Web3 Technologies: Challenges and Opportunities

Weikang Liu, Bin Cao, and Mugen Peng

Abstract

Different from "read" based Web1 and "read-write" based Web2, "read-write-own" based Web3 is proposed as a typical user-centric Internet to open the new generation of the World Wide Web. Web3 is the internet religious fundamentalism for data rights owned by users based on identity, data, network, and service, which requires the support of full-process data protection provided by a zero-trust and zero-touch environment. However, as to the traditional layered architecture like TCP/IP, data protection is an overlaid function, which is far away from the full-process data protection requirements. To this end, in order to build a zero-trust and zero-touch environment, a Web3 architecture is presented in this article as a promising paradigm. Meanwhile, the key principles for Web3 architecture designing are discussed, covering interoperability and interpretability of data, trustworthiness throughout network lifecycle, incentive for collaboration and sharing, and human-centric experience. Moreover, in order to achieve these principles, four aspects of enabling technologies are presented, including semantic, incentive, decentralized, and spatial technologies. Finally, some main challenges and open issues are also identified as a future direction for further work.

Introduction

Including the portal websites of early Sina, MySpace, and LiveJournal, the first generation of web technology, Web1, allows users to browse the static pages of text and images passively. In order to overcome the read-only limitation, the current generation, Web2, has enabled users to create and share their content for interactivity. In recent years, as mobile wireless technology advances, interactivity based on Web2 has become ubiquitous, leading to an explosive amount of user-generated data and spawning many successful platforms, such as Youtube, Facebook, Google, etc. While facilitating interaction with the entire world anytime, anywhere, and in any form, Web2 has also brought about a worrying status quo, where various platforms fully control the identities and data of users. Meanwhile, the independent identity and data management in different platforms also contributes to the problem of data island. Notably, these mentioned problems are rooted in the centralized model where Web2 platforms are third-party intermediaries for the exchange of information. In other words, with the development of Web2, internet religious fundamentalism, "it is for everyone," claimed by Tim BernersLee, has been far away from the root. As a result, platforms are opaque in this model, data operations cannot be regulated, and data security cannot be guaranteed, which may cause adverse social influence. For example, the data breach of Facebook is believed to have influenced the 2016 U.S. presidential election.

Figure 1 illustrates the evolution of Web1, Web2, and Web3. Different from "read" based Web1 and "read-write" based Web2, which is content-centric, "read-write-own" based Web3 is user-centric, where data does not rest with platforms. However, it makes no sense to consider data owned by users apart from multi-party collaborative environments. Therefore, as shown in Fig. 2, when considering whether the user owns the data, the following three factors should be considered: explicit sovereignty, well-defined responsibilities, and an environment that stimulates multi-party participation. The first relies on the combination of trust data and identities, while the second and third require the support of trust networks and services. Trust identities are generated and managed locally by users, and it can be used across various applications. It is the basis of data owned by the user. Trust data can be transferred to different applications with the user's permission, thus breaking down the problem of data island. In trust networks and services, malicious programs can be prevented from being set up to cause unreasonable data usage and value allocation. The construction of these four trust elements needs the support of a zero-trust and zero-touch environment. By adopting the concept of zero trust, no identity, data, network, or service will be pre-assigned static and coarse-grained privileges, thereby increasing the cost and reducing the temptation to do evil [1]. Zero-touch network and service management enables selfmonitoring, self-healing, and self-optimization without human intervention [2]. It can help the zero-trust concept to achieve continuous and automatic inspecting of all network behaviors, thus providing indicators for timely and dynamic adjustment of privileges.

Recently, much attention has been paid to Web3-based applications, including decentralized applications (Dapps), decentralized autonomous organizations (DAOs), and other related activities. In [3], a Dapp for crowdsourcing named

Weikang Liu and Mugen Peng are with the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China; Bin Cao (corresponding author) is with the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China, and also with the Zhejiang Lab, HangZhou 311121, China.

Digital Object Identifier: 10.1109/MNET.2023.3321546
Date of Current Version: 30 May 2024
Date of Publication: 6 October 2023

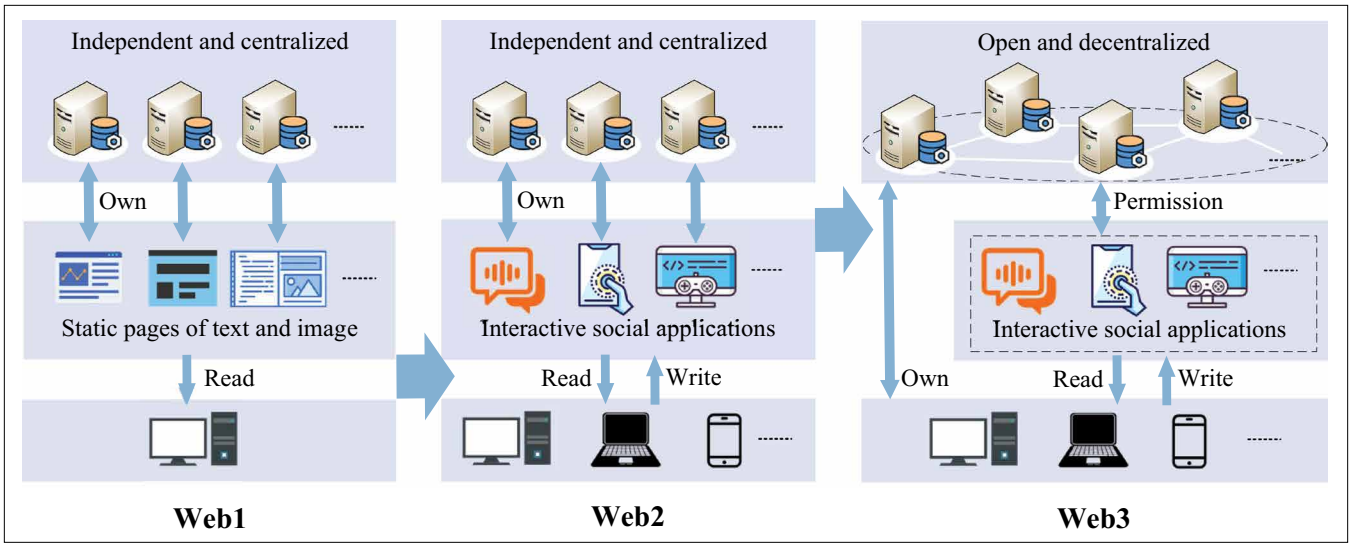

FIGURE 1. Evolution of Web1, Web2, and Web3.

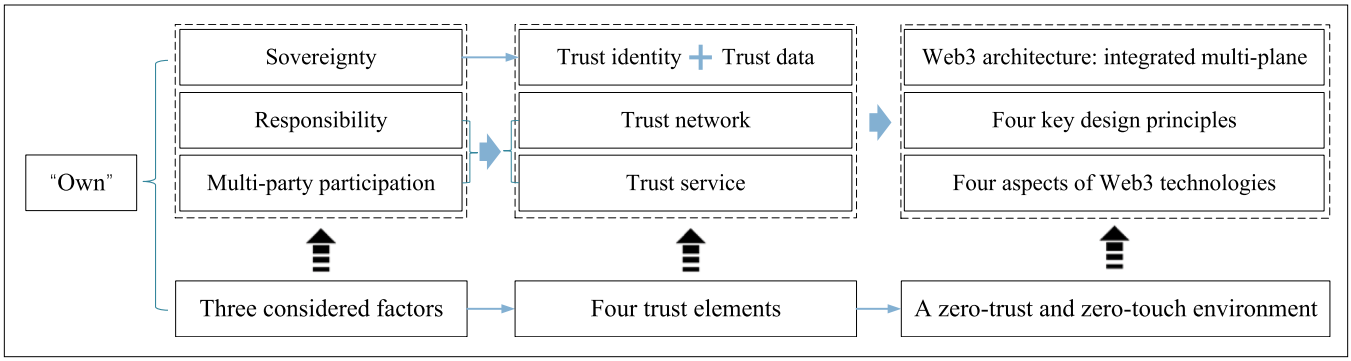

FIGURE 2. Road map for Web3.

CrowdBC has been conceptualized and implemented on the Ethereum network. The concept of DAO is introduced, and the main software platforms, as well as visualization tools for DAOs activity, are reviewed in [4]. To the best of our knowledge, no published work has been done to detail how to build a zero-trust and zero-touch environment for Web3. In addition, most of the current so-called Web3 activities rely on centralized platforms or entities like OpenSea, Coinbase, Binance, and so on, making it inherit the limitations of Web2. For example, digital assets of the Russian DAO users still can be violated. Then, to construct Web3 formally, we are inspired to provide a comprehensive discussion on its architecture and enabling technologies in this article.

The remainder of this article is organized as follows. In Section II, the proposed Web3 architecture is introduced in terms of its composed five planes. Section III provides the key principles to consider when designing this architecture. The enabling technologies to support these principles are discussed following that. Future challenges and open issues are presented in Section V. Finally, Section VI concludes this work and discusses future trends.

Web3 Architecture

A zero-trust and zero-touch environment can provide realtime data protection throughout the entire network process, thereby supporting the construction of the four trust elements, which are crucial for data rights to be owned by users. Fullprocess data protection requires the deployment of cross-layer functionalities. However, the traditional layered architecture like 5-layer TCP/IP is not conducive to deploying cross-layer functionalities, leaving data protection as its overlay [1]. To build a zero-trust and zero-touch environment for Web3, it is necessary to reorganize the architecture to provide hierarchical extensibility from top to down. Therefore, we are motivated to propose a Web3 architecture, which integrated multi-plane. Illustrated in Fig. 3, the proposed architecture consists of five interdependent planes: Application-as-a-Service (AaaS) plane, Artificial-Intelligence-as-a-Service (AIaaS) plane, Data-as-aService (DaaS) plane, Blockchain-as-a-Service (BaaS) plane, and Infrastructure-as-a-Service (IaaS) plane. The design of these five layers adheres to four key principles, and making this architecture align with them relies on four aspects of enabling technologies.

AaaS Plane

It is the top plane and provides users with applications and services in the form of web pages, mobile applications, etc. To avoid centralized dominance and facilitate censorship, they are deployed and managed in a decentralized manner. For example, front-end codes can be stored in decentralized storage systems on the DaaS plane,

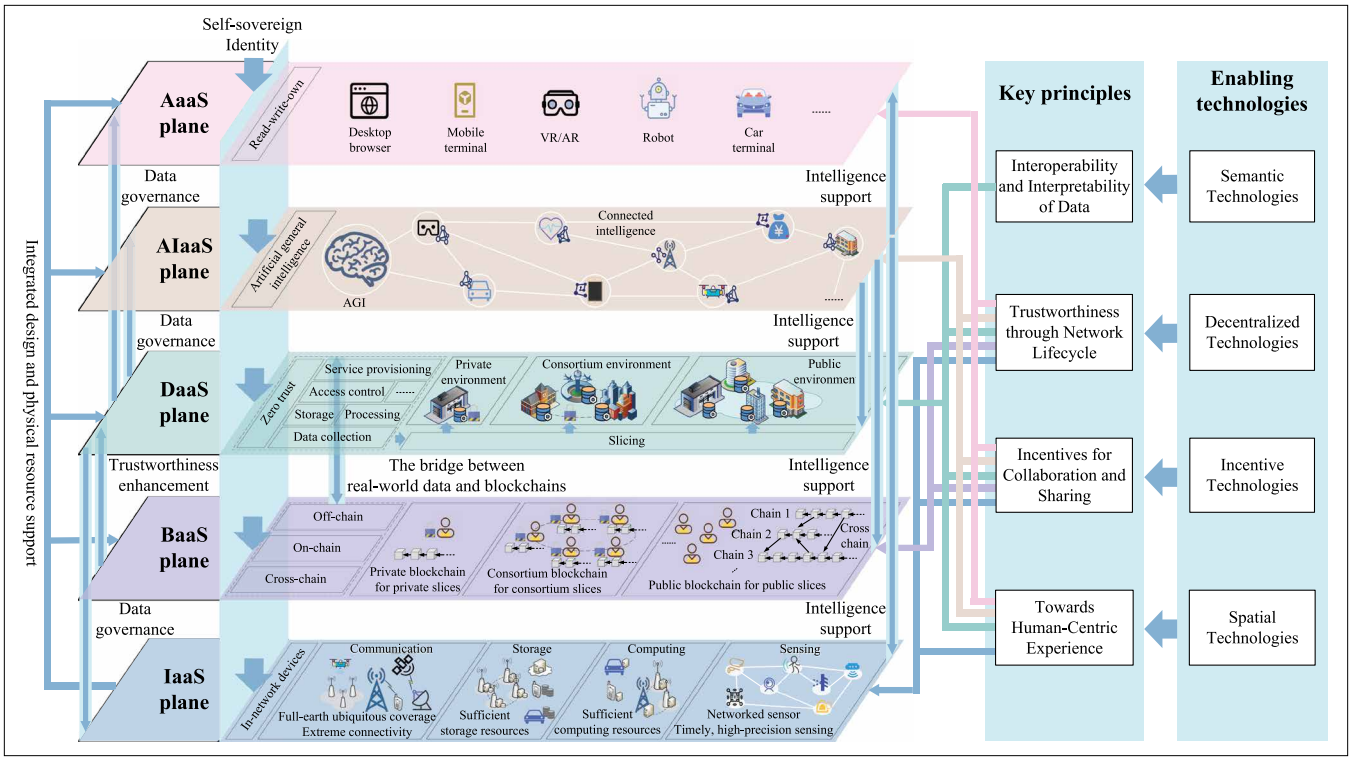

FIGURE 3. Web3 architecture.

such as Inter Planetary File System, SWARM, and so forth. Through the front-end interfaces, users can invoke the back-end program to create and manage Self-sovereign Identity (SSI), conduct decentralized transactions, earn profits, and write data into different storage systems as needed. It is worth emphasizing that SSI is completely controlled by the user, independent of specific applications and services [5]. Once created, it can be reused in any application or service on all five planes. Meanwhile, data tied to it can also be used in any authorized application and service. Till now, many related standards have been specified for implementing SSI and public key infrastructure in a decentralized manner, such as Decentralized Identifiers and Verifiable Credentials by the World Wide Web Consortium, Decentralized Key Management System by OASIS and Hyperledger, and so on. However, their deployment is still in the prototype stage.

AIaaS Plane

This plane determines the zero-touch characteristic of Web3. Based on the resource support of the DaaS and IaaS planes, its primary responsibility is to provide guidance for user configuration and operation, and to act as an engine for various zero-touch services on different planes. Aiming to achieve data ownership by users in multi-party collaborative environments, Web3 can finally break down the problem of data island. Then, it would be more conducive to data collection and sharing than Web2, which is essential to provide strong support for AI. In Web2, AI is confined to various domains and can only make decisions in a specific domain or task set. For example, AI for joint source and channel coding cannot be applied to resource allocation. However, in Web3, AI can break down domain boundaries based on easier access to data from different domains, thus making it possible to evolve toward artificial general intelligence (AGI). Meanwhile, data sinking from cloud to edge will facilitate the evolution of AI from centralized in-cloud learning to distributed ondevice learning, which will be of great importance for building connected intelligence in 6G. Including federated learning (FL), swarm learning, and split learning, many distributed learning architectures have been proposed and are believed to be better developed in Web3 for privacy protection.

DaaS Plane

This plane determines the zero-trust characteristic of Web3. While providing zero-trust data governance for the AaaS, AIaaS and IaaS planes, it also relies on the functional support of other planes, such as the intelligence support of the AIaaS plane, the trustworthiness enhancement of the BaaS plane, and the physical resource support of the IaaS plane. In Web3, data sinking from cloud to edge and owned by users would expose data to shifting perimeters, thereby reducing the importance of network perimeters in the security posture. To protect data regardless of location, this plane should be open, scalable, and independent of a particular platform, enabling the creation of slices for private, consortium, and public environments. This open environment makes it difficult for traditional perimeterbased security model to provide protection for Web3, and integrate support for various data regulations like the General Data Protection Regulation, etc. In response to this problem, Kindervag [6] has proposed the Zero Trust Model (ZTM) that focuses on users, assets, and resources rather than static perimeters. Its core principle is "verify and never trust," and it is expected to be used in Web3 to provide

security for the entire data lifecycle, covering data collection, data processing, data storage, data access, data service provisioning, and so on. Specifically, Web3 participants will assume no implicit trust, and will continuously analyze network traffic, inspect visitor behaviors, evaluate potential risks, and enact timely protections.

BaaS Plane

Blockchain offers a conceptual framework and approaches to establish distributed trust and address the free rider problem and Sybil attacks. Integrating various blockchain technologies, this plane aims to enhance the security and trustworthiness of data across and within slices in the DaaS plane. According to different read and write permissions required by slices, different blockchains can be used, such as private, consortium, and public blockchains. Private blockchains can be used in the slices created by a single organization or entity to improve data security, consortium blockchains can facilitate data sharing and value circulation in the slices created by an alliance, and public blockchains can provide data consistency and trustworthiness for the slices that are open to the public. Furthermore, many on-chain technologies are available to improve the blockchain running on slices, to accommodate their differentiated needs in scalability, security, and decentralization. Meanwhile, many cross-chain technologies have been proposed for blockchain interoperability, and can be used to enable value and data transfer between different slices. To bridge the trust gap between blockchains and the external world, many off-chain technologies have been proposed and can be used to consistently bind other storage systems in the DaaS plane to blockchains.

IaaS Plane

As the foundation of the above four planes, IaaS is made up of a collection of physical facilities to provide the communication, computing, and storage resources needed for the other four planes in Web3. In Web2, services are deployed on the network in an over-the-top (OTT) manner, and then the heterogeneous data needs to be aggregated to service providers for analysis and decision-making. This out-of-network framework makes the response occur above the network, and thus cannot deal with network dynamics in real time [7]. However, in order to support the reliable operations of Web3, real-time decision-making is indispensable, such as the real-time network traffic inspection and evaluation mentioned in DaaS. Fortunately, the development of in-network devices provides a way to optimize the infrastructure to implement functionalities within the network for real-time in-network decisions. With the help of in-network devices, AaaS, AIaaS, DaaS, BaaS, and IaaS planes can be integrated on demand to support native AI, native data protection, and native trustworthiness, which 6G also advocates.

Key Design Principles

In this section, we summarize the key principles to consider when designing five planes, which are

- **Interoperability and Interpretability of Data:** Due to the heterogeneity of data, diversity of data sources, and data machine-unprocessable, it would be challenging to meet the requirements of Web3 for automated and intelligent services, such as the connected intelligence mentioned in AIaaS, and the real-time network traffic inspection and evaluation mentioned in DaaS. Therefore, it is necessary to model data in a standard format for data interoperability and machine interpretability in Web3.
- **Trustworthiness Throughout Network Lifecycle:** Though blockchain lays a feasible technological foundation for solving the centralization problem and enabling transactions in trustless environments, it is not rigorous to simply assume that blockchain-based architectures can fully inherit the characteristics of blockchain. For example, OpenSea still retains the ability to remove user-uploaded non-fungible tokens (NFTs) from its homepage without requiring the user's permission. Therefore, it is necessary to consider an effective way to incorporate the design principles of blockchain into the proposed architecture for trustworthiness throughout the whole network lifecycle.
- **Incentives for Collaboration and Sharing:** Spontaneity is indispensable to the booming development of the Internet, where service providers and network operators voluntarily optimize their performance [8]. Similarly, for Web3's sustainable development, we also expect all the participants to voluntarily collaborate and share resources. However, without satisfactory compensation, participants will not interested in participating in the construction. Therefore, it is necessary to establish incentive mechanisms and corresponding business models to construct reasonable, stable and long-term collaboration and sharing.
- **Towards Human-Centric Experience:** Creating a more free and borderless environment to release the value of data and resources is the development goal of Internet. Following this goal, the ultimate vision of Web3 is to eliminate the barriers between virtuality and reality, achieving unimpeded flow of data, while providing extremely immersive and precise human-centric experience. To support the seamless reality-virtuality interaction, it is necessary to develop high-performance infrastructure capabilities and unified state description of objects in Web3.

Web3 Technologies

In order to support the summarized key design principles, this section focuses on the technologies from the following four aspects, which can help in-depth understand the features of Web3.

Semantic Technologies

Semantic Web was first envisioned by Tim Berners-Lee and is considered the earliest definition of Web3 [9]. However, it is not regarded as equivalent to Web3 in this article, but a series of technologies that can support the key principle **Interoperability and interpretability of data**. It can mainly be used in the DaaS plane. Specifically, it allows data to be processed, shared and

reused across application, entity and organization boundaries by providing a common framework, which includes the data model, taxonomies, ontologies, rules and query languages.

As the common data model used in Semantic Web, Resource Description Framework (RDF) has standardized a triplet representation to describe resources. With the help of RDF triples, webs of information about related things can be formed. Furthermore, for information machine-processable, it is essential to provide a common understanding of information between machines and humans. For this purpose, Semantic Web has specified taxonomies (such as RDF schema) and ontologies (such as Web Ontology Language OWL) to extend RDF vocabulary, where the defined semantics can be used for reasoning about the described knowledge. Meanwhile, rule languages have been standardized to supplement their knowledge representation, such as the Rule Interchange Format and the Semantic Web Rule Language. Finally, to access RDF data, a query language has been specified in the Simple Protocol and RDF Query Language for data retrieval and manipulation, relationship searching and discovery.

Enabling semantic ability on Web3 can eliminate the barrier of machines to automatically process massive Internet information at the data level, which lays the foundation for the scalability of the DaaS plane and the powerful AGI of the AIaaS plane. Moreover, in combination with the AIaaS plane, Web3 can be endowed with the ability of self-configuration, self-organization and self-adaptation, thus supporting various zero-touch services to automatically handle real-time situations [10].

Decentralized Technologies

The unprecedented success of Bitcoin shows us the ability of blockchain to build trust in a trustless and decentralized environment. The core of blockchain is following a certain rule while distrusting any user, device or traffic, which is consistent with the "verify and never trust" of ZTM. Traditional centralized model put too much trust in the central authority to follow this principle, and cannot meet the requirement of Web3. Fortunately, many decentralized technologies have been proposed to ensure the security, privacy and ownership of personal data, which can be used in Web3 to support the key principle **Trustworthiness throughout network lifecycle**. The following will introduce these technologies from the perspective of identity and data.

First, true control of identities is the prerequisite for users to own their data. To return its control to users, SSI has been proposed to enable users to create, verify and manage their identifiers in a decentralized manner without trusting third parties. Furthermore, in the proposed Web3 architecture, SSI is expected to become globally unique identities throughout the communication network from access, transport, storage to computing. Such a design is essential for Web3 to evaluate the comprehensive trust degree of users, but is challenging to implement due to the reliance on cross-industry and cross-domain collaboration, as well as the dependency on still evolving decentralized technologies like blockchain.

Next, the following will introduce the decentralized technologies related to data from four aspects: sensing, communication, computing, and storage. (i) Sensing: communication systems with wireless sensing capabilities, as well as a wide variety of large-scale deployed sensing devices, will provide high-volume multi-dimensional sensing data about physical worlds [11]. Based on such large and redundant data, the influence of malicious data can be eliminated by comparison and analysis, thus laying the foundation for data veracity. (ii) Communication: user-centric networks (UCNs) have been proposed to facilitate the transition from "network" to "my network", which is user-definable, user-configurable, and user-controllable [11]. Decentralized and interconnected UCNs will enable users to own their generated data and control how it is used and spread in digital worlds, thereby eliminating the potential for data misuse by centralized service providers. (iii) Computing: decentralized Software-Defined-Network paradigm can be used to abstract the shared underlying infrastructure and programmatically create cost-efficient slices for users on demand [12]. Open source software, as well as AGI in the AIaaS plane can guide and help users manipulate and manage their slices. Many privacy-preserving technologies can be used to protect data from being compromised, when they needs to be aggregated or interacted to realize data utility. Related technologies are cryptographic techniques (such as homomorphic encryption, secure multi-party computation, zero-knowledge proof), perturbative technologies (such as differential privacy), and anonymization technologies [13]. (iv) Storage: according to differentiated requirements, centralized and distributed storage systems of the DaaS plane, as well as different types of blockchains of the BaaS plane, can be used to support the slices.

Based on the synergy of these decentralized technologies, Web3 will be an open, decentralized, and user-centric web that is invulnerable to DDoS attacks and single points of failure. Meanwhile, participants in Web3 can overcome the natural boundary between systems to share information and collaborate freely and trustingly.

Incentive Technologies

As to decentralized Web3, incentive mechanisms will go far beyond user attraction and value creation. Besides stimulating contributions of knowledge, such as open source softwares and high-fidelity AI models, it can also promote the sharing and coordination of decentralized infrastructure resources, thus affecting the performance and security of Web3, like the operation of slices in the DaaS plane. However, self-interested and independent participants tend to behave for their own interests, which may be incompatible with the global interest. Faced with this dilemma, many application methods have been proposed for incentive mechanisms to regulate participant behaviors. They can be applied in all planes of Web3 to support the key principle **Incentives for collaboration and sharing**.

To ensure the sustainable operation of Web3, a well-designed incentive mechanism should first have the following properties according to [14]. (i) At the side of individual interest, the

benefits should be non-negative (i.e., Individual Rationality) and the allocation should be fair (i.e., Incentive Fairness). Meanwhile, privacy of participants should be protected (i.e., Incentive Privacy). (ii) At the side of global interests, the individual interest should be compatible with the interest of Web3 (i.e., Incentive Compatibility and Incentive Truthfulness). Meanwhile, social welfare maximization should be satisfied for greater attraction to participation (i.e., Social Welfare Maximization). (iii) At the side of operations, the incentive mechanism should be decentralized and automated to match Web3 (i.e., Incentive Automation). Meanwhile, in the absence of powerful centralized entities, the incentive mechanism should be lightweight, with acceptable physical resource consumption.

Secondly, based on these considerations, many economic theoretic approaches can be used to design incentive mechanisms for Web3, such as game theory, auction, contract and matching theory [15]. In a decentralized manner, they can be applied to facilitating the sharing and collaboration of physical, data and intelligence resources, regardless of various human and geographic constraints. Apparently, traditional centralized business models are no longer applicable to the enforcement of incentive mechanisms and the management of related resources in decentralized Web3. Without a top-down hierarchy, DAO provides a feasible reference for Web3 to establish corresponding business models. In these business models, the rules and procedures will be fully transparent to all involved participants, and the executions will be automatic without human intervention.

Last but not least, thoughtful design requirements, appropriate design approaches and matching business models are expected to help maximize the sustainable and scalable operation of Web3 while minimizing the incentive cost.

Spatial Technologies

Spatial Web, proposed by Peter Diamandis, is the latest vision of Web3 and has two main goals. One is to provide secure, trustworthy and privacy-preserving interactions and transactions for humans, machines and virtual economies, that can be achieved by the three aspects of enabling technologies introduced above. The other is the deep integration of physical, digital, and biological domains to eliminate the boundaries between reality and virtuality. Focusing on the reality-virtuality interaction, this subsection explains how it supports the key principle **Towards human-centric experience**.

The reality-virtuality interaction is realized by reality mapping to virtuality and virtuality reacting back to reality [8]. In the IaaS plane, 6G-enabled full-earth ubiquitous coverage, extreme connectivity, and networked sensing can provide comprehensive, real-time and high-resolution sensing, localization and imaging capabilities. They can be used to acquire sufficient information and knowledge about the physical and biological world, which are critical to forward map to virtual models aided by connected intelligence in the AIaaS plane. These high-fidelity virtual models of physical and biological objects can be used in digital twins to simulate the operations of real objects, capture the corresponding rules and help to put into practice in reality [8]. Meanwhile, with the help of immersive technologies such as extended reality video, haptic and multi-sensory information, and 3D holographic images, they can provide humans with immersive experiences regardless of the physical distance. Then, remote services like remote operations, haptic telemedicine, etc. will not be far away.

Besides the ultimate infrastructure capabilities and diverse presentation forms, the unified state description of real objects and corresponding virtual objects is crucial for the realityvirtuality interaction as well. Currently, NFTs not only thrive in virtuality for digital collectibles, game assets, etc., but also begin to be associated with more and more physical objects, such as cars, wines, and so on, providing Web3 with attempts to describe states of virtual and real objects. With these attempts, NFTs are expected to act as a link between reality and virtuality for Web3, facilitating the circulation of both tangible and intangible assets.

Finally, based on all the four design principles discussed above, an intelligent, trust, and sustainable cyber-physical space with an inclusive open ecosystem will be constructed, which also signals the arrival of a full-fledged Metaverse.

Challenges and Open Issues

In the development of Web3, there are many issues and challenges worthy of attention and discussion, which can be divided into two categories, on-going and potential ones.

On-Going Challenges and Open Issues

In the current transition phase of Web2 to Web3, there are a series of on-gonging issues and challenges summarized as follows:

- **Backward and Forward Compatibility:** In order not to affect the operations of current applications and services, it is necessary for Web3 to be strongly backward compatible with Web2. Meanwhile, in order to meet the increasing security requirements and application scenarios, Web3 also needs to be forward compatible, so as to support online upgrade and sustainable evolution. However, endowing Web3 with backward and forward compatibility requires reasonable and comprehensive design on its protocols, mechanisms and functions, which remains an open issue.
- **Unified and Lightweight Design:** As an open web, Web3 will face large-scale access and dynamically changing services, and then its complexity will increase exponentially. For a low-complexity Web3, unified standards and basic protocols are required, thereby decreasing the numbers of functionalities and realizing a lightweight architecture. However, unified standards and architectural solutions cannot be achieved without global consensus, which remains challenging.
- **Flexible Deployment, Management, and Services:** The shift from content-centric to user-centric makes the architecture and operations that underpin Web3 different from Web2. As a result, the value of traditional theoretical models for guiding the deployment,

management, and services of Web3 is greatly diminished. Therefore, a series of precise theoretical models for Web3 are urgently needed. Meanwhile, based on these theoretical models, how to achieve flexible and low-cost deployment without sacrificing security and decentralization remains challenging. Moreover, how to provide flexible services for applications through their flexible management is other open issue.

- **Professional Supervision and Inspection:** Currently, Web3 in baby stage is lack of unified standards, this makes the data cannot be freely circulated between authorized services and applications, and the globally unique SSI is not implemented to support the trust-worthiness throughout the network lifecycle. Therefore, professional supervision is needed to inspect whether the whole project code is safe, whether the permissions are reasonable, and whether the traffic is compliant.

Potential Challenges and Open Issues

In Web2, the enabling technology discussed in this paper still has some unsolved problems, such as the interpretability issue of AI, the trilemma issue of blockchain and so on. In the transition to Web3, these technologies are highly integrated, interpenetrated and intersected, thus making it possible for Web3 to break the inherent limitations of a single technology, and obtain technical breakthroughs that are difficult to achieve in Web2. However, in Web3, it is still necessary to further study which issues left over by Web2 can be solved, which issues still exist, and what new issues will be generated. Meanwhile, it is unknown what basic theoretical problems Web3 will face, how to define them, and how to solve them.

Conclusion

This article has proposed a Web3 architecture, which integrates five distinct planes, namely AaaS plane, AIaaS plane, DaaS plane, BaaS plane and IaaS plane. Supporting the deployment of cross-layer functionalities, this architecture aims to build a zero-trust and zero-touch environment, thus helping ensure data protection throughout the whole process. Meanwhile, for its sustainable development, this article has summarized four key principles, covering interoperability and interpretability of data, trustworthiness throughout network lifecycle, incentive for collaboration and sharing, and humancentric experience. With the goal of understanding further intricacies, this article has divided the technologies that underpin these key principles into four aspects: semantic, decentralized, incentive, and spatial technologies. Generally, this article can be seen as a pioneer work on Web3 architecture designing, which is expected to facilitate the implementation of Web3, although multiple issues and challenges are still there at this infancy stage.

Acknowledgment

This work was supported in part by the National Key (Research and Development) Program of China under Grant 2021YFB1714100, in part by the National Natural Science Foundation of China under Grant U22B2006, and in part by the Zhejiang Lab under Grant 2021KF0AB03.

References

[1] J. Kindervag, "Build security into your network's DNA: The zero trust network architecture," Forrester Research 27, Cambridge, MA, USA, Tech. Rep., 2010, pp. 1–27.
[2] *Zero-Touch Network and Service Management (ZSM); Reference Architecture*, document ETSI GS ZSM 002, ETSI Group Specification (GS), 2019.
[3] M. Li et al., "CrowdBC: A blockchain-based decentralized framework for crowdsourcing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 6, pp. 1251–1266, Jun. 2019.
[4] Y. El Faqir, J. Arroyo, and S. Hassan, "An overview of decentralized autonomous organizations on the blockchain," in *Proc. 16th Int. Symp. Open Collaboration*, Aug. 2020, pp. 1–8.
[5] K. C. Toth and A. Anderson-Priddy, "Self-sovereign digital identity: A paradigm shift for identity," *IEEE Secur. Privacy*, vol. 17, no. 3, pp. 17–27, May/Jun. 2019.
[6] J. Kindervag, "No more chewy centers: The zero trust model of information security," Forrester Research 3, Cambridge, MA, USA, Tech. Rep., Mar. 2016.
[7] M. Cao, L. Zhang, and B. Cao, "Toward on-device federated learning: A direct acyclic graph-based blockchain approach," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 34, no. 4, pp. 2028–2042, Apr. 2023.
[8] Q. Tang et al., "Internet of Intelligence: A survey on the enabling technologies, applications, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 3, pp. 1394–1434, 3rd Quart., 2022.
[9] D. Fensel and M. A. Musen, "The semantic web: A brain for humankind," *IEEE Intell. Syst.*, vol. 16, no. 2, pp. 24–25, Mar./Apr. 2001.
[10] C. Benzaid and T. Taleb, "AI-driven zero touch network and service management in 5G and beyond: Challenges and research directions," *IEEE Netw.*, vol. 34, no. 2, pp. 186–194, Mar./Apr. 2020.
[11] W. Tong and P. Zhu, *6G: The Next Horizon: From Connected People and Things to Connected Intelligence*. Cambridge, U.K.: Cambridge Univ. Press, 2021.
[12] D. E. Sarmiento et al., "Decentralized SDN control plane for a distributed Cloud-Edge infrastructure: A survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 256-281, 1st Quart., 2021.
[13] X. Yin, Y. Zhu, and J. Hu, "A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions," *ACM Comput. Surv.*, vol. 54, no. 6, pp. 1–36, Jul. 2021.
[14] B. Cao et al., "Blockchain systems, technologies, and applications: A methodology perspective," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 353–385, 1st Quart., 2022.
[15] X. Tu et al., "Incentive mechanisms for federated learning: From economic and game theoretic perspective," *IEEE Trans. Cogn. Commun. Netw.*, vol. 8, no. 3, pp. 1566–1593, Sep. 2022.

Biographies

Weikang Liu (Weikang_Liu@bupt.edu.cn) received the B.E degree in information and communication engineering from the Beijing University of Posts and Telecommunications in 2017. He is currently pursuing the Ph.D. degree with the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications. His research interests include blockchain and Web3.

Bin Cao (caobin@bupt.edu.cn) is a Full Professor with the School of Information and Communication Engineering, Beijing University of Posts and Telecommunications. He is/was an Associate/Guest Editor of IEEE Transactions on Mobile Computing, IEEE Internet of Things Journal, IEEE Communications Magazine, IEEE Transactions on Industrial Informatics, etc. His research is blockchain.

Mugen Peng (Fellow, IEEE) (pmg@bupt.edu.cn) is a Full Professor with the School of Information and Communication Engineering, Beijing University of Posts and Telecommunications. He was a recipient of the 2018 Heinrich Hertz Prize Paper Award, the 2014 IEEE ComSoc AP Outstanding Young Researcher Award, etc.