

Web 3.0: A Survey on the Architectures, Enabling Technologies, Applications, and Challenges

Bin Cao, *Senior Member, IEEE*, Shaohe Xiao, Long Shi, *Senior Member, IEEE*, Taotao Wang, *Member, IEEE*, Jinyu Chen, Jiaheng Wang, *Senior Member, IEEE*, Xintong Ling, *Member, IEEE*, Hao Xu, *Member, IEEE*, Shengli Zhang, *Senior Member, IEEE*, and Erwu Liu, *Senior Member, IEEE*

Abstract—Web 3.0 represents the next evolutionary stage of the Internet, characterized by a “read-write-own” paradigm that empowers users to control their own data. Driven by advancements in edge technologies and rising concerns about privacy and security, a growing number of Web 3.0 applications have emerged, sparking widespread concern and research in both the industrial and academic fields. To address the demands for secure identity management, trustworthy data circulation, and reliable network services, more emerging technologies beyond blockchain have been introduced to Web 3.0. However, this integration has also introduced increased complexity and ambiguity in Web 3.0’s implementation and future development. Therefore, this survey aims to provide a systematic review of Web 3.0, elucidating its definition, architecture, technologies, ecosystem, and future directions. The main contributions include identifying an adaptable Web 3.0 architecture that illustrates the correlation of each layer and functionalities, summarizing Web 3.0 workflow with three functions as identity management, data publication and retrieval, and network service. Besides that, this survey categorizes enabling technologies into five areas, highlighting the comparison of different technologies. As the Web 3.0 application ecosystem flourishes, this survey further explores use cases in finance, governance, and gaming, and introduces evaluation criteria tailored for Web 3.0 applications. Finally, we highlight some future research directions for the full realization of Web 3.0. This survey outlines the current landscape and advancements of Web 3.0, laying a solid foundation for future research and standardization, with the ultimate goal of realizing a decentralized and user-empowered digital infrastructure.

Index Terms—Web 3.0, Read-Write-Own, Decentralization, Blockchain, Communications and Networks, Artificial Intelligence.

I. INTRODUCTION

THE advent of Web 3.0 marks a revolutionary transition in the digital landscape, characterized by decentralized architectures, enhanced data privacy, and the proliferation of blockchain technologies. Recent progress in this domain has given rise to numerous emerging developments, ranging from decentralized finance (DeFi) and non-fungible tokens (NFTs) to advanced smart contracts and decentralized autonomous organizations (DAOs). These innovations are not only reshaping the way we interact with the Internet but also laying the groundwork for a more inclusive and secure digital future that is seen from the vein of the Internet.

A. Birth of Web 3.0

The term Web 3.0 denotes the third generation of the Internet, a concept initially identified by Jeffrey Zeldman [1] in 2006. It emerged in response to the limitations and unfulfilled needs of its predecessors, harnessing new technologies to overcome these challenges. The story of Web 3.0 has been told in many hold, however, to accurately define Web 3.0, comprehending the evolutionary stages of Web 1.0 and Web 2.0 is vital.

In 1989, Tim Berners-Lee introduced the World Wide Web, marking the inception of Web 1.0 during an era when the Internet was bound to limited functions. This period was characterized by users’ passively consuming content curated and hosted by emails, web portals and yellow pages, such as *Yahoo*, *AOL*, *craigslist*, *MSN*, etc., with limited interaction and data exchange. Equipped with foundational web technologies like web browsers powered by HTML with HTTP, Web 1.0 represents the dawn of the Internet era.

In contrast, Web 2.0 emphasizes the transition towards more interactive, user-generated content and the proliferation of social networks. Meanwhile, the evolution of mobile networks from 3G to 5G has dramatically improved Internet accessibility. The era of Web 2.0 introduced revolutionary services, including social media, mobile payments, and content delivery platforms. The participatory nature of Web 2.0 sparked a data revolution, leading to the emergence of tech behemoths such as Google, Facebook, Amazon, Tencent, etc., which now offer a wide array of services to day-to-day life. Concurrently, advances in cloud computing, the Internet of Things (IoT), and artificial intelligence (AI) have seamlessly integrated

This work is supported in part by the National Natural Science Foundation of China under Grant No. U22B2006; the Program of Science and Technology Cooperation of Nanjing with International/Hong Kong, Macao and Taiwan under Grant 202401019; the Young Elite Scientists Sponsorship Program By CAST 2023QNRC001; the Fundamental Research Funds for the Central Universities; Shanghai Rising-Star Program; Shanghai Pujiang Program; the Guangdong Basic and Applied Basic Research Foundation under grant 2024A1515012407; and the Research Center for FinTech and Digital-Intelligent Management at Shenzhen University. (*Corresponding author: Long Shi.*)

Bin Cao, Shaohe Xiao are with State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China. (e-mail: {caobin, xiaoshaohe}@bupt.edu.cn)

Long Shi, Jinyu Chen are with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing 210094, China. (e-mail: slong1007@gmail.com, Jinyu.Chen@njust.edu.cn)

Taotao Wang, Shengli Zhang are with the College of Electronics and Information Engineering, Shenzhen University, Shenzhen 518052, China. (e-mail: ttwang@szu.edu.cn, zsl@szu.edu.cn)

Jiaheng Wang, Xintong Ling are with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 211102, China, and also with the Purple Mountain Laboratories, Nanjing 211111, China. Jiaheng Wang is also with the School of Cyber Science and Engineering, Southeast University, Nanjing 211102, China. (e-mail: jhwang@seu.edu.cn, xtling@seu.edu.cn)

Hao Xu, Erwu Liu are with College of Electronic and Information Engineering, and Shanghai Institute of Intelligent Science and Technology, Tongji University, Shanghai, China. (e-mail: {hao.xu, erwu.liu}@ieee.org)

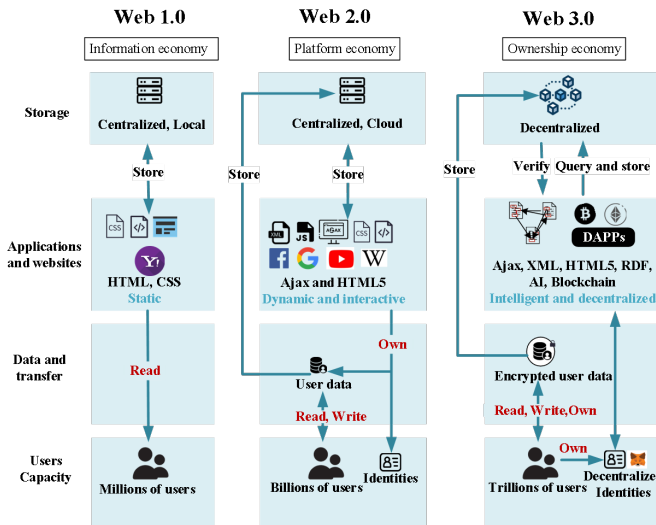


Fig. 1: Comparison of Web 1.0, Web 2.0 and Web 3.0

the Internet into traditional sectors like manufacturing, energy, healthcare, finance, and logistics. This integration has significantly boosted productivity, enhanced capabilities, and achieved notable cost efficiencies.

The advent of increasingly sophisticated communication networks and a wide range of online services covering every angle of living, entertainment, work, and business has led to a comprehensive digital transformation of our lives. However, the inherent flaws of Web 2.0 have precipitated a concerning status quo that users' data are at risk. The absence of an intrinsic digital identity means that data creation and exchange are monopolized by platforms and services, with login accounts serving merely as a makeshift solution for the lack of genuine ownership and digital rights. In this scenario, companies can control user data and may abuse it to gain benefits, compromising the security and openness of the Internet.

Distinct from its predecessors, Web 3.0 embodies the “read-write-own” paradigm, empowering users with full control over their data. Particularly, Web 3.0 envisions data as part of an autonomous infrastructure, eliminating the dependency on specific services and platforms. This independence facilitates data management and exchange without allegiance to any single entity, thereby ensuring data ownership. This transformation has laid the foundation for the emergence of valuable digital assets, exemplifying the fundamental essence of the Internet as an invaluable network. This represents the ultimate goal of Web 3.0, where blockchain technology serves as a remarkable foundation for its immense potential. A comparison of Web 1.0, Web 2.0, and Web 3.0 is illustrated in Fig.1.

B. Definitions of Web 3.0

The concept of Web 3.0 was initially introduced as the Semantic Web, a vision proposed by Tim Berners-Lee in 2009 [2], [3], which aimed to solve the problem of data heterogeneity and improve data interpretability and interoperability by extracting and linking data. It relied on frameworks such as Resource Description Framework (RDF) to standardize

data relationships and enable interoperability across disparate datasets.

The current understanding of Web 3.0, enriched by the development of blockchain, diverges from the semantic Web 3.0 proposed by Tim Berners-Lee. In 2014, Gavin Wood, co-founder of Ethereum, redefined Web 3.0 [4] as the next evolutionary phase of the Internet, underpinned by the principles of blockchain technology and the decentralization of network ecosystems. Within this framework, Web 3.0 is envisioned as a secure social operating system, facilitating decentralized, anonymous, secure, and trustless exchanges among users.

Subsequent definitions have expanded on this foundation, emphasizing features such as data ownership, decentralization, and user-centric, secure network governance. Notably, Ding *et al.* and prominent entities like Coinbase have characterized Web 3.0 as a distributed network grounded in blockchain, cryptocurrencies, and decentralized autonomous organizations (DAOs), highlighting its capacity to empower users and ensure trustless, permissionless interactions [5], [6]. Similarly, Murray *et al.* define it as a new Internet paradigm built on open blockchain technology, designed to decentralize online experiences and enable users to control and monetize their content [7]. Further elaborations by Cao *et al.* describe Web 3.0's objectives as reducing centralization, enhancing security, and supporting the creation and exchange of content, as well as immersive experiences [8]. Recent studies have also explored the integration of semantic communication with blockchain to advance Web 3.0's capabilities, arguing that such integration is crucial for the decentralized transmission of content semantics, supported by emerging technologies like virtual reality and artificial intelligence [9]–[11].

From the above research, it is observed that Web 3.0¹, characterized by “read-write-own”, gradually becomes an umbrella term encompassing emerging technologies like blockchain, artificial intelligence, semantic technologies, and communication technologies. The core objectives of Web 3.0 can be encapsulated as a novel network paradigm that amalgamates these emerging technologies to address five key dimensions:

¹As mentioned above, Web 3.0 is a conceptual description of the next stage of internet development, initially referred to as the “Semantic Web” or “Intelligent Web”, later incorporating characteristics such as data readability, writability, and ownability. The concept behind Web 3.0 emphasizes the evolution of the internet from the current to the next generation. On the other hand, Web 3 is a more specific term, typically referring to a decentralized network architecture based on blockchain technology. It emphasizes the importance of individual data rights, decentralized applications, digital asset ownership, smart contracts, and the vision of realizing the next generation of the internet through blockchain.

In the field of the internet and technology, the usage and definitions of terms often evolve with time and industry developments. Regarding the terms “Web 3” and “Web 3.0”, they may sometimes be used interchangeably or confused by people in certain contexts, leading to a trend of convergence between these terms. Although there were initially some distinctions in the descriptions of “Web 3” and “Web 3.0”, the understanding of these terms has gradually become more unified, with many considering them as different expressions of the same concept. Especially when discussing new-generation internet technologies like blockchain, decentralized applications, and smart contracts, “Web 3” and “Web 3.0” might be seen as two ways of describing the same concept.

Throughout this survey, we have solely used the term Web 3.0 to refer to the next generation of the internet, considering it as a broader concept that encompasses Web 3.

- **Decentralization and Democratization:** Web 3.0 is envisioned to counteract the centralization issues attributed to the dominance of technology giants by reconstructing a decentralized and democratized network. This initiative aims to vest users with unprecedented control and ownership over their data, identities, digital assets, and the broader network infrastructure. By eliminating reliance on prior trust or intermediaries, Web 3.0 fosters a culture of collaboration and sharing across a spectrum of entities, including devices, individuals, teams, and organizations.
- **Security and Privacy:** A principle of Web 3.0 is to cultivate a secure and trustworthy ecosystem for the seamless exchange of data, tokens, and digital assets. This vision is underpinned by a steadfast commitment to the zero-trust strategies, ensuring robust security and privacy safeguards.
- **Scalability and Interoperability:** Acknowledging the necessity to accommodate the demands of trillions of users, Web 3.0 prioritizes scalability and interoperability. These attributes are critical for facilitating the fluid distribution of content and digital assets across diverse platforms and applications within a multifaceted network landscape.
- **Tokenization and Token Economy:** Web 3.0 introduces innovative mechanisms for the tokenization, monetization, exchange, and trade of data and digital assets within a trustless framework. By circumventing traditional intermediaries, this model revolutionizes the paradigms of value creation and circulation through tokenomics and tokenization strategies.
- **Enhanced Performance and Customized Services:** Leveraging cutting-edge technologies such as edge-cloud computing, artificial intelligence, digital twins, and spatial technologies, Web 3.0 aspires to harness artificial general intelligence for optimizing network management, resource allocation, blockchain operations, data processing and transmission. This ambition translates into improved performance metrics and intelligent user services.

Web 3.0 signifies a transformative leap in the digital domain, fostering a decentralized ecosystem that amplifies data value circulation. This evolution redefines digital production and value distribution, extending services analogous to the physical world and promoting business digitalization. Furthermore, Web 3.0 enhances the digital marketplace through native digital rights and virtual content creation.

Technologically, it represents a systematic enhancement of the World Wide Web, surpassing Web 2.0's limitations by incorporating advanced technologies for improved connectivity. Innovations include high-speed data transmission through cloud-network convergence, enriched network protocols that emphasize trust and security, and a redefined network architecture facilitated by blockchain and digital identity technologies. Unlike traditional systems where trust is centralized, Web 3.0's trust emerges from decentralized, protocol-based consensus—such as cryptographic verification, distributed ledger validation, and algorithmic governance while partially intersecting with zero-trust principles. With Web 3.0's core

objectives that can be concluded as a vision to realize a decentralized, trusted network with token-based incentives, it can address emerging needs in various fields, paving the way for a more robust and versatile digital infrastructure.

C. Related Surveys

While Web 3.0 has demonstrated significant market value and received attention from both academic and industry fields, the definition and implementation of Web 3.0 remain ambiguous in different applications and literature. To address the demands for secure identity management, trustworthy data circulation, and reliable network services, more emerging technologies beyond blockchain have been introduced to Web 3.0. However, this integration has also introduced increased complexity and ambiguity in Web 3.0's implementation and future development. Therefore, a comprehensive review of it is necessary and timely. However, none of the existing works have provided a comprehensive review on Web 3.0, covering aspects ranging from adaptable architectures, technologies comparison, applications categories, evaluation criteria, and future directions, as shown in Table I. This survey seeks to fill this gap by providing an exhaustive overview of Web 3.0.

To clarify the novelty and necessity of this survey, we first review existing surveys on Web 3.0. Among current studies on Web 3.0's infrastructure and applications, Huang *et al.* in [12] categorized Web 3.0 applications and assessed their popularity across code and market levels, discussing the potential challenges and opportunities at the system, developer, and user levels. Focusing on the blockchain infrastructure and the applications of Web 3.0, Partha in [13] summarized the characteristics of Web 3.0 and compared different use cases in terms of decentralization, scalability, and interoperability. The authors also emphasized the importance of zero trust as a fundamental component for securing Web 3.0, comparing different zero-trust architectures in terms of their applicability. While these surveys have argued that Web 3.0 infrastructure and applications face challenges such as scalability, security, and performance, they have not provided a comprehensive evaluation criteria for Web 3.0, which is essential for assessing its applications.

To investigate the effect of emerging technologies on Web 3.0, Zhu *et al.* in [14] described the roles and necessity of blockchain, AI, and edge computing within the context of Web 3.0. Shen *et al.* in [15] provided a four-layer architecture and listed challenges faced by Web 3.0 in terms of data management, value cycle, ecological governance, and application scenarios. Ren *et al.* in [16] investigated the role of quantum information technology in building a resilient Web 3.0. These surveys have primarily focused on the roles that specific technologies played in Web 3.0, such as how AI technologies have addressed challenges related to data supply, value circulation, and ecological governance. However, they have not provided a systematic classification and comparison of these technologies, and a comprehensive and structural overview of Web 3.0 remains open.

From a perspective of workflow, Wang *et al.* in [17] developed a foundational model that breaks the operational workflows of Web 3.0 into 3 components: storage, computation,

TABLE I: Summary of existing surveys and tutorials

Aspect	Ref.	Main contributions	Uncovered points
Infrastructure and applications	[12]	· Investigating the categories of Web 3.0 application and their popularity from market level and code level. · Listing challenges faced by Web 3.0 on three levels: system level, developer level and user level.	· Lack of investigation on evaluation criteria of infrastructure and applications, which is important for assessing Web 3.0 applications.
	[13]	· Analysing the use cases and components of Web 3.0 ecosystem and presenting various zero-trust architectures.	
Emerging technologies for Web 3.0	[14]	· Describing the roles and necessity of blockchain, AI, and edge computing in Web 3.0.	· Lack of comprehensively categorising Web 3.0 technologies and comparison of different technologies. · Lack of exploration of Web 3.0 technical challenges.
	[15]	· Providing a four-layer architectural framework and an overview of AI and Web 3.0. · Listing challenges faced on data management, value cycle, ecological governance, and applications.	
	[16]	· Discussing improvements on the internal technologies of quantum blockchain. · Investigating potential quantum blockchain applications.	
Workflow	[17]	· Investigating current Web 3.0 projects and extracting an operational workflow with three-tiered components. · Evaluating workflows of different data management methodologies using blockchain metrics.	· Lack of comprehensive review on latest solutions emerging from the integration of various technologies and Web 3.0.
Decentralized technologies	[5]	· Giving the concept and characteristics of DeSci as Web 3.0 and DAO infrastructure.	· Focus on DeSci definition and lack of exploration of how it empowers Web 3.0. · Lack of discussion on DeAI's role in enhancing privacy and security of Web 3.0.
	[8]	· Studying DeAI definition and integration with Web 3.0, metaverse, and blockchain.	
	[18]	· Discussing decentralized technologies related blockchain and future directions of these technologies.	
Development in specific fields	[19]	· Discussing challenges Web 3.0 and DAO are facing. · Exploring potential of Web 3.0 and DAO in education.	· Lack of exploration of technical challenges and real-world use cases of Web 3.0 beyond specific domains like education and metaverse.
	[20]	· Reviewing Web 3.0 metaverse and its key components. · Proposing a three-layered framework to describe their features, missions, and relationships.	
Our work		· Identifying an adaptable architecture and workflow of Web 3.0. · Categorizing Web 3.0 technologies to 5 categories and giving a detailed comparison of different technologies where elaborates how to use them in Web 3.0. · First summarizing evaluation criteria related to Web 3.0 properties and performance metrics. · Exploring challenges, opportunities and future directions of Web 3.0.	

and access. However, this survey primarily approached Web 3.0 from the perspective of blockchain applications, summarizing the overall process while overlooking the architectural transformations introduced by Web 3.0. It overlooked both the impact of emerging technologies on Web 3.0 and recent academic work on Web 3.0.

Focusing on decentralization in Web 3.0, Korpál *et al.* in [18] discussed decentralized technologies related to blockchain. They identified three research directions for Web 3.0 encompassing the security and privacy of smart contracts, cyberattacks, and scalability and mass-adoption of Web 3.0. In [8], Cao *et al.* provided definitions of DeAI, Web 3.0, the metaverse, and Decentralized Science (DeSci), then discussed the applications of DeAI in Web 3.0. Ding *et al.* in [5] introduced the concept of DeSci and outlined a six-layered reference model, defining DeSci as a development paradigm emerging from advancements in blockchain, Web 3.0, and DAO infrastructures. These reviews on Web 3.0 decentralization technologies have not comprehensively explored either the role of DeAI and DeSci in enhancing Web 3.0, especially in terms of privacy and security, or the potential of other ad-

vanced AI technologies such as large language models, while focusing mainly on blockchain and decentralized storage.

In exploring the broader implications of Web 3.0 and DAOs on various sectors, Filipčić in [19] provided an overview of Web 3.0 technologies and their implications for education and research. The authors deemed that DAO could make the field of education and research more convenient for sharing data and ensuring data sovereignty, and argued that Web 3.0 and DAO were facing challenges such as high entry barriers, security issues, high energy consumption and low participation. In [20], Chen *et al.* reviewed the development of the metaverse over the past 30 years and highlighted three key communities: Web 3.0, immersive convergence, and crowd intelligence. The authors proposed an analysis framework from the community, society, and human layers and shared insights into several promising directions, encompassing three key socio-technical facets of Web 3.0 metaverse development. These surveys have discussed the impact of Web 3.0 on specific fields, such as education and the metaverse, while overlooking its technical challenges. In addition, they have not provided a comprehensive summary of relevant standards, policies, and future directions.

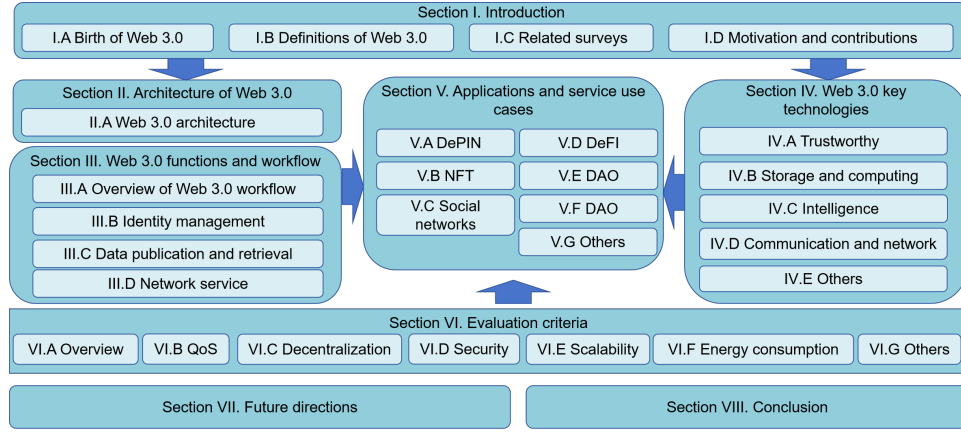


Fig. 2: The structure of this survey

D. Motivation and Contributions

Web 3.0 propels the Internet towards the realization of a technical innovation ecosystem across various domains, such as education [21], healthcare [22] and societal infrastructure [23]. Since users regain control over their identities and data, Web 3.0 is anticipated to mitigate the risk of private information leakage while facilitating the creation of verifiable proofs for trustworthy interactions. Supported by blockchain technologies, Web 3.0 holds the potential to revolutionize business models within creative industries and foster collaboration across diverse entities within a zero-trust framework [23].

Although Web 3.0 is widely recognized for its potential to significantly impact our lives, systematic reviews of its scope and implications remain scarce. Currently, Web 3.0 is still in its infancy, with its definitions and standards yet to be clearly established. There is a lack of consensus on a precise, unified definition, architecture, or workflow for Web 3.0. Moreover, the key technologies and challenges associated with Web 3.0 have not been comprehensively identified and reviewed. Research on its overall components and architectural design is limited, with only a few studies focusing on blockchain technology and its applications.

In this review, we aim to provide a systematic survey on Web 3.0 which reviews both the previous and the latest research work (i.e., from 2001 to 2024). The contributions of our survey are as follows.

- We provide an overview of the evolution of Web 3.0, delineating its definitions across five aspects: decentralization and democratization, security and privacy, scalability and interoperability, tokenization and token economy, enhanced performance and customized services;
- We identify an adaptable Web 3.0 architecture that aligns with the visions of Web 3.0 and summarize a workflow of Web 3.0 services;
- We categorize Web 3.0 pivotal technologies into five aspects and detail how these technologies are applied within the Web 3.0 context;
- We explore various Web 3.0 applications and use cases and first summarize a list of evaluation criteria of Web 3.0 applications;
- We discuss challenges, opportunities, and future directions of Web 3.0 and provide readers with a summary of

TABLE II: Comparison of Web 3.0 architectures

Architecture	Blockchain	Semantic communication	AI	Semantic Technologies	Zero Trust
[24]				✓	
[25] [6]	✓				
[26]	✓				✓
[15]	✓		✓		
[11] [10]	✓	✓	✓		
[27]	✓		✓	✓	✓
Our work	✓	✓	✓	✓	✓

current policies and standards.

The remainder of the survey is organized as follows. Section II reviews various Web 3.0 architectures and summarizes an adaptable architecture. Section III elaborates on the Web 3.0 workflow with 3 key functions. Section IV provides an in-depth analysis of each technology. Section V delves into primary applications and use cases of Web 3.0, and discusses challenges faced in Web 3.0 applications. Section VI identifies evaluation criteria for Web 3.0 applications. Section VII discusses open issues and future directions of Web 3.0. Finally, Section VIII summarizes the work. The organizational structure of this survey is shown in Fig.2.

II. ARCHITECTURE OF WEB 3.0

In this section, we provide a comprehensive review of Web 3.0 architecture and extract a backbone architecture for Web 3.0 covering different focuses of Web 3.0.

Current Web 3.0 architectures can be categorized into three types: Semantic Web 3.0, blockchain-based Web 3.0, and evolving Web 3.0 architectures. Semantic Web 3.0, proposed by Tim Berners-Lee [24], employs data description models to facilitate data representation and integration. Blockchain-based Web 3.0 architectures, proposed by industry leaders [6], [25], [26], leverage blockchain frameworks and zero-trust mechanisms emphasizing decentralization, security, privacy, interoperability, and scalability. Various use cases can be created through diverse combinations of components.

In the academic field, researchers focus on the future development of Web 3.0. Various Web 3.0 architectures have been proposed, incorporating technologies such as AI, semantic technologies, cryptography, and edge computing. It has been argued that Web 3.0 cannot achieve comprehensive data

protection and enhanced performance by solely relying on blockchain technology. Web 3.0 architectures have been evolving into new frameworks that integrate emerging technologies beyond blockchain, necessitating support at each layer [27].

A comparison of these architectures is presented in Table II. Notably, most proposed architectures encompass a blockchain layer and adopt a hierarchical design based on blockchain and existing network architectures. However, Web 3.0 architectures not only require blockchain technology to support upper-layer application services but also necessitate the reformation of underlying infrastructure to ensure privacy and security in data transmission and identity management. Furthermore, the implementation and roles of emerging technologies (e.g., AI, 5G, 6G, edge computing, and privacy-preserving technologies) remain insufficiently defined.

As Web 3.0 and emerging technologies continue to develop, it is anticipated that more novel Web 3.0 architectures will emerge to meet the diverse needs of the Web 3.0 ecosystem. In this section, we propose an adaptable architecture, as illustrated in Fig.3. The foundational layers are divided into infrastructure layer, blockchain layer, and user interface layer. The infrastructure layer primarily manages computing, storage, and communication resources. The blockchain layer governs data interactions and value distribution. The user interface layer hosts the design and delivery of Web 3.0 applications to users. Additionally, three supplementary functionalities correspond to three primary areas where emerging technologies can enhance Web 3.0: zero trust, semantics, and AI. “Zero trust” aims to implement fine-grained access control, authentication, and authorization within Web 3.0, ensuring user sovereignty over identity and data while securing interactions [27]. “Semantics” aims to reduce information overload, minimize energy consumption, and foster efficient interactions toward a participatory economy by extracting semantic information from raw data and enabling its decentralized sharing [10], [11]. “AI” facilitates intelligent decision-making at the infrastructure layer, enhances security and privacy at the blockchain layer, and provides intelligent services at the application layer [15]. In the following sections, we elaborate on each layer and supplementary functionality of the proposed architecture.

A. Web 3.0 Architecture

1) **Infrastructure layer:** The infrastructure layer, comprising both overlay and underlay networks, serves as the foundation for other layers.

The underlay network comprises multiple physical infrastructures and foundational networking technologies. It focuses on the physical transportation of data packets between devices, offering essential infrastructure, storage, computing, and communication resources for overlay networks and higher-tier services. In the context of Web 3.0, which encompasses a wide range of access devices, network types, and communication standards, the underlay network plays a vital role in facilitating seamless integration and functioning within a diverse network environment.

Positioned above the underlay network, the peer-to-peer (P2P) overlay network provides foundational support for decentralized value transfer and information exchange within the

blockchain layer. The P2P networks utilize diverse topologies and search mechanisms, enabling efficient data sharing and communication among nodes in a fully decentralized manner.

Within the infrastructure layer, components such as edge servers, mobile operators, terminals, and various network elements can serve as blockchain nodes. These nodes can be organized by DAO to engage in the consensus process. With the support of the blockchain layer, the infrastructure layer is adept at facilitating zero-trust identity authentication and verification across network devices, in addition to achieving improved coordination for resource utilization, which is also referred to the term of decentralized physical infrastructure networks (DePINs). These components combine to build a secure, privacy-protected, low-latency, efficient, and cost-effective infrastructure layer for supporting various applications and services.

2) **Blockchain layer:** The blockchain layer, integral to Web 3.0, is designed to create a secure and trustworthy environment for interactions and collaborations among various entities. Eliminating the reliance on a trusted third party, blockchain layer is essential to provide proof of ownership for users’ identities and digital assets, which is realized by enabling the creation and tokenization of them. The innovative mechanisms for the tokenization, monetization, exchange, and peer-to-peer trading of data and digital assets protect users’ data value and redistribute value from the application layer to the protocol layer, fostering a structure characterized by “fat protocols and thin applications” [28].

Depending on the specific needs for read and write access control dictated by various scenarios, different blockchain architectures—private, consortium, and public blockchains—are strategically chosen to align with the varied requirements and objectives of users and organizations.

Given the scalability and interoperability challenges faced by blockchain technology, layer 1 scaling solutions are insufficient to meet increasing user demand. Distributed data storage and layer 2 solutions have been proposed to improve blockchain scalability and interoperability.

3) **User Interface layer:** In this layer, Web 3.0 provides users with front-end interfaces to access different services. These interfaces often utilize UI libraries such as React, Vue.js, and Angular, alongside blockchain interaction tools like ethers.js and Web3.js, to query information or initiate transactions.

Through identity management (as detailed in identity management of Section III) and wallet connection, users can get access to a broad spectrum of Web 3.0 applications, including NFTs, DeFi, DAOs, the Metaverse, social networks, and gaming platforms (as detailed in Section V). Among these applications, as digital ownership certificates, NFTs can be associated with various digital objects like photos, videos, and audio files, marking a shift towards a new paradigm of digital ownership and value exchange. The NFT market is diverse, with six primary categories: Art, Collectibles, Gaming, the Metaverse, Utility and other [29], each delineating a distinct application and value domain within the NFT ecosystem.

4) **Zero trust:** Zero trust is a security paradigm based on the principle of “never trust, always verify” [30], which

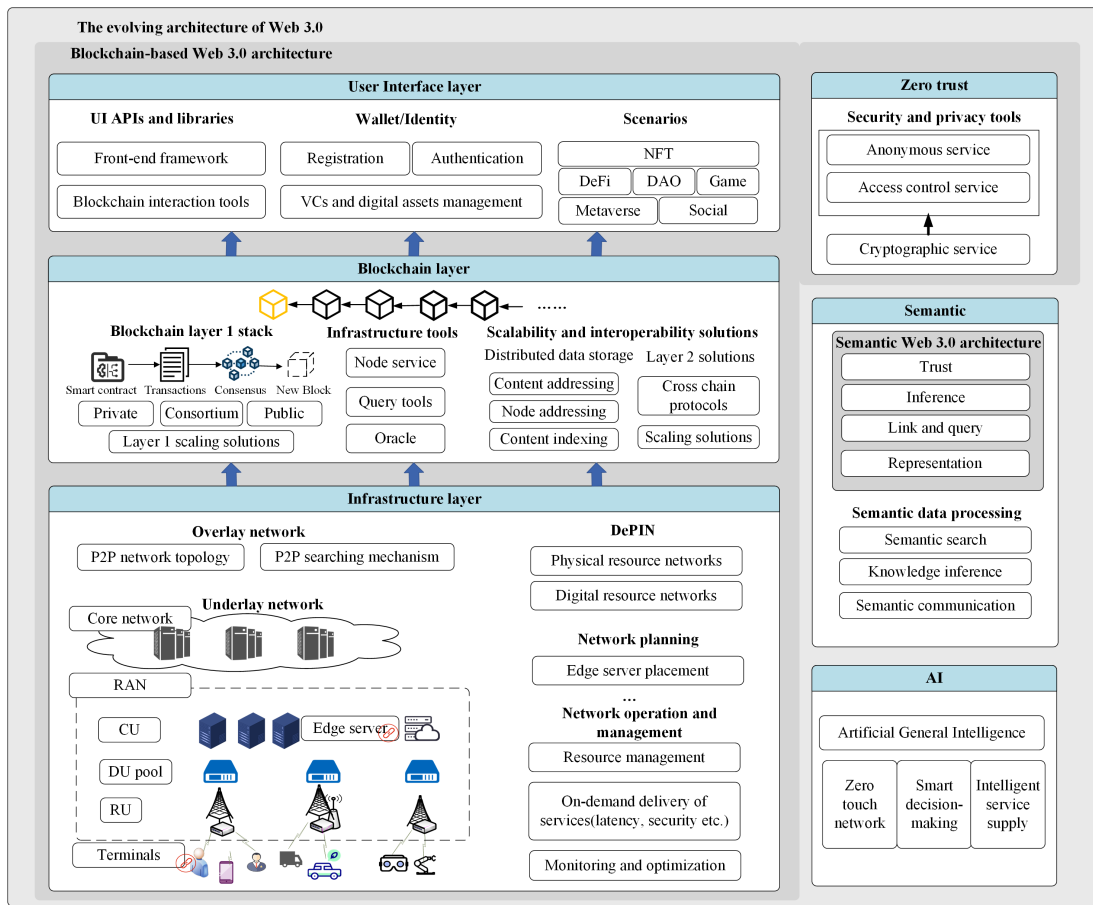


Fig. 3: The proposed Web 3.0 architecture

addresses privacy and security across communication, storage, computation and infrastructure. It enhances privacy by preventing data leaks during communication and processing activities and strengthens infrastructure security through automated detection of malicious behaviour and prompt authentication. The use of security and privacy tools such as cryptographic services supports dynamic, real-time access control and facilitates anonymous communication. Currently, quantum cryptography such as QKD is designed to distribute classical secret keys between two parties in a quantum ambient. With its quantum nature of detecting intrusions by measurement, a secure quantum channel can be built for data transmission and block propagation [31].

Since the prosperity of quantum computing technology subverts the conventional cryptosystems, existing digital signatures and hash functions within secrecy periods in the blockchain face the potential to be broken by enough processing power of quantum computing. To avoid threats, post-quantum cryptography has also been proposed [32].

While there are multiple vital issues in quantum computing and communication [33], quantum cryptography has been widely studied to improve Web 3.0 security. [34] proposed a novel quantum blockchain framework to drive Web 3.0 with information-theoretically security for decentralized data transferring and payment transactions. In that way, quantum computing can be applied in blockchain, infrastructure layers of Web 3.0 for secure identity authentication, consensus mech-

anism, block verification and propagation. It can also reform infrastructure layer for secure communication and intensive computational task as a security supplementary functionality.

Overall, this holistic implementation of the zero trust model significantly strengthens the security and privacy framework, addressing persistent challenges within Web 3.0.

5) **Semantic:** Since Web 3.0 emphasize the importance of data right and decentralized sharing, efficient data interaction is vital. Harnessing the power to derive insights from interconnected data and enhance communication across diverse data systems, semantics technologies play an important role in reducing information overload, minimizing energy consumption, and foster efficient interactions toward a participatory economy by extracting semantic information from raw data and enabling its decentralized sharing.

These semantic technologies utilize standards like XML [35], RDF [36], and Ontology, which underpin knowledge graph-based methods pivotal for applications in knowledge graphs, intelligent fault diagnosis [37], semantic similarity measurements, and knowledge-based semantic extraction in semantic communication [38]. These technologies facilitate semantic data processing through semantic search, knowledge inference, and semantic communication. Semantic search and knowledge inference boost Web 3.0's ability to retrieve relevant and accurate information. Meanwhile, semantic communication enhances efficient interactions within a shared knowledge environment in Web 3.0. It is worth noting that different

semantic data extraction methods such as machine learning other than knowledge-based semantic extraction method can be applied in semantic communication, while the encoded and decoded semantic information can interact with the blockchain layer through operations such as semantic verification, transfer, and storage [10], [11].

While semantic technologies enable interconnections between data, similar to other technologies that handle and process information, there are significant privacy and security considerations, along with relevant data policies—such as licensing terms and regulatory frameworks—that apply to both data and software assets [39]. The combination of semantic and blockchain signifies a transformative shift towards a decentralized, trustworthy, and interconnected web of information [9]. Some trustworthy technologies (as detailed in Section IV) such as cryptography and zero-knowledge proof have been used in semantic data interaction. For instance, in [40], the authors used multi-keyword ranked search over encrypted cloud data to preserve the privacy of semantic data. Integrated with blockchain, zero-knowledge proof has been used in [10] for semantic information transfer. Combining with zero-trust functionality, it is promising to support fine-grained access control for semantic functionality.

6) **AI:** Both Web 3.0 and AI play vital roles in complementing and enhancing each other. In recent years, the advent of Artificial General Intelligence (AGI) has witnessed significant progress in AI technologies. This evolution is exemplified by the rise of large language models (LLMs), which have propelled generative AI to the forefront of technological innovation. Web 3.0, on the other hand, is characterized by its decentralized, semantic, and interoperable design. It breaks down boundaries between domains [27], making data integration and sharing more seamless. The decentralized nature of Web 3.0, along with edge computing capabilities, enables more efficient resource allocation and intelligent network management. In this context, AI is poised to overcome resource limitations and data deficiency problems, evolving into Artificial Super Intelligence capable of performing tasks beyond human abilities. AI (as detailed in Section IV) is promising to act as a cognitive layer in Web 3.0 promoting semantic understanding between machines. This will boost Web 3.0 in efficient development, data analysis and security assistance [14].

Specifically, AI technologies such as generative AI can enhance Web 3.0 in the following aspects. Within the user interface layer, AI serves as a foundational tool for open-source development, fostering the integration of AI with various use cases to execute specific tasks. For instance, digital asset generation and circulation can be achieved with AI-generated content (AIGC) and digital twins technologies. Moreover, AI contributes to enhancing the scalability and security of the blockchain layer by monitoring and analyzing the vast amount of data generated. In the context of smart contracts, consensus mechanisms, and layer 1 scalability solutions, AI can support security vulnerabilities identification, dynamic decision-making processes, and improved performance. For the infrastructure layer, the existing human-centric model is insufficient to manage the complexity brought about by bil-

lions of users and devices. An intelligent, automated network based on the Zero Touch management model [41] is essential. Through real-time network monitoring, AI enables intelligent, real-time decision-making for malicious request detection, resource allocation, and task offloading.

B. Lessons Learned

In this section, we present a Web 3.0 architecture covering different focuses of Web 3.0. In this multi-layered architecture, with user ownership serving as its core vision, blockchain layer emerges as the core layer in Web 3.0, enabling the tokenization of data and cryptocurrency-promoted peer-to-peer trading. It plays a crucial role in supporting decentralized networks and promoting multi-party collaboration in the user interface and infrastructure layers. Enhanced by zero trust, semantic, and AI functionalities, Web 3.0 not only ensures the trustworthiness of data and identity throughout creation, transmission, and interaction but also improves decision-making efficiency and real-time performance across various applications.

However, various emerging technologies in the Web 3.0 architecture are currently immature. Most Web 3.0 applications rely exclusively on blockchain technology, which cannot guarantee full-process data security or support low-latency, computation-intensive applications.

III. WEB 3.0 FUNCTIONS AND WORKFLOW

This section offers an overview of the Web 3.0 service workflow and describes its core functions.

A. Overview of Web 3.0 Workflow

Compared to Web 2.0, Web 3.0 emphasizes data ownership, and separates the front and back-end with user data stored directly on the blockchain or outside of the blockchain. Unlike the platform-based data transfer in Web 2.0, a Web 3.0 application is merely a user interface built upon the combination of different infrastructure tools, and the creation, processing, and value transfer of user data are realized in the blockchain layer. This structure forms a “fat protocol and thin application” service model in the Web 3.0 ecosystem.

Some existing studies, such as those in [13], [42]–[44], have described the Web 3.0 workflow from a service perspective, highlighting user interactions through digital wallets² like Metamask to initiate transactions and query data via node providers and other tools. These workflows focus solely on a common use case of Web 3.0 services, spanning from the front-end to the blockchain platform, while neglecting the varied requirements of different applications and infrastructure-level networking.

This section, illustrated in Fig.4, delves into the workflow from the user interface layer to the infrastructure layer, addressing critical aspects such as data value, security, privacy,

²A digital wallet is a secure browser extension or software application that allows users to store and manage digital identifiers and verifiable credentials (VCs). In the context of Self-Sovereign Identity (SSI), digital wallets enable users to control and selectively disclose their identity information without relying on a centralized authority. They facilitate secure interactions with issuers and verifiers, supporting privacy-preserving features like zero-knowledge proofs.

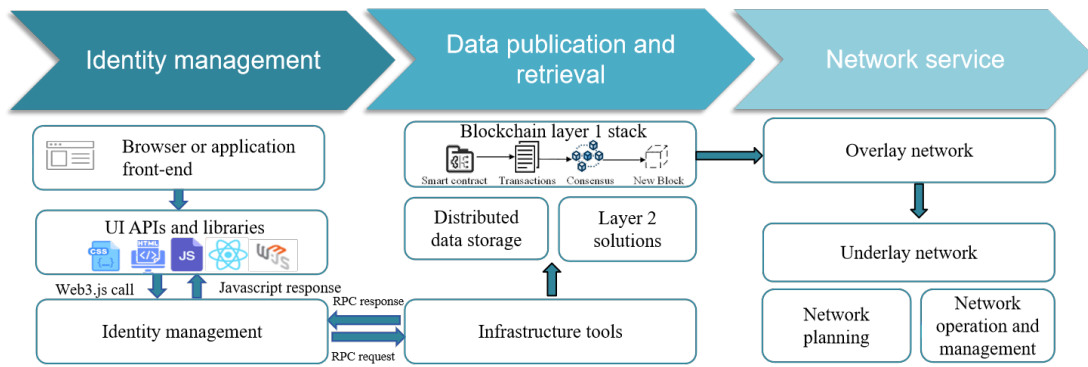


Fig. 4: A general workflow of Web 3.0 service

and open sharing. The literature suggests that Web 3.0 enhancements focus primarily on three functions: identity management [45], [46], data publication and retrieval [47]–[49], and network service [50]–[53]. Next, the detailed operation process of these functions will be summarized. Based on this process, various service development workflows and operational procedures can be formulated by combining different types of components. This approach ensures that specific application service requirements are met while maintaining secure and trusted data circulation.

B. Identity Management

In Web 3.0, the emphasis is on ensuring identity anonymity, trustworthiness, and interoperability across different applications. The aim is to provide users with a seamless experience while effectively safeguarding their privacy. The concept of Self-Sovereign Identity (SSI), which allows users to create and manage their identities, forms the foundation of data circulation and service delivery in Web 3.0. By integrating SSI with the zero trust principle and automatic authentication, Web 3.0 enables a non-perceptual and non-disturbing automated authentication process that enhances security.

Within the SSI framework, VC and Decentralized Identifier (DID) are two crucial components for standardizing user identities and establishing trust among user identities. W3C defines DID as a new type of identifier that facilitates a verifiable, decentralized digital identity, detailing specific technical mechanisms and formats [54]. VC is defined as a set of tamper-evident claims and metadata that cryptographically prove who issued it [55]. In recent years, blockchain, as a trustworthy technology, has become a widely accepted implementation platform for SSI by providing a trustless, decentralized database. With the aforementioned standards and technologies, the entities in the SSI-based identity management system (IDMS) solutions can interact with each other in a trustworthy environment [56], as shown in Fig. 5.

The generalized functions of an identity management system include account, authentication, authorization, and auditing (4A). These four functions form a framework or set of principles that facilitate identity authentication within a unified security management platform [57].

1) **Account:** Before getting access to Web 3.0 service, an account, which can be described as a digital identity mapping to the real identity, is needed to manage one's digital assets

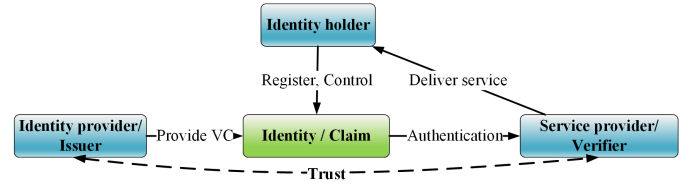


Fig. 5: Relationship of different entities in identity system

and keep track of one's activities. “Account” represents the functions of identity generation and registration.

In traditional blockchain systems, the public key refers to the account identifier and the private key serves as a cryptographic tool for controlling digital assets. However, the anonymity provided complicates creditworthiness assessment and information reliability. In Web 3.0, a trusted link between real and digital identities is essential. Various methods, such as using biometric data [45] and unique identification number (UIN) [58] for generating verifiable data, are proposed to ensure the authenticity and prevent fraud. Upon identity verification through a blockchain, which may involve checking additional credentials like VC, identities and VCs are encrypted and stored, with references on the blockchain for authentication. It is essential to note that Web 3.0 trust does not eliminate reliance on external actors entirely (e.g., trust in issuers), but it shifts the locus of trust to transparent, rule-bound processes where participants collectively enforce integrity through code and mathematics. For example, trust in zero-knowledge proofs should align with real-world trust anchors to reduce the trust cost. Specifically, the zero-knowledge proof issuer should maintain legal consistency with real trusted parties, such as governments, hospitals, or notary agencies. This system supports seamless integration of multiple identities across different applications, enhancing interoperability and establishing trust for subsequent authentications.

2) **Authentication:** Accessing a Web 3.0 service or initiating a transaction requires mutual authentication, closely linked to the “Account” function. Initially, users submit a signed message or identity proof to the service provider. Using cryptographic proofs such as digital signatures and privacy-preserving biometric protocols via a reliable platform like blockchain, service providers authenticate identities and credentials. Enhanced security is achieved through multifactor authentication, which combines multiple credentials to prevent unauthorized access even if one credential is compromised.

To ensure privacy protection and user anonymity, minimal disclosure of user information is paramount [59], [60]. Authentication may incorporate various privacy-preserving techniques, including smart contracts, zero-knowledge proof [61], public-key cryptography, threshold secret sharing [62], and biometric authentication [45], [63], among others. These measures are essential for safeguarding privacy while confirming user identities and credentials.

3) **Authorization:** Authorization is the process of determining the rights of a user or entity to perform a specific action within a system. Once authenticated, users in Web 3.0 can be authorized through access control models like Role-Based Access Control (RBAC) and others, which are adapted to its decentralized framework.

Within the Self-Sovereign Identity (SSI) system, DID and VC are crucial for the authorization process, with DIDs containing authorization policies and public key information for access request verification, and VCs serving as digital certificates that attest to specific attributes of the holder.

Moreover, Web 3.0 enhances security through encryption and digital signatures. Techniques like storing index sets in smart contracts for keyword searches of encrypted data and attribute-based access control via blockchain are implemented [48], [64]. Additionally, the Proxy Re-encryption (PRE) mechanism, facilitated by an authorized manager responsible for key distribution and data access management, is utilized [65]. Other solutions include distributing tokens or NFTs to grant specific rights to users [66], enhancing both security and operability within this decentralized ecosystem.

4) **Audit:** In Web 3.0, to prevent identity theft and ensure secure interactions, audit facilities must offer unbroken chains of evidence that trace the behavior of user identities within the network (as detailed in supervision and inspection of Section IV).

5) **Comparison of IDMS solutions:** Evolving from centralized identity to SSI, existing SSI literature can be divided into the following types based on different application scopes of identity system: communication network, Internet of Things (IoT), and healthcare. We reviewed some academic solutions and conducted a comparative summary of existing solutions regarding their application scopes.

In communication networks, advancements include a decentralized Radio Access Network (RAN) architecture proposed in [67], which integrates mobile network identifiers with blockchain addresses to eliminate dependence on Core Networks (CNs) for identification and authentication, significantly reducing latency and overheads. This approach has been extended in [46] to a three-tier identity management system that enhances mutual authentication from communication level [67] to service level and introduces flexible credential integration into user identities. To cope with the growing complexity of managing and orchestrating services in communication networks, based on blockchain-based SSI, researchers in [68] proposed a decentralized architecture to improve the involvement and integration of various entities such as Cloud Service Providers (CSPs), Vertical Service Providers (SPs), and Mobile Network Operators (MNOs).

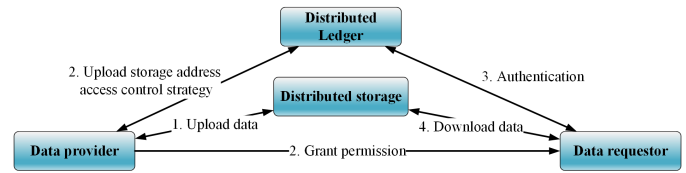


Fig. 6: Relationship of different entities in data publication and retrieval

In IoT, challenges like authentication delay and scalability are addressed through distributed identification management schemes such as those in [69], which utilize DID-chain and M-chain for efficient operation and management. Solutions also leverage smart contracts on platforms like Ethereum for registration and reputation evaluation [70], with various methods employed for generating unique DIDs [71]. Another notable development is the implementation of a decentralized SSI-enabled cloud storage model to streamline data collection and authentication in large-scale IoT systems [72], [73].

Healthcare applications focus on enhancing data privacy, access control, and system integration. Techniques such as Attribute-based Decentralized Access Control (ADAC) are implemented in smart contracts to manage Electronic Health Records (EHRs), using DIDs as unique identifiers and employing zero-knowledge proof (ZKP) for authentication without elaborating on broader application scenarios [74].

These developments illustrate the broadening scope of SSI applications, showcasing significant innovations in identity management across different sectors, enhancing security, privacy, and operational efficiency.

C. Data Publication and Retrieval

Web 3.0 highlights data ownership preventing the data monopoly in Web 2.0. Consequently, traditional centralized data storage methodologies are unsuitable for Web 3.0. Web 3.0's emphasis on security and scalability makes efficient data interaction and fine-grained, user-centric access control imperative.

Most research works apply new data publication and retrieval schemes relying on blockchain and distributed storage systems (as detailed in Section IV) for Web 3.0. A content-addressable mechanism is implemented in data searching and retrieval. Some works also introduce semantic technologies and AI, evolving Web 3.0 data management beyond traditional data storage to knowledge management. This evolution enables knowledge discovery and achieves more efficient data extraction and decision-making.

Containing data interaction entities including data providers (i.e., owners), data requestors (i.e., users), distributed ledgers, and distributed storage (i.e., storage providers), We discuss each steps shown in Fig. 6 respectively.

1) **Upload:** Before uploading data, after identity authentication, data is often encrypted on the client side to ensure that only authorized parties can access it. In Web 3.0, data is collected and stored within a decentralized data infrastructure. For instance, in a hybrid data storage approach, data is uploaded to distributed storage system such as InterPlanetary File System (IPFS), Arweave, or Sia. These systems return

the location of the data, like content ID (CID), to users and establish a storage agreement between the storage providers and the data owner through a smart contract, which defines the storage time, file size, and the cost that the user needs to pay. The access policies, storage addresses, search keywords, and metadata of the uploaded data can be recorded on a blockchain, providing a tamper-proof ledger of ownership and tracking the provenance of data.

2) **Download:** To ensure the integrity of the data stored by the storage provider, data storage audit mechanisms such as “Proof of Storage” can be used to prove that a certain node indeed provides a certain amount of data storage capacity to the network. This process begins when the client issues a challenge that can only be resolved by the provider if it possesses the actual data, thereby ensuring data integrity.

Following this, the system authenticates the requestor's identity, then verifies the requestor's permissions based on authorization mechanisms. If authorized by the data owner, data is decrypted on the client side according to the established access policy. During data retrieval, the result or a trusted data proof, such as ZKP, may be returned. In this process, data deliverers, or retrieval miners, are responsible for fulfilling retrieval requests. They locate and transmit the data stored across the network, with negotiated rewards dispensed upon the completion of data transfer. Seamless data retrieval is facilitated by data transfer protocols like BitSwap and Graphsync, while semantic technologies and AI enable more efficient knowledge retrieval.

3) **Comparison of data storage solutions:** We have reviewed several decentralized storage solutions in academic literature, focusing on their data storage schemes, audit mechanisms, and improvements made for enhancing scalability.

In terms of data storage scheme, considering privacy protection and security features, some encryption algorithms have been used to protect the confidentiality and integrity of stored data. In [48], [75], [76], the authors proposed efficient and secure data storage and sharing schemes using Attribute-Based Encryption (ABE) equipped with IPFS to flexible access control over encrypted data. Authors in [77] leveraged AES and RSA algorithms and hybrid storage system to protect firefighting IoT data storage and transmission. Mind Network [78] employ Fully Homomorphic Encryption (FHE) for zero-trust data transfer, allowing operations on encrypted data while preserving privacy.

Beyond these encryption schemes, to achieve secure data sharing and fine-grained access control of data, in some solutions [79], the data owner can give credential proofs to data requesters who are able to construct a non-interactive proof for their credentials. The blockchain nodes will verify credentials and accept the request only if the attached proof is valid. Combined with smart contracts, storage resources can be effectively allocated, and access permissions for data records can be stored through contracts to ensure dynamic access control [80].

Furthermore, blockchain supports data storage audits with various proof mechanisms to ensure data integrity and immutability. In [81], researchers conduct a comprehensive review of storage audit technologies, focusing on three critical

aspects encompassing storage integrity schemes, proof of data possession/retrievability, and proof of storage time and proof of replication.

It is observed that these advanced schemes in Web 3.0 data infrastructure allow users to store, retrieve, and maintain their data with security, privacy, immutability, and fine-grained access control. However, scalability remains a technical obstacle for Web 3.0 data infrastructure, which must have capacity and performance comparable to Web 2.0 [82]. In [49], the authors introduced a moving real-time service based on IPFS, where user requests are distributed across multiple clusters, each in different geographical regions and managed by a separate Kubernetes control plane. Upon receiving a content upload request, the controller encrypts and splits the content into segments for uploading to the IPFS network. Evaluations showed improvements in data throughput, service delay, and service interruption. Other research focused on modifying blockchain structures to improve search capabilities. Authors in [83] developed MapChain-D, a framework linking a data chain to an index chain for efficient data storage and retrieval. Another study [84] introduced MSTDB, a hybrid storage system that incorporates a Merkle Semantic Trie (MST) to reduce query times and facilitate semantic queries, including multi-keyword, range, Top-K, and cross-chain queries. These innovations aim to optimize the efficiency and functionality of Web 3.0 storage systems.

D. Network Service

Web 3.0 aims to offer reliable, intelligent, low-latency, and real-time network services for applications, emphasizing privacy and security throughout its framework. To ensure low-latency and high-reliability network services while safeguarding the privacy and security of user data throughout the entire process, Web 3.0 network service restructures the network architecture with decentralized network infrastructure and intelligent network management and planning.

1) **Decentralized network and infrastructure:** Web 3.0 emphasizes the decentralization of networks and infrastructure. By utilizing decentralized identity authentication, as demonstrated in identity management of this section, it is possible to further integrate network identities with digital identities. This approach subverts the traditional need for centralized authentication services to access networks, thereby reducing the communication overhead required for mutual authentication.

Moreover, network management and infrastructure management are also moving towards a decentralized manner. Through blockchain technology, trust is established among multiple parties, facilitating data integration and ensuring uniform decision-making. This is not limited to collaborations among operators. Individuals can also share physical facilities or digital resources through decentralized structures, as detailed in the DePIN application discussed in Section V.

2) **Intelligent network management and planning:** Based on the decentralized architecture, data integration and resource utilization can be significantly enhanced. With the rapid development of network services, intelligent technologies have been widely applied in network management and

planning to improve user experience, service quality. For example, from the perspective of network management, researchers in [53] use digital twins technology to virtualize and digitize networking for intelligent offloading decisions, ensuring low latency and high reliability in transmission. From the standpoint of network planning, researchers in [51] have developed a zero-trust model of edge server placement in the Internet of Vehicles (IoV) based on cloud-edge computing. This model incorporates Edge Server Placement (ESP) algorithms with anomaly detection using a non-cooperative game to minimize latency and maximize the coverage of base stations (BSs) with enhanced security.

However, the development of intelligent technologies also pose challenges on network security and data privacy. Currently, widely used network encryption protocols such as Internet Protocol Security (IPSec), Secure Sockets Layer (SSL)/Transport Layer Security (TLS), Quick UDP Internet Connections (QUIC) and anonymity mechanisms like the Onion Router (Tor) are not secure enough for dealing with privacy leakage problem since the introduction of machine learning and deep learning based encrypt traffic classification methods. In [85], the authors categorized it into three types: website fingerprinting (WF), application fingerprinting (AF), and user action identification. These types of traffic analysis aim to learn the websites being browsed, the applications being used, and the user's actions.

Although some defensive mechanisms such as WTF-PAD [86], Walkie-Talkie [87] have been used on Tor browser, defensive mechanisms for deep learning-based WF attacks still necessitate further research. A study proposed filter-assisted attack and augmentation-assisted attack to reduce the impact of noise on WF attacks [88]. They further proposed a list-based splitting defensive mechanism to defend against such attacks. In [89], the authors proposed a task involving the fine-grained packet-level classification within multi-tab Tor traffic named MTWFA-SEG, which appears to be a practical and formidable threat. With the rise of Web 3.0 applications, researchers have explored traffic analysis techniques to classify decentralized applications that share similar encryption settings on the same blockchain platforms [85]. A study extracted traffic interaction graph and utilized graph neural network (GNN) for application identification [90]. [91] achieved accurate and efficient classification of decentralized applications by applying transformer as classifier and using intra-flow and inter-flow features. Given the growing threats posed by machine learning and deep learning-based traffic fingerprinting attacks on privacy, it is crucial to further explore effective defensive mechanisms, such as traffic obfuscation strategies, to mitigate the impact of these advanced analysis techniques.

E. Lessons Learned

In this section, we present a Web 3.0 workflow along with its three critical functions: identity management, data publication and retrieval, and network service.

Diverse solutions have been adopted in these functions. Specifically, identity management utilizes DID, VC, ZKP, and biometrics within its 4A framework to reinforce privacy

protection and user control. Through the 4A functions, the data owner's ownership of application data in data publication and retrieval can be guaranteed in combination with different data storage and audit mechanisms. To ensure the quality of service, hybrid storage solutions that combine blockchain with distributed storage systems are being refined to ensure efficient data retrieval and support for real-time services. In network services, a more decentralized infrastructure is established, reducing authentication overheads, enhancing privacy, and promoting collaboration. By incorporating intelligent technologies into network planning and management, there is a potential to significantly enhance performance at the network service level.

In conclusion, identity management is integral to Web 3.0 services, adopting zero-trust strategies to secure data interactions and network services. Continuous enhancements in data and network management will solidify user control over data and improve support for real-time applications. The integration of these functions is transforming service delivery and network architecture into a new paradigm characterized by user control, trustworthiness, and enhanced performance.

IV. WEB 3.0 KEY TECHNOLOGIES

A. Trustworthy Technologies

By transitioning towards a decentralized internet, Web 3.0 is integrated with zero-trust strategies, ensuring dynamic and timely adjustment of access privileges for its applications. Key technologies such as distributed ledger technology, cryptography, zero-knowledge proofs, decentralized identities, and privacy computing are also integral to Web 3.0, enabling secure end-to-end data protection and trustworthy services.

1) *Zero Trust*: The traditional security model grants unrestricted access to network resources once a user, device, or application is authorized, assuming everything inside the network is trusted, which creates security risks by allowing cybercriminals to move freely if they breach the perimeter [124]. In contrast, zero trust (ZT), adhering to the principle of "never trust, always verify", lies a boundary-less security foundation for Web 3.0. The ZT technology has three critical pillars, i.e., access, authentication, and authorization. It enforces all access entities, such as user, data, infrastructure, and devices, to be continuously verified and evaluated based on several factors such as their identities, statuses, and environments. Based on the evaluation, it enables the principle of "least privilege", requiring all network actions and operations to be authenticated based on their intents, targets, and procedures, and authorized with limited operating time and space. The ZT concept was first proposed in 1994 [92] and known by Google BeyondCorp initiative [93]. In 2020, the national institute of standards and technology (NIST) of United States proposed a general ZT architecture [94], which further popularizes the application of ZT for a variety of scenarios in business and governments.

Recently, ZT applications have expanded beyond traditional IT frameworks to encompass Web 3.0 and metaverse. ZT can safeguard the access process in Web 3.0 environment [13], for example, providing fine-grained dynamic access control over critical network resources and managing cross-organizational

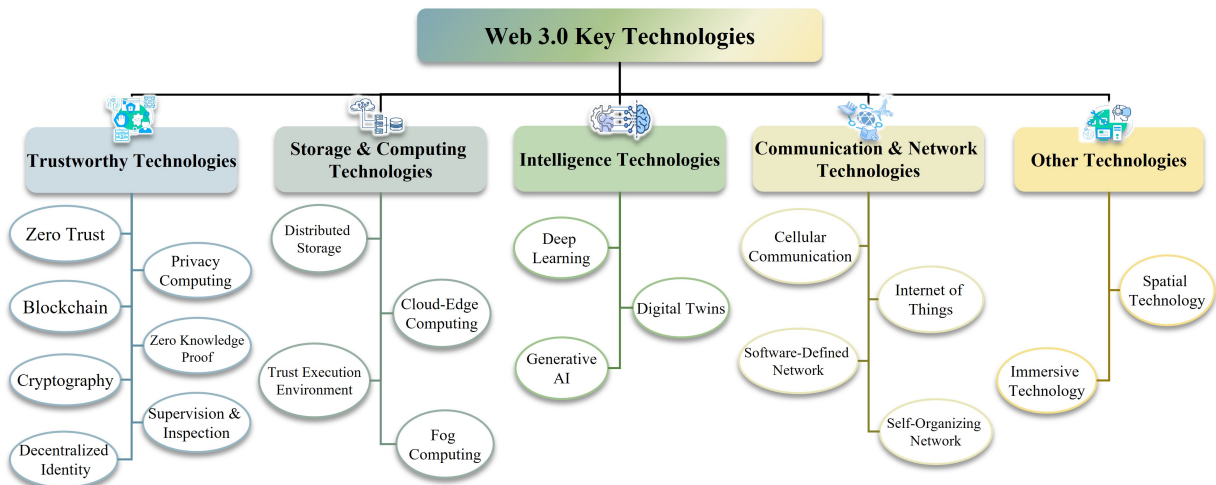


Fig. 7: Key Technologies of Web 3.0
TABLE III: Summary of Trustworthy Technologies

Technologies	Key Features	Potentials in Web 3.0	References
Zero trust	Never trust, always verify	Secure access, authentication and authorization process	[13], [92]–[96]
Blockchain	Decentralization, immutability, transparency, collective maintainence, and intelligent execution	Construct a decentralized, collectively maintained network structure	[97]–[110]
Cryptography	Confidentiality, integrity, and non-repudiation	Ensure data integrity and security during transmission and storage	[111]–[114]
Zero-knowledge proof	Prove a statement's truth without revealing its contents	Protect user privacy, data security and operation efficiency	[115]–[117]
Decentralized identity	Self-sovereignty, resistance to single points of failure	Efficient identity authentication and resistance to single point of failure	[43], [118], [119]
Supervision and inspection	Accountability and transparency	Strengthen the legitimacy of network operations	[120], [121]
Privacy computing	Encryption, multi-party computing, and differential privacy	Prevent privacy breaches during data processing and analysis	[52], [122], [123]

data access procedures [95]. ZT is also able to secure the authentication and authorization process in Web 3.0 [96] via sensitive detection of anomalous actions and entities, thus helping reduce the risks of network intrusion and implementing global proactive defense.

While ZT requires a much higher security level, deploying ZT in decentralized Web 3.0 brings difficulties in authentication and information sharing where traditional centralized authentication and information sharing is not applicable for ZT. For example, in the scenario of IoV, ZT faces the challenge of handover authentication because of the higher complexity and heterogeneity of IoV as well as high mobility of vehicles. To deal with it, in [125], the authors designs a hierarchical blockchain-assisted security information transfer and reputation management mechanism for reliable collaboration and efficient management in zero-trust IoV. To achieve efficiency and timeliness in information sharing, especially for time-sensitive IoT applications, [126] proposes a blockchain-based decentralized information sharing scheme in zero-trust IoT environments.

In the future, ZT will continue to serve as a critical security foundation for Web 3.0, providing strict, effective, and customizable security protections on network resources, user data, control operations, etc., and serving even more dynamic and challenging scenarios and applications.

2) *Blockchain*: Blockchain technology orchestrates encrypted records into a sequentially linked chain using cryptographic algorithms [127]. It embraces a number of characteristics such as decentralization, immutability, transparency, anonymity, collective maintainence, and intelligent execution [97]. Initially conceptualized by Bitcoin [98], the blockchain landscape has significantly evolved with developments by Ethereum [99] and Hyperledger [100]. These advancements showcase blockchain's adeptness in facilitating collaboration among entities within trust-less environments. In the Web 3.0 era, blockchain emerges as a cornerstone for a myriad of applications, enabling secure asset exchanges and trustworthy operations across critical sectors such as global finance (e.g. non-fungible token, decentralized finance), governmental affairs, healthcare systems, and communication infrastructures.

The fundamental blockchain components encompass consensus mechanisms and smart contracts. Consensus mechanisms are crucial for achieving agreement on status of ledger among all network participants. Smart contracts are designed to execute predefined digital operations in an enforceable and autonomous way, ensuring consistent results across multiple entities. In Web 3.0, blockchain can verify accuracy and consistency of digital content [101], [103], [128] and foster distributed trust in network environment [104], [105] via consensus mechanisms. Through smart contracts, blockchain can help perform Web 3.0 network operations efficiently, e.g.

TABLE IV: Comparison of Layer 1 and Layer 2 Blockchain Scalability Solutions

Solution	Type	Examples	Advantages	Limitations
Sharding	Layer 1	Ethereum 2.0 (Beacon Chain)	Increases throughput linearly; maintains decentralization.	Complex cross-shard communication; latency for cross-shard transactions.
Consensus Improvements	Layer 1	Ethereum 2.0 (PoS), Solana	Energy efficient; faster transaction speeds.	Validator centralization risks; potential impact on decentralization.
Block Size/Frequency	Layer 1	Bitcoin Cash, Solana	Simple to implement; directly increases throughput.	Larger blocks increase storage/bandwidth needs; centralization risks.
State Channels	Layer 2	Lightning Network, Raiden	Near-instant finality; low fees.	Limited use cases; requires participants to stay online.
Optimistic Rollups	Layer 2	Optimism	Reduces on-chain computation; secure via main chain.	Long withdrawal periods; fraud-proof reliance.
ZK-Rollups	Layer 2	zkSync	High scalability; fast finality; secure via main chain.	Computationally intensive; complex to implement.
Sidechains	Layer 2	Polygon, Ronin	Customizable; reduces main chain congestion.	Weaker security model; relies on sidechain consensus.
Plasma	Layer 2	OmiseGO	Scales by offloading to child chains; reduces main chain load.	Limited support for complex smart contracts; slower finality.

data sharing, task computing, and resource allocation [106]–[108].

Therefore, blockchain has become a promising approach to establish a decentralized architecture suited for next-generation network environments [109], [110]. In Web 3.0, blockchain promotes construction of decentralized network structure, ensures data reliability and operational efficiency. This technology plays an indispensable role in facilitating the transition from centralized framework of Web 2.0 to decentralized paradigm of Web 3.0.

Scalability remains one of the most critical challenges for blockchain systems, particularly in the context of Web 3.0 applications, which demand high throughput, low latency, and seamless interoperability. Current scalability solutions can be broadly categorized into Layer 1 (L1) and Layer 2 (L2) approaches. While both aim to address the scalability trilemma (balancing decentralization, scalability, and security), they do so through fundamentally different mechanisms. To provide a clearer understanding of the differences between the current main Layer 1 and Layer 2 solutions and their applicability to Web 3.0, we have summarized their key characteristics, advantages, limitations, and use cases in Table IV. This comparison aims to offer a concise overview for readers and serve as a reference for future research and development.

3) *Cryptography*: Cryptography facilitates algorithms, protocols, and systems to secure information and communications through the use of codes and ciphers, ensuring confidentiality, integrity, authentication, and non-repudiation in the presence of potential threats. It encompasses techniques such as symmetric and asymmetric encryption [111]. Symmetric encryption involves a scenario where both the sender (encryptor) and the receiver (decryptor) utilize the same key for encryption and decryption, respectively. Asymmetric encryption, on the other hand, relies on a pair of mathematically related but distinct keys: a public key for encryption and a private key for decryption. Additionally, a significant branch of cryptography involves one-way functions, such as hash functions, which transform input data (often an entire file) into fixed-length hash values. This transformation, designed to be unidirectional, is crucial for verifying data integrity and authenticity. These foundational elements are crucial to the infrastructure of modern cryptographic practices.

In Web 3.0, cryptography is crucial for ensuring data

integrity, adapting to the practical needs of the digital environment. With the evolution of Web 3.0, new encryption technologies have been developed by integrating and enhancing various algorithms to meet the specific security requirements during data transmission and storage [112]. As the number of devices and users grows, traditional encryption methods may not suffice for the communication quality and encryption efficiency required by resource-constrained users. This led to the development of lightweight encryption solutions, such as cost-effective dynamic key encryption algorithms [113]. Additionally, homomorphic encryption, particularly fully homomorphic encryption, represents a breakthrough in processing encrypted data without the need for decryption, thereby enhancing communication and computation efficiency [114].

Cryptography plays a pivotal role in protecting data privacy and serves as the cornerstone of information security, particularly in the decentralized and trustless Web 3.0 environment.

4) *Zero Knowledge Proof*: Zero-knowledge proof (ZKP), firstly introduced in 1987 [115], represents a methodology whereby a prover can demonstrate the truth of a statement to a verifier without disclosing any information beyond the statement's validity. This technique, for example, allows one to verify ownership of a message without revealing its contents. ZKP can be categorized into two primary types: interactive proofs, which involve multiple rounds of communication between the prover and the verifier, and non-interactive proofs, which simplify the verification process by enabling a proof to be produced once and verified by anyone.

In Web 3.0, ZKP offers a significant enhancement to online security through the preservation of user privacy and data integrity [116]. These proofs are pivotal in securing transactions by fostering a completely anonymous environment for all parties involved. Furthermore, when integrated with cryptographic techniques such as homomorphic encryption, ZKP facilitates the processing of encrypted data without the need for decryption, thereby mitigating the risk of data breaches and bolstering information security within Web 3.0 environments [117].

Looking ahead, ZKP occupies a leading position in protecting user privacy, data security and operation efficiency in a wide array of Web 3.0 applications.

5) *Decentralized Identity*: DID exhibits remarkable resistance to single points of failure and ensures efficient identity

authentication while diminishing reliance on central authorities and third-party services. Notably, DID-based verification processes do not require user information, which bolsters privacy and promotes a distributed approach to identity management [118]. Research efforts have explored the applications of DID to make identity management in Web 3.0 safe and reliable. Innovations such as the dynamic DID authorization process through smart contracts and DID-based privacy-preserving reputation protocols [119] illustrate the ongoing advancements in this field. Presently, corporations, including Microsoft, Baidu, and WeBank, have introduced DID solutions tailored for Web 3.0 [43], demonstrating the potential of DID to enhance the robustness and scalability of identity management systems.

DID is poised to become a cornerstone technology for identity management in Web 3.0. It promises to significantly propel network decentralization, enhance authentication efficacy, and protect the privacy and control rights of users.

6) *Supervision and Inspection*: Supervision and inspection refer to practices and mechanisms designed to monitor and evaluate the network activity, creating the audit trail of data processing and transmission. These methods possess the capability to accurately detect vulnerabilities or malicious activities and guarantee transparent, verifiable audit trails.

Supervision and inspection can not only establish an intact audit trail ledger, but also ensure transparency and security of digital behaviour records [120] in Web 3.0. Supervision and inspection can enhance security of network environment through timely interception of risky data and behaviors. Moreover, worked with blockchain, supervision and inspection mechanisms become even more potent within the Web 3.0 landscape. Blockchain augments the accountability of information and provides a tamper-proof audit trail [121], thereby bolstering the integrity of data.

By ensuring reliable and accountable audit trails of operations, supervision and inspection mechanisms strengthen the legitimacy of network operations, thereby securing Web 3.0 cybersecurity.

7) *Privacy Computing*: Privacy computing represents a collective of technologies designed to safeguard personal privacy during the stages of data processing and analysis [122]. It plays a pivotal role in reducing the risk of privacy breaches during frequent data exchanges, aligning with the stringent security demands of Web 3.0.

Privacy computing encompasses a suite of key elements such as encryption, multi-party computing, and differential privacy, which can provide secure data-computing schemes to maximize user control over sensitive data management. Privacy computing can safeguard against unauthorized access by encrypting the locations of nodes for data processing [52]. Also, multi-party computing can reduce data leakage risks through differential data storage and computing in multiple-level servers. Differential privacy introduces randomness into data processing, effectively preventing attackers from deducing individual information from aggregated data [123].

Consequently, privacy computing is posited as a formidable approach to solve conflict between data utility and privacy preservation under Web 3.0 environment.

B. Storage and Computing Technologies

Web 3.0 necessitates a secure, efficient data management system for compute-intensive applications that demand high reliability and low latency. Traditional storage and computing technologies often rely on centralized servers, which has hidden dangers, e.g. cybersecurity threats, privacy breaches, and high costs of document management [143]. To align with the vision of Web 3.0, storage and computing technologies should embrace properties of decentralization, privacy protection, immutability and cost-effectiveness. By providing enhanced security, data resilience, and higher availability, the integration of technologies such as distributed storage, cloud computing, edge/fog computing, and trusted execution environment with Web 3.0 is expected to better propel the Internet towards a decentralized, safer, and user-friendly future.

1) *Distributed Storage Technology*: Distributed storage is a foundational element of Web 3.0. It utilizes the collective resources of a node network to store and access data, ensuring data integrity and availability even in the cases of node failures or attacks. The inception of distributed storage was driven by the demand for scalable, secure, and resilient storage solutions.

Distributed storage systems comprise several key components, including storage nodes, consensus algorithms, and data replication mechanisms. Storage nodes are tasked with storing and serving data, while consensus algorithms guarantee that data is replicated and synchronized across nodes securely and consistently. Data replication mechanisms maintain data availability and reliability by storing multiple copies of data across various nodes. Distributed storage offers several key advantages for Web 3.0. It enhances data privacy and security by distributing data across multiple nodes. Data replication ensures system availability and reliability, even during node failures. These systems scale to accommodate growing data volumes and resist censorship, ensuring data accessibility and verifiability. Systems such as InterPlanetary File System utilize peer-to-peer network and incentive mechanisms for efficient, secure data storage and retrieval [129]. The emergence of cloud storage [130] and blockchain technology [52] collectively promote the decentralization of storage systems.

However, the widespread adoption of distributed nodes could introduce several security challenges, such as data tampering and unauthorized access [131]. As data is transmitted and synchronized across distributed nodes, attackers may intercept or tamper the data through man-in-the-middle attacks during transmissions. Additionally, the distribution of data across multiple nodes increases the attack surface. By targeting nodes with vulnerable access controls, attackers can potentially gain unauthorized access and compromise sensitive information. Advancements in areas such as zero trust, DID, and attribute-based encryption are expected to enhance the security and reliability [132] of distributed storage and accommodate the growing volume of data generated by Web 3.0 applications.

2) *Cloud Computing*: Cloud computing allows users to visit and utilize on-demand computing resources that are provided by remote servers or large data centers over the Internet. Mainstream cloud computing schemes include infrastructure

TABLE V: Summary of Storage and Computing Technologies

Technologies	Key Features	Potentials in Web 3.0	References
Distributed storage technology	Distributed, replicated and synchronized data across nodes	Provide scalable, reliable, and resilient data storage solutions	[52], [129]–[132]
Cloud computing	Resource pooling and virtualization, on-demand service	Enable resource-intensive, complex, and customized task processing	[133]–[135]
Edge/fog computing	Proximity to data source, low-latency, and scalability	Offer near-to-user, scalable and efficient data processing capabilities	[136]–[139]
Trusted execution environment	Isolated and confidential communication and execution	Guarantee chip-level, secure, and trustworthy operations and data storage	[140]–[142]

as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) [133].

Cloud computing, through distributed resources and virtualization, facilitates deployment of Web 3.0 application across multiple locations, reducing reliance on single data centers and improving data availability and processing [135]. Its elastic resource allocation enables infrastructure providers to efficiently manage resources for processing voluminous data in Web 3.0 [134], as well as to tailor solutions to accommodate smaller-scale requests. The convenience of accessing cloud services from any Internet-connected device promotes data sharing and user collaboration, and the fault tolerance and service-oriented architecture of cloud computing ensure its stable and efficient operation in Web 3.0.

Cloud computing is a powerful, flexible data processing method which provides distributed and cost-efficient solutions to meet the growing computing demands of Web 3.0.

3) *Edge/Fog Computing*: Edge computing is a pivotal computing paradigm that brings computation and data storage closer to the edge of the network, thereby offering real-time, adaptable, and scalable data processing capabilities proximate to users and devices [136]. Fog computing, an extension of edge computing, introduces an intermediary layer between cloud services and edge devices, enriching the computing landscape [137] [144]. Collectively, these computational paradigms supply expansive and distributed resources crucial for Web 3.0, significantly reducing latency, boosting network reliability, and expanding network capacities.

Compared to cloud computing, edge and fog computing processes data closer to users. This proximity not only reduces data transmission and offloading costs but also boosts transaction processing efficiency, lessens reliance on centralized data centers, and lowers the risk of data breaches [138]. These improvements enhance the reliability and resilience of the decentralized Web 3.0 ecosystem. Edge computing, by processing data at the network's edge, offers users enriched and real-time computing resources. For example, it provides immediate, customizable, and context-aware solutions for image processing and rendering, as well as rapid data analysis and cache acceleration. Concurrently, fog computing improves workload distribution across network nodes, easing the pressure on edge servers. Fog computing also enables the implementation of advanced access control measures on fog nodes, bolstering Web 3.0's data privacy and security protocols [139].

Fog and edge computing substantially protect the data privacy, security, and enhance user experience in Web 3.0. Their convergence heralds the advent of a more secure, efficient, and decentralized computing environment.

4) *Trusted Execution Environment*: Trusted execution environment (TEE) is a tamper-resistant processing environment running on a separated kernel. It guarantees the authenticity of the executed code, the integrity of the runtime states, and the confidentiality of its code, data and runtime states stored on a persistent memory [140]. In Web 3.0, TEE can ensure data security and privacy with trusted computing, providing users with a secure and reliable network environment.

TEE incorporates key designs such as safe isolation, secure boot, secure scheduling, inter-environment communication, remote certification, secure storage, and trusted I/O path. TEE provides a secure and trustworthy execution environment for Web 3.0 applications through hardware-level isolation. This isolation ensures that sensitive data will not be accessed or tampered with by unauthorized third parties when processed and stored. TEE provides reliable security for data privacy and meets the privacy protection requirements of Web 3.0. TEE can also ensure the integrity of data at startup through secure boot, and safeguards sensitive data and codes from malicious attackers or other applications through secure scheduling and inter-environment communication. Therefore, TEE can guarantee that critical parts of Web 3.0 applications (such as payment logic, authentication mechanisms, etc.) perform in the expected manner and prevent potential malicious tampering [141]. Furthermore, TEE provides a secure storage mechanism for storing critical data such as keys, certificates, and contract codes to prevent replay attacks and enforce state continuity, protecting the security and trust of Web 3.0 systems and applications [142].

The capabilities in protecting the confidentiality of sensitive operations and safeguarding user privacy makes TEE a key component in the Web 3.0 technology stack.

C. Intelligence Technology

In the evolving landscape of Web 3.0, research has broadened its focus from traditional concerns of storage and computation to place greater emphasis on extensive data analysis, nuanced feature extraction, and sophisticated user interaction. The advancement of intelligence technologies, including deep learning, generative artificial intelligence, and digital twins, is crucial to meeting these requirements. They promise to improve how we interact with digital content, augment the security of online environments, and bridge the gap between the physical and digital worlds in unprecedented ways, thereby enhancing interactivity, security and connectivity of Web 3.0.

1) *Deep Learning*: Deep learning (DL) employs artificial neural networks to analyze and learn from complex data patterns [145]. It plays a crucial role in incorporating smart

TABLE VI: Summary of Intelligence Technology

Technologies	Key Features	Potentials in Web 3.0	References
Deep learning	Automatic feature extraction and end-to-end, adaptive learning	Promote network traffic prediction, digital asset management, content review, and data processing	[145]–[152]
Generative artificial intelligence	Multimodal content understanding and generation	Enable convenient and personalized productivity tools	[153]–[155]
Digital twins	Realistic visualization, modeling and mirroring	Enable real-time, data-driven simulations and interactions	[156]–[158]

features and applications into Web 3.0. DL includes several types of implementation structures. Notable examples include deep neural networks (DNNs) [146], convolutional neural networks (CNNs) [147], and recurrent neural networks (RNNs) [148], each contributing uniquely to DL capabilities and applications. Among these structures, DNN provides the foundational architecture for learning hierarchical representations of data, while CNN excels in processing grid-like data such as images, and RNN is specialized for sequential data like text or time series. Additionally, deep reinforcement learning (DRL) combines DL principles with reinforcement learning, enabling machines to learn optimal behaviors through environmental interaction [149]. DRL stands out for its ability to make decisions in complex and uncertain environments, which makes DRL particularly useful in areas like autonomous vehicles and robotics, where adaptive and intelligent decision making is crucial.

In Web 3.0, DL can enhance network security by detecting potential network intrusions and predicting network behaviors [150]. DL can also generate digital assets for Web 3.0 and establish an efficient digital asset circulation system [151]. DL's contribution also extends to content ecosystem maintenance, where it supports content management systems in filtering inappropriate and false information. Moreover, DRL enables the optimization of data collection strategies in Web 3.0 decentralized storage systems, and can adaptively optimize the system's data throughput [152].

Looking ahead, DL's integration with Web 3.0 will promise more efficient, secure solutions for network prediction, digital asset management, content review, and data processing. This evolution will undoubtedly enable the handling of increasingly complex application scenarios in Web 3.0.

2) *Generative Artificial Intelligence*: Generative artificial intelligence (GAI), a cutting-edge domain within the broader AI landscape, stands out for its ability to autonomously generate novel, multimodal content, including text, images, and audio-video materials. GAI's potential for application spans a wide range, from revolutionizing content creation across various media to enabling more dynamic and personalized interactions within the burgeoning Web 3.0 networks [153].

The GAI field has significantly evolved, highlighted by launch of OpenAI's ChatGPT and the development of notable large language models, e.g., xAI's Grok-1, Meta's LLaMA 2, and Google's Gemini. GAI techniques can be categorized into creative and general techniques [154]. Creative techniques, including generative adversarial networks and diffusion models, excel in producing diverse content. General techniques, particularly the transformer model, revolutionize the natural language processing. These techniques collectively improve the efficiency and quality of content creation and distribution. Beyond content generation, GAI profoundly impact digital

assets and enrich data economy by analyzing comprehensive datasets to enhance information flow and add substantial value to data [155].

GAI serves as a pivotal force in accelerating the transition to Web 3.0, equipping us with reliable and convenient productivity tools. It opens up realms of business opportunities, fostering innovation and enabling the creation of new value in ways previously unimaginable.

3) *Digital Twins*: Digital twins (DTs) are digital replicas of real world physical component, product or equipment, which was first proposed in 2003. DT is founded on three main attributes, i.e., the real space, the virtual space, and the communication link between them [157]. The capability of DTs for dynamic sensing and intelligent decision-making serves as crucial technical foundations for engaging with the virtual world in Web 3.0 scenarios.

Recently, DTs have seen initial applications, e.g., data access management and smart manufacturing [156]. Digital twins are central to enabling intelligent decision-making through advanced simulations, thereby fostering Web 3.0 digital ecosystem which is both secure and efficient. DT revolutionizes the way to visualize designs, bringing them to life in stunning 3D. It allows for comprehensive testing and simulation within a virtual environment, outlining a vision for secure and efficient manufacturing process. Moreover, multiple DTs can be connected in a distributed and open way, thus mirroring large-scale and complex physical environments of Web 3.0 [158].

DTs will play a larger role in advanced simulation, real-time data mirroring, and decentralized decision-making, thereby enhancing interactivity, authenticity, and reliability across Web 3.0 digital platforms and services.

D. Communication and Network Technology

Web 3.0 use cases includes some high-fidelity ones like metaverse, rich mixed-reality experience which require reliable, low-latency and high-performance communication connectivity. 5G and promising 6G ensure pervasive connectivity with improved network efficiency and traffic capacity, providing reliable communication technical support for the use cases aforementioned [163]. Beyond communication technologies, there is a requirement that reshaping underlay network to a more decentralized and automated structure in consistent with user sovereignty and decentralization principle of Web 3.0 [46]. Applications of Internet of Things, software-defined networking and self-organizing network can facilitate this transformation of network structure and significantly enrich network functionality in Web 3.0.

1) *Cellular Communication*: Cellular communication, pivotal in connecting terminals and network devices through wireless channels, enables seamless connectivity while moving.

TABLE VII: Summary of Communication and Network Technology

Technologies	Key Features	Potentials in Web 3.0	References
Cellular communication	Extensive coverage, rapid transmission, and high-density connection	Enable pervasive and ultra-reliable wireless access and communications	[159]–[163]
Internet of things	Interconnectivity in the physical world, extensive information perception and processing	Enable physical information transmission, analysis, and sharing	[164], [165]
Software-defined networking	Programmable network controls, control and data plane separation	Provide flexible and manageable network solutions	[166]–[168]
Self-organizing network	Dynamic topologies, autonomous network management, and rapid deployment	Facilitate efficient and robust communication in complex environments	[169]–[171]

With evolution into the 5G and 6G era, cellular communication features the traits of extensive coverage, rapid transmission, and high-density connections [159], forming the backbone for pervasive and ultra-reliable wireless interaction in Web 3.0.

The application of 5G and 6G technologies marks a substantial increase in data rates compared to the prevalent 4G standards, catering to the escalating data demands and facilitating real-time interactions within the data-intensive digital sphere of Web 3.0 [160]. On the other hand, cellular communication will further enhance Web 3.0 applications on mobile devices, improving user experience. The expanded bandwidth of 5G and 6G can support multi-access and high-precision networked sensing services for terminal users in Web 3.0 [161], which aligns with the requirements of Web 3.0 interfaces and fostering the evolution of next-generation mobile devices and smart wearable devices [162]. As cellular communication offers a more user-friendly connection network [163], it can enhance user interaction for decentralized Web 3.0.

Cellular communication plays a crucial role in providing ubiquitous and high-quality connection, laying a open, secure, and efficient communication foundation for the construction and development of Web 3.0.

2) *Internet of Things*: Internet of things (IoT), comprising a network of interconnected sensors and objects, expands the boundary of Web 3.0 by providing real-world inputs to the digital world. Enabled by technologies like RFID tags, actuator nodes, and smart sensors [164], IoT facilitates an unprecedented scale of connectivity among physical objects, providing seamless information transmission, analysis, and sharing capabilities for Web 3.0.

As IoT evolves, it showcases enhanced diversity, intelligence, and security, aligning with the objectives of Web 3.0. User-friendly IoT architectures improve the customization and interoperability of services within the Web 3.0 ecosystem, allowing for interactions tailored to individual needs [164]. This adaptability plays a crucial role in addressing critical Web 3.0 requirements, such as security and privacy. Also, IoT utilizes sensors to realize automatic information perception, thus ensuring timeliness and improving utilization efficiency of data in the realm of Web 3.0. Furthermore, integrating blockchain and deep learning with IoT platforms facilitates secure data sharing and distributed storage [165], supporting real-time processing and analysis of IoT data at both the network's edge and the cloud. This integration reduces the overhead associated with data management and processing, streamlining operations within the Web 3.0 framework.

IoT can exploit the wealth of information from the physical world for enhanced information management and processing, paving the way for a Web 3.0 digital ecosystem characterized

by intelligent, secure interactions across a myriad of devices and platforms.

3) *Software-Defined Networking*: Software-Defined Networking (SDN) emerges as a transformative network architecture that enables direct programmability of network control, decoupled from packet forwarding [166]. This architectural innovation lends SDN exceptional adaptability, making it ideally suited to support the diverse, open, and dynamic application landscapes characteristic of the Web 3.0 ecosystem.

SDN architecture, comprising the infrastructure, controller, and application layers, uses APIs like Openflow for inter-layer communication, and separates control and data planes for agile network management. This separation boosts operational efficiency and adaptability, allowing for flexible network re-configuration and dynamic data path optimization to reduce latency [167]. SDN's streamlined API facilitates comprehensive network oversight, enabling establishment of attack detection frameworks against threats such as distributed denial of service (DDoS) attacks in Web 3.0 [168]. Additionally, SDN's integration with network feature virtualization (NFV) technology supports network slicing, which help resource optimization for varied business needs and service requirements in Web 3.0 environments.

SDN embraces specialized network management capabilities, such as flexible resource distribution and advanced security protocols, which can enhance the flexibility, security, and operational efficiency of networks within the Web 3.0 ecosystem.

4) *Self-Organizing Network*: Self-organizing networks (SON) are adept at self-configuration, optimization, and management, making them ideal for complex networking environments. They feature interconnected devices, rapid deployment, dynamic topologies, and robust management [169], facilitating scalable and flexible communication for heterogeneous networks in Web 3.0.

Research on SON includes vehicular ad-hoc networks (VANETs) and mobile ad-hoc networks (MANETs), with MANETs forming self-configuring networks of mobile devices connected wirelessly, and VANETs focusing on vehicle communication to improve traffic safety and reduce congestion [170]. SON's decentralized architecture enhances flexibility, making VANETs important in Web 3.0 for seamless vehicle information exchange and MANETs adaptable to changing conditions, ensuring resilient and efficient communication [171]. Moreover, integration with blockchain protects against security threats like data tampering and spoofing attacks, and incorporating swarm intelligence boosts spectral and energy efficiency.

Through its flexible network architectures, SON notably

TABLE VIII: Summary of Other Technologies

Technologies	Key Features	Potentials in Web 3.0	References
Spatial Technology	Collection and analysis of geographic data	Provide location-based services and satellite Internet coverage	[172], [173]
Immersive Technology	Real-time physical-digital interaction and multi-sensory engagement	Enrich user experience with interactive virtual environments	[174]–[176]

enhances the resilience of Web 3.0 networks by facilitating efficient, stable, and secure communication within complex and evolving environments.

E. Other Technologies

Beyond the technologies previously discussed, additional innovations are fortifying Web 3.0, enriching its capabilities and value. For instance, spatial technology provides precise 3D, wide area coverage and geolocation data, enhancing user experiences through precise, reliable spatial services. Immersive technology fosters lifelike and customizable services, improving user engagement. Together, these advancements are steering the development of Web 3.0 frameworks and applications towards a more open, interactive, and intelligent future.

1) *Spatial Technology*: Spatial technology, including geographic information systems (GIS), real-time location systems (RTLS), and satellite Internet, is key to acquiring, processing, and analyzing geospatial data, advancing Web 3.0's use of reliable and multidimensional spatial information [172].

In Web 3.0, broad and seamless spatial positioning coverage is essential. RTLS excels in real-time, precise object localization, benefiting healthcare, logistics, and manufacturing. Indoor positioning systems (IPS), using technologies like ultra-wideband (UWB), optical, and collaborative approaches [173], enable high-accuracy localization in enclosed spaces, supporting applications like communication systems. Satellite Internet frameworks, such as Starlink, OneWeb and StarNet, aim to provide global, high-speed Internet by deploying low earth orbit satellites, ensuring widespread access to Web 3.0 resources and services.

Spatial technology provides comprehensive and accurate spatial positioning capabilities, promoting seamless Internet coverage and accessibility in the Web 3.0 environment.

2) *Immersive Technology*: Immersive technology, including virtual reality (VR), augmented reality (AR) and mixed reality (MR), represents a transformative shift towards creating more engaging and interactive digital spaces [174]. Immersive technology marks a pivotal shift towards more experientially rich digital spaces.

Immersive technology, encompassing AR, VR, and MR, merges the digital with the real in unique ways. AR enhances real-world perception by overlaying virtual elements, VR immerses users in a virtual space, and MR combines both to allow interaction between real and virtual worlds. These technologies enrich user experience through advanced data visualization and sensory interfaces [175], fostering innovative interaction modes in Web 3.0. They enable creative socializing and collaboration, extending Web 3.0's reach to include phenomena like Web VR and VR communication [176], further deepening the interconnection between the physical and cyber worlds.

By simulating sensory experiences such as sight and hearing, immersive technology offers users the perception of being present in a virtual or augmented environment, thereby greatly enhancing user engagement and interactivity within Web 3.0. This technology promises a future of deeply immersive digital interactions in Web 3.0.

F. Lessons Learned

In this section, we show five pivotal technologies underpinning the evolution of Web 3.0, focusing on techniques that enhance trustworthiness, secure and efficient data storage and processing, intelligent services, multi-modal communications, and comprehensive network support. The discussed frameworks, mechanisms, algorithms, and underlying principles collectively address a number of concerns with regard to trust, security, scalability, and efficiency within Web 3.0.

Specifically, trustworthy technologies foster secure and confident interactions in Web 3.0, where trust is not a given. It ensures that data remains private and secure throughout its lifecycle. Storage and computing mechanisms significantly improve the efficiency and reliability of data management systems. Intelligent technologies address the complex challenges of analyzing vast amounts of data and securing networks, bridging the gap between the physical and digital realms in Web 3.0. Communication and network solutions provide secure, efficient, and adaptable foundations for a wide range of scenarios and applications. Furthermore, the development of Web 3.0 is also being driven by other emerging technologies, such as those offering spatial and immersive capabilities. Together, these technologies pave the way for a decentralized, intelligent, and autonomous Web 3.0 ecosystem, heralding a transformative era in digital interaction and service delivery.

Despite these potentials, key technologies of Web 3.0 also face a number of challenges. First, it is crucial to achieve a balance among decentralization, privacy protection, scalability, performance, and security, but this becomes particularly difficult in heterogeneous Web 3.0 environments. These environments often involve participants with varying trust demands and regulatory frameworks and thus require adaptive mechanisms to manage trust dynamically. Storage and computing technologies also encounter difficulties in ensuring data integrity and availability, especially under risks such as data retention and false replication. These challenges intensify with the need to process an exponentially growing volume of data while maintaining low operational costs. Meanwhile, intelligent technologies should enhance their capacity to efficiently handle increasingly diverse and unstructured datasets in Web 3.0. For real-time applications, there remains a pressing issue of achieving computational efficiency and accuracy under strict time constraints. Furthermore, the decentralized nature of Web 3.0 leads to variability in network performance. This complicates the design of communication and network

solutions to ensure consistent quality of service. In Web 3.0, minimizing latency and achieving seamless interoperability across decentralized, multi-party systems remain critical challenges for these technologies. In addition, spatial and immersive technologies present unique challenges in Web 3.0. Spatial technologies should address data accuracy, privacy, and scalability issues. Immersive technologies, on the other hand, require seamless integration with decentralized infrastructures to support shared and interoperable virtual environments. Finally, integrating these diverse technologies into a unified Web 3.0 ecosystem requires consistent efforts that include, for example, standardization, cross-platform compatibility, and data ethical considerations. It will be essential to address the aforementioned challenges properly to realize the full potential of these Web 3.0 technologies.

In summary, a substantial body of research recognizes the vital role of blockchain and AI within the Web 3.0 framework. These studies highlight the use of blockchain and AI in implementing essential Web 3.0 technologies, such as regulatory supervision, privacy computing, and distributed storage, as previously discussed. However, there remains a need for a more profound examination of the underlying principles and mechanisms of these technologies beyond mere implementation. Currently, there exists a significant research gap in this domain, offering a vast landscape for future investigation.

V. APPLICATIONS AND SERVICE USE CASES

Web 3.0 DApps have driven rapid evolution across a broad spectrum of scenarios. This section introduces several representatives of Web 3.0 applications and service use cases.

A. DePIN

DePIN, standing for Decentralized Physical Infrastructure Networks, is an emerging application field in the Web 3.0 industry. DePIN systems are built on blockchain as the secure and trustworthy data-recording system, with the Internet of Things (IoT) as the foundational hardware, and token economics as the incentive scheme. It encompasses a vast infrastructure network and economic system that includes wireless networks, energy, navigation maps, cloud storage, and other categories [177]. Compared to the traditional centralized physical infrastructure networks operated by enterprises, DePIN is identified by the following three characteristics:

- **Openness:** The decentralized infrastructure network constructed by DePIN allows anyone to join or exit, breaking down market barriers originally established by monopoly enterprises. This promotes free competitions and comprehensive developments within the industry.
- **Collective-Ownership:** DePIN are built on blockchain technology to create token-incentivized networks, where participants are economically rewarded for deploying and maintaining the physical infrastructures of the networks. This bottom-up approach ensures that the ownership of the network is decentralized among numerous participants, rather than controlled by a few shareholders or corporations.
- **Decentralization:** Decentralized networks, as opposed to traditional centralized infrastructure networks, offer

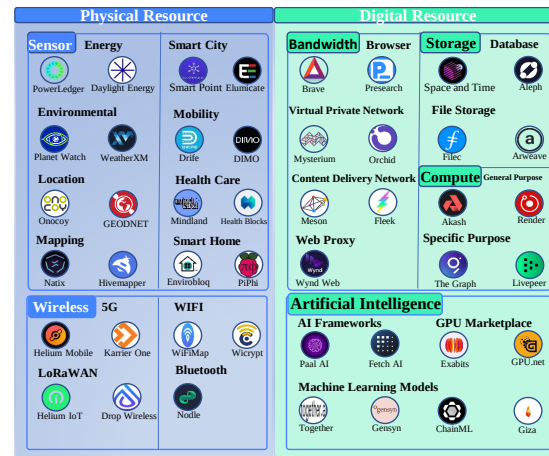


Fig. 8: The categories of the current DePIN systems.

greater robustness and security. The ownership of the network is distributed among numerous participants, making it more resistant to corruption, hijacking, and hacker attacks that often occur in centralized networks.

As shown in Fig. 8, DePIN systems can be roughly grouped into two major categories:

- 1) **Physical resource DePIN:** In these DePINs, the participants are incentivized to deploy physical devices in different geographic locations to provide unique and irreplaceable services that are related to the locations.
- 2) **Digital resource DePIN:** In these DePINs, the participants allocate their unused capacity of digital resources, such as bandwidth, storage, and computing power, to server other demanders.

The services provided by the physical resource DePIN can be mainly classified as sensor services and wireless services. DePIN create sensor services by utilizing the participant's deployed sensors to collect various real-world environmental data for other demanders. DePINs create wireless services by constructing decentralized wireless hotspots using the wireless networking devices deployed by the participants.

Services provided by digital resource DePIN can be classified mainly as bandwidth, storage, computing, and artificial intelligence services. The bandwidth services includes Browser, Virtual Private Network, Content Delivery Network, and Web Prox. The storage services include Database and File Storage. One well-known example of the File Storage network is Filecoin, where miners earn token incentives by storing files for users [178]. The computing services can be further divided into General Purpose Computing (such as Akash, which provides Computing Power to support many kinds of computation, i.e., AI, ML, and Web 3.0 applications [179]) and Specific Purpose Computing (such as Graph, which is dedicated to indexing and querying blockchain data [180]). The Artificial Intelligence services can be further classified into AI Frameworks that aid in the development and deployment of AI applications, Machine Learning Models that are pre-trained models deployed on the network for invocation, and GPU Marketplace in which users can rent idle GPUs and TPUs for computation.

In essence, DePIN signifies a transformative transition in the deployment and maintenance of physical infrastructure.

Despite the ability of DePIN to scale rapidly and its potential to disrupt large legacy industries, it currently faces several challenges. These challenges encompass the imperative need to ensure network scalability, uphold data privacy and security, and foster interoperability between DePIN networks. Conquering these obstacles is of paramount importance for the ascendance of DePIN as the preeminent paradigm for building and operating infrastructure in future large-scale applications.

B. NFT

Non-Fungible Tokens (NFTs) are distinct digital assets that serve as proof of ownership or authenticity for specific items or content, such as artwork, collectibles, virtual real estate, in-game items, and real-world assets. The implementation of NFTs typically relies on blockchain technology. NFTs can be classified into two main categories based on their blockchain implementations, with Ethereum and Bitcoin representing the respective types. Initially, NFTs emerged from smart contracts on the Ethereum blockchain, enabling developers to create NFTs that comply with proposals such as ERC-721 and ERC-1155 [181]. In contrast, the implementation of NFTs on the Bitcoin blockchain presented challenges due to its reliance on the script programming language. However, significant upgrades, such as Segregated Witness and Taproot [182], were completed on the Bitcoin Mainnet, addressing some programming issues and paving the way for a Bitcoin NFT ecosystem. Recently launched protocols such as ordinals [183] and atomicals [184] in 2023 have provided standardized approaches for implementing NFTs on Bitcoin, gaining substantial attention.

NFT solutions, fundamentally geared toward Web 3.0 decentralized applications, are expected to possess the following characteristics [185]:

- **Verifiability:** The metadata and ownership of NFTs can be publicly verified.
- **Transparent Execution:** The execution of NFT related activities, including minting, selling, and purchasing, are publicly visible.
- **Tamper-Resistance:** Once the metadata of NFT and the transactions of NFT have been confirmed onto blockchain, the corresponding records cannot be manipulated.
- **Availability:** Each NFT contains up-to-date user-friendly and clear ownership information.
- **Atomicity:** Each execution about NFTs must be completed in a consistent, isolated, and durable (ACID) atomic transaction.

NFTs can provide self-sovereignty for other Web 3.0 decentralized applications, such as Web 3.0 games. In Web 3.0 games, NFTs enable players to fully own in-game assets and collectibles and interact with these assets across different platforms, addressing the limitations of traditional games.

While NFTs offer unique advantages for Web 3.0 decentralized applications, they also have certain weaknesses that should be considered. Some of the technique weak points of NFTs are:

- **Scalability:** As NFTs gain popularity, the scalability of blockchain networks becomes a concern. The current implementations of Ethereum and Bitcoin face challenges

in handling high transaction volumes, resulting in increased fees and slower transaction times for NFT-related activities.

- **Interoperability:** NFTs are often built on specific blockchain platforms, which can limit their interoperability across different ecosystems. This lack of interoperability hinders the seamless transfer and usage of NFTs across multiple platforms or applications.
- **Standardization and Regulation:** The NFT ecosystem lacks standardized frameworks and regulations, which can lead to challenges in areas such as intellectual property rights, copyright infringement, and fraud prevention. The absence of clear guidelines and standards may hinder the broader adoption and trust in NFTs.
- **Market Volatility and Speculation:** The NFT market has witnessed significant volatility, with prices of NFTs fluctuating drastically. This volatility introduces risks for both creators and investors, as the value of NFTs can be highly speculative and subject to market sentiment.

It is important to acknowledge these weaknesses and address them through ongoing research to ensure the long-term sustainability and development of NFTs in the Web 3.0 world.

C. Social Networks

In Web 2.0, social networks are web-based services dominated by platforms such as Facebook, YouTube, and TikTok, which allow users to interact with the network rather than merely consuming its content. While Web 2.0 social networks provide convenience to users, they may also bring about several issues, including:

- **Data Silos:** Web 2.0 social network services are provided by centralized third-party entities that often collect significant amounts of user data, including personal profiles, interests, interactions, and behavior. This data can be exploited for commercial purposes, such as targeted advertising and sales, thereby exposing users to the risks of attacks and data breaches.
- **Information Leakage:** Insufficient security and data protection measures on the platforms can lead to the hacking or accidental disclosure of users' personal information, posing potential privacy and security concerns.
- **Filter Bubbles:** The platform's recommendation algorithms may exhibit biases, causing users to be trapped in information bubbles where they can only access a narrow range of information, lacking diversity and objective viewpoints.

Web 3.0 social networks aim to create an open and decentralized platform to address the drawbacks of Web 2.0 social networks [186]. As shown in Fig. 9, the protocol stack of Web 3.0 social networks can be divided into three layers: the application layer, the middle layer, and the underlying layer. In the application layer, Web 3.0 social network provides three different types of applications: many-to-many, one-to-one, and one-to-many. In the middle layer, along with the essential user-generated content, several decentralized features differentiate Web 3.0 social networks from Web 2.0 social networks. These include self-sovereign identity (SSI), virtual asset, financial system, and governance system. The

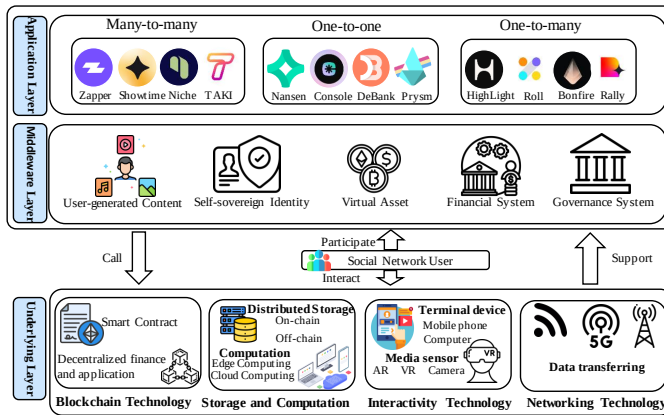


Fig. 9: The protocol stack of Web 3.0 social networks.

underlying layer consists of the foundational technologies and hardware that support the middle layer, such as blockchain technology, decentralized storage technology, edge and cloud computing technology, end-user devices, media sensors, and communication networks.

Based on smart contracts and decentralized storage technology, SSI can help users better control their digital identities and data [187]. Users possess the autonomy to decide whether to share their data with third parties, thereby reducing the risks associated with centralized platforms exerting control over user data and its potential misuse. Furthermore, Web 3.0 social networks prioritize user participation and governance. Through governance systems built on smart contracts and DAOs [188], users can participate in the decision-making and management processes of social networks, collectively determining platform rules and development directions. Transparent governance mechanisms enable users to comprehend how recommendation algorithms function, ensuring algorithm fairness and transparency, and permitting personalized settings to customize recommendations. This reduces the presence of algorithmic biases, enabling users to access a more diverse and objective range of information and avoid information bubbles. Additionally, Web 3.0 social network services incorporate AR and VR technologies into the hardware, providing users with a more immersive social experience [189].

Currently, one of the pressing challenges for Web 3.0 social networks is the decentralized storage of dynamic data. This capability is crucial for supporting applications such as streaming media and social media. Given the immutability of on-chain data, constructing social network applications directly atop this data layer is challenging. Protocols like Ceramic, Livepeer, Lit Protocol, and Tableland [190]–[193] are designed to address this issue. These protocols focus on managing and storing dynamic data such as images, videos, and text. Ceramic Network, for instance, aims to tackle this problem by providing a data layer on top of IPFS. It manages and tracks state transitions and associates data with data structures that facilitate easy read and write operations. Similarly, Tableland offers a technical solution to address the limited storage space in EVM smart contracts. It establishes a data layer that allows users to store, read, and write data in a more cost-effective manner compared to a pure EVM environment, providing more storage capacity. Once the challenge of decentralized storage

for dynamic data is resolved, Web 3.0 social networks will find widespread applications, offering users worldwide a more open, transparent, democratic, and inclusive experience.

D. DeFi

DeFi, an abbreviation for Decentralized Finance, refers to the peer-to-peer financial services provided on blockchains. DeFi offers services similar to traditional finance, such as lending, insurance, asset management, derivative trading, and asset exchange. However, as illustrated in Fig. 10, the core difference is that DeFi relies on decentralized technologies as the trust endorsements rather than centralized third-party institutions, which traditional finance relies on. Compared to traditional finance dependent on centralized third-party institutions, DeFi usually exhibits the following four characteristics [194]:

- **Non-custodial:** Participants have full control over their own funds at all times.
- **Permissionless:** Anyone can interact with the financial services without being subject to the intervention or censorship from a third-party.
- **Code Openness:** Anyone can audit the system's state.
- **Composability:** The financial services can be combined in arbitrary ways, allowing for the creation of new financial products and services.

DeFi services are typically provided in the form of decentralized applications (DApps). Various DApps can be developed on the blockchain through the creation and invocation of various smart contracts. To implement DeFi protocols effectively, smart contracts need to possess the following characteristics: i) sufficient expressive ability to encode protocol rules; ii) allow for conditional executions and bounded iterations; iii) enable communications between contexts through message calls (typically transactions) within the same execution; iv) support atomicity, meaning transactions either fully succeed (state is updated) or fully fail (state remains unchanged), preventing any execution from resulting in an invalid state.

DeFi projects can be categorized into lending, trading, payment, wallet, protocol interface, infrastructure, and data analysis types. Below are some examples of different types of DeFi projects. MakerDAO [195], launched in 2014 and built on Ethereum, is a DeFi project focused on lending functionality. It allows users to borrow digital assets pegged to the value of the US dollar by using certain tokens in Ethereum as collateral. Uniswap [196], a DeFi project for trading functionality, is a decentralized exchange built on Ethereum. Instead of using the traditional order book model, this exchange employs an automated market maker model, enabling users to swap tokens between different assets. Flexa [197], a payment-oriented project, offers a payment network for merchants to accept digital cryptocurrencies, mitigating fraud or volatility risks through off-chain collateralization. Other DeFi projects include Alpha Wallet, Lightning Network, Bamboo Relay, 0x Tracker, catering to wallet, protocol interface, infrastructure, and data analysis applications, respectively.

While DeFi introduces numerous benefits such as transparency, accessibility, and innovation, it also poses significant risks, particularly in the context of financial crimes like

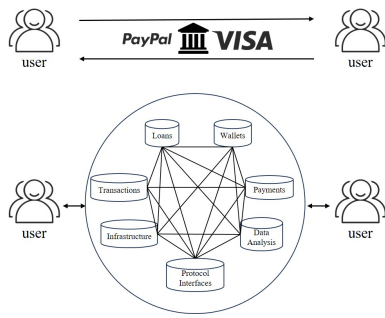


Fig. 10: The schematic diagram comparing traditional centralized finance and DeFi.

money laundering. Unlike traditional finance, DeFi operates on permissionless and pseudonymous blockchains, where users can interact with financial services without undergoing Know-Your-Customer (KYC) or Anti-Money Laundering (AML) checks. This lack of identity verification and oversight creates opportunities for malicious actors to exploit DeFi platforms for laundering illicit funds. For example, users can create multiple wallet addresses on different blockchains without revealing their real-world identities, and moreover DeFi protocols often facilitate cross-chain asset transfers, enabling users to obscure transaction trails by moving funds across multiple blockchains, making it challenging to trace the origin of funds. To address these risks, several regulatory and technological measures can be implemented to enhance the security and compliance of DeFi platforms:

- **Regulatory Measures:** i) **Mandatory Compliance Frameworks:** Governments and regulatory bodies could establish mandatory compliance frameworks for DeFi platforms, requiring them to integrate KYC/AML procedures while balancing user privacy. ii) **On-Chain Analytics:** Regulators can leverage blockchain analytics tools to monitor suspicious activities, identify patterns of money laundering, and trace illicit funds across DeFi protocols. iii) **Global Coordination:** Given the borderless nature of DeFi, international cooperation among regulators is essential to establish consistent standards and prevent jurisdictional arbitrage.
- **Technological Solutions:** i) **Decentralized Identity Solutions:** Integrating decentralized identity (DID) systems into DeFi platforms can enable privacy-preserving KYC processes, allowing users to prove their identities without exposing sensitive information. ii) **Smart Contract Auditing:** Regular audits of smart contracts can ensure that DeFi protocols do not include features that enable money laundering or other illicit activities. iii) **Transaction Monitoring Tools:** Advanced machine learning algorithms can be deployed to detect anomalous transaction patterns indicative of money laundering. iv) **Zero-Knowledge Proofs (ZKPs):** ZKPs can be used to verify compliance with KYC/AML regulations without revealing user identities, striking a balance between privacy and security.
- **Community and Ecosystem Initiatives:** i) **Self-Regulation:** DeFi communities can adopt self-regulatory practices, such as implementing voluntary KYC measures or flag-

ging suspicious activities. ii) **Educational Campaigns:** Educating users and developers about the risks of money laundering and the importance of compliance can foster a more secure DeFi ecosystem.

While DeFi holds the potential to revolutionize the financial industry, its permissionless and decentralized nature introduces unique challenges, particularly in combating money laundering. By adopting a combination of regulatory frameworks, technological innovations, and community-driven initiatives, the risks associated with illicit activities can be mitigated without undermining the core principles of decentralization and user autonomy. Future research should explore the balance between regulation and decentralization to ensure that DeFi remains a secure and inclusive financial ecosystem.

E. DAO

With the rapid emergence of the Web 3.0 concept, DAOs have flourished as a novel organizational form. The management and operational rules of such organizations are typically encoded on the blockchain in the form of smart contracts, allowing them to function autonomously without centralized entities or third-party interventions [198].

In 2016, Diedrich [199] proposed that people could encode the operational rules of organizations, enabling distributed, automated, and self-governed organizations on blockchain platforms like Ethereum. That same year, The DAO [200], a decentralized investment fund guided by a decentralized group of investors and secured by Ethereum, was launched as the world's first DAO project. The investors of The DAO, can hold tokens that grant them the rights to review, vote, and receive profit dividends from The DAO. Within the same year, Aragon introduced a set of DAO smart contract templates [201]. In 2017, Maker DAO launched a collateral-backed stablecoin called DAI, combining the low volatility of fiat currency with the decentralized nature of cryptocurrencies [195]. Perez Riaza [202] studied 122 cryptocurrency datasets and found that DAOs exhibited higher efficiency compared to other projects, serving as catalysts for improving market efficiency.

However, the development of DAOs still faces numerous challenges. In 2016, The DAO suffered a hack in its founding year, leading to a hard fork in Ethereum [203]. Additionally, research and analysis of 1,859 DAOs [204] revealed that most DAOs were inactive, primarily due to the high interaction costs. Simultaneously, the increase of token prices attracted a large number of speculators to DAOs, other than real participants and contributors to DAOs.

In recent years, the improvement of DAOs has generally followed the three directions illustrated in Fig. 11: the cost reduction, the speculation suppression, and the people-centric approach. Although smart contracts can automatically execute specified operations, the cost of invoking smart contracts is prohibitively high due to the throughput limitations of the current main blockchain platforms, preventing DAOs from autonomously executing a large volume of high-frequency organizational actions [205]. To address the issue of expensive execution costs, Q.org [206] and Metis [207] have developed Layer 2 solutions applicable to DAOs. Through mechanisms such as Snapshot [208], Aragon Govern [201], DAOs can

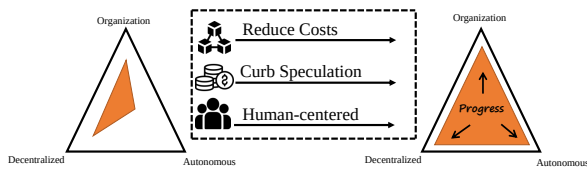


Fig. 11: The three directions on how to improve DAOs.

organize off-chain votes without consuming any transaction fees since the entire process does not require the initiation of any on-chain transactions. Furthermore, Giveth [209], SeeDAO [210], and HashKey [211] are attempting to create a new token theory that combines tokens, soulbound tokens (SBTs), and regular NFTs. By binding SBTs to individuals or organizations, the transferability of tokens and NFTs can be limited to discourage speculation. At the same time, linking reputation to SBTs can increase the transparency and accountability of organizations, as SBTs record an individual's or organization's reputation and contributions. The Polygon Foundation proposes that DAOs should draw inspiration from game design to create fairer and more reasonable incentive mechanisms and individual growth paths, fostering healthy DAO communities.

F. Games

The video games in the world of Web 3.0 are built on blockchain. Currently, there is no precise definition for Web 3.0's blockchain games, but they generally refer to games that store tokens (such as in-game items) in a distributed ledger on a cryptocurrency network [212]. These games incorporate concepts like NFTs and DAOs to design innovative game-play mechanics and provide new gaming experiences.

CryptoKitties, launched in 2017 [213], is considered the first blockchain game. Built on the Ethereum platform, it combines game-play with NFTs, allowing players to trade and breed virtual NFT cats for profit.

Following the success of CryptoKitties, Axie Infinity was introduced in 2018 [214] and has continued to expand the playability of blockchain games. Players collect NFT pets to participate in battles, earning tokens called SLP for feeding and breeding. Additionally, PvP battles, pet trading, and rare pet collection can also generate profits for players.

In recent years, with the increasing interest in blockchain games, more and more of them have been developed, covering a wide range of game genres. Pixels is an open-world Web 3.0 game launched in 2021, where players engage in farming activities by collecting various resources [215]. MATR1X is an innovative platform that combines culture, entertainment, Web 3.0, artificial intelligence (AI), and esports [216]. The MATR1X platform has released two highly anticipated games: MATR1X FIRE and MATR1X BATTLE, which offer classic first-person shooter (FPS) and battle royale gameplay, respectively. Other examples include Apeiron, which combines god simulation, roguelike, action role-playing (ARPG), and card game-play [217], and Wreck League, a mech combat game based on NFTs [218]. There's also Treeverse, an open-world MMORPG game [219].

These blockchain games record game assets using ERC-20 or NFT tokens and implement decentralized operations and management to some extent through DAOs. Play-to-Earn is

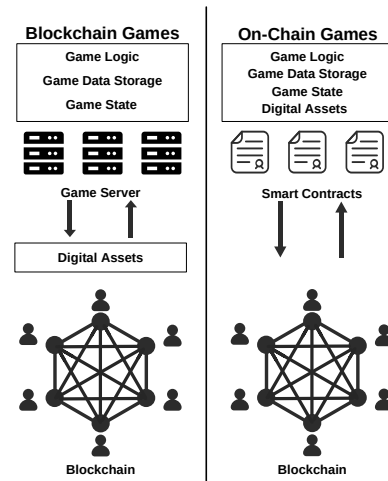


Fig. 12: The schematic diagram comparing blockchain games and on-chain games.

a prominent business model, where players can earn actual income by playing the games and trading in-game items.

As illustrated in Fig. 12, in these mentioned blockchain games, the blockchain is primarily used for recording digital assets, while fast-response features such as combat and movement are still implemented by traditional game servers; however, there is also another form of Web 3.0 games called fully on-chain games, where all game states and logic are executed on the blockchain. For example, Dark Forest is a fully on-chain MMO space conquest real-time strategy game based on the “dark forest” concept [220]. It utilizes on-chain technology and zk-SNARKs to achieve its unique game-play experience. Fully on-chain games are a relatively niche segment within the Web 3.0 ecosystem, but there are still community members, researchers, and developers actively exploring the boundaries of fully on-chain games.

G. Metaverse

Metaverse refers to an immersive virtual or digital universe where individuals embody an alternate self through emerging technologies such as augmented reality (AR) and virtual reality (VR), and interact with others within the virtual world [221]. In Metaverse, participants can interact, create, and own digital assets, as well as engage in various social, economic, and gaming activities. It is a concept that envisions a shared virtual space that transcends individual platforms and applications, allowing users to immerse themselves in a decentralized and interconnected digital realm.

Blockchain technology plays a crucial role in enabling the development of Metaverses by providing the necessary infrastructure for secure and transparent transactions, ownership verification, and decentralized governance. Metaverses built on blockchain ensure the integrity and immutability of digital assets, allowing users to have true ownership and control over their virtual possessions. NFTs, DAOs, and DeFi can fundamentally transform the virtual world of the Metaverse into a decentralized and democratic virtual society with its own economy and governance system [222]. For example, through the use of NFTs, blockchain-based metaverses enable the creation, trade, and ownership of unique digital assets, such

as virtual real estate, artwork, avatars, items, and more. The project of Sandbox [223] transitioned to be as a Web 3.0 Metaverse in 2020 by utilizing blockchain technology. In Sandbox, users can create various tools and NFTs on the user-generated content (UGC) platform provided by the project team and obtain ownership over their creations. Additionally, blockchain technology facilitates interoperability between different Metaverses and applications, enabling seamless transfer of assets and data across various platforms. This interoperability allows users to have a consistent experience and access their assets across multiple Metaverse environments.

The concept of Metaverse has gained significant attention and popularity in recent years, driven by the rise of virtual reality, augmented reality, and blockchain technology. It offers the potential for new forms of social interaction, immersive gaming experiences, virtual economies, and even opportunities for real-world integration. However, it is important to note that the development and realization of a fully-fledged Metaverse are still ongoing and require advancements in various technologies, including blockchain, virtual reality, artificial intelligence, and user experience design. The Metaverse represents an exciting frontier in the evolution of digital experiences, presenting possibilities for innovation, creativity, and new ways of interaction in the digital realm.

H. Challenges faced in Web 3.0 Applications

Currently, these emerging Web 3.0 applications have some common challenges that need to be addressed.

- **Scalability:** Many Web 3.0 applications face scalability challenges, especially when experiencing high transaction volumes. This can lead to network congestion, slower transaction times, and increased transaction fees, limiting the scalability and mass adoption of these applications.
- **User Experience:** The user experience of Web 3.0 applications can be complex and unfamiliar to traditional internet users. Issues such as wallet management, transaction confirmations, and interacting with smart contracts can create barriers to entry and hinder mainstream adoption.
- **Interoperability:** Achieving interoperability between different Web 3.0 applications and blockchain networks is still a challenge. Lack of standardization and compatibility can limit the seamless transfer of assets and data between different platforms, hindering the overall user experience and utility of Web 3.0 applications.
- **Security and Smart Contract Risks:** Web 3.0 applications are susceptible to security vulnerabilities, including smart contract bugs, hacks, and exploits. The irreversible nature of blockchain transactions can magnify the impact of these risks, leading to significant financial losses and reputational damage.
- **Regulatory Uncertainty:** The regulatory landscape surrounding Web 3.0 applications and cryptocurrencies is still evolving and varies across jurisdictions. This uncertainty can create compliance challenges and limit the growth and adoption of Web 3.0 applications, particularly in areas such as DeFi and tokenized assets.
- **Lack of Real-World Integration:** While Web 3.0 applications offer innovative solutions, their integration

with traditional systems and real-world use cases is still limited. Bridging the gap between Web 3.0 and existing infrastructures, regulations, and financial systems remains a challenge to achieve widespread adoption.

Addressing these challenges is crucial for the continued development and success of Web 3.0 applications. Solutions such as new smart contract virtual machines, blockchain sharding, new consensus mechanisms, layer 2 scaling, improved user interfaces, interoperability protocols, enhanced security auditing, regulatory clarity, and collaborations with traditional industries may overcome these challenges and unlock the full potential of Web 3.0 technologies.

VI. EVALUATION CRITERIA

This section presents a comprehensive evaluation of Web 3.0 based on Quality of Service (QoS), decentralization, security, scalability, and energy consumption.

A. Overview of Evaluation criteria

Nowadays, the Web 3.0 applications have covered a wide range of areas such as finance, gaming, and social media (as detailed in Section V). Establishing evaluation criteria for these applications is paramount for both users and developers. These criteria provide universal benchmarks to assess an application's performance, usability, and overall effectiveness [224]. Serving as metrics, they can empower users to adequately choose DApps that match their needs and guide developers in creating Web 3.0 technologies that fulfill their intended goals. However, specific characterizations of universally applicable evaluation criteria for Web 3.0 are rather challenging due to the following factors. Firstly, Web 3.0 is still in development, and the underlying frameworks are continuously evolving, rendering relevant performance metrics quickly outdated. Secondly, as the landscape of Web 3.0 is significantly diverse, the performance criteria of different applications built on various blockchains, protocols, and architectures vary significantly. For instance, the DeFi applications (see Section V-D) demand high transaction speed, while the blockchain-based decentralized social networks (see Section V-C) prioritize the needs of scalability and user experience.

In response to these challenges, we conduct a thorough literature review of academic papers and real-world applications of Web 3.0 [225]–[229]. Building upon this review, we introduce the key evaluation metrics for Web 3.0 that include QoS, decentralization, security, scalability, and energy consumption. These metrics enable us to quantify and evaluate the performance of Web 3.0 applications, platforms, and components such as consensus mechanisms.

B. Quality of Service (QoS)

In Web 3.0, QoS refers to the user experience of a network service. This includes factors such as availability, reliability, latency, and throughput.

1) **Availability:** Availability indicates the percentage of time that the network is operational and accessible to users [230]. Generally, high availability ensures a smooth user experience and minimizes disruptions, which is indispensable for the Web 3.0 applications that rely on consistent network access. Industry standards typically recommend annual uptime

of at least 99.999% (i.e., 5 nines availability) for most network applications [231]–[233]. For example, a decentralized storage network (DSN) such as IPFS [234] has an uptime of 99.999%, which equates to a maximum of 5 minutes and 26 seconds of annual downtime. This exemplifies the significance of availability for user access and data retrieval in DSN.

2) **Reliability**: Reliability is used to assess a network's consistency and fault tolerance in service delivery [235]. Consistent performance is a key aspect of reliability, as it guarantees uniform transaction speeds, latency, and overall performance across the Web 3.0 network. This provides users with reliable and predictable interactions, regardless of the volume of usage or time. In addition, fault tolerance is another crucial aspect of reliability. It ensures the network's overall service remains available even if individual components experience failures, such as hardware malfunctions or software bugs. Let us take IPFS for example that allows users to store data securely on a distributed network of computers instead of relying on centralized servers. The consistency of IPFS performance is specified as predictable average upload and download speeds to guarantee reliable data transfers with minimal fluctuations. Then, fault tolerance is further bolstered by IPFS's error correction mechanisms, such as replication verification and exchange [236]. These mechanisms proactively detect and recover corrupted data copies across the network, and thereby safeguards data integrity and prevents loss during potential node issues.

3) **Latency**: In the Web 3.0 applications, latency, defined as the time delay between action initialization and response reception over a network, significantly impacts user experience and responsiveness [237], [238]. Latency stems from two key factors:

- **Network Propagation Delay** refers to the time required for a transaction to travel across the network and reach all participating nodes. The delay fluctuation is attributed to factors like network congestion and geographical distances between nodes.
- **Validation and Consensus Delay** represents the time required for validators to verify a transaction's legitimacy and reach a consensus on its inclusion within the blockchain. This delay hinges on the complexity of the validation process and the underlying consensus mechanism (e.g., the delay of PoW is dramatically larger than PoS and Practical Byzantine Fault Tolerance (PBFT) [239] due to solving extremely complicated hash puzzles).

Apparently, high latency significantly degrades the user experience in the Web 3.0 applications [240]. Prolonged waiting time for transaction confirmation (e.g., minute-long delays for basic transactions) unavoidably results in user frustration and dissatisfaction, ultimately hindering the widespread use of the Web 3.0 applications.

Industry standards recommend a target latency of less than 100 milliseconds (ms) for real-time applications and less than 500ms for non-real-time applications. Specifically, real-time applications, such as online gaming, live auctions, and decentralized financial trading, necessitate prompt feedback and responsiveness for optimal performance. These applications

rely on near-instantaneous user interaction, and even a tiny delay (e.g., 100ms) can cause perceptible lags. The 100ms threshold is generally considered to be the limit of human perception, beyond which most users become aware of delays, diminishing the perceived real-time interaction. Non-real-time applications can tolerate higher latency without a critical impact on user experience. Nevertheless, exceeding 500ms may negatively affect user experience, particularly in scenarios involving frequent interactions (e.g., social networks).

4) **Throughput**: Throughput, as a key aspect of QoS in Web 3.0, refers to the rate of successful data transfer or transaction processing achieved within a network over a specific timeframe. Essentially, it quantifies the volume of data processed or the number of transactions completed per unit time, typically measured in transactions per second (TPS).

The throughput of Web 3.0 is influenced by the following factors. Firstly, larger transactions require more processing power and storage space on the blockchain, which results in lower throughput. Similarly, network congestion arises when many users attempt transactions simultaneously, leading to slower processing time and reduced throughput. Secondly, the usage of the distributed consensus mechanism imposes a significant impact on the throughput. In particular, traditional PoW relies on intensive hash computations. This limits the number of transactions processed per block and hinders overall throughput. Conversely, some PoS variants (e.g., [241]–[243]) prioritize efficiency in order to offer higher throughput. Lastly, the underlying blockchain architecture also affects throughput. For example, block size, validation process, and network infrastructure contribute to the overall throughput capacity.

Low throughput in Web 3.0 presents two significant challenges that negatively impact user experience (UX): limited scalability and network congestion [244], [245]. Insufficient throughput limits the network's capacity to handle growing user demand and transaction volume. This, in turn, inhibits application growth and scalability. During periods of high usage for the Web 3.0 applications, exceeding the network's throughput capacity can result in network congestion. This can disrupt network stability, potentially cause transaction failures, and even degrade UX.

With the reference to [246], we list the throughput of mainstream Web 3.0 applications in Table IX.

C. Decentralization

Decentralization distributes control and decision-making from a central authority (e.g., individual, organization, or group) to a network of participants. This reduces the reliance on trust between participants and discourages any single entity from manipulating the network [247]. Despite widespread claims of decentralization, many Web 3.0 projects exhibit substantial discrepancies in how control is distributed, how transparency is implemented, and how participation opportunities are offered. Evaluating these aspects is crucial to understanding the nuances of decentralization and ensuring that projects adhere to their decentralized design principles.

To evaluate the degree of decentralization in the Web 3.0 projects, we take into account various factors, including permissionless participation, transparency, governance model,

TABLE IX: Estimated Throughput Thresholds for Various Application Types

Application Type	Estimated Throughput Threshold (TPS)	Rationale
Voting systems	10-100	Security and transparency are paramount, with moderate transaction speed needs.
Internet of Things applications	10-100	May involve frequent sensor data updates, but might not require high individual transaction speed.
Supply chain management	100-500	Requires reliable data tracking and record-keeping, with moderate transaction speed demands.
Social Applications	100-500	Users do not require immediate confirmation for most actions. Focuses on information sharing and community building.
Decentralized Storage	500-1,000	While fast data retrieval is desirable, immediate confirmation might not be crucial for every storage operation.
Exchange Applications	1,000-5,000	Faster transaction processing is crucial during periods of high trading activity.
Decentralized Finance Applications	2,000-10,000	Users expect fast and efficient execution of financial transactions.
Gaming Applications	5,000+	Requires near-instantaneous transaction processing for smooth and responsive gameplay.

consensus mechanism, network scale, Gini coefficient, and Nakamoto coefficient.

1) **Permissionless participation:** The Web 3.0 applications are characterized by permissionless participation, which signifies an open and accessible environment [248]. In other words, individuals can join and contribute without needing approval from a central authority. This fosters a level playing field by providing equal opportunities for all participants, governed by established protocols and rules.

By lowering entry barriers, permissionless participation empowers individuals with Internet access to contribute their skills and ideas. Such behavior fosters innovation and contributes to a more diverse and robust ecosystem.

2) **Transparency:** In Web 3.0, transparency ensures the openness and accessibility of information within decentralized networks and applications. In particular, in a decentralized environment without any centralized coordination, mutual trust among distributed nodes becomes paramount [249]. Transparency assessment of Web 3.0 includes the following critical criteria. Firstly, data visualization tools and user-friendly interfaces are provided for effective data representation. Secondly, comprehensive and user-friendly tutorials should be readily available to facilitate fundamental understanding of the network's operations. Lastly, the public availability of the project's codebase as open-source software allows users to directly review and verify the code's functionality.

3) **Governance model:** DApps in Web 3.0 rely on governance models to define the structure, processes, and protocols for collaborative project management and control. Effective governance models are essential for promoting collective decision-making to align community interests, ensure fairness and transparency, promote a sustainable ecosystem, and mitigate potential risks [250]. The governance models of Web 3.0 primarily fall into three categories: on-chain, off-chain, and hybrid.

- **On-chain governance** embeds proposal and voting mechanisms directly within the blockchain. Voting rights, tied to token ownership, ensure alignment with token holder incentives [251].
- **Off-chain governance** relies on external platforms such as forums, chat applications, or dedicated applications for discussions and voting [252]. This approach encourages

broader community participation but may raise concerns about data security and vote manipulation.

- **Hybrid governance** combines elements of both on-chain and off-chain models, potentially offering enhanced flexibility and security [253], [254].

4) **Consensus Mechanisms:** In Web 3.0, the decentralization of consensus mechanisms determines the distribution of transaction verification and network state agreement among participants. Generally, a larger number of independent nodes and a more equal distribution of power lead to higher decentralization. Consensus mechanisms can be further categorized based on the level of decentralization: highly decentralized, moderately decentralized, and partially decentralized.

- **Highly decentralized** consensus mechanisms involve a large number of active participants, which strengthens the network's robustness and resistance to censorship. Examples include PoW blockchains like Bitcoin, wherein miners compete to solve cryptographic puzzles to validate transactions. Other mechanisms in this category include PoS [255] and Proof of Age [256].
- **Moderately decentralized** consensus mechanisms involve a smaller group of participants rather than highly decentralized ones. However, these participants are not pre-selected or given special privileges. Examples include Directed Acyclic Graph (DAG) [257], variations of Byzantine Fault Tolerance (BFT) [239], [258], and Delegated Proof of Stake (DPoS).
- **Partially decentralized** consensus mechanisms involve a limited number of participants, that require permission or hold special privileges. These systems offer faster transaction processing but raise concerns about censorship and control due to the limited number of validators. Examples include Proof of Authority [259], Proof of Activity [260], and Federated Byzantine Agreement [261].

5) **Network scale:** A larger network scale, measured by the number of independent nodes participating in a blockchain network, is the indicator of greater decentralization. This wider distribution of power across the network reduces the potential influence of any individual actor (e.g., a user or a corporation). Furthermore, inherent redundancy of a large and distributed node enhances network resilience. This ensures that

the network remains functional even if some nodes become compromised or unavailable. Additionally, a larger and more diverse node scale renders successful network attacks more challenging. This is due to the fact that malicious nodes need to compromise a significant portion of nodes to disrupt operations.

From [262]–[265], we analyze the number of nodes for popular blockchain networks on March 1, 2024. Bitcoin maintains the largest network with 18,224 nodes, while Ethereum operates 7,106 nodes. Other blockchain networks demonstrate varying levels of decentralization: Binance Smart Chain, Dash, Litecoin, and Dogecoin comprise 1,506, 2,989, 898, and 622 nodes, respectively.

6) Gini coefficient: The Gini coefficient is a widely recognized metric to measure income inequality. It offers valuable insights into resource distribution within Web 3.0 networks [266]. The coefficient ranges from 0 (i.e., perfect equality) to 1 (i.e., perfect inequality) and can be used to analyze token distribution, voting power, and mining or staking rewards. For example, a high Gini coefficient in token distribution indicates that a small number of entities hold a large share of tokens. This ownership concentration can centralize power and decision-making within the network, potentially undermining the decentralization of the Web 3.0 networks. Similarly, voting rights in many Web 3.0 projects are linked to token ownership. A skewed token distribution can result in voting power imbalances, which can further hinder the degree of decentralization. The Gini coefficients of Bitcoin, Ethereum under PoW, and Ethereum under PoS are 0.6538, 0.8298, and 0.8457, respectively [225], [267].

While the Gini coefficient sheds light on token distribution, it exhibits limitations as a measure of decentralization in blockchains. It overlooks other critical aspects, such as node distribution, decision-making processes, and control over the infrastructure. Furthermore, the Gini coefficient fails to capture the full spectrum of power dynamics within a network. Even projects with balanced token distribution can be susceptible to centralization if certain actors hold undue influence or control resources. Moreover, its applicability is limited in Web 3.0 projects without native tokens or where token ownership does not directly translate to voting rights. To address these shortcomings, the Nakamoto coefficient has been proposed as a more comprehensive measure of blockchain decentralization.

7) Nakamoto coefficient: The Nakamoto coefficient, named in honor of Bitcoin's creator, is a metric used to evaluate the level of decentralization within a blockchain network [268]. More precisely, the Nakamoto coefficient quantifies the minimum number of colluding entities (e.g., nodes, miners, or validators) required to compromise a critical resource within a decentralized network. This critical resource could be computing power, stake, or any other factors essential for network security. In simpler terms, a higher Nakamoto coefficient signifies that more entities are required to control a majority of the network's resources, indicating a higher degree of decentralization.

The Nakamoto coefficient can be mathematically defined for a subsystem s with K participants. Each participant wields a certain proportion (i.e., p_i) of control over the

subsystem, where p_i represents the relative influence or stake each participant holds within the subsystem. The coefficient of this subsystem (i.e., N_s represented by the sum of their proportions) is then calculated as the minimum number of participants whose aggregated control exceeds 51%:

$$N_s := \min \left\{ k \in [1, \dots, K] : \sum_{i=1}^k p_i \geq 0.51 \right\}.$$

The Nakamoto coefficients of Bitcoin, Ethereum under PoW, and Ethereum under PoS are 5,401, 285, and 275, respectively [225].

D. Security

Web 3.0's emphasis on decentralization and trustworthiness reduces dependence on centralized authorities through the distributed architecture of the blockchain. However, this distributed architecture introduces a significant challenge [269]–[271], i.e., heightened vulnerability to malicious nodes without robust security measures. Furthermore, the financial nature of Web 3.0, where users hold and transact cryptocurrencies and digital assets, amplifies the impact of security breaches.

Smart contracts, immutable programs deployed on the blockchain, define the core functionalities and business logic of Web 3.0 applications. They automate tasks, manage user interactions, and ensure transparent execution of operations within the application. However, these contracts can be susceptible to permanent exploitation due to vulnerabilities (e.g., reentrancy attacks [272] and integer overflow errors [273]). Such vulnerabilities can lead to stolen funds or manipulated systems. Furthermore, inadequate security exposes Web 3.0 platforms to Sybil attacks [274], where malicious nodes create fake identities to gain undue influence. For instance, Certik's 2023 Web 3.0 Security Report [275] documented 751 successful attacks on Web 3.0 projects, resulting in over \$1.84 billion in losses.

1) Account security level: In contrast to traditional username-password accounts, the Web 3.0 accounts rely on cryptographic private keys. These keys safeguard access to user funds and assets stored on the blockchain. If compromised, evildoers can steal the user's cryptocurrency holdings or manipulate their digital assets. Unlike Web 2.0, Web 3.0 lacks a central authority to recover lost funds or reset accounts. Therefore, the responsibility for secure private key storage falls entirely on the user.

The authors of [276] propose two dimensions for evaluating the security level of Web 3.0 accounts: multi-factor authentication and recovery options. Firstly, multi-factor authentication refers to additional verification methods required during account recovery, such as verification codes or biometrics. Secondly, recovery options represent the number of independent channels available for account retrieval, with a minimum of two recommended to avoid single points of failure. Table X details the established security levels based on the two dimensions.

2) Consensus security: Web 3.0 security hinges on the robust consensus mechanisms employed by blockchain. These mechanisms ensure that all participating nodes agree on the validity of transactions and the current state of the distributed

TABLE X: Web 3.0 Account Security Levels

Level	Factor Authentication	Recovery Paths	Explanation
0	0	0	Irrecoverable
1	1	0	No additional validation beyond the mnemonic phrase.
2	1	1	Only one factor needs to be verified during recovery.
3	1	2	During recovery, multiple factors must be verified simultaneously.
4	2+	1	Each recovery path requires verification of one factor.
5	2+	2	Each recovery path requires simultaneous verification of multiple factors.

ledger. Without secure consensus mechanisms, blockchains become vulnerable to manipulation, such as double-spending attacks [277]. This vulnerability inevitably imposes a negative impact on Web 3.0 and potentially compromises the security of DApps.

Today, prevalent consensus mechanisms in Web 3.0 include PoW, PoS, and PBFT. Each mechanism offers unique security characteristics along with inherent trade-offs.

- **PoW** secures the Web 3.0 networks by making it computationally expensive to engage in malicious activities like double-spending attacks and Sybil attacks. This high computational cost discourages such attempts but comes at the expense of limited scalability and significant energy consumption. Additionally, PoW remains susceptible to 51% attacks, where a malicious actor gains control over a majority of the mining hash rate, potentially manipulating the network [278].
- **PoS** presents a more scalable and energy-efficient alternative to PoW. PoS secures the network by requiring validators to have a stake in the cryptocurrency. This stake incentivizes validators to act honestly, preventing double-spending and Sybil attacks. However, PoS introduces new security challenges. A major concern is the “nothing-at-stake” problem [279], where validators with minimal stake might have less incentive to rigorously validate transactions. Another concern is the potential susceptibility of PoS to collusion attacks [280], where a large group of validators could conspire to manipulate the network if they collude.
- **PBFT** addresses a specific class of failures in distributed systems known as Byzantine faults. These faults manifest as unpredictable and potentially malicious behavior from nodes. Specifically, PBFT can tolerate up to f Byzantine failures in a network with N validator nodes, where $f = \frac{N-1}{3}$. This tolerance renders PBFT particularly suitable for permissioned networks with a limited number of known and trusted validators.

E. Scalability

Web 3.0 scalability refers to the capacity of a network or application to adapt to a growing number of users, transactions, and data, while maintaining performance and security [281]. Without scalability, the Web 3.0 networks would struggle to accommodate the increasing number of users, transactions, and

TABLE XI: Scalability Comparison of Consensus Mechanisms in Web 3.0

Consensus Mechanism	TPS	Scalability	Project Examples
PoW	5-7	Limited	Bitcoin (BTC), Litecoin (LTC)
PoS	100-1000	Moderate	Ethereum 2.0 (ETH), Cardano (ADA), Polkadot (DOT)
DPoS	1000-10000	Moderate	EOS (EOS), Tron (TRX)
BFT	1000-10000	The scalability is impacted by the number of validators.	Hyperledger Fabric, Solana (SOL)
DAG	Potentially millions of TPS	High	IOTA (MIOTA), Hedera Hashgraph (HBAR)

data, which significantly result in slow transactions and high fees.

In this subsection, we focus on three primary factors that influence Web 3.0 scalability: throughput, block size, and confirmation time.

1) **Throughput**: Throughput, as mentioned in Section VI-B, refers to the number of transactions that a blockchain network can process per unit of time. Here, we explore the impact of consensus mechanisms on throughput in Web 3.0.

As established earlier, consensus mechanisms ensure agreement among network participants on transaction validity and the ledger state. Firstly, PoW relies on miners solving computationally intensive cryptographic puzzles to validate transactions. This process leads to a slow transaction processing rate and limited throughput due to its high computational demands. Secondly, PoS utilizes validators who stake cryptocurrency to secure the network. Validation is based on factors like stake size and randomness. This leads to increased throughput compared to PoW blockchains. Third, PBFT achieves consensus through communication between validators, which can enable significantly higher throughput compared with PoW or PoS. However, as the scale of the blockchain network scale expands, the communication overhead among distributed nodes increases exponentially. This makes PBFT unaffordable for large-scale the Web 3.0 networks. Lastly, DAG-based consensus mechanisms [282] allow for parallel processing of transactions, potentially enabling very high throughput.

From the performance analysis from [264], [283], Table XI presents a comparative overview of the scalability potential of leading consensus mechanisms in Web 3.0.

2) **Block size**: Within Web 3.0, the block size is the maximum amount of data that a block can hold. These blocks act as containers for storing transaction details and other relevant information. The size of the blocks directly impacts the scalability of the blockchain network.

Ideally, enlarging the block size theoretically has the potential to improve scalability, due to faster transaction confirmation and a better user experience [284], followed by significant drawbacks in terms of increased storage requirements, slower validation and propagation, and extended validation times. Firstly, larger block sizes require more storage space and

computing power, making it more difficult for individual nodes to store the entire blockchain. Additionally, larger blocks take longer to validate and propagate throughout the network, making them more susceptible to certain attacks such as reorganization attacks [285]. Finally, validators take longer to process transactions because they need to handle the increased data volume within larger blocks.

Different blockchains have adopted varying strategies for block size management. Bitcoin, for instance, currently employs a fixed block size for the sake of security and decentralization. In spite of simplicity, the choice of the invariant block size is suboptimal as the transaction volume grows [286]. On the other hand, Ethereum dynamically adjusts the block size according to network conditions. This dynamic offers the potential for improved scalability by accommodating fluctuations in transaction volume. However, the dynamic strategy introduces additional complexity in terms of network congestion control and governance.

With data sourced from [264], we analyze the average block sizes of popular blockchains from March 1, 2024, to March 31, 2024. The block sizes of Bitcoin, Ethereum, Litecoin, Dogecoin, and Dash are 1744.55 KB, 113.50 KB, 237.90 KB, 175.58 KB, and 17.11 KB, respectively.

3) **Confirmation time:** In Web 3.0, confirmation time refers to the duration required for a transaction to be irreversibly recorded on the blockchain network. Specifically, within a blockchain network, the journey of a transaction begins when it is submitted by a user. The transaction is then propagated, or broadcast, to other nodes on the network. Then, validators verify the transaction's validity and include it within a block. Once the block containing the transaction is added to the blockchain ledger, the transaction is considered confirmed.

The number of confirmations required to finalize a transaction varies over different blockchains. Generally, more confirmations enhance transaction security. With each confirmation (i.e., an additional block added to the blockchain), the computational effort required to successfully reverse the transaction increases exponentially. This significantly diminishes the likelihood of a successful rollback attack [287].

Several factors affect confirmation time in blockchain networks: network traffic, block size, and the consensus mechanism employed. Heavy network congestion significantly extends confirmation time due to increased competition for limited block space. Conversely, larger block sizes can potentially accelerate transaction confirmation time by including more transactions per block. Additionally, different consensus mechanisms lead to varying confirmation times. For example, PoW blockchains, with their computationally intensive mining processes, typically exhibit slower confirmation times than PoS blockchains, which have faster validation mechanisms.

We present the confirmation and irreversibility time of popular blockchains, based on data from [264] in Table XII.

F. Energy consumption

1) **Sustainability:** The sustainability of Web 3.0 requires a comprehensive approach that goes beyond simply reducing energy consumption. It necessitates a holistic evaluation of Web 3.0 technologies' environmental, social, and economic

TABLE XII: Comparison of Confirmation Time and Irreversibility Time in Popular Blockchains

Blockchains	Consensus	Confirmation Time (Average)	Irreversibility Time
Bitcoin	PoW	10 minutes	6 confirmations (1 hour)
Ethereum	PoS	12 seconds	20 confirmations (4-6 minutes)
Binance Smart Chain	PoS	3 seconds	25 confirmations (1-2 minutes)
Avalanche	PoS	2 seconds	12 confirmations (24 seconds)

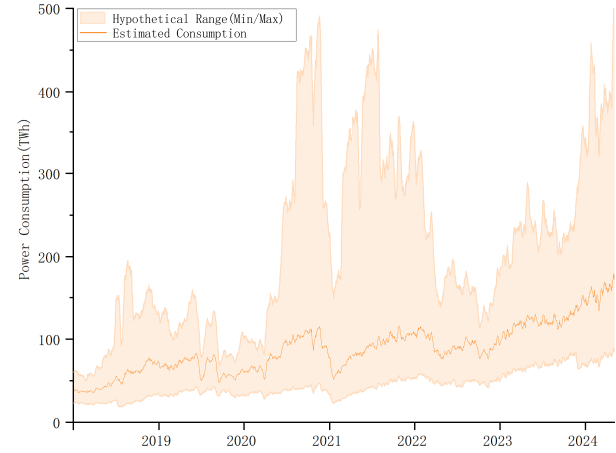


Fig. 13: Historical annualised electricity consumption

impacts (ESG). As Web 3.0 rapidly expands, its responsibility to operate sustainably becomes paramount. This translates to minimizing environmental damage and mitigating its contribution to climate change [288]. Sustainable practices are not merely environmentally friendly but are critical for Web 3.0's long-term viability [289].

According to [290], the energy consumption and carbon footprints per transaction for Bitcoin, Ethereum, and Visa as of July 2021 differ significantly. Bitcoin transactions have the highest environmental footprint at 844.13 kg of CO₂ and 1,777.11 kWh of energy per transaction. Ethereum follows with 59.55 kg CO₂ and 125.36 kWh, while Visa transactions are just 0.00045 kg CO₂ and 0.0015 kWh each.

2) **Cambridge Bitcoin Electricity Consumption Index (CBEI):** Developed by the University of Cambridge [291], CBEI estimates the daily energy consumption of the Bitcoin network. This index leverages hash rate data and incorporates factors like mining difficulty, geographical distribution of miners, and hardware assumptions to calculate energy consumption. These insights offer valuable information about the environmental impact of Bitcoin mining. Fig.13 illustrates Bitcoin's power consumption from 2019 to 2024 according to the CBEI.

G. Others

1) **Privacy:** Web 3.0's core principles of user empowerment enable anonymous interaction with DApps for basic functionality [52], [292]. However, additional verification may be required for specific purposes. This approach grants users fine-grained control (i.e., meaning very detailed control) over the data they share with DApps and with whom they share it. DApps themselves are designed to collect and store only

the minimal data necessary for their functionalities, thus minimizing privacy exposure and potential risks. Furthermore, DApps must clearly disclose their data collection, usage, and storage practices. Finally, user-friendly guidance on managing privacy settings empowers users to make informed choices about their data.

2) **Interoperability:** Interoperability is a foundational aspect of Web 3.0 that enables seamless communication and data exchange across blockchain networks, applications, and protocols. Generally, three key metrics can be utilized to assess its effectiveness [143], [293]–[295]. The first metric assesses support for cross-chain communication standards like the Inter-Blockchain Communication (IBC) protocol and tokenization standards like ERC-20 and ERC-721. These standards facilitate asset and data transfer between different blockchains. The second metric to assess interoperability is whether DApps leverage standardized data formats like JSON-RPC and RESTful APIs for communication. Using standardized data format enables seamless data exchange and integration between the Web 3.0 services. Finally, an assessment of cross-platform user identity management capabilities is crucial. This involves support for decentralized identity protocols like Decentralized Identity Foundation (DIF) and authentication mechanisms like Open Authorization (OAuth) and allows user verification and authentication across different networks and applications.

3) **Transaction fees:** Transaction fees are charges paid to validators for processing and validating transactions on a blockchain network. Users pay these fees when interacting with the blockchain, such as sending cryptocurrency or using DApps. High transaction fees can make Web 3.0 applications too expensive for everyday use. The evaluation of transaction fees helps users to assess the cost-effectiveness of using the Web 3.0 applications. Transaction fees are influenced by multiple factors, including network demand, transaction complexity, and the consensus mechanism. Firstly, as demand for network transactions increases, transaction fees tend to rise due to competition among many users for limited block space. This results in transactions with higher transaction fees being more likely to be included in the block. Additionally, complex transactions, such as those involving smart contracts, often pay higher fees due to their computational requirements. Finally, PoW-based blockchains typically have higher fees compared to those using PoS consensus mechanisms. Overall, based on their needs, users can choose the blockchain with the most suitable transaction fees.

Based on [264], we analyze transaction fees across popular blockchains on March 1, 2024. Bitcoin fees typically range from \$2–\$10 on average but can exceed \$50 during peak demand. Similarly, Ethereum fees range from \$5–\$50, occasionally spiking above \$200. Comparatively, other blockchains such as Litecoin (\$0.10–\$1), Solana (\$0.01–\$0.10), and Cardano (\$0.10–\$0.50) offer significantly lower fees.

H. Lessons Learned

A multi-faceted evaluation through the lens of QoS, decentralization, security, scalability, and energy consumption reveals the performance metrics of the Web 3.0 applications.

While Web 3.0 empowers users with greater control and fosters a potentially trustless internet, several significant challenges persist. Challenges include achieving high transaction throughput, ensuring true decentralization without sacrificing security, and scaling efficiently with minimal environmental impact. Furthermore, robust security practices and continuous vulnerability assessments are crucial to maintaining trust in decentralized systems. Striking a balance between decentralization and scalability remains a key focus, with promising solutions emerging like sharding and layer-2 protocols. Finally, addressing the energy consumption concerns associated with specific consensus mechanisms, such as PoW, necessitates the exploration of sustainable approaches. By embracing these insights and fostering progressive innovation, Web 3.0 can evolve into a more user-centric, secure, scalable, and environmentally conscious decentralized internet.

VII. FUTURE DIRECTIONS

A. Future Directions in Web 3.0 Policy and Standardization

In the rapidly evolving digital landscape, Web 3.0 represents the next frontier, promising a decentralized, user-empowered internet. However, the shift towards a new paradigm of Web 3.0 raises complex policy and standardization challenges. In this survey, we explore future directions in Web 3.0 policy and standardization, focusing on legal pluralism, governance, and the establishment of de facto standards and standardization bodies. The transition from Web 2.0 to Web 3.0 is characterized by a move away from centralized control towards a more distributed and user-centric framework. This shift necessitates rethinking the regulatory environment, as traditional models may not suffice for the unique dynamics of Web 3.0.

Recent legislative initiatives such as the Data Act, Digital Service Act, and Digital Market Act in the European Union signal a significant paradigm shift in digital regulation [296]. These acts aim to balance the promotion of innovation with the protection of users' rights and the establishment of fair competition. In Web 3.0, these regulations must adapt to the complexities of decentralized networks, where data ownership and control are distributed among users rather than centralized entities, particularly through public blockchain-based infrastructure.

While promising, the evolution towards Web 3.0 demands more sophisticated legal and ethical frameworks to ensure it aligns with our fundamental values and rights protection within decentralized ecosystems. Foreseeable conflicts between this emerging web architecture and current legislation are clear. One notable area of potential conflict is the Right to be Forgotten (Rtbf), as mandated by the General Data Protection Regulation (GDPR) Article 16 and other data privacy laws [297], in contrast to the principles of Web 3.0. A fundamental tension exists because personal data, once utilized to train AI systems of Web 3.0, becomes deeply integrated into the models' architecture, including parameters, neural network weights, and decision-making processes, while some records may also be retained by Web 3.0 infrastructure.

On the other hand, standardization is crucial for ensuring that Web 3.0 technologies are interoperable, secure, and user-

friendly. It involves developing common protocols and guidelines that can be adopted universally. As Web 3.0 technologies mature, there is a growing need for industry-wide standards that facilitate seamless interaction between different platforms and applications while ensuring compliance with regulatory requirements.

B. Future Directions in Web 3.0 Governance

Governance in Web 3.0 extends beyond traditional legal frameworks to include community-driven models that reflect the decentralized nature of the technology. Web 3.0 governance must be inclusive and participatory to reflect the diverse interests of stakeholders and involve a broad range of participants in governance processes, from developers and users to regulators and civil society organizations. To facilitate community participation in decision-making, tools and platforms that enable transparent and efficient governance processes are necessary. These may include voting systems built on blockchain technology, collaborative platforms for proposal development, and mechanisms for consensus-building among stakeholders [298]. DAOs represent a new form of organizational structure that operates without central oversight. Regulations for DAOs must address issues such as liability, decision-making authority, and the distribution of financial resources while respecting the autonomous nature of these entities [299].

As Web 3.0 continues to develop, ensuring interoperability between different blockchain networks and technologies becomes increasingly important. Regulatory frameworks should promote mechanisms that enable different blockchain networks to communicate and interact seamlessly. This interoperability is essential for creating a cohesive Web 3.0 ecosystem where users can easily access services across different platforms without technical barriers. Effective governance models require evolutionary adaptability, blending flexibility with a forward-looking strategy that forecasts and accommodates technological advancements. This approach demands policies that are both resilient to change and consistent across the ecosystem. Contrastingly, experimental frameworks like Nation3's cloud-based nation-state concept offer a radical reimagining of governance for the Web 3.0 era [300]. This model shifts from adaptation to transformation, advocating a decentralized, dynamic governance structure that anticipates and actively shapes the future of digital innovation. Such visions propose not just a response to technological evolution but a proactive, foundational redesign of governance mechanisms to ensure stability and foster innovation in a rapidly changing digital world.

C. Standardization and De Facto Standards

The development of standards is a critical aspect of Web 3.0's maturation. Standards ensure that technologies are developed in a way that is consistent with regulatory requirements and user expectations. It delves into how the emerging Web 3.0 ecosystem is shaping up in terms of formal standardization efforts and the establishment of widely adopted practices and technologies that become standards in practice, even if not officially recognized as such. Recently, communities led by

professionals have been developing standards for Web 3.0 through two distinct approaches: one by legal institutions recognized by authorities and the other through consensus within public Web 3.0 communities. The latter approach often leads to de facto standards as the project's influence grows.

1) *An Overview of Ongoing Web 3.0 Standards:* From an internet and telecommunications perspective, several Standards Development Organizations (SDOs) are actively working on Web 3.0-related standards. These organizations include international ones, e.g., International Telecommunication Union Telecommunication Standardization Sector (ITU-T), Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), and Institute of Electrical and Electronics Engineers (IEEE), European Telecommunications Standards Institute (ETSI) along with others and regional SDOs, e.g., China Communications Standards Association (CCSA), Trusted Blockchain Initiatives (TBI). A diagram illustrating the major SDOs involved in Web 3.0 can provide a visual representation of the standardization landscape.

2) *De Facto Standards in Web 3.0:* De facto standards refer to technologies, protocols, or practices that gain widespread acceptance and become the default choice within an industry, not through formal standardization processes but rather through widespread use and consensus among stakeholders. In the Web 3.0 space, several de facto standards have emerged, including: Bitcoin, the first and most well-known cryptocurrency, has established a set of standards and protocols that have become de facto standards within the cryptocurrency world. While Bitcoin's core protocol itself is a standard for how Bitcoin nodes communicate and validate transactions, there are additional standards and proposals that have been developed to enhance its functionality, security, and usability. The associated standardization process is undertaken by BIP (Bitcoin Improvement Proposals): BIPs are the standard way of communicating ideas and innovations within the Bitcoin community. They propose changes to the Bitcoin protocol, new features, and processes and conventions for the community. As one of the earliest and most widely used blockchain platforms for DApps and smart contracts, Ethereum has become a de facto standard for building dApps. Notable examples are ERC-20 and ERC-721 Tokens: These Ethereum token standards have become de facto standards for creating fungible (ERC-20) and NFTs (ERC-721), respectively, facilitating a wide range of applications from cryptocurrencies to digital collectibles. Other Web 3.0 projects, such as the InterPlanetary File System (IPFS), may become de facto standards in their designated fields of application. IPFS has become a widely adopted method for decentralized storage, enabling files to be stored and accessed in a distributed manner across the internet. The dynamic between formal standardization efforts and the emergence of de facto standards is crucial in shaping the development and adoption of Web 3.0 technologies. While formal standards ensure interoperability and reliability, de facto standards can drive innovation and rapid adoption within the community.

D. Lessons Learned

The evolution towards Web 3.0 presents both opportunities and challenges for policymakers and standard-makers. As Web

TABLE XIII: Table of Major SDOs Involved in Web3-related Standards

Category	Organization Name	Focus Area	Examples of Work Groups/Standards
International	International Telecommunication Union Telecommunication Standardization Sector (ITU-T)	Telecommunications standards globally	- Focus Group on Application of Distributed Ledger Technology
International	Internet Engineering Task Force (IETF)	Internet standards, including protocols and architecture	- Network Working Group drafts on ALTO for the blockchain
International	World Wide Web Consortium (W3C)	Web standards, including HTML, CSS, and Web accessibility	- Blockchain Community Group and DID Working Group
International	Institute of Electrical and Electronics Engineers (IEEE)	Electrical engineering and computing standards, including blockchain	Blockchain Technical Communities and IEEE Standard Association
International	European Telecommunications Standards Institute (ETSI)	Telecommunications and broadcasting standards in Europe	- Industry Specification Group (ISG) Permitted Distributed Ledger (PDL)
Regional	China Communications Standards Association (CCSA)	Telecommunications standards in China	- CCSA ST8 WG6
Regional	Trusted Blockchain Initiatives (TBI)	Blockchain standards and practices, likely with a focus on specific regions or sectors	- Development of best practices and standards for blockchain technology to enhance trust and interoperability

3.0 moves forward, it must develop regulatory frameworks and standards that foster innovation while protecting users' rights and ensuring fair competition. Legal pluralism, decentralized governance models, interoperability, technological governance, and the establishment of de facto standards will be key areas of focus in shaping the future of Web 3.0 policy and standardization. By addressing these areas thoughtfully and collaboratively, Web 3.0 will become a robust, decentralized internet that empowers users and supports sustainable growth in the digital economy.

VIII. CONCLUSION

Web 3.0 promises to reshape the current Web 2.0 paradigm, offering unprecedented opportunities for creation and collaboration. This survey systematically reviews the development of Web 3.0, defining it as a new generation of World Wide Web (WWW) characterized by decentralization, intelligence, interoperability, and scalability. The architecture presented herein highlights Web 3.0's potential to provide a trustworthy environment for digital interactions, extending from the infrastructure layer to the interface layer with enhanced performance. Building on key technologies, Web 3.0 is poised to revolutionize various domains with an ecosystem that includes applications like DePINs, NFTs, and Social Networks, evaluated across multiple metrics. Furthermore, we discuss future directions and open issues in policy, governance, and standardization. Although still in its infancy, Web 3.0 represents a significant advancement in the landscape and experience of future network services and applications, empowering users to regain ownership of their identities and digital assets. This timely study aims to illuminate the research landscape of Web 3.0 and inspire further contributions from researchers and practitioners in this evolving field.

REFERENCES

- [1] J. Zeldman. (2006, Jan.) Web 3.0 (CTAN). Accessed on 01/03/2024. [Online]. Available: <https://alistapart.com/article/web3point0/>
- [2] T. Berners-Lee. (1998) The world wide web: A very short personal history. Accessed on 01/06/2024. [Online]. Available: <http://www.w3.org/People/Berners-Lee/ShortHistory.html>
- [3] B.-L. T. Hendler J. Lassila O. "The semantic web," *SCI. AM.*, vol. 284, no. 5, pp. 34–43, May 2001.
- [4] G. Wood. (2014) Dapps: What web 3 looks like. Accessed on 01/06/2023. [Online]. Available: <http://gawwood.com/dappsweb3.html>
- [5] W. Ding, J. Hou, J. Li, C. Guo, J. Qin, R. Kozma, and F.-Y. Wang, "Desci based on web3 and dao: A comprehensive overview and reference model," *IEEE Trans. Comput. Social Syst.*, vol. 9, no. 5, pp. 1563–1573, Sept. 2022.
- [6] J. M. Connor Dempsey, Angie Wang. (2022, Jan.) A simple guide to the web3 stack. Accessed on 01/06/2024. [Online]. Available: <https://www.coinbase.com/blog/a-simple-guide-to-the-web3-stack>
- [7] A. Murray, D. Kim, and J. Combs, "The promise of a decentralized internet: What is web3 and how can firms prepare?" *Bus. Horiz.*, vol. 66, no. 2, pp. 191–202, Apr. 2023. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0007681322000714>
- [8] L. Cao, "Decentralized ai: Edge intelligence and smart blockchain, metaverse, web3, and desc," *IEEE Intell. Syst.*, vol. 37, no. 3, pp. 6–19, Jul. 2022.
- [9] K. Shkempi, P. Kochovski, T. G. Papaioannou, C. Barelle, and V. Stankovski, "Semantic web and blockchain technologies: Convergence, challenges and research trends," *J. Web Semant.*, vol. 79, Oct. 2023, Art. no. 100809, doi: 10.1016/j.websem.2023.100809.
- [10] Y. Lin, Z. Gao, Y. Tu, H. Du, D. Niyato, J. Kang, and H. Yang, "A blockchain-based semantic exchange framework for web 3.0 toward participatory economy," *IEEE Commun. Mag.*, vol. 61, no. 8, pp. 94–100, Jun. 2023.
- [11] Y. Lin, Z. Gao, H. Du, D. Niyato, J. Kang, R. Deng, and X. S. Shen, "A unified blockchain-semantic framework for wireless edge intelligence enabled Web 3.0," *IEEE Wireless Commun.*, early access, Mar. 2023, 10.1109/MWC.018.2200568.
- [12] R. Huang, J. Chen, Y. Wang, T. Bi, L. Nie, and Z. Zheng, "An overview of web3 technology: Infrastructure, applications, and popularity," *Blockchain: Research and Applications*, vol. 5, no. 1, p. 100173, Mar. 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2096720923000489>
- [13] P. P. Ray, "Web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions," *Internet Things Cyber-Phys. Syst.*, vol. 3, pp. 213–248, May 2023. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2667345223000305>
- [14] J. Zhu, F. Li, and J. Chen, "A survey of blockchain, artificial intelligence, and edge computing for web 3.0," *Computer Science Review*, vol. 54, p. 100667, Nov. 2024.
- [15] M. Shen, Z. Tan, D. Niyato, Y. Liu, J. Kang, Z. Xiong, L. Zhu, W. Wang, and X. S. Shen, "Artificial intelligence for web 3.0: A comprehensive survey," *ACM Comput. Surv.*, vol. 56, no. 10, May 2024. [Online]. Available: <https://doi.org/10.1145/3657284>
- [16] X. Ren, M. Xu, D. Niyato, J. Kang, Z. Xiong, C. Qiu, and X. Wang, "Building resilient web 3.0 with quantum information technologies and blockchain: An ambilateral view," *arXiv preprint arXiv:2303.13050*, Mar. 2023.
- [17] Q. Wang, R. Li, Q. Wang, S. Chen, M. Ryan, and T. Hardjono, "Exploring web3 from the view of blockchain," *arXiv preprint arXiv:2206.08821*, pp. 1–4, Jun. 2022.
- [18] G. Korpall and D. Scott, "Decentralization and web3 technologies," *TechRxiv*, May 2022. [Online]. Available: <http://dx.doi.org/10.36227/techrxiv.19727734.v1>
- [19] S. Filipčić, "Web3 & daos: an overview of the development and possibilities for the implementation in research and education," in

- Proc. 2022 45th Jubilee Int'l. Conf. Information, Communication and Electronic Technology (MIPRO)*. IEEE, May 2022, pp. 1278–1283.
- [20] H. Chen, H. Duan, M. Abdallah, Y. Zhu, Y. Wen, A. E. Saddik, and W. Cai, "Web3 metaverse: State-of-the-art and vision," *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 20, no. 4, Dec. 2023. [Online]. Available: <https://doi.org/10.1145/3630258>
- [21] A. Razzaq, "A web3 secure platform for assessments and educational resources based on blockchain," *Comput. Appl. Eng. Educ.*, vol. 32, no. 1, p. e22677, Sept. 2023.
- [22] X. Song, G. Xu, Y. Huang, and J. Dong, "Did-hvc-based web3 healthcare data security and privacy protection scheme," *Future Gener. Comput. Syst.*, vol. 158, pp. 267–276, Sept. 2024.
- [23] N. Kshetri, "Policy, ethical, social, and environmental considerations of web3 and the metaverse," *IT Prof.*, vol. 24, no. 3, pp. 4–8, Jun. 2022.
- [24] T. Berners-Lee. (2023) Layer cake. Accessed on 01/06/2023. [Online]. Available: <https://www.w3.org/2007/03/layerCake.png>
- [25] K. Samani. The web3 stack, 2019 edition. Accessed on 01/03/2024. [Online]. Available: <https://multico.in.capital/2019/12/13/the-web3-stack-2019-edition/>
- [26] Web3 architecture. Web3 foundation. Accessed on 01/03/2024. [Online]. Available: <https://2018.web3summit.com/speakers/>
- [27] W. Liu, B. Cao, and M. Peng, "Web3 technologies: Challenges and opportunities," *IEEE Netw.*, vol. 38, no. 3, pp. 187–193, Oct. 2023.
- [28] A. Singh, G. Kumar, R. Saha, M. Conti, M. Alazab, and R. Thomas, "A survey and taxonomy of consensus protocols for blockchains," *J. Syst. Archit.*, vol. 127, p. 102503, Jun. 2022.
- [29] M. Nadini, L. Alessandretti, F. Di Giacinto, M. Martino, L. M. Aiello, and A. Baronchelli, "Mapping the nft revolution: market trends, trade networks, and visual features," *Sci. Rep.*, vol. 11, no. 1, p. 20902, Oct. 2021.
- [30] M. Hussain, S. Pal, Z. Jadidi, E. Foo, and S. Kanhere, "Federated zero trust architecture using artificial intelligence," *IEEE Wireless Commun.*, vol. 31, no. 2, pp. 30–35, Apr. 2024.
- [31] A. Coladangelo and O. Sattath, "A quantum money solution to the blockchain scalability problem," *Quantum*, vol. 4, p. 297, Jul. 2020.
- [32] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, Sept. 2017.
- [33] Z. Yang, M. Zolanvari, and R. Jain, "A survey of important issues in quantum computing and communications," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 2, pp. 1059–1094, Mar. 2023.
- [34] M. Xu, X. Ren, D. Niyato, J. Kang, C. Qiu, Z. Xiong, X. Wang, and V. C. Leung, "When quantum information technologies meet blockchain in web 3.0," *IEEE Network*, vol. 38, no. 2, pp. 255–263, 2023.
- [35] J. Domingue, D. Fensel, and J. A. Hendler, *Handbook of semantic web technologies*. Springer Science & Business Media, 2011.
- [36] W3C. (2023) Rdf 1.2 semantics. Accessed on 01/03/2024. [Online]. Available: <https://www.w3.org/TR/2023/WD-rdf12-semantics-20230615/>
- [37] Y. Chi, H. Duan, W. Cai, Z. J. Wang, and V. C. M. Leung, "Knowledge inference over web 3.0 for intelligent fault diagnosis in industrial internet of things," *IEEE Trans. Network Sci. Eng.*, pp. 1–14, Dec. 2023.
- [38] D. Wheeler and B. Natarajan, "Engineering semantic communication: A survey," *IEEE Access*, vol. 11, pp. 13 965–13 995, Feb. 2023.
- [39] S. Kirrane, S. Villata, and M. d'Aquin, "Privacy, security and policies: A review of problems and solutions with semantic web technologies," *Semantic Web*, vol. 9, no. 2, pp. 153–161, 2018.
- [40] Z. Fu, F. Huang, K. Ren, J. Weng, and C. Wang, "Privacy-preserving smart semantic search based on conceptual graphs over encrypted outsourced data," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 8, pp. 1874–1884, Apr. 2017.
- [41] E. Coronado, R. Behraves, T. Subramanya, A. Fernández-Fernández, S. Siddiqui, X. Costa-Pérez, and R. Riggio, "Zero touch management: A survey of network automation solutions for 5g and 6g networks," *IEEE Commun. Surv. Tutorials*, Oct. 2022.
- [42] P. Kasireddy. (2021) The architecture of a web3 application. Accessed on 01/06/2024. [Online]. Available: <https://www.preethekasireddy.com/post/the-architecture-of-a-web-3-0-application>
- [43] Q. Yang, H. Huang, K. Lin, and J. Wu, *An Introduction to Web3 and Metaverse*. SG: Springer Nature Singapore, May 2023, pp. 1–25. [Online]. Available: https://doi.org/10.1007/978-981-99-3648-9_1
- [44] S. Wan, H. Lin, W. Gan, J. Chen, and P. S. Yu, "Web3: The next internet revolution," *arXiv preprint arXiv:2304.06111*, May 2023.
- [45] T. Wang, S. Zhang, Q. Yang, and S. C. Liew, "Account service network: A unified decentralized web 3.0 portal with credible anonymity," *IEEE Netw.*, pp. 1–1, Oct. 2023.
- [46] H. Xu, Y. Sun, Z. Li, Y. Sun, L. Zhang, and X. Zhang, "decontroller: A web3 native cyberspace infrastructure perspective," *IEEE Commun. Mag.*, vol. 61, no. 8, pp. 68–74, Jun. 2023.
- [47] N. Keizer, O. Ascigil, M. Król, D. Kutscher, and G. Pavlou, "A survey on content retrieval on the decentralised web," *ACM Comput. Surv.*, vol. 56, no. 8, pp. 1–39, Apr. 2024.
- [48] B. Gong, C. Guo, Y.-J. Liu, and Q. Wang, "Towards secure data storage in web 3.0: Ciphertext-policy attribute-based encryption," *IEEE Netw.*, pp. 1–1, Oct. 2023.
- [49] R. H. Kim, H. Song, and G. S. Park, "Moving real-time services to web 3.0: Challenges and opportunities," *IEEE Trans. Services Comput.*, vol. 16, no. 6, pp. 4041–4059, Aug. 2023.
- [50] P. Consul, I. Budhiraja, and D. Garg, "A hybrid secure resource allocation and trajectory optimization approach for mobile edge computing using federated learning based on web 3.0," *IEEE Trans. Consum. Electron.*, pp. 1–1, Dec. 2023.
- [51] Z. Liu, X. Xu, F. Han, Q. Zhao, L. Qi, W. Dou, and X. Zhou, "Secure edge server placement with non-cooperative game for Internet of Vehicles in Web 3.0," *IEEE Trans. Network Sci. Eng.*, pp. 1–12, early access, Oct. 2023, doi: 10.1109/TNSE.2023.3321139.
- [52] S. Guo, F. Zhang, S. Guo, S. Xu, and F. Qi, "Blockchain-assisted privacy-preserving data computing architecture for Web3," *IEEE Commun. Mag.*, vol. 61, no. 8, pp. 28–34, Aug. 2023.
- [53] Q. Wang, P. Wang, W. Sun, and Y. Zhang, "Low-latency communications for digital twin empowered web 3.0," *IEEE Netw.*, vol. 37, no. 6, pp. 26–33, Oct. 2023.
- [54] Decentralized identifiers (dids) v1.0. W3C. Accessed on 01/03/2024. [Online]. Available: <https://www.w3.org/TR/did-core/>
- [55] W. Recommendation. (2022) Verifiable credentials data model v1.1. Accessed on 01/06/2024. [Online]. Available: <https://www.w3.org/TR/vc-data-model/>
- [56] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Comput. Sci. Rev.*, vol. 30, pp. 80–86, Nov. 2018.
- [57] W. Xu, Y. Xie, M. Lv, H. Sun, A. Li, and H. Zhao, "Sdp security control technology based on zero trust," in *Proc. IEEE 4th Int. Conf. Civil Aviation Saf. Inf. Technol. (ICCAST)*, Oct. 2022, pp. 611–616.
- [58] N. K. Dewangan, P. Chandrakar, S. Kumari, and J. J. Rodrigues, "Enhanced privacy-preserving in student certificate management in blockchain and interplanetary file system," *Multimedia Tools and Applications*, vol. 82, no. 8, pp. 12 595–12 614, Sept. 2022.
- [59] K. Cameron, "The laws of identity," *Microsoft Corp.*, vol. 12, pp. 8–11, May 2005.
- [60] C. Allan. (2016) The path to self sovereign identity. Accessed on 01/06/2024. [Online]. Available: <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>
- [61] L. Zhou, A. Diro, A. Saini, S. Kaisar, and P. C. Hiep, "Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities," *J. Inf. Secur. Appl.*, vol. 80, p. 103678, Feb. 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2214212623002624>
- [62] L. Wei, Y. Zhang, J. Cui, H. Zhong, I. Bolodurina, and D. He, "A threshold-based full-decentralized authentication and key agreement scheme for vanets powered by consortium blockchain," *IEEE Trans. Mobile Comput.*, Jun. 2024.
- [63] H. L. J. L. Y. S. a. Z. W. Qiuyun Lyu, Shaopeng Cheng, "Nssia: A new self-sovereign identity scheme with accountability," *Secur. Commun. Netw.*, Sept. 2022.
- [64] S. Wang, D. Zhang, and Y. Zhang, "Blockchain-based personal health records sharing scheme with data integrity verifiable," *IEEE Access*, vol. 7, pp. 102 887–102 901, Jul. 2019.
- [65] I. Keshta, Y. Aoudni, M. Sandhu, A. Singh, P. A. Xalikovich, A. Rizwan, M. Soni, and S. Lalar, "Blockchain aware proxy re-encryption algorithm-based data sharing scheme," *Phys. Commun.*, vol. 58, p. 102048, Jun. 2023. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1874490723000514>
- [66] U. Khalil, M. Uddin, O. A. Malik, and O. W. Hong, "A novel nft solution for assets digitization and authentication in cyber-physical systems: Blueprint and evaluation," *IEEE Open J. Comput. Soc.*, vol. 5, pp. 131–143, Mar. 2024.
- [67] H. Xu, L. Zhang, Y. Sun *et al.*, "Be-ran: Blockchain-enabled open ran with decentralized identity management and privacy-preserving communication," *arXiv preprint arXiv:2101.10856*, Jan. 2021.

- [68] E. Zeydan, J. Baranda, J. Mangues-Bafalluy, S. S. Arslan, and Y. Turk, "A trustworthy framework for multi-cloud service management: Self-sovereign identity integration," *IEEE Trans. Network Sci. Eng.*, pp. 1–13, Feb. 2024.
- [69] R. Xiong, W. Ren, X. Hao, J. He, and K.-K. R. Choo, "Bdim: A blockchain-based decentralized identity management scheme for large scale internet of things," *IEEE Internet Things J.*, vol. 10, no. 24, pp. 22 581–22 590, Dec. 2023.
- [70] L. Shi, T. Wang, Z. Xiong, Z. Wang, Y. Liu, and J. Li, "Blockchain-aided decentralized trust management of edge computing: Towards reliable off-chain and on-chain trust," *IEEE Netw.*, May 2024, early access, doi: 10.1109/TWC.2023.3323974.
- [71] M. A. Bouras, Q. Lu, S. Dhelim, and H. Ning, "A lightweight blockchain-based iot identity management approach," *Future Internet*, vol. 13, no. 2, Jan. 2021. [Online]. Available: <https://www.mdpi.com/1999-5903/13/2/24>
- [72] E. S. Fathalla, M. Azab, C. Xin, and H. Wu, "Pt-ssim: A proactive, trustworthy self-sovereign identity management system," *IEEE Internet Things J.*, vol. 10, no. 19, pp. 17 155–17 169, May 2023.
- [73] R. Li, T. Song, B. Mei, H. Li, X. Cheng, and L. Sun, "Blockchain for large-scale internet of things data storage and protection," *IEEE Trans. Service Comput.*, vol. 12, no. 5, pp. 762–771, Sept.–Oct. 2019.
- [74] H. Saidi, N. Labraoui, A. A. Ari, L. A. Maglaras, and J. H. M. Emati, "Dsmac: Privacy-aware decentralized self-management of data access control based on blockchain for health data," *IEEE Access*, vol. 10, pp. 101 011–101 028, Sept. 2022.
- [75] L. Hong, K. Zhang, J. Gong, H. Qian *et al.*, "A practical and efficient blockchain-assisted attribute-based encryption scheme for access control and data sharing," *Secur. Commun. Netw.*, vol. 2022, Sept. 2022.
- [76] G. Verma and S. Kanrar, "Secure keyword search over encrypted cloud data using blockchain in digital document sharing," *Wireless Pers. Commun.*, vol. 134, no. 2, pp. 975–996, Apr. 2024.
- [77] L. Li, D. Jin, T. Zhang, and N. Li, "A secure, reliable and low-cost distributed storage scheme based on blockchain and ipfs for firefighting iot data," *IEEE Access*, vol. 11, pp. 97 318–97 330, Sept. 2023.
- [78] M. Network. (2022) Mind network overview. Accessed on 01/06/2024. [Online]. Available: <https://mind-network.gitbook.io/mindnetwork/mindnetwork-overview/mind-networks-zero-trust-solution>
- [79] H. G. Do and W. K. Ng, "Blockchain-based system for secure data storage with private keyword search," in *Proc. IEEE SERVICES, Honolulu, HI, USA*, Jun. 2017, pp. 90–93.
- [80] M. Sookhak, M. R. Jabbarpour, N. S. Safa, and F. R. Yu, "Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues," *J. Netw. Comput. Appl.*, vol. 178, p. 102950, Mar. 2021. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1084804520304045>
- [81] Y. Du, H. Duan, A. Zhou, C. Wang, M. H. Au, and Q. Wang, "Enabling secure and efficient decentralized storage auditing with blockchain," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 5, pp. 3038–3054, Oct. 2022.
- [82] S. Yang and M. Li, "Web3.0 data infrastructure: Challenges and opportunities," *IEEE Netw.*, vol. 37, no. 1, pp. 4–5, Apr. 2023.
- [83] T. Wu, G. Jourjon, K. Thilakarathna, and P. L. Yeoh, "Mapchain-d: A distributed blockchain for iiot data storage and communications," *IEEE Trans. Ind. Informat.*, vol. 19, no. 9, pp. 9766–9776, Jan. 2023.
- [84] E. Zhou, Z. Hong, Y. Xiao, D. Zhao, Q. Pei, S. Guo, and R. Akerkar, "Mstdb: A hybrid storage-empowered scalable semantic blockchain database," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 8, pp. 8228–8244, Aug. 2023.
- [85] M. Shen, K. Ye, X. Liu, L. Zhu, J. Kang, S. Yu, Q. Li, and K. Xu, "Machine learning-powered encrypted network traffic analysis: A comprehensive survey," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 1, pp. 791–824, 2023.
- [86] M. Juarez, M. Imani, M. Perry, C. Diaz, and M. Wright, "Toward an efficient website fingerprinting defense," in *Computer Security–ESORICS 2016: 21st European Symposium on Research in Computer Security, Heraklion, Greece, September 26–30, 2016, Proceedings, Part I 21*. Springer, 2016, pp. 27–46.
- [87] T. Wang and I. Goldberg, "{Walkie-Talkie}: An efficient defense against passive website fingerprinting attacks," in *26th USENIX Security Symposium (USENIX Security 17)*, 2017, pp. 1375–1390.
- [88] Y. Qian, G. Huang, C. Ma, M. Ding, L. Yuan, Z. Chen, and K. Wang, "Enhancing resilience in website fingerprinting: Novel adversary strategies for noisy traffic environments," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 7216–7231, 2024.
- [89] H. Yin, Y. Liu, Z. Guo, and Y. Wang, "From traces to packets: Realistic deep learning based multi-tab website fingerprinting attacks," *Tsinghua Science and Technology*, vol. 30, no. 2, pp. 830–850, Dec. 2024.
- [90] M. Shen, J. Zhang, L. Zhu, K. Xu, and X. Du, "Accurate decentralized application identification via encrypted traffic analysis using graph neural networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 2367–2380, Jan. 2021.
- [91] Q. Meng, Q. Yuan, W. Niu, Y. Wang, S. Lu, G. Li, X. Wang, and W. He, "Iit: Accurate decentralized application identification through mining intra- and inter-flow relationships," *IEEE Trans. Netw. Service Manag.*, pp. 1–1, Oct. 2024.
- [92] S. P. Marsh, "Formalising trust as a computational concept," Ph.D. dissertation, Dept. Comput. Sci. Math., Stirling Univ., Scotland, UK, 1994.
- [93] B. A. E. Beyer, C. M. Beske, J. Peck, and M. Saltonstall, "Migrating to beyondcorp: Maintaining productivity while improving security," *Login*, vol. 42, no. 2, pp. 1–7, 2017, iSSN 1044-6397. [Online]. Available: <https://research.google/pubs/migrating-to-beyondcorp-maintaining-productivity-while-improving-security/>
- [94] S. M. S. Rose, O. Borchert and S. Connelly, "Zero trust architecture," Nat. Inst. Standards Technol., Gaithersburg, MD, US, Tech. Rep. SP 800-207, Aug. 2020.
- [95] K. Gai, Y. She, L. Zhu, K.-K. R. Choo, and Z. Wan, "A blockchain-based access control scheme for zero trust cross-organizational data sharing," *ACM Trans. Internet Technol.*, vol. 23, no. 3, pp. 1–25, Aug. 2023. [Online]. Available: <https://doi.org/10.1145/3511899>
- [96] P. Dhiman, N. Saini, Y. Gulzar, S. Turaev, A. Kaur, K. U. Nisa, and Y. Hamid, "A review and comparative analysis of relevant approaches of zero trust network model," *Sens.*, vol. 24, no. 4, Feb. 2024. [Online]. Available: <https://www.mdpi.com/1424-8220/24/4/1328>
- [97] J. Wang, X. Ling, Y. Le, Y. Huang, and X. You, "Blockchain-enabled wireless communications: a new paradigm towards 6G," *Natl. Sci. Rev.*, vol. 8, no. 9, p. nwab069, Apr. 2021. [Online]. Available: <https://doi.org/10.1093/nsr/nwab069>
- [98] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Washington, DC, US, Bitcoin, White Paper, Oct. 2008. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [99] V. Buterin, "A next-generation smart contract and decentralized application platform," Zug, CH, Ethereum, Whitepaper, Jan. 2014. [Online]. Available: <https://ethereum.org/en/whitepaper/>
- [100] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proc. ACM 13th EuroSys Conf. (EuroSys'18)*, ser. EuroSys '18, New York, US, Apr. 2018, pp. 1–15. [Online]. Available: <https://doi.org/10.1145/3190508.3190538>
- [101] Y. Jiang, Y. Le, J. Wang, and X. You, "Gas-pbft: A game-based node selection consensus mechanism for internet of things," in *Proc. 14th Int. Conf. Wireless Commun. Signal Process. (WCSP'22)*, Nanjing, CN, Nov. 2022, pp. 17–21.
- [102] X. Liu, Y. Liu, Q. Hu, L. Fang, and J. Yang, "Research on the comprehensive application of cloud technology and Web 3.0," in *Proc. 2023 Int. Conf. Power Commun. Comput. Networking Technol.*, ser. PCCNT '23, no. 84. New York, NY, US: Association for Computing Machinery, 2024, pp. 1–7. [Online]. Available: <https://doi.org/10.1145/3630138.3630533>
- [103] K. Huang, Y. Le, Y. Jiang, J. Wang, and X. Ling, "Blockchain-enabled secure data interactions for responsive cyber-physical spaces," in *Proc. IEEE Global Commun. Conf. (GLOBECOM) Workshop*, Cape Town, South Africa, Dec. 2024.
- [104] X. Ling, P. Chen, Y. Le, J. Wang, and X. You, "Blockchain-based network hawkeye function: Building the trust triangle in 6G," *IEEE Netw.*, vol. 36, no. 4, pp. 104–111, Oct. 2022.
- [105] X. Ling, Y. Le, J. Wang, Y. Huang, and X. You, "Trust and trustworthiness in information and communications technologies," *accepted in IEEE Wireless Commun.*, Dec. 2024.
- [106] Y. Le, X. Ling, J. Wang, R. Guo, Y. Huang, C.-X. Wang, and X. You, "Resource sharing and trading of blockchain radio access networks: Architecture and prototype design," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 12 025–12 043, Jul. 2023.
- [107] W. Cao, X. Ling, J. Wang, Z. Ding, and X. Gao, "A framework for qos-guaranteed fast access services in blockchain radio access network," *IEEE Trans. Wireless Commun.*, vol. 23, no. 4, pp. 2711–2725, Apr. 2024.
- [108] Y. Le, X. Ling, S. Chen, J. Wang, W. Tan, Y. Huang, and X. You, "Modeling blockchain-based wireless access services and applications: A queuing perspective," *IEEE Trans. Commun.*, pp. 1–1, early access, Nov. 2024.

- [109] X. Ling, Y. Le, J. Wang, Z. Ding, and X. Gao, "Practical modeling and analysis of blockchain radio access network," *IEEE Trans. Commun.*, vol. 69, no. 2, pp. 1021–1037, Feb. 2021.
- [110] Z. Cui, X. Ling, X. Zhou, and J. Wang, "A bagging-based consensus protocol for distributed learning," in *Proc. IEEE Global Commun. Conf. (GLOBECOM) Workshop*, Cape Town, South Africa, Dec. 2024.
- [111] M. Hellman, "New directions in cryptography," *IEEE Trans. on Inf. Theory*, vol. 22, no. 6, pp. 644–654, Jun. 1976.
- [112] A. Anjana and A. Singh, "An enhanced three layer cryptographic algorithm for cloud information security," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 17, pp. 615–627, Feb. 2024.
- [113] S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, "Security of internet of things based on cryptographic algorithms: a survey," *Wireless Netw.*, vol. 27, no. 2, pp. 1515–1555, Jan. 2021.
- [114] N. M. Hijazi, M. Aloqaily, M. Guizani, B. Ouni, and F. Karray, "Secure federated learning with fully homomorphic encryption for iot communications," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 4289–4300, Aug. 2024.
- [115] U. Fiege, A. Fiat, and A. Shamir, "Zero knowledge proofs of identity," in *Proc. 19th Annu. ACM Symp. Theory Comput. (STOC'87)*, ser. STOC '87. New York, NY, US: Association for Computing Machinery, Jan. 1987, pp. 210–217. [Online]. Available: <https://doi.org/10.1145/28395.28419>
- [116] S. Jeong and B. Ahn, "Implementation of real estate contract system using zero knowledge proof algorithm based blockchain," *J. Supercomput.*, vol. 77, no. 10, pp. 11 881–11 893, Mar. 2021.
- [117] Y. Wu and S. Kasahara, "Smart contract-based e-voting system using homomorphic encryption and zero-knowledge proof," in *Proc. Appl. Cryptogr. Netw. Security Workshops (ACNS'23)*, Cham, CH, Oct. 2023, pp. 67–83.
- [118] H. Gao, P. Duan, X. Pan, X. Zhang, K. Ye, and Z. Zhong, "Blockchain-enabled supervised secure data sharing and delegation scheme in Web3.0," *J. Cloud Comput.*, vol. 13, no. 21, Jan. 2024. [Online]. Available: <https://doi.org/10.1186/s13677-023-00575-8>
- [119] S. You, K. Radivojevic, J. Nabrzycki, and P. Brenner, "Persona preserving reputation protocol (P2RP) for enhanced security, privacy, and trust in blockchain oracles," *Cluster Comput.*, Jan. 2024. [Online]. Available: <https://doi.org/10.1007/s10586-023-04222-4>
- [120] M. Neovius, J. Karlsson, M. Westerlund, and G. Pulkkis, "Providing tamper-resistant audit trails for cloud forensics with distributed ledger based solutions," *Cloud Comput. 2018*, vol. 11, no. 3&4, p. 29, Feb. 2018.
- [121] A. Ahmad, M. Saad, L. Njilla, C. Kamhoua, M. Bassiouni, and A. Mohaisen, "Blocktrail: A scalable multichain solution for blockchain-based audit trails," in *Proc. IEEE Int. Conf. Commun. (ICC'19)*, Shanghai, CN, May 2019, pp. 1–6.
- [122] F. Li, H. Li, B. Niu, and J. Chen, "Privacy computing: Concept, computing framework, and future development trends," *Eng.*, vol. 5, no. 6, pp. 1179–1192, Dec. 2019. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2095809919308240>
- [123] H. Liu, H. Luo, S. Li, T. Dong, G. Chen, Y. Meng, and H. Zhu, "Privacy computing with right to be forgotten in trusted execution environment," in *Proc. IEEE Global Commun. Conf. (GLOBECOM'23)*, Kuala Lumpur, MY, Dec. 2023, pp. 2566–2571.
- [124] M. A. Azad, S. Abdullah, J. Arshad, H. Lallie, and Y. H. Ahmed, "Verify and trust: A multidimensional survey of zero-trust security in the age of iot," *Internet of Things*, vol. 27, p. 101227, Oct. 2024.
- [125] H. Fang, Y. Zhu, Y. Zhang, and X. Wang, "Decentralized edge collaboration for seamless handover authentication in zero-trust iot," *IEEE Trans. Wireless Commun.*, vol. 23, no. 8, pp. 8760–8772, Jan 2024.
- [126] Y. Liu, X. Hao, W. Ren, R. Xiong, T. Zhu, K.-K. R. Choo, and G. Min, "A blockchain-based decentralized, fair and authenticated information sharing scheme in zero trust internet-of-things," *IEEE Transactions on Computers*, vol. 72, no. 2, pp. 501–512, Feb. 2023.
- [127] B. Cao, Z. Wang, L. Zhang, D. Feng, M. Peng, L. Zhang, and Z. Han, "Blockchain systems, technologies, and applications: A methodology perspective," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 1, pp. 353–385, 2023.
- [128] Z. Liu, X. Zhang, G. Li, H. Cui, J. Wang, and B. Xiao, "A secure and reliable blockchain-based audit log system," in *Proc. IEEE Int. Conf. Commun. (ICC2024)*, Denver, USA, Jun. 2024, pp. 2010–2015.
- [129] M. V. Anand, S. Mithun, L. D. Shree, and M. Ranjith, "Survey on connecting to the decentralized storage using IPFS protocol with web 3 technology," in *Proc. Int. Conf. Adv. Technol. (ICONAT'23)*. Goa, IN: IEEE, Jan. 2023, pp. 1–4.
- [130] Q. He, Z. Li, and X. Zhang, "Study on cloud storage system based on distributed storage systems," in *Proc. Int. Conf. Comput. Inf. Sci. (ICCIS'10)*, Chengdu, CN, Dec. 2010.
- [131] I. Gupta, A. K. Singh, C.-N. Lee, and R. Buyya, "Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions," *IEEE Access*, vol. 10, pp. 71 247–71 277, Jul. 2022.
- [132] X. Song, G. Xu, Y. Huang, and Y. Liu, "Decentralized authentication scheme incorporating reputation and attribute signature for cross-web3 applications," *IEEE Internet Things J.*, pp. 1–1, early access, Jan. 2025.
- [133] A. K. Sandhu, "Big data with cloud computing: Discussions and challenges," *Big Data Min. Anal.*, vol. 5, no. 1, pp. 32–40, Mar. 2022.
- [134] M. Amani, A. Ghorbanian, S. A. Ahmadi, M. Kakooei, A. Moghimi, S. M. Mirmazloumi, S. H. A. Moghaddam, S. Mahdavi, M. Ghahremanloo, S. Parsian, Q. Wu, and M. Brisco, "Google earth engine cloud computing platform for remote sensing big data applications: A comprehensive review," *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.*, vol. 13, pp. 5326–5350, Sep. 2020.
- [135] X.-Q. Pham, T.-D. Nguyen, T. Huynh-The, E.-N. Huh, and D.-S. Kim, "Distributed cloud computing: Architecture, enabling technologies, and open challenges," *IEEE Consum. Electron. Mag.*, vol. 12, no. 3, pp. 98–106, May 2023.
- [136] J. Pan and J. McElhannon, "Future edge cloud and edge computing for Internet of Things applications," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 439–449, Feb. 2018.
- [137] T.-A. N. Abdali, R. Hassan, A. H. M. Aman, and Q. N. Nguyen, "Fog computing advancement: Concept, architecture, applications, advantages, and open issues," *IEEE Access*, vol. 9, pp. 75 961–75 980, May 2021.
- [138] M. Aazam, S. Zeadally, and K. A. Harras, "Deploying fog computing in Industrial Internet of Things and industry 4.0," *IEEE Trans. Ind. Inf.*, vol. 14, no. 10, pp. 4674–4682, Jul. 2018.
- [139] J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing fog computing for Internet of Things applications: Challenges and solutions," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 1, pp. 601–628, Oct. 2018.
- [140] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted Execution Environment: What it is, and what it is not," in *Proc. IEEE 14th Trustcom/BigDataSE/ISPA (TBI'15)*, vol. 1, Helsinki, FI, Aug. 2015, pp. 57–64.
- [141] J. Zhu, R. Hou, X. Wang, W. Wang, J. Cao, B. Zhao, Z. Wang, Y. Zhang, J. Ying, L. Zhang, and D. Meng, "Enabling rack-scale confidential computing using heterogeneous Trusted Execution Environment," in *Proc. IEEE 41th Symp. Secur. and Privacy (SP'20)*, San Francisco, US, May 2020, pp. 1450–1465.
- [142] Y. Wang, J. Li, S. Zhao, and F. Yu, "Hybridchain: A novel architecture confidentiality-preserving and performant permissioned blockchain using Trusted Execution Environment," *IEEE Access*, vol. 8, pp. 190 652–190 662, Oct. 2020.
- [143] A. Park, M. Wilson, K. Robson, D. Demetis, and J. Kietzmann, "Interoperability: Our exciting and terrifying web3 future," *Bus. Horiz.*, vol. 66, no. 4, pp. 529–541, Jul./Aug. 2023. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0007681322001318>
- [144] Z. Wang, B. Cao, C. Liu, C. Xu, and L. Zhang, "Blockchain-based fog radio access networks: Architecture, key technologies, and challenges," *Digital Commun. Netw.*, vol. 8, no. 5, pp. 720–726, 2022. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2352864821001036>
- [145] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nat.*, vol. 521, no. 7553, pp. 436–444, May 2015.
- [146] V. Sze, Y.-H. Chen, T.-J. Yang, and J. S. Emer, "Efficient processing of deep neural networks: A tutorial and survey," *Proc. IEEE*, vol. 105, no. 12, pp. 2295–2329, Dec. 2017.
- [147] K. O'Shea and R. Nash, "An introduction to convolutional neural networks," *arXiv Prepr. arXiv:1511.08458*, Nov. 2015.
- [148] H. Salehinejad, S. Sankar, J. Barfett, E. Colak, and S. Valaee, "Recent advances in recurrent neural networks," *arXiv Prepr. arXiv:1801.01078*, Dec. 2017.
- [149] K. Arulkumaran, M. P. Deisenroth, M. Brundage, and A. A. Bharath, "Deep reinforcement learning: A brief survey," *IEEE Signal Process. Mag.*, vol. 34, no. 6, pp. 26–38, Nov. 2017.
- [150] M. Shen, M. Wei, L. Zhu, and M. Wang, "Classification of encrypted traffic with second-order markov chains and application attribute bigrams," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 8, pp. 1830–1843, Apr. 2017.
- [151] A. Agarwal, M. Dahleh, and T. Sarkar, "A marketplace for data: An algorithmic solution," in *Proc. 2019 ACM Conf. Econ. Comput. (EC)*, New York, US, Jun. 2019, pp. 701–726.

- [152] J. Yun, Y. Goh, and J.-M. Chung, "DQN-Based optimization framework for secure sharded blockchain systems," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 708–722, Jul. 2021.
- [153] F. Fui-Hoon Nah, R. Zheng, J. Cai, K. Siau, and L. Chen, "Generative AI and ChatGPT: Applications, challenges, and AI-human collaboration," *J. Inf. Technol. Case Appl. Res.*, vol. 25, no. 3, pp. 277–304, Jul. 2023.
- [154] C. Zhang, C. Zhang, S. Zheng, Y. Qiao, C. Li *et al.*, "A complete survey on generative AI (AIGC): Is chatgpt from gpt-4 to gpt-5 all you need?" *arXiv Prepr. arXiv:2303.11717*, Mar. 2023.
- [155] A. Bandi, P. V. S. R. Adapa, and Y. E. V. P. K. Kuchi, "The power of generative AI: A review of requirements, models, input–output formats, evaluation metrics, and challenges," *Future Internet*, vol. 15, no. 8, p. 260, Jun. 2023.
- [156] Z. Huang, Y. Shen, J. Li, M. Fey, and C. Brecher, "A survey on AI-driven digital twins in industry 4.0: Smart manufacturing and advanced robotics," *Sens.*, vol. 21, no. 19, p. 6340, Jul. 2021.
- [157] S. Mihai, M. Yaqoob, D. V. Hung, P. Towakel, M. Raza, M. Karamanoglu, B. Barn, D. Shetve, R. V. Prasad *et al.*, "Digital twins: A survey on enabling technologies, challenges, trends and future prospects," *IEEE Commun. Surv. Tutorials*, vol. 24, no. 4, pp. 2255–2291, Sep. 2022.
- [158] A. Ricci, A. Croatti, S. Mariani, S. Montagna, and M. Picone, "Web of digital twins," *ACM Trans. Internet Technol.*, vol. 22, no. 4, pp. 1–30, Nov. 2022.
- [159] X. You, C.-X. Wang, J. Huang, X. Gao, Z. Zhang, M. Wang, Y. Huang, C. Zhang, Y. Jiang, J. Wang *et al.*, "Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts," *Sci. China Inf. Sci.*, vol. 64, no. 110301, pp. 1–74, Nov. 2021.
- [160] M. Elatoubi, "Phishing in Web 3.0: Opportunities for the attackers, challenges for the defenders," *ARIS2-Advanced Res. Inf. Syst. Secur.*, vol. 3, no. 2, pp. 11–25, Dec. 2023.
- [161] F. Tang, X. Chen, M. Zhao, and N. Kato, "The roadmap of communication and networking in 6G for the metaverse," *IEEE Wireless Commun.*, vol. 30, no. 4, pp. 72–81, Jun. 2022.
- [162] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G networks: Use cases and technologies," *IEEE Commun. Mag.*, vol. 58, no. 3, pp. 55–61, Mar. 2020.
- [163] C.-X. Wang, X. You, X. Gao, X. Zhu, Z. Li, C. Zhang, H. Wang, Y. Huang, Y. Chen, H. Haas, J. S. Thompson, E. G. Larsson, M. D. Renzo, W. Tong, P. Zhu, X. Shen, H. V. Poor, and L. Hanzo, "On the road to 6g: Visions, requirements, key technologies, and testbeds," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 2, pp. 905–974, Feb. 2023.
- [164] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Feb. 2013.
- [165] A. Razzaq, A. B. Altamimi, A. Alreshidi, S. A. K. Ghayyur, W. Khan, and M. Alsaffar, "IoT data sharing platform in Web 3.0 using blockchain technology," *Electron.*, vol. 12, no. 5, Mar. 2023, Art. no. 1233, doi: 10.3390/electronics12051233.
- [166] W. Xia, Y. Wen, C. H. Foh, D. Niyato, and H. Xie, "A survey on Software-Defined Networking," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 1, pp. 27–51, Jun. 2015.
- [167] S. H. A. Kazmi, F. Qamar, R. Hassan, and K. Nisar, "Routing-based interference mitigation in SDN enabled beyond 5G communication networks: A comprehensive survey," *IEEE Access*, vol. 11, pp. 4023–4041, Jan. 2023.
- [168] J. A. Pérez-Díaz, I. A. Valdovinos, K.-K. R. Choo, and D. Zhu, "A flexible SDN-based architecture for identifying and mitigating low-rate DDos attacks using machine learning," *IEEE Access*, vol. 8, pp. 155 859–155 872, Aug. 2020.
- [169] R. Ramanathan and J. Redi, "A brief overview of ad hoc networks: challenges and directions," *IEEE Commun. Mag.*, vol. 40, no. 5, pp. 20–22, May 2002.
- [170] C. Cooper, D. Franklin, M. Ros, F. Safaei, and M. Abolhasan, "A comparative survey of vanet clustering techniques," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 1, pp. 657–681, Firstquarter 2017.
- [171] A. G. Papidas and G. C. Polyzos, "Self-organizing networks for 5g and beyond: A view from the top," *Future Internet*, vol. 14, no. 3, Mar. 2022. [Online]. Available: <https://www.mdpi.com/1999-5903/14/3/95>
- [172] S. Agrawal and R. Gupta, "Web GIS and its architecture: a review," *Arabian J. Geosci.*, vol. 10, pp. 1–13, Nov. 2017, Art. no. 518, doi: 10.1007/s12517-017-3296-2.
- [173] P. Pascacio, S. Casteleyn, J. Torres-Sospedra, E. S. Lohan, and J. Nurmi, "Collaborative indoor positioning systems: A systematic review," *Sens.*, vol. 21, no. 3, Feb. 2021. [Online]. Available: <https://www.mdpi.com/1424-8220/21/3/1002>
- [174] A. Suh and J. Prophet, "The state of immersive technology research: A literature analysis," *Comput. Hum. Behav.*, vol. 86, pp. 77–90, Sep. 2018. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0747563218301857>
- [175] C. Dibbern, M. Uhr, D. Krupke, and F. Steinicke, "Can WebVR further the adoption of Virtual Reality?" in *Proc. Mensch Comput. 2018 - Usability Prof. (UP'18)*, Bonn, DE, Sep. 2018, pp. 377–384.
- [176] S. N. B. Gunkel, R. Hindriks, K. M. E. Assal, H. M. Stokking, S. Dijkstra-Soudarissanane, F. t. Haar, and O. Niamut, "Vrcomm: an end-to-end web system for real-time photorealistic social VR communication," in *Proc. 12th ACM Multimedia Syst. Conf. (MMSys'21)*, ser. MMSys '21. New York, NY, US: Association for Computing Machinery, Feb. 2021, pp. 65–79. [Online]. Available: <https://doi.org/10.1145/3458305.3459595>
- [177] X. Fan and L. Xu, "Towards a rollout-centric scalable architecture for decentralized physical infrastructure networks: A position paper," in *Proceedings of the Fifth ACM International Workshop on Blockchain-enabled Networked Sensor Systems*, 2023, pp. 9–12.
- [178] Y. Parasas and D. Dias, "The interplanetary file system and the filecoin network," in *2020 50th Annual IEEE-IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S)*. IEEE, 2020, pp. 80–80.
- [179] Akash Network. [Online]. Available: <https://akash.network>
- [180] The Graph. [Online]. Available: <https://thegraph.com>
- [181] G. Wang and M. Nixon, "Sok: Tokenization on blockchain," in *Proceedings of the 14th IEEE/ACM International Conference on Utility and Cloud Computing Companion*, 2021, pp. 1–9.
- [182] A. Jain and E. S. Pilli, "Sok: Digital signatures and taproot transactions in bitcoin," in *International Conference on Information Systems Security*. Springer, 2023, pp. 360–379.
- [183] Ordinals. [Online]. Available: <https://ordinals.com/>
- [184] Atomicals Protocols. [Online]. Available: <https://atomicals.xyz/>
- [185] Q. Wang, R. Li, Q. Wang, and S. Chen, "Non-fungible token (nft): Overview, evaluation, opportunities and challenges," *arXiv preprint arXiv:2105.07447*, 2021.
- [186] T. Sarathchandra and D. Jayawikrama, "A decentralized social network architecture," in *2021 International Research Conference on Smart Computing and Systems Engineering (SCSE)*, vol. 4. IEEE, 2021, pp. 251–257.
- [187] N. Naik and P. Jenkins, "Sovrin network for decentralized digital identity: Analysing a self-sovereign identity system based on distributed ledger technology," in *2021 IEEE International Symposium on Systems Engineering (ISSE)*. IEEE, 2021, pp. 1–7.
- [188] Y. El Faqr, J. Arroyo, and 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.
- [189] A. Chandrashekhar, S. H. Saheb, S. K. Panda, S. Balamurugan, and S.-L. Peng, *Metaverse and Immersive Technologies: An Introduction to Industrial, Business and Social Applications*. John Wiley & Sons, 2023.
- [190] Ceramic - The Composable Data Network. [Online]. Available: <https://ceramic.network>
- [191] Livepeer. [Online]. Available: <https://livepeer.org>
- [192] Lit Protocol. [Online]. Available: <https://www.litprotocol.com>
- [193] Tableland - The Decentralized Cloud Database. [Online]. Available: <https://tableland.xyz>
- [194] S. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. Knottenbelt, "Sok: Decentralized finance (defi)," in *Proceedings of the 4th ACM Conference on Advances in Financial Technologies*, 2022, pp. 30–46.
- [195] MakerDAO. [Online]. Available: <https://makerdao.com/>
- [196] Uniswap Protocol. [Online]. Available: <https://uniswap.org/>
- [197] Flexa. [Online]. Available: <https://flexa.network/>
- [198] S. Wang, W. Ding, J. Li, Y. Yuan, L. Ouyang, and F.-Y. Wang, "Decentralized autonomous organizations: Concept, model, and applications," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 5, pp. 870–878, 2019.
- [199] H. Diedrich, *Ethereum: Blockchains, digital assets, smart contracts, decentralized autonomous organizations*. Wildfire publishing Sydney, Australia, 2016.
- [200] S. Tikhomirov, "Ethereum: state of knowledge and research perspectives," in *Foundations and Practice of Security: 10th International Symposium, FPS 2017, Nancy, France, October 23-25, 2017, Revised Selected Papers 10*. Springer, 2018, pp. 206–221.
- [201] Aragon. [Online]. Available: <https://aragon.org/>

- [202] B. P. Riaza and J.-Y. Gnabo, "Decentralized autonomous organizations (daos): catalysts for enhanced market efficiency," *Finance Research Letters*, vol. 58, p. 104445, 2023.
- [203] S. Tikhomirov, E. Voskresenskaya, I. Ivanitskiy, R. Takhaviev, E. Marchenko, and Y. Alexandrov, "Smartcheck: Static analysis of ethereum smart contracts," in *Proceedings of the 1st international workshop on emerging trends in software engineering for blockchain*, 2018, pp. 9–16.
- [204] O. Rikken, M. Janssen, and Z. Kwee, "The ins and outs of decentralized autonomous organizations (daos)," *Available at SSRN 3989559*, 2021.
- [205] Y. Faqir-Rhazoui, M.-J. Ariza-Garzón, J. Arroyo, and S. Hassan, "Effect of the gas price surges on user activity in the daos of the ethereum blockchain," in *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–7.
- [206] Q Protocol. [Online]. Available: <https://q.org/>
- [207] Ethereum Layer 2 Rollup platform - Metis. [Online]. Available: <https://www.metis.io/>
- [208] Snapshot docs. [Online]. Available: <https://docs.snapshot.org/>
- [209] Giveth. [Online]. Available: <https://giveth.io/>
- [210] SEEDAO. [Online]. Available: <https://seedao.xyz/>
- [211] HashKey Exchange. [Online]. Available: <https://www.hashkey.com/>
- [212] O. J. Scholten, N. G. J. Hughes, S. Deterding, A. Drachen, J. A. Walker, and D. Zendle, "Ethereum crypto-games: Mechanics, prevalence, and gambling similarities," in *Proceedings of the annual symposium on computer-human interaction in play*, 2019, pp. 379–389.
- [213] CryptoKitties. [Online]. Available: <https://www.cryptokitties.co/>
- [214] Axie Infinity. [Online]. Available: <https://axieinfinity.com/>
- [215] Pixels. [Online]. Available: <https://www.pixels.xyz/>
- [216] MATRIX. [Online]. Available: <https://matr1x.io/>
- [217] Apeiron. [Online]. Available: <https://apeironnft.com/>
- [218] Wreck League. [Online]. Available: <https://wreckleague.xyz/>
- [219] Treeverse. [Online]. Available: <https://treeverse.net/>
- [220] Dark Forest. [Online]. Available: <https://zkga.me/>
- [221] Y. Lee, C. Moon, H. Ko, S.-H. Lee, and B. Yoo, "Unified representation for xr content and its rendering method," in *Proceedings of the 25th International Conference on 3D Web Technology*, 2020, pp. 1–10.
- [222] V. T. Truong, L. Le, and D. Niyato, "Blockchain meets metaverse and digital asset management: A comprehensive survey," *Ieee Access*, vol. 11, pp. 26 258–26 288, 2023.
- [223] The Sandbox Game. [Online]. Available: <https://www.sandbox.game/>
- [224] K. Dempsey, V. Pillitteri, C. Baer, R. Niemeyer, R. Rudman, and S. Urban, "Assessing information security continuous monitoring (iscm) programs: Developing an iscm program assessment," National Institute of Standards and Technology, Tech. Rep., 2020.
- [225] M. Juodis, E. Filatovas, and R. Paulavičius, "Overview and empirical analysis of wealth decentralization in blockchain networks," *ICT Express*, 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2405959524000079>
- [226] Quality of service. Accessed on 11/12/2024. [Online]. Available: https://en.wikipedia.org/wiki/Quality_of_service
- [227] M. Shen, Z. Tan, D. Niyato, Y. Liu, J. Kang, Z. Xiong, L. Zhu, W. Wang, and X. Shen, "Artificial intelligence for web 3.0: A comprehensive survey," *ACM Computing Surveys*, vol. 56, no. 10, pp. 1–39, 2024.
- [228] S. M. H. Bamakan, A. Motavali, and A. Babaei Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Systems with Applications*, vol. 154, p. 113385, 2020.
- [229] Measuring success in web3: Performance metrics for the decentralized internet revolution. Accessed on 11/12/2024. [Online]. Available: <https://www.linkedin.com/pulse/measuring-success-web3-performance-metrics-decentralized-internet/>
- [230] C. Melo, F. Oliveira, J. Dantas, J. Araujo, P. Pereira, R. Maciel, and P. Maciel, "Performance and availability evaluation of the blockchain platform hyperledger fabric," *The Journal of Supercomputing*, vol. 78, no. 10, pp. 12 505–12 527, Jul. 2022. [Online]. Available: <https://doi.org/10.1007/s11227-022-04361-2>
- [231] High availability. (Accessed on 17/05/2024). [Online]. Available: https://en.wikipedia.org/wiki/High_availability
- [232] Deciding what level of availability you need. (Accessed on 21/04/2024). [Online]. Available: <https://www.ibm.com/docs/en/i/7.5?topic=roadmap-deciding-what-level-availability-you-need>
- [233] I. Keskin and G. Soykan, "Reliability, availability, and life-cycle cost (lcc) analysis of combined cooling, heating and power (cchp) integration to data centers considering electricity and cooling supplies," *Energy Conversion and Management*, vol. 291, p. 117254, 2023. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0196890423006003>
- [234] J. Benet, "Ipfis-content addressed, versioned, p2p file system," *arXiv preprint arXiv:1407.3561*, 2014.
- [235] S. K. Lo, X. Xu, M. Staples, and L. Yao, "Reliability analysis for blockchain oracles," *Computers & Electrical Engineering*, vol. 83, p. 106582, 2020. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0045790619316179>
- [236] S. K. Dwivedi, R. Amin, and S. Vollala, "Blockchain-based secured ipfs-enable event storage technique with authentication protocol in vanet," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 12, pp. 1913–1922, 2021.
- [237] what is latency. (Accessed on 30/05/2024). [Online]. Available: <https://www.cloudflare.com/learning/performance/glossary/what-is-latency/>
- [238] what is latency. (Accessed on 21/04/2024). [Online]. Available: <https://www.ibm.com/topics/latency>
- [239] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems (TOCS)*, vol. 20, no. 4, pp. 398–461, 2002.
- [240] Z. Liu, Y. Xiang, J. Shi, P. Gao, H. Wang, X. Xiao, B. Wen, Q. Li, and Y.-C. Hu, "Make web3.0 connected," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 5, pp. 2965–2981, May 2022.
- [241] G. Xu, Y. Liu, and P. W. Khan, "Improvement of the dpos consensus mechanism in blockchain based on vague sets," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4252–4259, 2020.
- [242] Q. Hu, B. Yan, Y. Han, and J. Yu, "An improved delegated proof of stake consensus algorithm," *Procedia Computer Science*, vol. 187, pp. 341–346, 2021, 2020 International Conference on Identification, Information and Knowledge in the Internet of Things, IIKI2020. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1877050921009133>
- [243] S. Wu, Z. Song, P. Wei, P. Tang, and Q. Yuan, "Improving privacy of anonymous proof-of-stake protocols," in *International Conference on Cryptology and Network Security*. Springer, 2023, pp. 368–391.
- [244] T. Wang, Q. Wang, Z. Shen, Z. Jia, and Z. Shao, "Understanding characteristics and system implications of dag-based blockchain in iot environments," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14 478–14 489, 2021.
- [245] L. Zhang, H. Xu, O. Onireti, M. A. Imran, and B. Cao, "How much communication resource is needed to run a wireless blockchain network?" *IEEE Netw.*, vol. 36, no. 1, pp. 128–135, 2021.
- [246] DappRadar. (Accessed on 22/05/2024). [Online]. Available: <https://dappradar.com/>
- [247] What is Decentralization in Blockchain? (Accessed on 11/04/2024). [Online]. Available: <https://aws.amazon.com/blockchain/decentralization-on-blockchain>
- [248] J. Zheng and D. K. C. Lee, "Understanding the evolution of the internet: Web 1.0 to web3. 0, web3 and web 3," *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*, 2023.
- [249] A. M. Gomez-Trujillo, J. Velez-Orcampo, and M. A. Gonzalez-Perez, *Trust, Transparency, and Technology: Blockchain and Its Relevance in the Context of the 2030 Agenda*. Cham: Springer International Publishing, 2021, pp. 561–580. [Online]. Available: https://doi.org/10.1007/978-3-030-42412-1_28
- [250] O. Rikken, M. Janssen, and Z. Kwee, "Governance challenges of blockchain and decentralized autonomous organizations," *Information Policy*, vol. 24, no. 4, pp. 397–417, 2019.
- [251] T. Dursun and B. B. Üstündağ, "A novel framework for policy based on-chain governance of blockchain networks," *Information Processing & Management*, vol. 58, no. 4, p. 102556, 2021. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0306457321000601>
- [252] W. Reijers, I. Wuisman, M. Mannan, P. De Filippi, C. Wray, V. Rae-Looi, A. Cubillos Vélez, and L. Orgad, "Now the code runs itself: On-chain and off-chain governance of blockchain technologies," *Topoi*, vol. 40, pp. 821–831, 2021.
- [253] S. Cao, T. Miller, M. Foth, W. Powell, X. Boyen, and C. Turner-Morris, "Integrating on-chain and off-chain governance for supply chain transparency and integrity," *CoRR*, vol. abs/2111.08455, 2021. [Online]. Available: <https://arxiv.org/abs/2111.08455>
- [254] N.-P. Chen, K.-Y. Shen, and C.-J. Liang, "Hybrid decision model for evaluating blockchain business strategy: A bank's perspective," *Sustainability*, vol. 13, no. 11, p. 5809, 2021.
- [255] S. King and S. Nadal, "Pcoin: Peer-to-peer crypto-currency with proof-of-stake," *self-published paper*, August, vol. 19, no. 1, 2012.
- [256] L. Shi, T. Wang, J. Li, S. Zhang, and S. Guo, "Pooling is not favorable: Decentralize mining power of pow blockchain using age-of-work," *IEEE Transactions on Cloud Computing*, vol. 11, no. 3, pp. 2756–2769, 2023.

- [257] H. Pervez, M. Muneeb, M. U. Irfan, and I. U. Haq, "A comparative analysis of dag-based blockchain architectures," in *2018 12th International conference on open source systems and technologies (ICOSST)*. IEEE, 2018, pp. 27–34.
- [258] M. Yin, D. Malkhi, M. K. Reiter, G. G. Gueta, and I. Abraham, "Hot-stuff: Bft consensus with linearity and responsiveness," in *Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing*, 2019, pp. 347–356.
- [259] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, V. Sassone *et al.*, "Pbft vs proof-of-authority: Applying the cap theorem to permissioned blockchain," in *CEUR workshop proceedings*, vol. 2058. CEUR-WS, 2018.
- [260] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y," *ACM SIGMETRICS Performance Evaluation Review*, vol. 42, no. 3, pp. 34–37, 2014.
- [261] D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus," *Stellar Development Foundation*, vol. 32, pp. 1–45, 2015.
- [262] bitnodes. (Accessed on 15/04/2024). [Online]. Available: <https://bitnodes.io>
- [263] etherscan. (Accessed on 18/04/2024). [Online]. Available: <https://etherscan.io/nodetracker>
- [264] blockchair. (Accessed on 12/05/2024). [Online]. Available: <https://blockchair.com/nodes>
- [265] bscscan. (Accessed on 11/05/2024). [Online]. Available: <https://bscscan.com/nodetracker>
- [266] M. Goldberg and F. Schär, "Metaverse governance: An empirical analysis of voting within decentralized autonomous organizations," *Journal of Business Research*, vol. 160, p. 113764, 2023. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0148296323001224>
- [267] S. Rahman, I. M. Siddique, and E. D. Smith, "Analyzing bitcoin's decentralization: Coefficient of variation approach and 21 million divisibility," *Advancement of IoT in Blockchain Technology and its Applications*, vol. 2, no. 3, pp. 8–17, 2023.
- [268] Quantifying Decentralization. (Accessed on 01/04/2024). [Online]. Available: <https://news.earn.com/quantifying-decentralization-e39db233c28e>
- [269] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Computing Surveys (CSUR)*, vol. 52, no. 3, pp. 1–34, 2019.
- [270] H. Wang, T. Wang, L. Shi, N. Liu, and S. Zhang, "A blockchain-empowered framework for decentralized trust management in internet of battlefield things," *Computer Networks*, vol. 237, p. 110048, 2023. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1389128623004930>
- [271] J. Leng, M. Zhou, J. L. Zhao, Y. Huang, and Y. Bian, "Blockchain security: A survey of techniques and research directions," *IEEE Trans. Service Comput.*, vol. 15, no. 4, pp. 2490–2510, Nov. 2020.
- [272] C. Liu, H. Liu, Z. Cao, Z. Chen, B. Chen, and B. Roscoe, "Reguard: finding reentrancy bugs in smart contracts," in *Proceedings of the 40th International Conference on Software Engineering: Companion Proceedings*, ser. ICSE '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 65–68. [Online]. Available: <https://doi.org/10.1145/3183440.3183495>
- [273] C. F. Torres, J. Schütte, and R. State, "Osiris: Hunting for integer bugs in ethereum smart contracts," in *Proceedings of the 34th Annual Computer Security Applications Conference*, ser. ACSAC '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 664–676. [Online]. Available: <https://doi.org/10.1145/3274694.3274737>
- [274] J. R. Douceur, "The sybil attack," in *Peer-to-Peer Systems*, P. Druschel, F. Kaashoek, and A. Rowstron, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 251–260.
- [275] Hack3d: The Web3 Security Report 2023. (Accessed on 15/05/2024). [Online]. Available: <https://indd.adobe.com/view/1f5aebc9-648a-451c-abd9-d3b471840d4d>
- [276] A brief introduction to the security level standards for web3 accounts. (Accessed on 09/03/2024). [Online]. Available: https://medium.com/@tinyverse_space/a-brief-introduction-to-the-security-level-standards-for-web3-accounts-705251fbba7
- [277] S. Zhang and J.-H. Lee, "Double-spending with a sybil attack in the bitcoin decentralized network," *IEEE transactions on Industrial Informatics*, vol. 15, no. 10, pp. 5715–5722, 2019.
- [278] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Applied sciences*, vol. 9, no. 9, p. 1788, 2019.
- [279] W. Li, S. Andreina, J.-M. Bohli, and G. Karame, "Securing proof-of-stake blockchain protocols," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, J. Garcia-Alfaro, G. Navarro-Arribas, H. Hartenstein, and J. Herrera-Joancomartí, Eds. Cham: Springer International Publishing, 2017, pp. 297–315.
- [280] C. Marforio, A. Francillon, and S. Capkun, "Application collusion attack on the permission-based security model and its implications for modern smartphone systems," ETH Zurich, Tech. Rep., 2011.
- [281] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey," *IEEE Access*, vol. 8, pp. 16 440–16 455, 2020.
- [282] W. Yang, L. Shi, H. Liang, and W. Zhang, "Trusted mobile edge computing: Dag blockchain-aided trust management and resource allocation," *IEEE Trans. Wireless Commun.*, 2023, early access, doi: 10.1109/TWC.2023.3323974.
- [283] C. Fan, S. Ghaemi, H. Khazaei, and P. Musilek, "Performance evaluation of blockchain systems: A systematic survey," *IEEE Access*, vol. 8, pp. 126 927–126 950, 2020.
- [284] J. Göbel and A. Krzesinski, "Increased block size and bitcoin blockchain dynamics," in *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, 2017, pp. 1–6.
- [285] C. Schwarz-Schilling, J. Neu, B. Monnot, A. Asgaonkar, E. N. Tas, and D. Tse, "Three attacks on proof-of-stake ethereum," in *Financial Cryptography and Data Security*, I. Eyal and J. Garay, Eds. Cham: Springer International Publishing, 2022, pp. 560–576.
- [286] M. Cao, H. Wang, T. Yuan, K. Xu, K. Lei, and J. Wang, "Meta-regulation: Adaptive adjustment to block size and creation interval for blockchain systems," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 12, pp. 3702–3718, 2022.
- [287] M. Brandenburger, C. Cachin, R. Kapitza, and A. Sorniotti, "Blockchain and trusted computing: Problems, pitfalls, and a solution for hyperledger fabric," *arXiv preprint arXiv:1805.08541*, 2018.
- [288] P. Howson, "Tackling climate change with blockchain," *Nature Climate Change*, vol. 9, no. 9, pp. 644–645, 2019.
- [289] C. Zhou, H. Chen, S. Wang, X. Sun, A. El Saddik, and W. Cai, "Harnessing web3 on carbon offset market for sustainability: Framework and a case study," *IEEE Wireless Communications*, vol. 30, no. 5, pp. 104–111, 2023.
- [290] V. Kohli, S. Chakravarty, V. Chamola, K. S. Sangwan, and S. Zeadally, "An analysis of energy consumption and carbon footprints of cryptocurrencies and possible solutions," *Digital Commun. Networks*, vol. 9, no. 1, pp. 79–89, 2023.
- [291] Cambridge Bitcoin Electricity Consumption Index. (Accessed on 01/05/2024). [Online]. Available: <https://ccaf.io/cbnsi/cbeci>
- [292] C. Ferreira Torres, F. Willi, and S. Shinde, "Is your wallet snitching on you? an analysis on the privacy implications of web3," in *Proceedings of the 32nd USENIX Security Symposium*, J. Calandrino and C. Troncoso, Eds. Berkeley, CA: USENIX Association, 2023, Conference Paper, pp. 769 – 786, 32nd USENIX Security Symposium (USENIX Security 2023); Conference Location: Anaheim, CA, USA; Conference Date: August 9–11, 2023.
- [293] R. Rezaei, T. K. Chiew, S. P. Lee, and Z. Shams Aliee, "Interoperability evaluation models: A systematic review," *Computers in Industry*, vol. 65, no. 1, pp. 1–23, 2014. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0166361513001887>
- [294] P. Xia, J. Li, L. Shi, B. Cao, W. Tan, J. Weng, Y. Liu, and Z. Han, "A reputation-aided lightweight consensus service framework for multi-chain metaverse," *IEEE Netw.*, 2024, early access, doi: 10.1109/MNET.2024.3382346.
- [295] T. Li, C. Yang, Q. Yang, S. Lan, S. Zhou, X. Luo, H. Huang, and Z. Zheng, "Metaopera: A cross-metaverse interoperability protocol," *IEEE Wireless Communications*, vol. 30, no. 5, pp. 136–143, 2023.
- [296] J. BAHKKE and R. Thomas, "Towards the next technological transition: Commission presents EU strategy to lead on Web 4.0 and virtual worlds," European Commission, Strasbourg, Tech. Rep., 2023. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3718
- [297] European Parliament and Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council. [Online]. Available: <https://data.europa.eu/eli/reg/2016/679/oj>
- [298] Information Commissioner's Office, "Regulatory Sandbox," 2023. [Online]. Available: <https://ico.org.uk/for-organisations/advice-and-services/regulatory-sandbox/>
- [299] FCA, "Regulatory Sandbox," *George Washington Law Review*, vol. 87, no. 3, pp. 579–645, 2015.
- [300] Nation3. (2024) <https://nation3.org/manifeto>. Accessed on 01/06/2024. [Online]. Available: <https://nation3.org/manifeto>



Bin Cao (Senior Member, IEEE) is a full professor in the State Key Laboratory of Networking and Switching Technology at Beijing University of Posts and Telecommunications (BUPT). He received his Ph.D. degree (Honors) in communication and information systems from the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China (UESTC) in 2014. He was a research fellow at the National University of Singapore from July 2015 to July 2016. He

serves/served as numerous Associate/Guest Editors and coauthors for IEEE transactions/magazine/journal/conference. He is the Founding Vice Chair of Special Interest Group on Wireless Blockchain Networks in IEEE Cognitive Networks Technical Committee. He received the IEEE Outstanding Leadership Award in 2020, the IEEE TEMS Mid-Career Award in 2021, the Best Paper Award at IEEE BMSB 2021, IEEE IoTJ 2022, DCN 2023 and IEEE AIoT 2024. He is ranked as the World's Top 2% most-cited scientists by Stanford University and has published many ESI Hot/Highly Cited Papers. His research interest are wireless communications, network protocol, parallel and distributed system.



Taotao Wang (Member, IEEE) received the Ph.D. degree in information engineering from The Chinese University of Hong Kong (CUHK) in 2015. From 2015 to 2016, he was a postdoc research fellow at the Institute of Network Coding (INC) of CUHK. He is currently a tenured associate professor at the College of Electronics and Information Engineering, Shenzhen University (SZU). He was the recipient of the Hong Kong PhD Fellowship Scheme award in 2011. He received the Star of Tomorrow award (excellent intern) at the Microsoft Research Asia

in 2012. He received the Excellent Reviewer Award from the journal of IEEE Wireless Communications Letters in 2016. He was the recipient of the Best Paper Award (Runner-up) and the Best Student Paper Award of IEEE CPSCOM 2021. He has been awarded the winner prize of the ScalingX Zero-Knowledge Hackathon and the silver prize of Hong Kong Web 3.0 Innovation Hackathon in 2023. He has served as a member of the technical committee of IEEE CIC ICC 2019 and IEEE ICC 2020, an associate editor of IEEE TENCON 2020, the symposia chair of IEEE WOCC 2022, and the workshop co-chair of IEEE TrustCom 2025. He has co-authored over 100 research papers and holds more than 10 patents. His research interests include blockchain and web 3.0, trusted AI, wireless networking and communications.



Shaohu Xiao is currently pursuing the M.Eng. degree in information and communication engineering with the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications. Her research interests include blockchain and federated learning.



Jinyu Chen is currently pursuing the Ph.D. degree in Information and communication Engineering at the School of Electronic and Optical Engineering, Nanjing University of Science and Technology. His research interests cover distributed storage systems, cache optimization, and AI-driven storage architecture.



Jiaheng Wang (M'10–SM'14) received the Ph.D. degree in electronic and computer engineering from the Hong Kong University of Science and Technology, Kowloon, Hong Kong, in 2010, and the B.E. and M.S. degrees from the Southeast University, Nanjing, China, in 2001 and 2006, respectively.

He is currently a Full Professor at the National Mobile Communications Research Laboratory (NCRL), Southeast University, Nanjing, China. He is also with Purple Mountain Laboratories Nanjing, China. From 2010 to 2011, he was with the Signal Processing Laboratory, KTH Royal Institute of Technology, Stockholm, Sweden. He also held visiting positions at the Friedrich Alexander University Erlangen-Nürnberg, Nürnberg, Germany, and the University of Macau, Macau. His research interests are mainly on communication systems, wireless networks and network security.

Dr. Wang has published more than 200 articles on international journals and conferences. He serves as an Associate Editor for the IEEE Transactions on Wireless Communications and an Associate Editor for the IEEE Transactions on Communications. He was a Senior Area Editor for the IEEE Signal Processing Letters. He was a recipient of the Humboldt Fellowship for Experienced Researchers and the best paper awards of IEEE GLOBECOM 2019, ADHOCNETS 2019, and WCSP 2022 and 2014.



Long Shi (Senior Member, IEEE) received the Ph.D. degree in Electrical Engineering from the University of New South Wales, Sydney, Australia, in 2012. From 2013 to 2016, he was a Postdoctoral Fellow at the Institute of Network Coding, Chinese University of Hong Kong, China. From 2014 to 2017, he was a Lecturer at Nanjing University of Aeronautics and Astronautics, Nanjing, China. From 2017 to 2020, he was a Research Fellow at the Singapore University of Technology and Design. Now he is a Professor at the School of Electronic and Optical Engineering,

Nanjing University of Science and Technology, Nanjing, China. His research interests include wireless communications, decentralized security, and edge intelligence. He is serving as an editor of IEEE Transactions on Cognitive Communications and Networking.



Xintong Ling (S'15–M'18) is currently an Associate Professor with the National Mobile Communications Research Laboratory, Southeast University, and also with the Purple Mountain Laboratories, Nanjing. He received the B.E. and Ph.D. degrees in electrical engineering from Southeast University, Nanjing, China, in 2013 and 2018, respectively. His current research interests focus on future generation wireless communications, including distributed systems, blockchain technologies, wireless networking, and signal processing. He was selected in Young

Elite Scientists Sponsorship Program by China Association for Science and Technology.



Hao Xu (Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Glasgow. He is currently an Assistant Professor with the College of Electronics and Information Engineering, Tongji University. His research interests include wireless communication, wireless blockchain, consensus, and blockchain-enabled radio access networks. He actively contributes to standardization efforts as a Rapporteur in ETSI and O-RAN Alliance, where he drives technical reports and specifications for next-generation wireless systems.

He has served as a workshop organizer (e.g., FCN, IEEE WF-IoT) and invited speaker at industry forums, bridging academic research with industrial deployment.



Shengli Zhang (Senior Member, IEEE) received the B.Eng. and M.Eng. degrees in electronic engineering and communication and information engineering from the University of Science and Technology of China (USTC), Hefei, China, in 2002 and 2005, respectively, and the Ph.D. degree in information engineering from the Chinese University of Hong Kong (CUHK) in 2008. He is currently a Full Professor and Vice Dean of the College of Electronic and Information Engineering at Shenzhen University, where he also serves as the Executive Deputy

Director of the Blockchain Research Center. From 2014 to 2015, he was a Visiting Associate Professor at Stanford University. Prof. Zhang is the pioneer of physical-layer network coding (PNC) and has published over 200 IEEE top journal and ACM conference papers. His research interests include blockchain, physical-layer network coding, and wireless networks. He has served as an Editor for IEEE TVT, IEEE WCL, and IET Communications and as a TPC member for several IEEE conferences. He has received numerous awards, including the ACM Mobihoc Best Demonstration Award and the China Communications Society Natural Science Award.