasks close to the data source, reducing the need for network transmissions. This is important for Web 3.0 applications as they typically require real-time interactions. With the proliferation of 5G, fast communication with edge devices has been greatly improved. Users can get fast responses from Web 3.0 applications running on edge devices. Therefore, with the help of edge computing, the user experience can be greatly enhanced, driving the widespread adoption of Web 3.0.

5.1.3. Enhanced security and privacy

In the architecture of edge computing, the natural isolation of edge devices improves the overall security and privacy of the Web 3.0 ecosystem. In edge computing, data is stored and processed locally on edge devices, minimizing the need for data to travel to and from centralized data servers. This reduces the risk of data being compromised during transmission. In addition, distributed data storage and processing across a wide range of edge devices protects data from a single point of failure. As data is fragmented and stored on multiple edge devices, an attacker would need to simultaneously compromise a significant number of devices to access or tamper with the information, which is challenging. For example, in the well-designed Web 3.0 ecosystem with Byzantine fault tolerance, an adversary might need to corrupt more than 33% of the devices to attack the system. Otherwise, the Web 3.0 ecosystem can continuously provide services. Moreover, since data is stored and processed on edge devices, without being collected by the centralized data servers, data privacy can be enhanced.

5.1.4. Greater availability

The Web 3.0 ecosystem needs to function regardless of connectivity. The architecture of edge computing can provide the resilience to prevent a single point of system failure. In addition, edge computing allows data to be stored and processed locally on edge devices close to where data is generated. This can significantly shorten the distance of data transfer. Moreover, edge computing allows local edge devices to perform data preprocessing, content caching, and load balancing. This reduces the amount of data that needs to be transferred over a constrained network. These three aspects improve the availability of Web 3.0 as well as the accessibility of its applications.

5.1.5. Highly cost-effective

Mass adoption of Web 3.0 will benefit from a variety of applications. Edge computing provides a more cost-effective solution for application development and deployment by allowing businesses or individuals to utilize edge devices. Specifically, edge computing enables the utilization of existing client devices, thereby eliminating the requirement for costly infrastructure. As such, the development of edge applications requires less upfront equipment investments and deployment time. Moreover, with edge computing, businesses can optimize their IT costs by processing data locally rather than in the cloud or large data centers [104, 105]. In the Web 3.0 ecosystem, enterprises will benefit from utilizing edge computing infrastructure to reduce dependence on cloud providers, resulting in lower workloads and faster content delivery. For example, MadeiraMadeira, a leading Brazilian retailtech, has significantly reduced its operating costs by offloading up to 90% of transmitted data to edge computing resources [106].

5.2. Integration of edge computing and blockchain: a storage solution for Web 3.0

Edge computing and blockchain are separate but interdependent technologies in Web 3.0. Edge computing can provide the infrastructure for blockchain nodes to store and verify transactions. Blockchain, on the other hand, can be truly decentralized by creating an open and secure computing environment. Since both edge computing and blockchain are developed based on the concept of decentralized and distributed networks, they can become a powerful combination by complementing each other [107, 108]. The main benefit of this combination is that it enables secure communication and data processing, including data storage and computation, without the need for centralized servers. In this section, we will discuss in-depth how the integration of edge computing and blockchain can provide a decentralized storage solution for Web 3.0 applications that require high performance, low latency, secure, and decentralized storage. Specifically, we will first introduce the main building blocks. Then, we will parse their functionalities to propose an edge storage solution.

5.2.1. Building blocks

The proposed decentralized storage solution consists of four main functional modules: network architecture, incentive mechanism, data integrity, and access control. These modules play a vital role in ensuring the effectiveness and security of the storage system.

• *Network architecture*: Edge nodes act as storage nodes while edge devices act as data centers. These edge nodes are registered on the blockchain network in a specific way to provide excess storage space that can be used by the storage network. For example, a deposit is required to complete registration on the Ethereum network. When data needs to be stored, the data is distributed to available edge nodes for redundant storage. The reliability of storage is guaranteed by the blockchain-based token system. Blockchain networks run in parallel to act as administrators. Data is hash-mapped to corresponding edge node locations for tracking and maintenance. In addition, the blockchain strictly enforces the access control mechanism and verifies the integrity of the data. Incentives are made by tracking and monitoring the amount of storage provided by each edge node and the integrity of the data. Users and dApps interact with the storage network through APIs that communicate with the blockchain network. Specifically, edge nodes provide a decentralized storage layer. Blockchain manages the storage network and enforces policies. The API acts as the interface between users and dApps. The key is that this architecture combines the advantages of blockchain with the distributed resources of edge computing.

• *Incentive mechanism*: An important component of this storage solution is the incentive mechanism that rewards edge nodes for providing storage. An effective incentive mechanism can solve the information asymmetry problem between users and the network [109]. When an edge node initially registers to join the network, it needs to deposit a certain amount of tokens. The deposited amount depends on the amount of storage that the edge node wishes to provide. This ensures that edge nodes are committed to providing reliable and accessible storage. If an edge node does not perform as promised, it will lose the deposited tokens. On the other hand, edge nodes can obtain corresponding rewards by meeting certain conditions. For example, they provide the amount of storage promised at registration and keep that storage accessible. They also need to regularly verify data integrity.

• *Data integrity*: Blockchain verifies the integrity of data by maintaining hash values. When data is uploaded to the storage network, SC is responsible for distributing it to available edge nodes. Specifically, edge nodes first hash the data to generate a unique hash value. Then, the hash value and corresponding metadata will be recorded on the blockchain. Notably, edge nodes must periodically provide hash values of the data to prove that they have the correct version of the data. In this way, it can be ensured that the data stored on the edge nodes matches the original data uploaded to the storage network. If an edge node fails to provide the correct hash value, it will be tagged as an invalid storage node. Users can choose whether to download the required data according to the latest tag. The downloaded data is hashed locally using the same algorithm (e.g., SHA256). This local hash value is then compared to the hash value stored on the blockchain. If the hashes do not match, the data has been corrupted or modified. Users will need to re-download the required data from other edge nodes. In this way, even if some edge nodes are offline, users can obtain the correct data with the help of the original hash value stored on the blockchain.

• *Access control*: As a Web 3.0 storage solution, blockchain does not exist as a database but is used as a decentralized and immutable ledger. Data ownership, access rights, and decryption keys are all recorded on the blockchain. A large number of edge devices serve as actual storage units. At this point, the encrypted data is stored on the edge device, while the decryption key is managed by the blockchain. When a user requests access to the data, the blockchain is first responsible for checking whether the user has the appropriate permissions. Access rights can also be further divided and enforced by the blockchain. For example, a small number of designated users can read and write data, while other users can only read data. In addition, access rights can be restricted to access only specific parts of the data, rather than the entire dataset. Authenticated users will be given the appropriate decryption key to access the data. The blockchain distributes the decryption keys only to users with appropriate access rights. In this case, only authorized users with the correct decryption key can access the data. This ensures that data remains secure even if the edge node is compromised. Moreover, activity logs of access attempts, key distribution, and successful access are recorded in the immutable ledger so that any unauthorized access attempts can be detected.

5.2.2. A decentralized storage solution

The proposed framework (see Fig. 11) aims to provide decentralized, secure, reliable, and low-latency storage by utilizing the integration of distributed edge resources with blockchain technology. Edge nodes first register on the blockchain network. As part of the registration process, edge nodes must post a deposit of a certain value to signify their commitment to providing storage resource services. A blockchain-based token incentive system is used to reward edge nodes for reliably con-

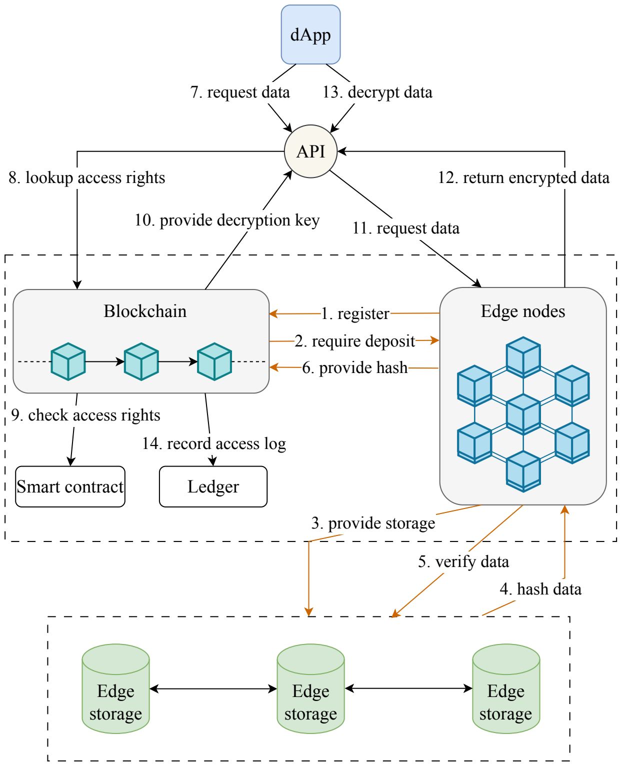

Figure 11: A decentralized storage solution in Web 3.0.

tributing their storage. When storing data, edge nodes initially hash the data through a cryptographic hash function, such as SHA256, to generate a unique identifier. Edge nodes are then responsible for periodically verifying data integrity by comparing hash values. The latest hash is submitted to the blockchain network for review and modification, in order to ensure only valid data hashes are maintained. This allows data reliability and integrity to be guaranteed even if some edge nodes become unavailable. Additionally, the blockchain network is used to manage access control, decryption keys, and access logging in a decentralized manner. Specifically, when a dApp requests data through the API, the blockchain uses predefined SCs to check whether it has the appropriate access right. If authorized, the blockchain will provide the decryption key to the API. The API then requests data from the specified edge node and returns encrypted data. At this point, the API can use the key to decrypt the encrypted data and provide the plaintext to the user. Afterward, the blockchain records an immutable log of the access.

5.3. Integration of edge computing and AI: a computing solution for Web 3.0

The convergence of edge computing and AI is known as edge AI, where AI models are deployed and executed at the edge of the network, close to where the data is generated [110–112]. Edge AI is a promising combination for enhancing the functionalities of Web 3.0. With edge AI, edge devices can perform data analysis locally, without relying on traditional centralized servers. In this way, Web 3.0 applications that require high-speed data processing can give fast responses to complex environments. For example, edge AI can power edge devices such as robots, drones, and self-driving cars that require real-time analysis of sensor data. Edge AI can also improve the privacy and security of Web 3.0 applications by processing data at the edge device. In addition, since the architecture of edge computing is distributed and redundant, the Web 3.0 system can continue to operate even if some edge nodes are damaged or offline. All of these characteristics are highly compatible with the Web 3.0 vision. In this section, we will proceed to explain how edge AI can provide a decentralized computing solution for Web 3.0. Specifically, we will first introduce the main building blocks. Then, we will use a sequence diagram to demonstrate the proposed edge AI-based decentralized computing solution.

5.3.1. Building blocks

The proposed decentralized computing solution consists of five core components: network deployment, model deployment, incentive mechanism, collaborative learning, and communication-efficient protocol. They are designed to function in an integrated manner to facilitate efficient and effective edge operations.

- *Network deployment*: The first step is to deploy an edge network consisting of a large number of edge devices. Edge devices refer to any machines at the edge of the network that can perform specific tasks. For example, various types of IoT sensors, edge servers, smart devices, and so on. Specifically, IoT sensors are responsible for collecting data from the surrounding environment. Edge servers are designed to aggregate data from multiple IoT sensors and perform computations accordingly. Smart devices can both collect and process data.

- *Model deployment*: Through the edge network, AI models can be deployed to edge devices as needed by Web 3.0 applications. These AI models can perform various tasks such as CV, NLP, and predictive analytics. Specifically, CV models can be deployed on edge devices such as cameras and IoT sensors for object detection and recognition. NLP models can be used to perform language-related tasks on smart devices. Predictive models can analyze real-time data streams from IoT sensors for anomaly detection and predictive maintenance.

- *Incentive mechanism*: A proper incentive mechanism is significant for developing decentralized computing solutions in the Web 3.0 ecosystem. Owners of edge devices will have an incentive to participate and share their data and computing resources, driving more effective edge AI-based computing solutions. Rewards can be offered in a variety of ways. For example, owners of edge devices and data contributors can be rewarded with tokens for sharing data and resources. In the decentralized community, they can also gain a higher reputation, such as badges and rankings, for the quantity and quality of data and resources they provide, thereby unlocking more community services.

- *Collaborative learning*: Collaborative learning is fundamentally a decentralized form of learning, which matches the decentralized nature of Web 3.0. In the context of edge AI, each edge device can train a local model based on the local data. Then honest edge devices within the edge network collaborate and share parameters to create a more general global model.

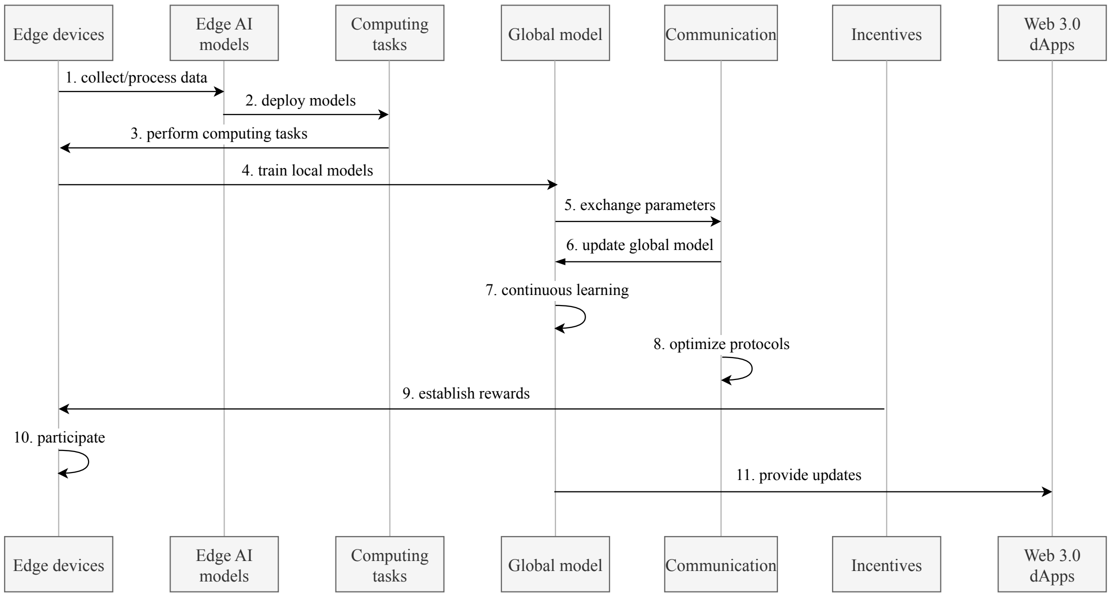

Figure 12: Workflow of a decentralized computing solution in Web 3.0.

Since there is no central authority, edge nodes can exchange learning parameters through P2P communication to optimize the global model. Furthermore, collaborative learning can help improve the global model by combining data from multiple data resources without sharing the original data.

• *Communication-efficient protocol*: Communication overhead is often the bottleneck in distributed systems. The performance of a distributed system is usually measured by the communication complexity. Communication complexity refers to the amount of data that needs to be communicated in the form of bits or messages between edge nodes in the network. Reducing communication complexity is critical to the scalability, bandwidth requirements, and network latency of the Web 3.0 ecosystem. There are several ways to significantly reduce communication overhead. First, the most fundamental way is to develop communication-efficient decentralized algorithms. Second, priorities can be assessed based on the incentive mechanism. In this way, the model parameters provided by edge nodes or devices with high priority will be adopted. Finally, limiting the frequency of model updates is also a straightforward way to reduce communication overhead. For example, changes in model parameters of edge nodes or devices only trigger communication when a certain threshold is reached.

5.3.2. A decentralized computing solution

As shown in Fig. 12, deploying edge AI models can process data efficiently and effectively. This eliminates the need for extensive data exchange with centralized servers and provides real-time feedback to perform tasks such as object detection using computer vision or malware analysis using LLMs. Edge devices train local models using their own data and share parameters with the global model. This sharing enables the global model to be continuously improved through collaboration, creating a positive loop ecosystem. Optimization of communication protocols is critical to creating decentralized ecosystems where data and resources may be limited, as they allow efficient sharing of parameters between edge devices and global models. By optimizing communication, the communication overhead of edge devices is mitigated, making it easier for them to participate and contribute to the growth and improvement of the global model. The incentive mechanism creates a mutually beneficial relationship that can further encourage edge devices to share resources and strengthen the global model to support various applications in the Web 3.0 ecosystem.

5.4. Case study on the integration of edge computing, AI, and blockchain in Web 3.0

In this section, we explore the security and privacy issues associated with unmanned aerial vehicle (UAV)-assisted mobile edge computing (MEC) systems within the Web 3.0 scenario. With the rapid advancement of IoT and 5G technologies, the number of mobile devices has increased dramatically, leading to the emergence of computationally intensive tasks such as self-driving cars and navigation systems. However, mobile devices often have difficulty completing these tasks due to limited computing power. MEC provides a solution by allowing users to offload tasks to edge servers. These servers can significantly reduce transmission delays and energy consumption, enabling efficient processing of computationally intensive applications. Conventional MEC networks face major challenges in remote areas, emergencies, and natural disasters. UAV-assisted MEC networks address these issues with controllable mobility and easy deployment, expanding network coverage and capacity [113, 114]. However, in the Web 3.0 scenario, the communication between UAVs and mobile users during computation offloading raises security and privacy concerns.

To this end, an innovative hybrid secure resource allocation and trajectory optimization approach is proposed in [115]. It focuses on enhancing data security and optimizing resource allocation in UAV-assisted MEC systems using blockchain and federated learning based on Web 3.0. To create a secure communication environment in the UAV-assisted MEC system, blockchain technology is used to ensure the integrity and authenticity of data throughout the network. This robust security mechanism helps reduce the risks associated with malicious attacks and eavesdropping, providing a trusted framework for data exchange between UAVs and MEC servers.

Additionally, federated learning is employed to train machine learning models locally on UAVs to protect data privacy and reduce communication overhead. By leveraging federated learning, the MEC system can optimize resource allocation and UAV trajectories in real time, enabling dynamic adjustments to the changing network conditions and user needs. This approach ensures a balanced computational load across the network, resulting in more efficient use of resources and improved overall performance of the MEC system.

In the context of Web 3.0, collaborative learning is a valuable alternative to federated learning. Similar to federated learning, collaborative learning also involves multiple participants working together to optimize a global model, but without the need for a centralized server, thus promoting a decentralized approach to data sharing and model training [116]. This approach is in line with the decentralized principles of Web 3.0 and enhances data privacy and security. By incorporating collaborative learning, UAV-assisted MEC systems can further decentralize control and promote a more robust user-driven ecosystem. This not only optimizes resource allocation and UAV trajectories but also supports the decentralized and user-centric vision of Web 3.0, ensuring efficient and secure computation across the network.

5.5. Practical applications of edge computing in Web 3.0

In this section, we further explore the applications of edge computing in Web 3.0, as shown in Fig. 13, to provide intuitions on how edge computing can be used in the Web 3.0 ecosystem. Yang *et al.* in [117] presented a novel distributed channel access scheme for smart manufacturing industries in Web 3.0. The authors introduced an edge-cloud collaboration framework to support autonomous wireless access point selection. Additionally, they developed a user-centric active channel access scheme to optimize resource allocation. Furthermore, a specialized multi-agent reinforcement learning model was built to effectively leverage key input information for enhancing communication. Liu *et al.* in [118] proposed a secure edge server placement (ESP) method for the Internet of Vehicles in Web 3.0. The proposed method leveraged a zero-trust security model to ensure that only tasks passing anomaly detection are executed, protecting edge servers from potential damage and resource waste. The proposed method formulated ESP as an optimization problem focused on minimizing latency and maximizing base station coverage. It employed non-cooperative game theory to integrate anomaly detection into the ESP algorithm. Xu *et al.* [119] proposed a dynamic offloading strategy for vehicular edge networks within a Web3 framework. The proposed approach combined CNN partitioning and game theory to optimize offloading decisions in this dynamic environment,

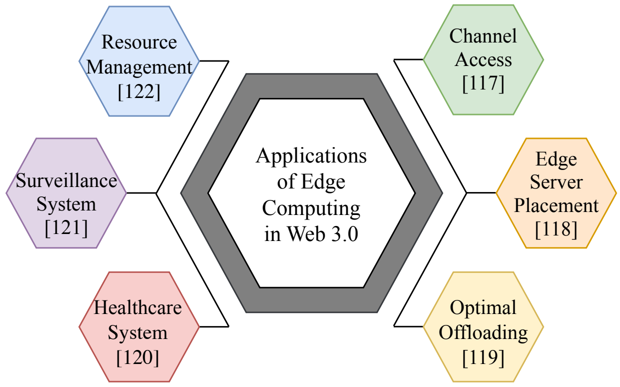

Figure 13: Applications of edge computing in Web 3.0.

improving resource efficiency and reducing latency. Specifically, the strategy involves constructing an edge-cloud collaboration framework for distributed CNN processing to ensure that Web3 applications can be processed within acceptable latency and energy consumption constraints. It also implemented a spatial CNN partitioning scheme for more fine-grained partitioning of CNNs and employed a game-theoretic approach during the offloading phase to improve the quality of service of the entire system. Singh and Chatterjee in [120] proposed a smart healthcare system based on edge computing, aiming to address the challenges posed by the growing number of sensitive patient data faced by modern healthcare systems. The proposed system incorporated an intermediary edge computing layer tasked with preserving low latency and protecting patient privacy. This edge computing layer was used to encrypt and handle patient data privacy by applying Privacy-Preserving-Searchable-Encryption techniques. Additionally, an access control mechanism was also implemented by the layer to restrict unauthorized access to patient data stored remotely. Wang *et al.* in [121] proposed a video surveillance system based on the integration of edge computing, permissioned blockchain, IPFS technology, and CNNs. The goal was to address challenges often encountered in large-scale video surveillance, such as massive device access, high bandwidth requirements, vulnerabilities to attack, and real-time monitoring. Respectively, the system used edge computing to facilitate extensive wireless sensor information gathering and data processing in a distributed manner. Permissioned blockchain underlain the framework to ensure reliability and robustness. IPFS technology was used for massive video data storage to reduce bandwidth usage. CNN technology permitted object recognition within video streams, achieving real-time surveillance. Luong *et al.* in [122] presented a DL-based approach for deriving an optimal auction mechanism to coordinate edge resources in a decentralized environment. The proposed method involves a multi-layer neural network that integrates an analytical solution for optimal auction design. The neural network transforms miners' bids, calculates allocation and payment rules, and uses miners' valuation data for training. The goal is to optimize the expected revenue for the Edge Computing Service Provider while ensuring incentive compatibility and individual rationality.

5.6. *Summary and insights*

The exponential growth of the IoT has resulted in billions of devices being deployed around us. These edge devices are increasingly becoming the foundational carrier for supporting Web 3.0, generating massive amounts of heterogeneous and confidential data. In traditional centralized architectures, it is easy to unify and coordinate real-time data processing, computation, and decision-making. However, in a decentralized Web 3.0, this task becomes extremely challenging. Security implications are an important aspect of edge computing in the Web 3.0 environment. The decentralized nature of Web 3.0 raises significant concerns about data integrity and privacy. Ensuring data integrity is complicated by the fact that data is processed and stored on edge devices. Additionally, privacy is another major concern in decentralized environments. The absence of traditional centralized oversight and control mechanisms makes it difficult to enforce privacy policies and prevent unauthorized access. To ensure data integrity, consistency, and privacy in decentralized Web 3.0, effective solutions are needed to replace traditional centralized solutions. One promising method is Asynchronous Verifiable Information Dispersal (AVID), which is a primitive with emerging applications in fault-tolerant replication and distributed storage [123, 124]. This approach was initially designed to solve the file storage problem by distributing files to a set of decentralized nodes in a storage-efficient manner. In Web 3.0, the AVID system can facilitate the secure and confidential dispersal and retrieval of data on demand.

6. Use cases for Web 3.0

Although Web 3.0 is still in its emerging stage, it has a solid technological foundation. Blockchain, AI, and edge computing will enable Web 3.0 to play an important role in various fields. Notably, when it comes to Web 3.0 applications, Metaverse may come up in the discussion. However, Metaverse is considered to be a different kind of web state than Web 3.0. The main differences between Web 3.0 and Metaverse are provided in Table 4.

Table 4: Main differences between Web 3.0 and metaverse.

Attributes	Web 3.0	Metaverse
Definition	a new version of Web	digital reality
Focus	ownership	experience
Interface	front-end	VR/AR
Architecture	fully decentralized	centralized/decentralized
Key technology	blockchain/AI	extended reality

Metaverse is a gigantic and shared virtual space created when the physical world converges with the virtual world. As opposed to Web 3.0, which is primarily concerned with who will own and govern the Web, Metaverse focuses on how people will interact with it. Moreover, people may still browse the Web using the front ends of various end devices for Web 3.0. However, Metaverse users will access the Web using virtual reality headsets while navigating a digital avatar across the virtual environment. If Metaverse manifests, it may do so in a centralized manner (e.g., Horizon World) or a decentralized manner (e.g., Decentraland), or any combination of the two [125, 126]. Although there is a lot of overlap in the technology support for Web 3.0 and Metaverse, Web 3.0 relies more on blockchain, AI, and some other emerging technologies while Metaverse relies on extended reality technologies such as virtual reality (VR), augmented reality (AR), and mixed reality (MR). Therefore, even though the two concepts of Web 3.0 and Metaverse are highly related, the overlap does not necessarily mean that either is an application of the other. Metaverse aims to correlate the digital and physical worlds so that social life, the real economy, and physical identity can all find their counterparts in the virtual world. Web 3.0 incorporates many similar features and characteristics but is distinguished by its focus on decentralization, trustless, permissionless, and individual data ownership.

In this section, we will introduce three use cases in Web 3.0, i.e., NFTs, DeFi, and DAO. Firstly, we will show how they can work together through a specific NFT trading process as shown in Fig. 14. Next, we will discuss these three main use-cases in terms of definition, relationship to blockchain and AI, applications, and corresponding issues.

A key criterion for successful NFT trading is decentralization, which enables trustlessness and security. To achieve this, the entire trading process must be carried out by SCs deployed on the blockchain. Furthermore, exchange contracts are designed to interact with all other NFT exchange contracts, which implies a widely adopted and recognized standard interface (e.g., ERC-721) should be used. Additionally, a DAO should be coded into the exchange SC such that users can collectively manage the trading process. Notably, the exchange SC does not store NFT data itself, rather it only maintains information required to perform the transfer of ownership (e.g., NFT token ID, seller address, and buyer address). The actual NFT data is retrieved from a separate SC dedicated to minting the NFT. Specifically, the seller first uploads data to a decentralized database (e.g., IPFS) in order to subsequently mint the corresponding NFT. Mint SC then retrieves data and uses it to mint NFT. Minted NFT will also be stored in the decentralized database and listed through the Exchange SC. On the buyer side, they send requests to Exchange SC to load NFTs and provide offers. Typically, the seller will accept the offer with highest bid. To accomplish this, Exchange SC will transfer the bid to the seller and NFT ownership to the buyer.

6.1. *NFTs*

1) What is an NFT? An NFT is a token that represents a unique digital asset. It can be used to represent ownership and authenticity. The assets cannot be exchanged with one another since each person has a digital signature, making them distinct and non-interchangeable.

2) Blockchain for NFTs: NFTs are minted through SCs deployed on the blockchain, which determines the characteristics of the NFTs. The main features are listed below [127–130].

• *Ownership*: Ownership depends on where the private key associated with the NFT is stored. Transferring the private key

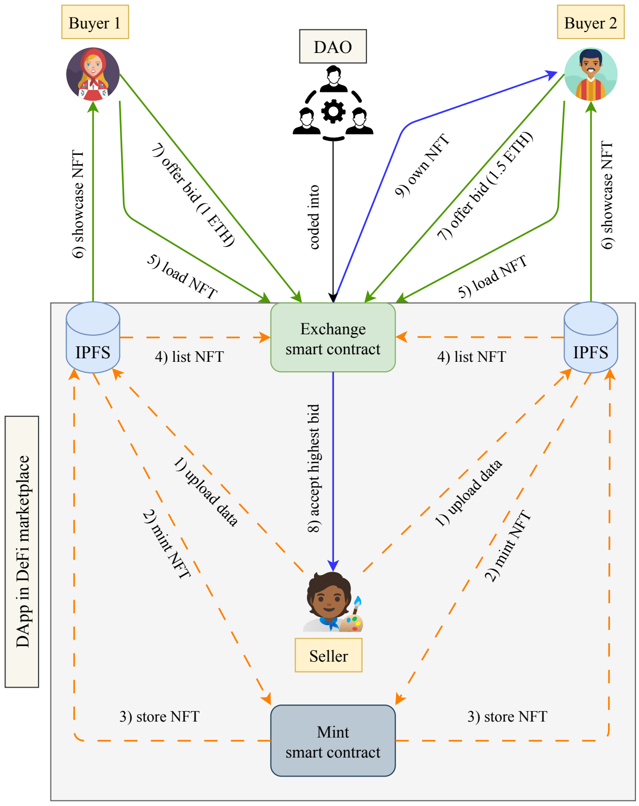

Figure 14: NFT trading process monitored by the DAO in the DeFi market.

is a change of ownership, enabling the transaction of the NFT.

• *Scarcity*: Each NFT has a unique ID, making it a scarce and non-fungible asset. Therefore, proof of ownership can be used throughout the network, effectively verifying the owner.

• *Interoperability*: Users are allowed to seamlessly trade or share NFTs across multiple blockchain-based ecosystems, increasing the liquidity and reach of NFTs.

• *Immutability*: Creating an NFT means that the ownership, origin of the NFT, and any associated data or metadata are permanently stored on the blockchain and cannot be changed.

• *Programmability*: The ownership and logic of NFTs can be programmed through SC. This allows more complex functions, such as transfer rules and scarcity, to be encoded into SC.

• *Transparency*: Blockchain provides an immutable and transparent record of ownership, attributes, and SCs associated with NFTs. In this case, the integrity and provenance of unique digital assets can be ensured.

It is worth noting that an NFT can only have one owner at a time. This owner can add more attributes related to the asset in the NFT. The public ledger can be viewed by anybody, making it simple to verify and trace an NFT's ownership. In this way, creators can monetize their work, trade it globally, and have indisputable rights over their creations.

3) AI for NFTs: AI and NFTs have a symbiotic relationship. AI greatly enhances NFTs through scarcity, personalization, and market optimization. In turn, NFTs provide a way to record, verify, and potentially monetize AI's contributions. Together, they are transforming collection, creativity, identity, work, and value. Specifically, there are a variety of ways that AI can be used in the context of NFTs.

• *Originality*: In art, generative AI models can be used to generate new ideas and designs by studying large databases of human-created artwork. This is especially useful for creators who want to issue large numbers of NFTs quickly.

• *Verification*: Blockchain is used to establish proof of ownership of NFTs. AI can play a complementary role by using techniques, such as fingerprinting, metadata analysis, and content matching, to further verify NFT ownership claims on blockchains.

• *Enhanced interactivity*: AI-powered NFT can leverage DL methods to make the tokenized assets more dynamic and interactive. The owner of NFTs can program to respond to certain commands or generate new designs, allowing the output of tokenized assets to evolve.

• *Optimization*: AI can provide valuable insights into pricing, improving liquidity, and maximizing the value of NFT by analyzing historical sales data and attributes of successful NFT, especially for items, collections, and assets with limited supply.

• *Personalization*: AI provides personalized recommendations about purchasing or collecting new NFTs by analyzing a user's collection, interests, and preferences, leading to a more curated and valuable collection.

• *Wider ecosystem*: AI can be used to analyze the NFT market and forecast trends and demands, helping investors and collectors make more informed decisions when trading NFTs.

4) Applications for NFT: In this section, we will explore various notable applications of NFTs, that showcase how blockchain and AI can drive the advancement of NFTs.

• *Securechain*: Securechain is a hybrid verification system designed to protect NFTs stored in hot wallets from wallet-draining attacks [131]. The main idea is that with a hybrid system, transfer verification can be created on-chain and accepted or rejected off-chain, unlike current solutions such as transferring NFTs to cold wallets. It needs to be made clear that cold wallets make it inconvenient to use NFTs. In addition, since the private keys of hot wallets cannot be changed, once the key is compromised, users will be responsible for all resulting losses. In terms of specific implementation, there are various security measures such as authentication controller, contract controller, authority controller, user controller, and verification controller. Additionally, the event listening module allows the backend to monitor SC for any on-chain changes. All these functionalities are designed to ensure that the backend only accepts verifications, but strictly prohibits any changes to the verified information, as this information is permanently recorded in the blockchain ledger.

• *NFTool*: NFTool is an NFT platform powered by a suite of tools including a chatbot, an NFT minting tool, SC auditor, NFT search, and built-in NFT deployment [132]. Specifically, a ChatGPT-style chatbot that serves as an intelligent guide ca-

Table 5: Issues of NFTs.

	Types	Description
Technical	Complexity	The complex development of NFTs has not yet been simplified by high-quality tools.
	Storage	The URL where the artwork is stored makes the artwork itself vulnerable to link damage.
	Fees	Artists pay more on average in the NFT market than they earn in sales.
	SC risks	SC vulnerability caused a massive attack leading to the NFT theft incident.
	Rapid innovation	This creates a challenge of continuous change for those who adopt the technology.
	Usability	Slow confirmation and high gas prices will limit the rapid growth of NFTs.
	Extensibility	It is difficult to interact with other ecosystems.
	Cybersecurity	It is challenging to identify fake NFT stores and malicious proxies.
	Security and privacy	NFT data is at risk of being lost or misused by malicious parties.
Others	Regulatory	New technologies bring unique regulatory and legal considerations.
	Environmental concerns	Transactions result in high energy consumption and consequent greenhouse gas emissions.
	Anti-money laundering	Decentralized transactions can lead to money laundering.
	Copyright	The public nature makes it easy for anyone to copy the referenced documents.
	Ponzi scheme	Critics have likened NFT to a Ponzi scheme.

pable of handling related cross-chain functions and issues. To avoid creative concepts remaining un-minted, users can follow the detailed instructions of Mint NFT to launch their own NFTs on different chains. However, errors in SCs can be easily exploited by malicious actors. It is crucial to utilize the SC analysis tool to ensure SCs are tested thoroughly and ready for deployment. In addition, the NFT Search tool enables the exploration of NFT collections across the blockchain by utilizing Covalent, Zora, and Graph. Users can convert fiat currencies into corresponding cryptocurrencies to help deploy SCs.

• *StoryChain*: StoryChain is a new interpretation of story editing, leveraging Artificial Intelligence Generated Content (AIGC) and blockchain technology to enable collaborative story creation [133]. With StoryChain, users can collaboratively craft stories comprising distinctive chapters and artistic works. Notably, each page is an NFT minted for the corresponding user. During the story creation process, the contract first verifies the appropriateness of the user prompt, then ChatGPT generates the text and illustrates it with an AI image generator. The entire story, along with the resulting images, will then be uploaded to IPFS. The generated hash is submitted to the contract to mint the NFT for the author. This way, authors will have a permanent record of ownership and chapter details accessible on-chain via IPFS. Alternatively, a voting mechanism allows the story community to democratically select the direction of future entries, treating each story like a DAO. The proposed chapter is subject to consensus among NFT owners to determine the direction of the story.

5) Issues: Items that typically end up lost on the Web can now be monetized through NFT technology. However, both the NFT technology and the NFT market are currently in their infancy. Critical infrastructure, including technology platforms and trading platforms, will continue to exist in a centralized form. We list the main issues from both technical and non-technical perspectives in Table 5 [127, 128, 134–136].

6.2. DeFi

1) What is DeFi? DeFi manages financial services primarily using blockchain technology and a number of cryptocurrencies. It is an alternative to the global financial system of the Web 3.0 era and aims to democratize finance, which is difficult to achieve in the traditional financial system [137–140]. The biggest difference between DeFi and traditional financial institutions is that DeFi is decentralized and does not use a third party to carry out financial operations. DeFi is open and transparent and performs a range of functions based on the issuance code, which cannot be modified by any node and can only be updated if necessary with the consent of most nodes on the chain. A more detailed comparison of several key aspects is shown in Table 6 [141].

2) Blockchain for DeFi: Blockchain is the core technology that replaces traditional centralized institutions and enables decentralized financial services as shown in Fig. 15 [142, 143]. Cryptocurrencies, SCs, stablecoins, and dApps are the four components that comprise DeFi and are all based on blockchain technology [144].

• *Cryptocurrency*: As one of the earliest and most successful deployments of blockchain, cryptocurrencies are ubiquitous in the decentralized world. It has underpinned the rise and continued success of DeFi. DeFi's successful operation requires the support of cryptocurrencies because they enable many core functions. For example, cryptocurrencies are used to represent and transfer value. Without cryptocurrencies, basic lending and borrowing functions would not be possible.

• *SCs*: As a blockchain-based program, an SC can be activated automatically when certain criteria are met. It eliminates third parties or central authorities typically required in traditional financial transactions. It also allows users to program

Table 6: Differences between DeFi and traditional finance.

Attributes	DeFi	Traditional finance
Infrastructure	Decentralization	Centralization
Custody	Users	Companies
Currency	Digital asset	Fiat currency
Speed	Minutes	Depends (manual processing)
Auditability	Anyone	Authenticated organizations
Collateral	Required	Optional
Anonymity	Yes	No
Permission	No	Yes
Availability	Yes	No
Transparency	Yes	No

any transaction into code, decentralizing the financial process. When a SC goes live, no one can change it. As a result, many of the business terms found in traditional financial industry agreements can be transferred to SCs and enforced through code.

• *Stablecoins*: One of the main drawbacks of many cryptocurrencies is their excessive volatility, which greatly reduces the incentive to participate for those users who do not have sufficient risk tolerance. To solve this problem, the concept of stablecoins was created. A stablecoin is a cryptocurrency with a fiat stable price. It is designed to maintain price parity with a stable asset, such as the US dollar or gold, to provide the necessary stability.

• *dApps*: A dApp is essentially an application that runs on the blockchain. Unlike traditional applications that run on large servers, dApps are created and deployed on the blockchain through SCs. The main benefits are their permissionless nature and resistance to censorship.

3) AI for DeFi: DeFi aims to democratize finance to bridge the limitations of traditional finance. It can provide financial services to anyone, anywhere, regardless of location, income, or background [145–147]. With the rapid and widespread deployment of AI in multiple fields, AI is promising to provide novel solutions to enhance the DeFi ecosystem. Specifically, it can be reflected in the following aspects.

• *Fraud detection*: AI can analyze transaction data, user behavior, and transaction patterns to detect anomalies that may indicate fraud, scams, or money laundering in DeFi's platform and protocols. Take money laundering as an example, various techniques have been proposed to detect money laundering activities (see Section 4.5).

• *Risk analysis*: AI can assess the risks of different DeFi projects based on technology, market, operations, regulations, management team, and other factors. This can help DeFi users make informed decisions about which projects to invest in and which to avoid.

• *Automated trading*: AI bots can analyze real-time market data, trends, and opportunities on the DeFi platform to automatically trade digital assets and provide liquidity to generate

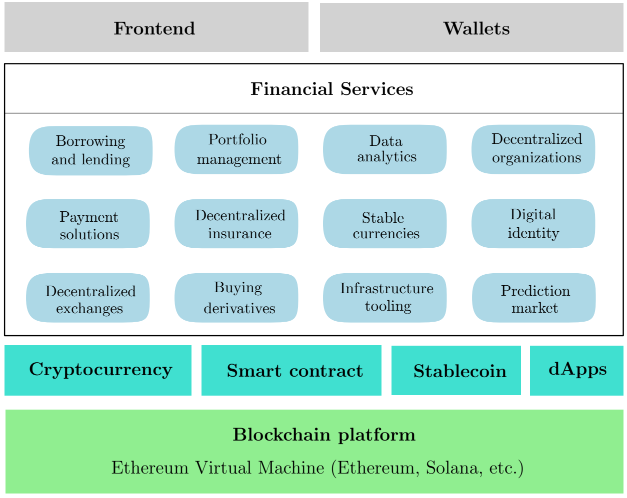

Figure 15: DeFi stack.

maximum profits.

• *Credit scoring*: AI can analyze DeFi users' transaction history, loan data, and collateral information to generate credit scores for them. These scores can then be used to determine their eligibility for loans and credit limits under the DeFi loan agreement.

• *Personalization*: By understanding the user profile, investment goals, risk appetite, and portfolio details, AI can provide customized recommendations about interest rates and lending options that are best suited for each DeFi user.

• *Product development*: Generative AI allows for rapid understanding of DeFi users' needs and issues, developing new products and expanding DeFi's ecosystem.

4) Applications for DeFi: In this section, we will show how blockchain and AI technologies can improve the DeFi ecosystem by exploring several applications of DeFi.

• *Agrosurance*: Agrosurance aims to revolutionize how agricultural insurance and liquidity are managed by developing an innovative platform that delivers transparent, reliable, and decentralized solutions [148]. This platform consists of five SCs, each with a unique purpose. Specifically, AgroCoin contract allows the transfer and management of AgroCoins between users. AgroSuranceLand contract represents and manages land assets by minting them into NFTs. StakeManager contract enables users to earn AgroCoins through staking to incentivize liquidity and participation within agricultural insurance. InsuranceManage uses Chainlink DONs to obtain off-chain real-time data to trigger predefined rules to calculate insurance premiums and verify claim eligibility. FundManager contract acts as a repository for managed funds, storing tokens received from the InsuranceManager and StakeManager contracts.

• *Prompt DeFi*: Prompt DeFi simplifies the interaction process with DeFi into simple voice commands, attracting more users without relevant backgrounds to enter the DeFi world [149]. This platform uses ChatGPT to execute transactions based on text prompts. In addition, the use of the web3auth

Table 7: Issues of DeFi.

	Types	Description
Technical	Scalability	The slow-transaction nature of the consensus mechanism limits large-scale adoption.
	Oracle	It is difficult for off-chain data to be reported securely on-chain.
	Operational security	A malicious third party could break the SC once they get the key.
	Custodial risk	The theft of private keys can be catastrophic for users.
	Bias	Data-driven decisions on DeFi protocols may reflect or even amplify biases.
	Limited data	Limited transaction data makes it difficult to train accurate AI models.
	Integration	Integrating centralized AI models and systems into a decentralized DeFi protocol is difficult.
Others	Regulatory	Finding the right regulatory balance will be tricky.
	Collateralization	Over-collateralization will limit DeFi lending business.
	Dependencies	The openness and composability of DeFi introduce dependencies to the system.
	Responsibility	DeFi shifts the responsibility from the third party to the user.

library greatly simplifies the account creation process, making new users interacting with Web 3.0 as easy as with Web 2.0. For example, Prompt DeFi integrates prominent DeFi platforms, including Uniswap, Lido, and Aave. This allows users to easily send and exchange tokens through Uniswap, deposit funds into Lido, and manage loans in Aave. Furthermore, the platform utilizes Chainlink Automations to incorporate additional portfolio triggers, enhancing the overall user experience.

• *RoboFI*: RoboFi is a robotic DeFi ecosystem that enables robotic entities to generate and trade Energy Attribute Certificates (EACs) via a decentralized infrastructure powered by blockchain [150]. In RoboFi, two robotic entities provide commercial services for humans and other robots. One of the robots, called EAC provider, owns a solar power plant that produces green electricity. When 1 MWh of electricity is generated, 1 EAC NFT is created to confirm the fact and origin of this electricity. The other robot, called EAC consumer, is charged from the common power grid of the RoboFi ecosystem. To be sustainable, the EAC consumer needs to confirm the origin and track of consumed electricity by connecting to the RoboFi NFT EACs trading platform. The EAC consumer can showcase that it has the certificate to use the corresponding amount of green energy, confirming the creation of sustainable value.

5) Issues: While DeFi can minimize transaction risks by eliminating third parties and enabling the exchange of financial assets on a trustless basis, innovations always come with a new set of issues. In particular, DeFi has not been stress tested for long-term or widespread use. As shown in Table 7, a number of key issues must be addressed in order to offer customers and institutions a reliable, fault-tolerant ecosystem that can handle new financial applications at scales [144, 151, 152].

6.3. DAOs

1) What is a DAO? A DAO is an organization that operates fully autonomously on a blockchain, conforming to rules encoded through SCs and their underlying consensus mechanisms. It is designed to reduce or bypass the need for cascading human intervention or centralized coordination [153]. For this reason, a DAO is often referred to as a trustless system, which differs from the traditional model of management by a small group of people. All the rules are set up in advance in a SC and executed by P2P computing nodes. A more detailed comparison between DAOs and traditional organizations is shown in Table 8 [154, 155].

2) Blockchain for DAO: The underlying technology of DAO is blockchain. It relies heavily on SCs, which are transparent, verifiable, autonomous, and publicly auditable. The workflow of DAO is shown in Fig. 16. SCs are used to establish the rules of DAO, which are set by a core team of community members. Due to the tamper-proof nature of blockchain, once the contract is in effect on the blockchain, no one can change the code without a consensus reached through a vote of the members. The rules and logic in the code strictly limit its functionality [156–158]. Financing is typically achieved through a token offering, in which case tokens are sold to raise funds and replenish the coffers of DAO. Token holders receive voting rights in exchange for their money. The voting rights are usually proportional to their holdings. Once fundraising is complete, DAO is ready for deployment. No particular organization has the right to change the code in SC. It is entirely up to the token holders to decide. Based on these features, DAO can provide significant support for many applications.

3) AI for DAO: The combination of DAO and AI can be complementary. AI plays a pivotal role in bringing more functionality and greater efficiency to DAOs. AI gains the resources it lacks; on the other hand, DAO gets critical autonomous decision-making capabilities from AI [159]. In the context of Web 3.0, AI can enhance DAOs to fit their mission in numerous ways.

• *Autonomous functions*: AI can autonomously perform certain automated tasks, such as computation and data analysis, based on constraints, goals, and rules defined by a DAO.

• *Enhanced control*: AI integrated into a DAO has no centralized control by the nature of DAOs. Its knowledge and capabilities will be designed to serve the overall goals and tasks of a

Table 8: Differences between DAOs and traditional organizations.

Attributes	DAOs	Traditional organizations
Trust	Blockchain	Experience
Governance	Community	Main stakeholders
Structure	Democratic	Hierarchical
Transparency	Complete	Restricted
Pattern	Collaboration	Competition
Service	Fully automated	Centralized automation
Access	Open	Closed
Affiliation	Multiple	One
Cost	Low	High

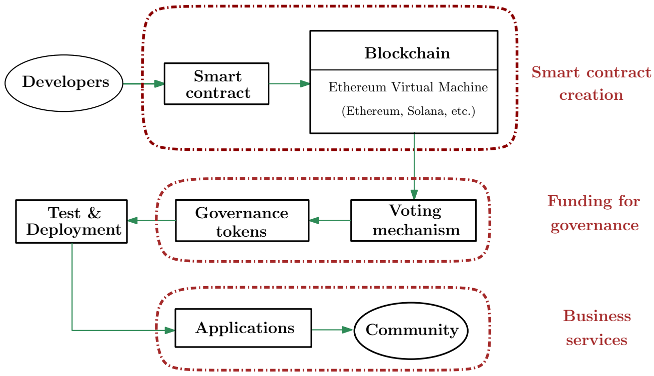

Figure 16: DAO workflow.

DAO in a transparent and decentralized manner, thus enhancing decentralized control.

• *Facilitate collaboration*: AI integrated into DAOs helps facilitate collaboration among different stakeholders by providing shared information, coordination tools, and alignment metrics.

• *SCs*: Generative AI can aid in the rapid development of SCs by precisely coding the goals and rules of the DAO so that the SC enforces these terms in a fair manner.

• *Monitoring*: AI can help continuously monitor key metrics, risks, and processes within a DAO, providing comprehensive reporting for greater transparency and accountability.

4) Applications for DAO: In this section, we will show the promise of DAO powered by blockchain and AI technologies in decentralized governance through specific applications.

• *OmniGovern DAO*: OmniGovern is a decentralized governance system deployed on a Layer 2 blockchain, designed to simplify on-chain governance [160]. To enable seamless governance across blockchains, Layerzero acts as an interoperable middleware that connects multiple blockchains with Omnichain Fungible Token, facilitating gas-less transactions through a relay mechanism. Worldcoin's authentication mechanism is used to eliminate potential bot activity to ensure the integrity and authenticity of votes and proposals. OmniGovern implements robust account abstraction on the Base Gorelli chain to simplify the complexity of user interaction with the platform by masking complex blockchain details. Additionally, Covalent's integration ensures transparency of voting results, proposal history, and token analysis, promoting trust and accountability.

• *Rooster DAO*: Rooster DAO is an investment fund managed in the form of DAO, focusing solely on investments in the Dotsama ecosystem [161]. To incentivize active participation, every member of Rooster Dao owns an evolving NFT that represents their level of engagement in investment proposals and voting. As members actively contribute, the rooster image gains color and levels up. Moreover, when a member proposes a highly profitable investment, all members collectively transfer a portion of the profits to the proposer. Specifically, there are two types of SCs. The NFT management contract is responsible for creating collections owned by the contract itself, minting and transferring NFTs, validating ownership, and adding resources to or removing resources from NFTs. The governance contract interacts with the NFT management contract to track proposals, authorizations, and votes.

• *DAOasis*: DAOasis provides a social networking platform facilitating the creation and management of multisigniture authorities [162]. This empowers users to execute transactions to manage their digital assets, handle customized transactions, and perform secure cross-chain interoperability. Specifically, Polybase is a decentralized database that provides a secure and decentralized method for data interaction. The Gnosis Safe wallet offers users the ability to create accounts and safes. The Safe is a multi-signature wallet that requires a minimum number of signatures to perform a transaction, ensuring maximum security for all involved parties. Connext facilitates seamless interactions across multiple blockchains by enabling cross-chain transactions and fund transfers.

5) Issues: Although DAOs are still in the early stages of development, it has attracted widespread attention. However, improperly building or maintaining a DAO can have serious consequences. Since a DAO directly controls assets, vulnerabilities always can cause catastrophic damage. In addition, due to their infrastructure, DAOs suffer from many of the same limitations and security issues as the blockchains on which they operate. Beyond that, some of the major limitations, as well as issues, are listed in Table 9 [163–166].

7. Challenges and Future Research Directions

Advanced technologies, represented by blockchain, AI, and edge computing are driving the rapid development of the Web 3.0 ecosystem, which is expected to revolutionize the way people interact with the Web. However, the fast iteration of these technologies also presents many challenges and limitations to Web 3.0. The miscreants are well aware of this and try to exploit this iterative gap for their nefarious purposes. As a result, some major challenges need to be addressed urgently. In the following, we will discuss some of the major challenges that Web 3.0 is facing [167–170]. Additionally, we also discuss the potential research directions for building a future Web 3.0 ecosystem.

Table 9: Issues of DAOs.

	Types	Description
Technical	Security	The code is extremely difficult to fix, thus leaving a vulnerability.
	Speed	Every user is given an opportunity to vote, which requires a longer voting period.
	Engagement	Abandoning participation in governance will lead to a re-centralization of power.
	Pseudonym	Pseudonyms may hinder efforts to combat financial crime.
	Unfairness	Autonomous attributes may be undermined by a few users who have a larger voice.
	Consistency	Data bias makes it challenging to fully align AI's mission with DAO's goals.
	Autonomy	The integration of AI into DAOs brings some centralization of control and power.
	Transparency	The lack of interpretability of AI can pose a challenge to DAO's decision-making process.
Others	Regulatory	The legal status is typically ambiguous and may change depending on the jurisdiction.
	Inefficiency	It is easy for a DAO to spend much more time discussing than implementing.
	Social	Inactive or non-voting shareholders can cause disruptions in an organization's operations.
	Education	It is difficult for people with different backgrounds to develop strategies together.

7.1. Major challenges

1) Scalability: Scalability has proven to be a major obstacle to the rapid development of the Web 3.0 ecosystem. Scalability refers to the ability of a network to develop and adapt to growing demands as more users are added to the network without compromising its security or effectiveness. As a typical problem of the blockchain trilemma, there is no general solution as of today. As the underlying ecology of Web 3.0, the blockchain platform often needs to make a trade-off between scalability, decentralization, and security in different scenarios. For example, Blockchain 3.0 chooses to sacrifice security for high throughput and fast transactions. This results in lower fault tolerance than those in Blockchain 1.0 and Blockchain 2.0. This could make Web 3.0 solutions based on such blockchain platforms more vulnerable to attacks. Meanwhile, digital wallets, existing as Web 3.0 portals, typically as browser extensions, pose security issues since digital wallets are connected to the blockchain through a centralized platform at this stage. Once the centralized platform is compromised, users will suffer huge financial losses. Therefore, the resolution of the trilemma, or how to make effective trade-offs, will greatly affect the development and deployment of Web 3.0.

2) Centralization: While Web 3.0 has made some progress since entering the mainstream, most Web 3.0 protocols have remained relatively slow to evolve. To enable Web 3.0 to quickly support smart contracts, DeFi, NFTs, etc., Web 3.0 protocols have coalesced around centralized platforms, relying on them to run servers and enable rapid iteration. Examples include OpenSea, Etherscan, and MetaMask, which rely on Infura, a backend and infrastructure-as-a-service provider. This has led to the ridiculous phenomenon that so-called decentralized protocols and applications run on a centralized infrastructure. This is what the opponents say: the Web has not changed in essence; it has just been repackaged. On top of that, centralized infrastructures are becoming more secure and have low latency. People have been accustomed to the current network model, which makes Web 3.0 a difficult long-term and reliable competitor. Therefore, at this stage of development, the focus of Web 3.0 still needs to be on the revolution of the back end to achieve true decentralization.

3) Unconscious bias: Unconscious bias refers to implicit attitudes and stereotypes that influence people's understanding, actions, and decisions in an unconscious manner. In the early stages of Web 3.0, unconscious bias seems to be creeping in. One study found that female and darker-skinned NFTs are valued less than their male and lighter-skinned counterparts. The study highlights how these biases are reflected in the digital realm, mirroring societal prejudices that exist in the physical world [171]. Additionally, another study showed significant racial bias in a commercially used AI system used to predict patient outcomes. Black patients were much sicker than white patients for a given risk score. Correcting this bias would increase the percentage of Black patients receiving extra help from 17.7% to 46.5% [172]. These two examples illustrate how unconscious bias can negatively impact the DeFi and healthcare sectors in Web 3.0. Addressing these biases is critical because leveraging biased datasets can severely harm the Web 3.0 ecosystem. Given these signs of impending problems, unconscious bias will become one of the major challenges for the Web 3.0 ecosystem.

4) Resource management: Managing a large number of interconnected and heterogeneous devices poses significant challenges to the Web 3.0 ecosystem. As devices become more connected through edge computing architecture, threats can spread more easily between devices. A vulnerability in one device may affect many other devices or even paralyze the entire system [173]. The devices come in many forms, with various hardware, software, operating systems, and use cases. This high degree of heterogeneity means that generic security solutions need to consider a large number of potential configurations and usage patterns. It becomes incredibly difficult to develop a security approach that perfectly addresses each unique scenario. On the one hand, solutions designed for maximum generality may lack accuracy for certain device types or environments; on the other hand, an approach that is too specific will not be able to scale and cover the entire content of the device ecosystem. How to achieve the proper trade-off between generality and accuracy is the key to solving the problem [174]. Furthermore, coordinating edge computing resources in a decentralized manner is a challenging task. It involves distributing decision-making and control mechanisms among multiple nodes within the network. This approach aligns with Web 3.0 principles, which aim to distribute power and control among network participants. This requires further exploration of edge computing and blockchain technologies such as consensus protocols and SCs.

5) Difficulty in development and maintenance: Web 3.0 development mainly refers to the development of dApps on top of existing blockchain platforms. Developers do not need to design new consensus protocols but still need to deeply understand the working mechanisms behind them. The difference between the programming languages and frameworks used for traditional development also brings new challenges to the development of dApps. In addition, the immutability of the blockchain implies the characteristic that smart contracts published to the blockchain are extremely difficult to change after deployment, making the maintenance of dApps more difficult. A small error in the code can cause huge damage. Even if a problem is found, it is impossible to react correctly in a short time. This places extremely demanding requirements on Web 3.0 developers to ensure that the code is error-free after release.

6) Accessibility: Currently, the barriers for users to enter the Web 3.0 ecosystem remain high. It is still not easy for users to move to the platforms of some Web 3.0 projects. The reason lies not only in technical aspects but also in other aspects, such as geographical location and regulations. Web 3.0 typically relies on P2P architectures such as blockchain and edge computing, empowered by AI. However, varying restrictions on emerging technologies across different countries and states create additional non-technical barriers. Moreover, Web 3.0 lacks integration with modern web browsers, making it difficult for users to interact with them. For ordinary users, they have no ideological motivation or interest in taking on the additional costs and responsibilities of running these complex systems directly. The technical feasibility of Web 3.0 will not be an incentive for users to use it unless there is a compelling personal need for its unique features. One may prefer to maintain the current state of affairs, which also poses a significant challenge to the development of Web 3.0.

7.2. Future research directions

1) Cross-shard communication: Although the concept of sharding has been proposed for years in the context of blockchain technology, mainstream Web 3.0 platforms have yet to fully integrate sharding technology. The development and implementation of practical sharding techniques for Web 3.0 applications remain an ongoing area of research. Specifically, cross-shard communication is an urgent problem that needs to be solved as it requires additional protocols and mechanisms to ensure the consistency and validity of data and transactions across shards. Sharding security is also important for Web 3.0. It refers to the risk of malicious nodes taking over a shard and manipulating its operations. One attractive solution to strengthen shard security is by using randomization and incentives to assign nodes to shards while applying cryptographic proofs (e.g., ZK proofs) to detect malicious behavior.

Additionally, Layer 2 solutions are another important research direction that could complement sharding. By combining sharding with Layer 2 solutions, blockchain networks can dramatically increase their throughput, thus realizing the Web 3.0 decentralized vision. For example, state channels allow high-frequency transactions to be processed off-chain within individual shards, while only settlement states are periodically committed on-chain. Cross-shard state channels are used to maintain interconnectivity. In this way, the scaling issue will be effectively mitigated by combining Layer 1 sharding with Layer 2 solutions, which allows blockchain-powered Web 3.0 to support massive data concurrency.

2) Bias mitigation: The main reason for introducing bias is usually that the training data is unbalanced or unrepresentative. However, data diversity is not always fully achieved in the real world due to factors such as structural inequalities and historical patterns. When AI systems developed based on such data become widely used, bias can create a vicious cycle. This is particularly concerning as generative AI plays an increasingly important role in creating vast amounts of new digital content in the decentralized Web 3.0 ecosystem. It is crucial to ensure that such content is not biased.

Given the prevalence of generative AI, a promising research direction is to build an AIGC-driven bias-free Web 3.0 ecosystem. Specifically, unconscious bias in Web 3.0 can be effectively reduced by leveraging AIGC to generate training data that scales diversity and inclusion. Furthermore, to build a more inclusive and secure Web 3.0, it is necessary to rethink fairness as well as privacy and security in AIGC-driven Web 3.0. An unfair AIGC model may further exacerbate inequalities in the Web 3.0 ecosystem. It is critical to ensure that AIGC algorithms are designed to promote inclusivity and avoid reinforcing bias.

3) Adaptive resource allocation: Adaptive and scalable resource allocation approaches are crucial for the advancement of the Web 3.0 ecosystem. One potential research direction is the modular architecture and protocol design of Web 3.0 enabled by edge computing to adapt to different device types, configurations, and use cases. These frameworks should enable seamless integration and interoperability between heterogeneous devices to facilitate communication and collaboration across the Web 3.0 ecosystem. Additionally, since edge devices may dynamically join or leave the network, the allocation of resources and tasks becomes more challenging. Developing decentralized algorithms and mechanisms for resource allocation, load balancing, and task offloading helps optimize resource utilization and ensure efficient coordination among edge devices.

Specifically, intelligent resource allocation algorithms should efficiently distribute tasks among edge devices to maximize resource utilization while minimizing latency and energy consumption. Second, load balancing mechanisms should consider factors such as device capacity, network congestion, and task demands to ensure optimal resource utilization and prevent the overloading of specific devices. Third, effective task offloading strategies are needed to determine when and which tasks should be offloaded from edge devices to other edge devices or edge computing clusters for acceleration, load balancing, etc. These strategies should consider aspects such as task characteristics, network conditions, and device capabilities to minimize latency and improve system performance, facilitating the scheduling of task processing in a system-wide view.

8. Conclusion

This paper thoroughly investigated the impact of blockchain, AI, and edge computing on Web 3.0, highlighting these technologies as key drivers of the next generation of the Web. Technically, Web 3.0 is a back-end evolution based on blockchain technology that allows for the distribution of power and trust, enabling users to have more control over their personal data and digital assets. AI can empower Web 3.0 with key features, such as intelligent automation, enhanced security, and improved governance, while Web 3.0 can provide AI with two most important elements: data and computing power. Edge computing brings practical benefits such as low latency and cost-effective performance to Web 3.0. Our extensive literature review and analysis of practical applications reveal significant advancements in the role of each technology in Web 3.0. We identified several key findings:

The blockchain-based Web 3.0 inherits challenges from blockchain technology, particularly scalability and interoperability. Solutions such as off-chain, cross-chain, and layer 2 technologies can effectively solve these challenges. However, when specific companies develop proprietary technologies, they tend to ignore the core principle of Web 3.0: decentralization. This creates the paradox that decentralized technology is provided by centralized entities. To ensure that the Web 3.0 ecosystem remains truly decentralized, supervision should be delegated to DAOs rather than individual companies.

Additionally, incorporating generative AI into Web 3.0 requires careful consideration of regulatory frameworks. While generative AI enhances the semantic and intelligent capabilities of Web 3.0, it also raises challenges related to data privacy, ethical use, and accountability. Effective regulation is essential to ensure that AI applications adhere to the principles of transparency, fairness, and user consent. Without strong regulatory oversight, the deployment of AI technologies in decentralized Web 3.0 environments could perpetuate bias, compromise data security, and undermine user trust.

Moreover, through extensive research on various practical applications, we have identified that decentralized storage and computing are fundamental to the practical implementation of Web 3.0. Upper-layer applications rely on these core technologies. However, our findings indicate that decentralized solutions based on edge computing frameworks have not received adequate attention. To bridge this gap, we propose decentralized storage and computing methods to support these applications effectively. Our exploration focuses on how decentralized storage and computing can address the challenges of data ownership and security in Web 3.0.

Overall, Web 3.0 is envisioned as an ecosystem, built on blockchain, powered by AI, and optimized via edge computing, with the potential to fundamentally change the way people interact with information. We expect that this survey can facilitate a clearer understanding of Web 3.0 and inspire further innovative research within this emerging field.

Acknowledgments

This work was supported in part by the NSF Established Program to Stimulate Competitive Research (EPSCoR)-Louisiana Materials Design Alliance (LAMDA) Program under Grant OIA-1946231, and in part by AT&T (BellSouth / South Central Bell) Endowed Professorship.

References

[1] Statista, Worldwide digital population 2024, https://www.statista.com/statistics/617136/digital-population-worldwide/#statisticContainer, Accessed: Feb. 1, 2024.

[2] Statista, Global number of breached user accounts Q1 2020-Q4 2023, https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/, Accessed: Mar. 23, 2024.

[3] Coinbase, International survey of Web3 adoption (Oct. 2022).

[4] Consensys, The state of Web3 perception around the world, https://consensys.io/insight-report/web3-and-crypto-global-survey-2023, Accessed: Nov. 21, 2023.

[5] S. Vojíř, J. Kučera, Towards re-decentralized future of the web: Privacy, security and technology development, Acta Informatica Pragensia 2021 (3) (2021) 349–369.

[6] J. Zarrin, et al., Blockchain for decentralization of Internet: prospects, trends, and challenges, Cluster Computing 24 (4) (2021) 2841–2866.

[7] Q. Wang, et al., Exploring Web3 from the view of blockchain, arXiv preprint arXiv:2206.08821 (2022).

[8] P. Ray, Web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions, Internet of Things and Cyber-Physical Systems (2023).

[9] W. Gan, et al., Web 3.0: The future of Internet, arXiv preprint arXiv:2304.06032 (2023).

[10] X. Ren, et al., Building resilient Web 3.0 with quantum information technologies and blockchain: An ambilateral view, arXiv preprint arXiv:2303.13050 (2023).

[11] R. Huang, et al., An overview of Web3. 0 technology: Infrastructure, applications, and popularity, arXiv preprint arXiv:2305.00427 (2023).

[12] M. Shen, et al., Artificial intelligence for Web 3.0: A comprehensive survey, arXiv preprint arXiv:2309.09972 (2023).

[13] G. Wood, DApps: What Web 3.0 looks like, https://gavwood.com/dappsweb3.html, Accessed: Nov. 21, 2023.

[14] A. Beniiche, et al., Society 5.0: Internet as if people mattered, IEEE Wireless Communications 29 (6) (2022) 160–168.

[15] A. Park, et al., Interoperability: Our exciting and terrifying Web3 future, Business Horizons 66 (4) (2023) 529–541.

[16] G. Wood, Less-techy: What is Web 3.0?, https://gavwood.com/web3lt.html, Accessed: Nov. 21, 2023.

[17] T. Berners-Lee, et al., Solid protocol, https://solidproject.org/TR/protocol#terminology, Accessed: Dec. 31, 2022.

[18] E. Agbozo, et al., Applying multi-criteria decision making to prioritization of Web 3.0 development factors, in: E-business technologies conference proceedings, Vol. 3, 2023, pp. 229–232.

[19] I. C. Education, Artificial intelligence (AI), https://www.ibm.com/cloud/learn/what-is-artificial-intelligence, Accessed: Feb. 1, 2024.

[20] H. Hua, et al., Edge computing with artificial intelligence: A machine learning perspective, ACM Computing Surveys 55 (9) (2023) 1–35.

[21] J. Bambacht, J. Pouwelse, Web3: A decentralized societal infrastructure for identity, trust, money, and data, arXiv preprint arXiv:2203.00398 (2022).

[22] G. Huang, et al., Efficient and low overhead website fingerprinting attacks and defenses based on TCP/IP traffic, in: Proceedings of the ACM Web Conference 2023, 2023, pp. 1991–1999.

[23] W. D. la Cadena, et al., Trafficsliver: Fighting website fingerprinting attacks with traffic splitting, in: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, 2020, pp. 1971–1985.

[24] S. Voshmgir, Token Economy: How the Web3 reinvents the Internet, Vol. 2, Token Kitchen, 2020.

[25] P. Kasireddy, The architecture of a Web 3.0 application, `https://www.preethikasireddy.com/post/the-architecture-of-a-web-3-0-application`, Accessed: Jul. 16, 2023.

[26] H. Xu, et al., deController: a Web3 native cyberspace infrastructure perspective, IEEE Communications Magazine (2023).

[27] U. Gallersdorfer, L. Klaassen, C. Stoll, Energy efficiency and carbon footprint of Proof of Stake blockchain protocols (Jan. 2022).

[28] V. Kohli, et al., An analysis of energy consumption and carbon footprints of cryptocurrencies and possible solutions, Digital Communications and Networks 9 (1) (2022) 79–89.

[29] AlgorandTechnologies, The importance of low transaction costs & lower carbon emissions to mint NFTs, `https://algorandtechnologies.com/news/the-importance-of-low-transaction-costs--lower-carbon`, Accessed: Jul. 31, 2024.

[30] L. Breidenbach, et al., Chainlink 2.0: Next steps in the evolution of decentralized oracle networks, Chainlink Labs 1 (2021) 1–136.

[31] V. Buterin, Chain interoperability, R3 Research Paper 9 (2016).

[32] R. Belchior, A. Vasconcelos, S. Guerreiro, M. Correia, A survey on blockchain interoperability: Past, present, and future trends, ACM Computing Surveys 54 (8) (2021) 1–41.

[33] G. Wang, Q. Wang, S. Chen, Exploring blockchains interoperability: A systematic survey, ACM Computing Surveys (2023).

[34] M. Borkowski, D. McDonald, C. Ritzer, S. Schulte, Towards atomic cross-chain token transfers: State of the art and open questions within tast, Distributed Systems Group TU Wien (Technische Universit at Wien), Report 8 (2018).

[35] Multichain, Multichain bridge, `https://docs.multichain.org/getting-started/introduction`, Accessed: Feb. 1, 2024.

[36] Threshold, tBTC bitcoin bridge, `https://docs.threshold.network/applications/tbtc-v2`, Accessed: Feb. 1, 2024.

[37] ParityTech, parity-bridges-common, `https://github.com/paritytech/parity-bridges-common`, Accessed: Jul. 31, 2024.

[38] Solana, Wormhole, `https://solana.com/ecosystem/wormhole`, Accessed: Feb. 1, 2024.

[39] C. Smith, et al., Scaling, `https://ethereum.org/en/developers/docs/scaling/`, Accessed: Jan. 26, 2024.

[40] Ethereum, Danksharding, `https://ethereum.org/en/roadmap/danksharding/`, Accessed: Jan. 17, 2024.

[41] P. Joseph, D. Thaddeus, The bitcoin lightning network: Scalable off-chain instant payments (2016).

[42] Raiden-Network, What is the raiden network?, `https://raiden.network/101.html`, Accessed: Feb. 1, 2024.

[43] A. Cahill, S. Deshpande, Layer-2 scaling solutions: A framework for comparison (May 2022).

[44] Liquid-Network, The liquid network, `https://liquid.net/`, Accessed: Feb. 1, 2024.

[45] A. Tripathi, Introduction to Polygon PoS, `https://docs.polygon.technology/pos/architecture/`, Accessed: Jul. 16, 2023.

[46] A. De Salve, L. Franceschi, A. Lisi, P. Mori, L. Ricci, L2dart: A trust management system integrating blockchain and off-chain computation, ACM Transactions on Internet Technology 23 (1) (2023) 1–30.

[47] J. Benet, IPFS - content addressed, versioned, P2P file system, arXiv preprint arXiv:1407.3561 (2014).

[48] Y. Lin, et al., A unified blockchain-semantic framework for wireless edge intelligence enabled Web 3.0, IEEE Wireless Communications (2023).

[49] D. Palanikkumar, et al., An enhanced decentralized social network based on Web3 and IPFS using blockchain, in: 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), 2023, pp. 616–623.

[50] A. Petcu, et al., A secure and decentralized authentication mechanism based on Web 3.0 and Ethereum blockchain technology, Applied Sciences 13 (4) (2023).

[51] A. Razzaq, et al., IoT data sharing platform in Web 3.0 using blockchain technology, Electronics 12 (5) (2023).

[52] Y. Lin, et al., A blockchain-based semantic exchange framework for Web 3.0 toward participatory economy, IEEE Communications Magazine (Aug. 2023).

[53] S. Guo, et al., Blockchain-assisted privacy-preserving data computing architecture for Web3, IEEE Communications Magazine 61 (8) (2023) 28–34.

[54] Y. Qiu, et al., Fog-assisted blockchain radio access network for Web3, IEEE Communications Magazine (Aug. 2023).

[55] Z. Liu, et al., Make Web 3.0 connected, IEEE Transactions on Dependable and Secure Computing 19 (2022) 2965–2981.

[56] G. Yu, et al., Towards Web3 applications: Easing the access and transition, arXiv preprint arXiv:2210.05903 (2022).

[57] A. Chopra, et al., Va3: A Web 3.0 based I2I power transaction platform, in: 2022 7th IEEE Workshop on the Electronic Grid (eGRID), 2022, pp. 1–5.

[58] P. Drakatos, et al., Triastore: A Web 3.0 blockchain datastore for massive IoT workloads, in: 2021 22nd IEEE International Conference on Mobile Data Management (MDM), 2021, pp. 187–192.

[59] G. Liu, et al., Semantic communications for artificial intelligence generated content (AIGC) toward effective content creation, arXiv preprint arXiv:2308.04942 (2023).

[60] L. Xia, et al., Generative AI for semantic communication: Architecture, challenges, and outlook, arXiv preprint arXiv:2308.15483 (2023).

[61] R. Cheng, et al., A wireless AI-generated content (AIGC) provisioning framework empowered by semantic communication, arXiv preprint arXiv:2310.17705 (2023).

[62] H. Du, et al., Enabling AI-generated content (AIGC) services in wireless edge networks, arXiv preprint arXiv:2301.03220 (2023).

[63] Y. Liu, et al., Blockchain-empowered lifecycle management for AI-generated content (AIGC) products in edge networks, arXiv preprint arXiv:2303.02836 (2023).

[64] J. Wang, et al., A unified framework for guiding generative AI with wireless perception in resource constrained mobile edge networks, arXiv preprint arXiv:2309.01426 (2023).

[65] Y. Cao, et al., A comprehensive survey of AI-generated content (AIGC): A history of generative AI from GAN to ChatGPT, arXiv preprint arXiv:2303.04226 (2023).

[66] C. Zhang, et al., A complete survey on generative AI (AIGC): Is ChatGPT from GPT-4 to GPT-5 all you need?, arXiv preprint arXiv:2303.11717 (2023).

[67] M. Treviso, et al., Efficient methods for natural language processing: A survey, Transactions of the Association for Computational Linguistics 11 (2023) 826–860.

[68] C. Qin, et al., Is ChatGPT a general-purpose natural language processing task solver?, arXiv preprint arXiv:2302.06476 (2023).

[69] D. Khurana, A. Koli, K. Khatter, S. Singh, Natural language processing: State of the art, current trends and challenges, Multimedia tools and applications 82 (3) (2023) 3713–3744.

[70] N. Le, et al., Deep reinforcement learning in computer vision: A comprehensive survey, Artificial Intelligence Review (2022) 1–87.

[71] Y. Bi, et al., A survey on evolutionary computation for computer vision and image analysis: Past, present, and future trends, IEEE Transactions on Evolutionary Computation (2022).

[72] A. Vaswani, et al., Attention is all you need, Advances in neural information processing systems 30 (2017).

[73] I. Goodfellow, et al., Generative adversarial nets, in: Advances in neural information processing systems, 2014, pp. 2672–2680.

[74] D. Kingma, et al., Auto-encoding variational bayes, arXiv preprint arXiv:1312.6114 (2013).

[75] K. Gregor, et al., Deep autoregressive networks, in: International Conference on Machine Learning, 2014, pp. 1242–1250.

[76] AletheaAI, Robert Alice, `https://www.sothebys.com/en/buy/auction/2021/natively-digital-a-curated-nft-sale-2/to-the-young-artists-of-cyberspace`, Accessed: Nov. 21, 2023.

[77] J. Pregelj, Web3 plugin for ChatGPT, `https://github.com/jerne`

jpregelj/web3-chatgpt-plugin, Accessed: Nov. 21, 2023.
[78] D. Sathavara, et al., SuperCool-AI, https://devpost.com/software/supercool-ai, Accessed: Feb. 1, 2024.
[79] M. Sokoli, et al., Web3GPT, https://ethglobal.com/showcase/web3-gpt4-jkaja, Accessed: Feb. 1, 2024.
[80] J. Savage, ETHGPT, https://github.com/Jsavage1325/ETHGPT, Accessed: Nov. 21, 2023.
[81] C. Yang, et al., FlashGPT, https://github.com/alt-research/flashGPT, Accessed: Nov. 21, 2023.
[82] TokenGPT, Tokengpt, https://ethglobal.com/showcase/tokengpt-ko8x6, Accessed: Nov. 21, 2023.
[83] M. Zhang, CoinGPT, https://github.com/mccowanzhang/coingpt, Accessed: Nov. 21, 2023.
[84] Memosys, Greg, Defi-companion-covalent, https://github.com/gregfromstl/defi-companion, Accessed: Nov. 21, 2023.
[85] Aegis, Aegis: Whitepaper v2, https://www.aiaegis.org/wp.pdf, Accessed: Jan. 25, 2024.
[86] X. Tang, et al., Deep learning-based solution for smart contract vulnerabilities detection, Scientific Reports 13 (1) (2023) 20106.
[87] K. Gupta, et al., Secure Semantic Snap, https://ethglobal.com/showcase/sss-secure-semantic-snap-6d89g, Accessed: Nov. 21, 2023.
[88] A. Alam, et al., MedDAO, https://github.com/Arsalaan-Alam/hackfs, Accessed: Nov. 21, 2023.
[89] S. Das, et al., Practical asynchronous high-threshold distributed key generation and distributed polynomial sampling, in: 32nd USENIX Security Symposium (USENIX Security 23), 2023, pp. 5359–5376.
[90] S. Das, et al., A new paradigm for verifiable secret sharing, cryptology ePrint Archive (2023).
[91] W. Zhang, et al., A secure revocable fine-grained access control and data sharing scheme for SCADA in IIoT systems, IEEE Internet of Things Journal 9 (3) (2021) 1976–1984.
[92] J. Zhang, et al., Revocable and privacy-preserving decentralized data sharing framework for fog-assisted Internet of Things, IEEE Internet of Things Journal 9 (13) (2021) 10446–10463.
[93] G. Yu, et al., Predicting NFT classification with GNN: A recommender system for Web3 assets, in: 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2023, pp. 1–5.
[94] I. Alarab, S. Prakoonwit, Graph-based LSTM for anti-money laundering: Experimenting temporal graph convolutional network with bitcoin data, Neural Processing Letters 55 (1) (2023) 689–707.
[95] M. Xu, et al., When quantum information technologies meet blockchain in Web 3.0, IEEE Network (2023).
[96] R. Madhwal, J. Pouwelse, Web3recommend: Decentralised recommendations with trust and relevance, arXiv preprint arXiv:2307.01411 (2023).
[97] M. Unzeelah, Z. Memon, Fighting against fake news by connecting machine learning approaches with Web3, in: 2022 International Conference on Emerging Trends in Smart Technologies (ICETST), 2022, pp. 1–6.
[98] J. Kim, et al., A machine learning approach to anomaly detection based on traffic monitoring for secure blockchain networking, IEEE Transactions on Network and Service Management 19 (3) (2022) 3619–3632.
[99] T. Huynh-The, C.-H. Hua, N. A. Tu, D.-S. Kim, 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.
[100] N. Keizer, et al., The case for AI based Web3 reputation systems, in: 2021 IFIP Networking Conference (IFIP Networking), 2021, pp. 1–2.
[101] C. Mistry, U. Thakker, R. Gupta, M. S. Obaidat, S. Tanwar, N. Kumar, J. J. P. C. Rodrigues, Medblock: An AI-enabled and blockchain-driven medical healthcare system for COVID-19, in: ICC 2021 - IEEE International Conference on Communications, 2021, pp. 1–6.
[102] Y. Zhuang, Z. Liu, P. Qian, Q. Liu, X. Wang, Q. He, Smart contract vulnerability detection using graph neural network, in: Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence, IJCAI-20, 2020, pp. 3283–3290.
[103] Z. Xiong, et al., When mobile blockchain meets edge computing, IEEE Communications Magazine 56 (8) (2018) 33–39.
[104] T. Qiu, et al., Edge computing in industrial Internet of Things: Architecture, advances and challenges, IEEE Communications Surveys & Tutorials 22 (4) (2020) 2462–2488.
[105] L. Lin, et al., Computation offloading toward edge computing, Proceedings of the IEEE 107 (8) (2019) 1584–1607.
[106] Azion, Madeiramadeira reduces cloud provider costs by 90% and improves site performance by delivering content with azion, https://www.azion.com/en/success-case/madeiramadeira/, Accessed: Jul. 16, 2023.
[107] M. Liu, et al., Computation offloading and content caching in wireless blockchain networks with mobile edge computing, IEEE Transactions on Vehicular Technology 67 (11) (2018) 11008–11021.
[108] Y. Zhu, et al., Blockchain-enabled access management system for edge computing, Electronics 10 (9) (2021).
[109] D. Doe, et al., Promoting the sustainability of blockchain in Web 3.0 and the Metaverse through diversified incentive mechanism design, IEEE Open Journal of the Computer Society (2023).
[110] X. Wang, et al., Convergence of edge computing and deep learning: A comprehensive survey, IEEE Communications Surveys & Tutorials 22 (2) (2020) 869–904.
[111] S. Deng, et al., Edge intelligence: The confluence of edge computing and artificial intelligence, IEEE Internet of Things Journal 7 (8) (2020) 7457–7469.
[112] L. Cao, Decentralized AI: Edge intelligence and smart blockchain, metaverse, Web3, and desci, IEEE Intelligent Systems 37 (3) (2022) 6–19.
[113] D. Wang, Y. Jia, M. Dong, K. Ota, L. Liang, Blockchain-integrated UAV-assisted mobile edge computing: Trajectory planning and resource allocation, IEEE Transactions on Vehicular Technology 73 (1) (2024) 1263–1275.
[114] Q. Tang, Z. Fei, J. Zheng, B. Li, L. Guo, J. Wang, Secure aerial computing: Convergence of mobile edge computing and blockchain for UAV networks, IEEE Transactions on Vehicular Technology 71 (11) (2022) 12073–12087.
[115] P. Consul, I. Budhiraja, D. Garg, A hybrid secure resource allocation and trajectory optimization approach for mobile edge computing using federated learning based on Web 3.0, IEEE Transactions on Consumer Electronics 70 (1) (2024) 1167–1179.
[116] E.-M. El-Mhamdi, S. Farhadkhani, R. Guerraoui, A. Guirguis, L.-N. Hoang, S. Rouault, Collaborative learning in the jungle (decentralized, byzantine, heterogeneous, asynchronous and nonconvex learning), in: Proceedings of the 35th International Conference on Neural Information Processing Systems, 2024, pp. 25044–25057.
[117] C. Yang, Y. Wang, S. Lan, L. Zhu, Multi-agent reinforcement learning based distributed channel access for industrial edge-cloud Web 3.0, IEEE Transactions on Network Science and Engineering (2024) 1–12.
[118] Z. Liu, X. Xu, F. Han, Q. Zhao, L. Qi, W. Dou, X. Zhou, Secure edge server placement with non-cooperative game for Internet of Vehicles in Web 3.0, IEEE Transactions on Network Science and Engineering (2023) 1–12.
[119] X. Xu, S. Tang, L. Qi, X. Zhou, F. Dai, W. Dou, CNN partitioning and offloading for vehicular edge networks in Web3, IEEE Commun. Magazine 61 (8) (2023) 36–42.
[120] A. Singh, K. Chatterjee, Securing smart healthcare system with edge computing, Computers & Security 108 (2021).
[121] R. Wang, et al., A video surveillance system based on permissioned blockchains and edge computing, in: 2019 IEEE international conference on big data and smart computing (BigComp), 2019, pp. 1–6.
[122] N. Luong, et al., Optimal auction for edge computing resource management in mobile blockchain networks: A deep learning approach, in: 2018 IEEE international conference on communications (ICC), 2018, pp. 1–6.
[123] N. Alhaddad, S. Das, S. Duan, L. Ren, M. Varia, Z. Xiang, H. Zhang, Asynchronous verifiable information dispersal with near-optimal communication, Cryptology ePrint Archive (2022).
[124] S. Das, Z. Xiang, L. Ren, Asynchronous data dissemination and its applications, in: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, 2021, pp. 2705–2721.
[125] Y. K. Dwivedi, et al., Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy, International Journal of Information Management 66 (2022) 102542.
[126] Decentraland, What is Decentraland?, https://decentraland.org/, Accessed: Jul. 31, 2024.
[127] Q. Wang, R. Li, Q. Wang, S. Chen, Non-fungible token (NFT): Overview, evaluation, opportunities and challenges, arXiv preprint

arXiv:2105.07447 (2021).
[128] W. Rehman, H. Zainab, J. Imran, N. Bawany, NFTs: Applications and challenges, in: International Arab Conference on Information Technology (ACIT), IEEE, 2021, pp. 1–7.
[129] U. Chohan, Non-fungible tokens: Blockchains, scarcity, and value, Critical Blockchain Research Initiative (CBRI) Working Papers (2021).
[130] L. Yang, et al., Generic-NFT: A generic non-fungible token architecture for flexible value transfer in Web3, techRxiv preprint (2023).
[131] E. Lopez, Securechain, https://github.com/eduardfina/Securechain, Accessed: Nov. 21, 2023.
[132] J. Zhu, et al., NFTool, https://github.com/Bobliuuu/NFTool, Accessed: Nov. 21, 2023.
[133] C. Adiloglu, StoryChain, https://storychain.ai, Accessed: Nov. 21, 2023.
[134] K. Busch, Non-fungible tokens (NFTs) (Jul. 2022).
[135] Q. Wang, et al., Non-fungible token (NFT): Overview, evaluation, opportunities and challenges, arXiv preprint arXiv:2105.07447 (2021).
[136] R. Kräussl, A. Tugnetti, Non-fungible tokens (NFTs): A review of pricing determinants, applications and opportunities, Applications and Opportunities (2022).
[137] D. Zetzsche, D. Arner, R. Buckley, Decentralized finance, Journal of Financial Regulation 6 (2) (2020) 172–203.
[138] S. Werner, et al., SoK: Decentralized finance (DeFi), arXiv preprint arXiv:2101.08778 (2021).
[139] P. Winter, A. Lorimer, P. Snyder, B. Livshits, What's in your wallet? privacy and security issues in Web 3.0, arXiv preprint arXiv:2109.06836 (2021).
[140] E. Jiang, et al., Decentralized finance (DeFi): A survey, arXiv preprint arXiv:2308.05282 (2023).
[141] Q. Kaihua, et al., CeFi vs. DeFi–comparing centralized to decentralized finance, arXiv preprint arXiv:2106.08157 (2021).
[142] F. Schär, Decentralized finance: On blockchain-and smart contract-based financial markets, FRB of St. Louis Review (2021).
[143] Y. Chen, C. Bellavitis, Blockchain disruption and decentralized finance: The rise of decentralized business models, Journal of Business Venturing Insights 13 (2020) e00151.
[144] C. Harvey, A. Ramachandran, J. Santoro, DeFi and the Future of Finance, John Wiley & Sons, 2021.
[145] X. Zhao, et al., FinBrain: when finance meets AI 2.0, Frontiers of Information Technology & Electronic Engineering 20 (7) (2019) 914–924.
[146] L. Cao, AI in finance: A review, Available at SSRN 3647625 (2020).
[147] N. Sadman, et al., Promise of AI in DeFi, A systematic review, Digital 2 (1) (2022) 88–103.
[148] Y. Goyal, et al., AgroSurance, https://github.com/agrosurance, Accessed: Nov. 21, 2023.
[149] A. Kondaurova, K. Orlov, Prompt DeFi, https://github.com/Digberi/promptdefi-web, Accessed: Nov. 21, 2023.
[150] A. Dubyk, et al., RoboFI, https://devpost.com/software/robofi, Accessed: Nov. 21, 2023.
[151] C. Chen, et al., When digital economy meets Web 3.0: Applications and challenges, IEEE Open Journal of the Computer Society (2022).
[152] W. Ma, et al., A comprehensive study of governance issues in decentralized finance applications, arXiv preprint arXiv:2311.01433 (2023).
[153] R. Qin, et al., Web3-based decentralized autonomous organizations and operations: Architectures, models, and mechanisms, IEEE Transactions on Systems, Man, and Cybernetics: Systems 53 (4) (2022) 2073–2082.
[154] S. Wang, et al., Decentralized autonomous organizations: Concept, model, and applications, IEEE Transactions on Computational Social Systems 6 (5) (2019) 870–878.
[155] R. Qin, et al., Web3-based decentralized autonomous organizations and operations: Architectures, models, and mechanisms, IEEE Transactions on Systems, Man, and Cybernetics: Systems (2022).
[156] Y. E. Faqir, J. Arroyo, S. Hassan, An overview of decentralized autonomous organizations on the blockchain, in: Proceedings of the 16th international symposium on open collaboration, 2020, pp. 1–8.
[157] X. Zhao, et al., Task management in decentralized autonomous organization, Journal of Operations Management 68 (6-7) (2022) 649–674.
[158] C. Santana, L. Albareda, Blockchain and the emergence of decentralized autonomous organizations (DAOs): An integrative model and research agenda, Technological Forecasting and Social Change 182 (2022) 121806.
[159] M. Haque, M. H. S. Hossain, A comprehensive review and architecture of a decentralized automated direct government system using artificial intelligence and blockchain, International Journal of Scientific & Engineering Research 13 (2022).
[160] K. Nayan, OmniGovern DAO, https://github.com/kamalbuilds/OmniGovern-DAO/, Accessed: Nov. 21, 2023.
[161] D. Duportail, Rooster DAO, https://github.com/RoosterDao, Accessed: Nov. 21, 2023.
[162] S. Kapadia, A. Aghadi, N. Lionis, DAOasis, https://github.com/Suhel-Kap/DAOasis, Accessed: Nov. 21, 2023.
[163] W. Ding, et al., Desci based on Web3 and DAO: A comprehensive overview and reference model, IEEE Transactions on Computational Social Systems 9 (5) (2022) 1563–1573.
[164] G. Yu, et al., Leveraging architectural approaches in Web3 applications-a DAO perspective focused, in: 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2023, pp. 1–6.
[165] D. Gogel, B. Kremer, A. Slavin, K. Werbach, Decentralized autonomous organizations: Beyond the hype, White Paper (Jun. 2022).
[166] J. Tan, et al., Open problems in DAOs, arXiv preprint arXiv:2310.19201 (2023).
[167] R. Rudman, R. Bruwer, Defining Web 3.0: Opportunities and challenges, The Electronic Library (2016).
[168] D. Sheridan, et al., Web3 challenges and opportunities for the market, arXiv preprint arXiv:2209.02446 (2022).
[169] Y. Fan, et al., The current opportunities and challenges of Web 3.0, arXiv preprint arXiv:2306.03351 (2023).
[170] C. Barabas, N. Narula, E. Zuckerman, Defending Internet freedom through decentralization: Back to the future, The Center for Civic Media & The Digital Currency Initiative MIT Media Lab (2017).
[171] H. Zhong, M. Hamilton, Exploring gender and race biases in the NFT market, Finance Research Letters 53 (May 2023).
[172] Z. Obermeyer, B. Powers, C. Vogeli, S. Mullainathan, Dissecting racial bias in an algorithm used to manage the health of populations, Science 366 (6464) (2019) 447–453.
[173] M. Antonakakis, et al., Understanding the mirai botnet, in: 26th USENIX security symposium (USENIX Security 17), 2017, pp. 1093–1110.
[174] X. Jin, et al., Edge security: Challenges and issues, arXiv preprint arXiv:2206.07164 (2022).