blockchains

Review

Web3: Exploring Decentralized Technologies and Applications for the Future of Empowerment and Ownership

Yiwei Lai [1], Jingyi Yang [1], Mingzhe Liu [1,2,*], Yibei Li [1] and Shanlin Li [1]

[1] College of Computer Science and Cyber Security, Chengdu University of Technology, Chengdu 610059, China; laiyiwei@stu.cdut.edu.cn (Y.L.); 2022020925@stu.cdut.edu.cn (J.Y.); liyibei@stu.cdut.edu.cn (Y.L.); lishanlin@stu.cdut.edu.cn (S.L.)
[2] School of Data Science and Artificial Intelligence, Wenzhou University of Technology, Wenzhou 325000, China
* Correspondence: liumz@cdut.edu.cn

Abstract: The emergence of the World Wide Web has revolutionized online communication, aiming to achieve global information sharing and communication. However, the current Web 2.0 architecture, which relies on centralized platforms, presents limitations such as restricted user rights, data privacy concerns, and dependence on centralized institutions. Web3, as a concept describing the next evolutionary stage of the internet, offers a solution to these issues by reshaping the internet infrastructure. Web3 provides a foundation for autonomous digital experiences and drives the advancement of the digital economy. This paper offers a thorough exploration of Web3, covering its key technologies, applications, challenges, and opportunities. We begin by introducing the core technologies behind Web3, followed by an exploration of its prominent applications. Finally, we analyze the challenges faced by Web3 and discuss potential research opportunities to address these challenges in the future. In summary, this study comprehensively elaborates on Web3 and lays a solid foundation for subsequent research work, encouraging researchers to explore new frontiers.

Keywords: Web3; blockchain; smart contract; decentralization; ownership

check for updates

Citation: Lai, Y.; Yang, J.; Liu, M.; Li, Y.; Li, S. Web3: Exploring Decentralized Technologies and Applications for the Future of Empowerment and Ownership. *Blockchains* **2023**, *1*, 111–131. https://doi.org/10.3390/blockchains1020008

Academic Editors: Keke Gai and Liehuang Zhu

Received: 28 October 2023
Revised: 24 November 2023
Accepted: 7 December 2023
Published: 11 December 2023

1. Introduction

Since bidding farewell to the Web 1.0 era in 2004, which was limited to information exchange and portal display, we have entered the era of Web 2.0. During this era, users have gained the capacity to generate and share their content, while platforms have harnessed user-generated content (UGC) to engage a broad and extensive user community. However, as Web 2.0 further evolves, it has given rise to several challenges. First, users may encounter the loss of content or files when logging into an account that has been inactive for an extended period, compromising account security. Second, account privacy is threatened by issues such as intrusive advertisements and unsolicited calls resulting from the leakage of personal information tied to mobile phone accounts. Lastly, reliance on regulatory agencies to ensure trust limits industrial development due to factors such as administrative efficiency and the availability of regulatory bodies. To address these challenges, the decentralization of networks and the ownership of data become paramount. The advent of Web3 offers conceptual solutions to these issues.

Web3, proposed by Gavin Wood in 2014, represents the next evolutionary phase of the internet, with distinct value attributes in contrast to Web 1.0 and Web 2.0 [1]. While Web3 has gained significant attention in recent years, it is often mistakenly conflated with Web 3.0. Web 3.0 encompasses the Semantic Web, which enhances data resource access efficiency through data reuse and interlinking between websites, mainly involving P2P technology [2] and Resource Description Framework (RDF) [3]. In contrast, Web3 utilizes blockchains [4] and cryptocurrency to establish a decentralized network, with core technologies including decentralized storage [5], Decentralized Applications (DApps) [6], and smart contracts [7]. The fundamental idea of Web3 is that it can realize a serverless internet, that is, an internet where users generate content that belongs to the users themselves. Figure 1 summarizes the key characteristics of the internet throughout its evolution.

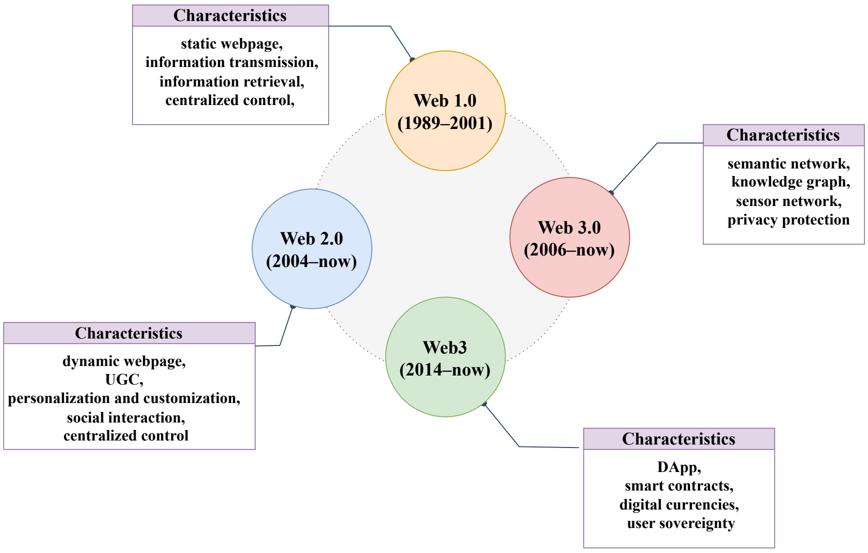

Figure 1. The evolution of key characteristics of the internet.

The main architecture of Web3, as depicted in Figure 2, comprises several key components: the client, digital wallet [8], web server, application server, database server, and blockchain server. The Web3 workflow unfolds as follows. First of all, upon the completion of signature verification within the client interface (whether a browser or a DApp), users proceed to connect with their digital wallets. It is noteworthy that digital wallets encompass features such as token transfers, digital identification, and user data authorization. Second, users can initiate a sequence of requests over the internet. These requests are then transmitted to both the web server and the blockchain server. Importantly, blockchain servers meticulously record users' online activities, while web servers are designed to engage with the application server through pertinent APIs. Finally, the application server facilitates access to both the distributed database server (utilizing SQL operations) and the blockchain server (via the Remote Call Protocol, or RPC). On the one hand, the blockchain server executes smart contracts in response to diverse calls originating from wallets and application servers. On the other hand, the distributed database enables storage and retrieval operations for large-scale data. It is worth noting that the Web3 servers operate in a decentralized manner, in contrast to the centralized network architecture of traditional web services.

The introduction of Web3 has sparked the interest and research enthusiasm of numerous scholars, offering a vision for creating a decentralized, secure, private, and interoperable internet. Many scholars have conducted in-depth research in this field. Presently, research on Web3 extends beyond the realms of education [9] and finance, encompassing various related fields. For instance, Keizer et al. [10] devised a model for decentralized score calculation, leveraging reinforcement deep learning to personalize Web3 reputation scores. Borgen [11] presented a framework for sensitive data that utilizes Ethereum [12] and Inter Planetary File System (IPFS) [5], constructing a Web3 system with privacy protection and access control. Khan and Ozbay [13] proposed AFFIRM, a privacy protection framework that enables efficient data generation, verification, storage, and retrieval in Web3 applications, facilitating local training of machine learning algorithms.

In addition, there have been many related reviews exploring the basic principles and early development of Web3, as listed in Table 1. Chen et al. [14] offer a comprehensive overview of the integration of web3 with the key elements of the digital economy and present a future outlook for the model's development within this economic framework. However, it is worth noting that this study primarily focuses on the digital economy, and the designed technologies lack depth and specificity. Ref. [15] provides an overview of contemporary Web3 research, employing Latent Dirichlet Allocation to pinpoint seven research topics. However, it is noteworthy that there is a lack of specific analysis regarding the architecture of Web3. In addition, while there are papers such as [16,17] that summarize the technical foundations of Web3 and can aid researchers in further studying the topic, it is important to note that these papers provide a limited perspective by primarily focusing on Web3's supporting technologies, such as blockchain and social identity, without offering a comprehensive analysis.

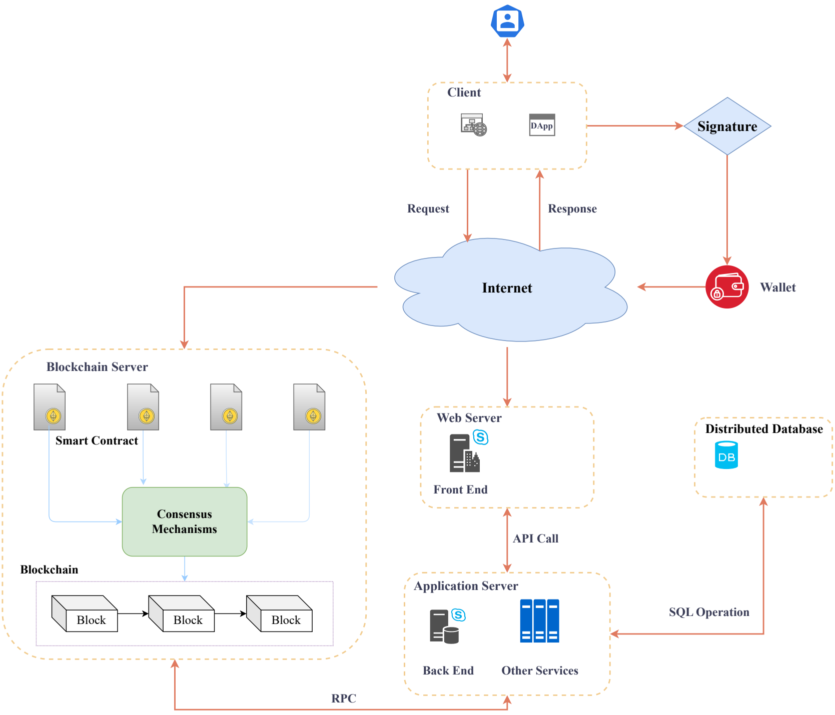

Figure 2. Web3 architecture.

Table 1. Related work.

Title	Year	Work	Limitation
When Digital Economy Meets Web3.0: Applications and Challenges [14]	2022	A comprehensive examination of the integration of Web3 in the digital economy and its prospective evolution.	Primarily concentrates on the digital economy, with designed technologies lacking depth and specificity.
Web3.0: A Review And Research Agenda [15]	2022	A Web3 research overview with the use of Latent Dirichlet Allocation to identify key research topics.	There is a lack of specific analysis on the Web3 architecture.
Decentralized Society: Finding Web3's Soul [16]	2022	Foundational Web3 technologies summarized to facilitate further research.	Offers a restricted viewpoint underlying social identity.
Web3: The Next Internet Revolution [17]	2023	Foundational Web3 technologies summarized to facilitate further research.	Offers a restricted viewpoint underlying blockchain.

The studies mentioned above strive to offer a glimpse into Web3 and set the stage for future research. Overall, however, they lack a complete introduction and analysis of the technologies and related applications involved in Web3. In contrast, the present paper surveys Web3-related literature from 2014 to October 2023, conducting a thorough analysis to compile a more comprehensive collection of Web3-related technologies and applications. Our primary contributions are outlined below:

- We conducted a survey of 84 papers related to Web3, providing an analysis of the current research status.

- We detail and explain the relevant technologies and applications of Web3 to provide enhanced clarity on the key techniques of system construction and application scenarios of Web3.
- Through an SWOT analysis, we have performed an objective analysis of the present challenges and outlined future development trends for Web3.

The rest of this paper follows the structure outlined below. Section 2 discusses the review methods. Section 3 provides an explanation of the technical components integral to Web3, elucidating its technical feasibility. Section 4 presents illustrative examples of noteworthy Web3 applications. Section 5 highlights the opportunities and challenges encountered in the realm of Web3, and concludes with a forward-looking perspective on future research directions. Lastly, Section 6 provides a succinct summary of the paper.

2. Materials and Methods

In this section, we introduce the pertinent literature research conducted prior to organizing this review. We meticulously reviewed and studied the collected literature, thereby substantiating the perspectives elaborated in the subsequent text.

In our quest to thoroughly explore the landscape of Web3-related research, we systematically conducted a literature review using the Web of Science platform. The search covered all accessible databases from 2014 to October 2023, with a central focus on pinpointing scholarly papers linked to Web3. Meanwhile, to refine our search accuracy, we incorporated pertinent keywords and subject terms in harmony with the Web3 paradigm. In upholding a standard of relevance and quality, we meticulously defined our inclusion criteria, solely considering papers that addressed Web3 technologies, applications, and related concepts. The search encompassed various disciplines, reflecting the interdisciplinary nature of Web3.

Our search process successfully identified 84 papers, with each paper undergoing rigorous examination to align with our study objectives. These carefully selected papers form the cornerstone for the subsequent analysis and discussion in this paper. Figure 3 illustrates the temporal distribution of these 84 papers in a bar chart, showcasing an overall increase in the number of papers over time. Clearly, in contrast to 2021, there has been a significant upsurge in the publication of Web3-related papers in 2022 and 2023, underscoring the heightened enthusiasm among researchers for Web3 research.

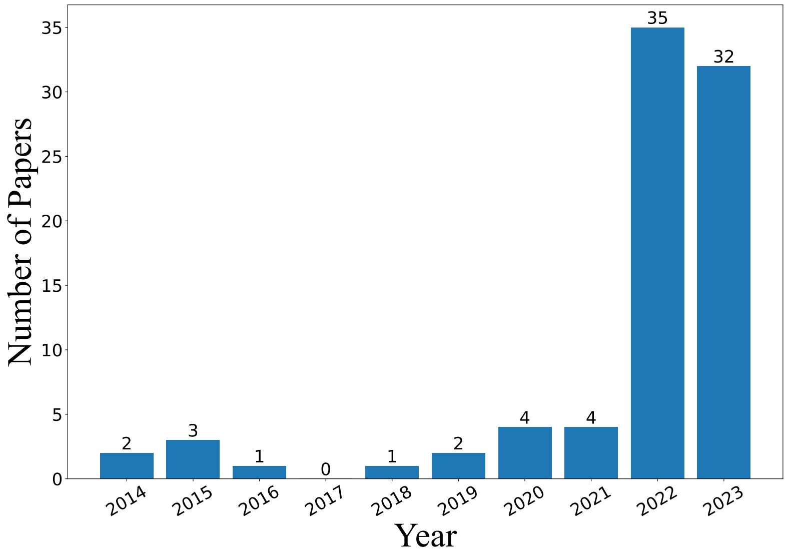

Figure 3. Publication trends of Web3-related papers by year.

In addition to the aforementioned analysis of the distribution of Web3-related papers, we list papers with high citation frequency and strong correlation with Web3 in Table 2. Undoubtedly, these papers on Web3 encompass a range of technologies, notably blockchain, decentralized storage, self-sovereign identity, and non-fungible tokens. Moreover, the diverse applications of Web3 primarily revolve around decentralized autonomous organizations, decentralized finance, and the metaverse. These technologies and applications have played a pivotal role in shaping the architecture of Web3 and propelling its advancement. An introduction and analysis of the key technologies and main applications of Web3 is provided in the following sections.

Table 2. List of relevant papers.

Author	Year	Citation	Topic	Key Techniques	The Applications Involved
Kumar et al. [18]	2020	202	They proposed a smart healthcare system.	Blockchain, Smart Contracts	Metaverse
Belk et al. [19]	2022	162	They introduced a novel theoretical concept of ownership within the metaverse.	Blockchain, Non-Fungible Tokens	Metaverse
Wang et al. [20]	2022	50	They explored the last decade's research, introducing the concept of DeMetaverses.	Blockchain	Metaverse, Decentralized Autonomous Organizations
Schlatt et al. [21]	2022	45	They proposed a blockchain-based solution to achieve the goal of 'know(ing) your customer' without compromising customer privacy.	Blockchain, Self-Sovereign Identity, Digital Wallets	-
Qin et al. [22]	2022	27	They proposed a five-tier intelligent architecture for Decentralized Autonomous Organizations.	Blockchain, Smart Contracts	Decentralized Autonomous Organizations, Metaverse
Subramanian et al. [23]	2022	19	They developed a digital pathology system leveraging smart contracts and non-fungible tokens.	Blockchain, Decentralized Storage, Non-Fungible Tokens, Smart Contracts	-
Buldas et al. [24]	2022	19	They introduced a shared blockchain technology and developed the Alphabill platform.	Blockchain	Decentralized Finance
David Vidal-Tom ´as [25]	2023	45	The author conducted a review of the existing metaverse economy and evaluated the metaverse economy of Web3.	Non-fungible tokens	Metaverse, Decentralized Finance

3. Key Technologies in Web3

In this section, we delve into several fundamental Web3 technologies, which encompass blockchain, decentralized data storage, self-sovereign identity (SSI), and non-fungible tokens (NFT).

3.1. Blockchains

Blockchain possesses decentralized characteristics [26], playing a pivotal role in Web3 and restoring data ownership to users [27]. As illustrated in Figure 4, the operational concept of blockchain starts with transaction generation; the transaction is then validated, aggregated into blocks, and finally added to the growing blockchain through consensus mechanisms. Below, we introduce the key technology stack of the blockchain.

3.1.1. Digital Signatures

Digital signature are pivotal for network security, and find extensive applications in identity authentication, data privacy protection, and tamper resistance [28]. When using an encryption algorithm to generate a digital signature, the sender uses a hash operation to convert the data into hash code and then encrypt it with its own private key. Next, the sender transmits the original data along with the ciphertext to the recipient. After receiving the data, the recipient employs the sender's public key to perform hash operations on the ciphertext and compares the decoded data with the hash code. Consistency between the two verifies that the sender's data remains intact and that the identity is reliable.

3.1.2. Merkle Trees

Merkle trees [4] play a crucial role in the storage of blockchain data. As shown in Figure 5, a Merkle tree operates as a binary tree, with hash values stored in its nodes and each leaf node representing the hash value of an individual transaction. The process of constructing a Merkle tree involves hashing the hash values of each pair of nodes together in order to generate a new hash value. Subsequently, this new hash value is stored in a new node, becoming the parent node of the two original nodes. This process is iteratively repeated until only a single hash value remains (the Merkle root), representing the culmination of all transactions. This structure allows any node downloading block information to verify transaction data from various sources, thereby ensuring data integrity. Moreover, the Merkle root is very sensitive to changes in transactions, meaning that even a minor alteration will trigger substantial modifications.

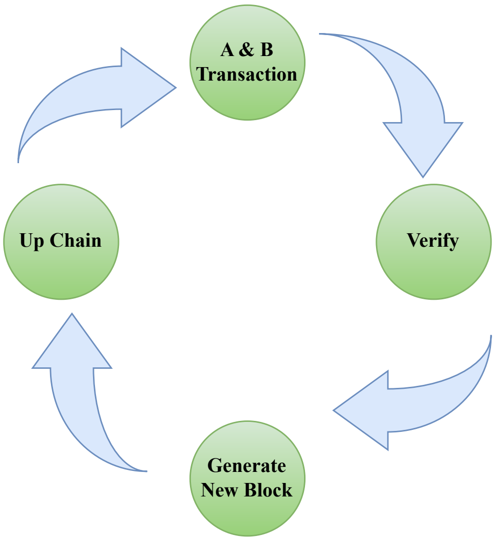

Figure 4. Workflow of blockchain.

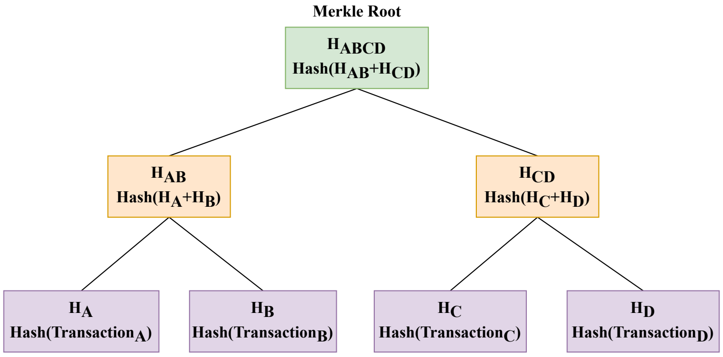

Figure 5. Structure of a Merkle tree.

It is important to acknowledge that while Web3 heavily depends on blockchain technology and its decentralized storage, relying solely on blockchain as the storage solution for Web3 is not practical [17]. First, storing a large volume of data directly on a blockchain can significantly impact performance, as each node in the blockchain network needs to store the entire ledger information. Second, the transaction processing speed of the blockchain system itself requires improvement, making it even more challenging to handle substantial amounts of data efficiently [29]. Fortunately, there are already decentralized storage solutions and technologies related to Web3, which we introduce later.

3.1.3. Consensus Mechanisms

To address the issue of trust among nodes and ensure transaction consistency and security, a blockchain needs a consensus mechanism that establishes rules or algorithms that nodes must adhere to. The consensus algorithm follows a workflow encompassing three stages. First, in the proposal stage, a node suggests a candidate block or transaction. Then, during the broadcast phase, the node shares the candidate information with other nodes. Finally, in the verification and voting stage, other nodes assess the received candidate information and determine the final valid block or transaction based on voting outcomes. This process ensures network consistency and security. The most common consensus mechanisms, including Proof of Work (PoW) [30], Proof of Stake (PoS) [31], Delegated Proof of Authority (DPoS) [32], and Practical Byzantine Fault Tolerance (PBFT) [33], each possess their own strengths and weaknesses. Their applications vary depending upon the goals, performance requirements, security considerations, and desired level of decentralization within the network.

3.1.4. Smart Contracts

In essence, a smart contract operating on a blockchain is a modular, reusable, and automatically executed script. Therefore, they are widely used in blockchain-related systems such as carbon trading systems [34] and recommendation systems [35]. Smart contracts need to be programmed in a computer language, with Solidity being widely used today. Solidity, a programming language officially designed and supported by Ethereum, is specifically tailored for writing smart contracts. These contracts are deployed onto the blockchain as code, enabling users to establish agreements regarding rights and obligations. The execution process involves writing the contract, compiling it, deploying it onto the blockchain system, and utilizing specific commands to invoke the smart contract.

3.2. Data Storage

At the heart of Web3 lies the principle of decentralization, which eliminates the risks associated with single points of failure and control inherent in the traditional centralized architectures of the internet. Decentralized file storage, such as blockchain-based storage systems, are the basis for sharing and storing data between different nodes of Web3, and make up its core technology [36]. This technology plays a pivotal role in Web3, as it enables users to disperse their data across multiple nodes through the blockchain storage system, thereby enhancing transparency and granting users greater control over their data [37].

The process of decentralized storage based on blockchains, as shown in Figure 6, encompasses file uploading and downloading. During a file upload, the system undertakes two main tasks. On one hand, the user's uploaded data undergoes fragmentation, encryption, and redundancy processing according to a specified algorithm. The resulting redundant data slices are stored across multiple independent network nodes, while the file metadata are simultaneously recorded on the blockchain. On the other hand, users pay fees to the blockchain, which rewards them with virtual currency. During the file download process, users initiate queries to the blockchain using the file's hash value [38]. The blockchain responds by providing metadata information, enabling users to retrieve file data from storage nodes in a peer-to-peer network. These processes highlight several key characteristics of decentralized storage based on blockchains: (1) fragmented and encrypted files are stored as ciphertext in other storage nodes, allowing only the data owner's key to access the complete data; (2) the decentralized distributed architecture enables storage devices to swiftly respond to requests from multiple locations, enhancing system efficiency; and (3) the issuance of blockchain-based virtual currency offers a viable solution for storage incentives. Notable decentralized storage systems based on blockchains include Filecoin, Storj, and Sia, which are further explored in the subsequent subsections.

3.2.1. Filecoin

Aiming to distribute storage by rewarding users who contribute storage capacity to the system, Filecoin [39] is a decentralized storage network constructed atop IPFS. The incentive model of Filecoin is based on two key assumptions: the expectation of a substantial increase in real data storage in the future, and the anticipation that real data will occupy a significant portion of the storage space. Within this network, two primary roles exist: storage parties, who request storage through transactions, and storage miners, who accept these transactions and provide storage space. Filecoin incorporates two mechanisms to ensure that data storage parties maintain their commitments and incentivize storage miners: Proof of Replication (PoRep) [40] validates whether storage providers have replicated users' data as required, ensuring that these replicated data are actually stored at different physical locations to guarantee data redundancy and security, while Proof of Spacetime (PoSt) [41] verifies whether storage providers maintain continuous storage of user data, rather than deleting the data at some point in time. Storage parties must demonstrate that they have received and encoded all the data into physical replicas, as well as provide proof that the random portion of the stored data remains intact. In essence, Filecoin can be regarded as the incentivization layer of IPFS, offering data storage and retrieval capabilities alongside IPFS.

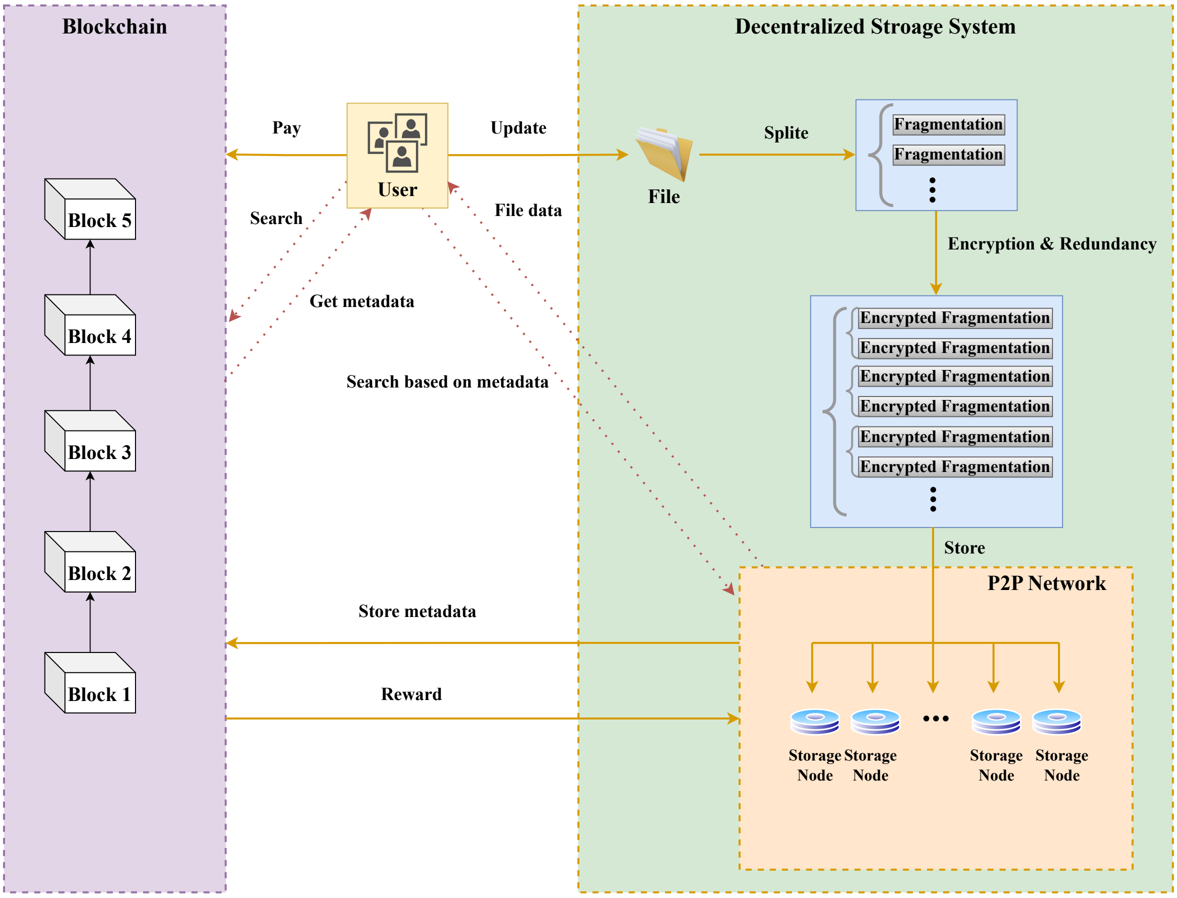

Figure 6. File upload and download process of blockchain-based decentralized storage.

3.2.2. Storj

Utilizing the Ethereum platform to ensure encryption of user-uploaded content at all times, Storj [42] is a decentralized content storage and distribution network. It enables users to rent hard disk space from others using encrypted currency tokens and offers virtual currency rewards on a monthly basis based on the provided storage space. Notably, Storj uses a centralized server for user authentication [43]. This server is responsible for verifying and authenticating users before they can access the network. When authenticated, users can store and retrieve data from the decentralized storage network. Thus, while Storj primarily operates as a decentralized network for storage, it relies on centralized authentication to ensure secure access for users. Users have the option of encrypting their files before uploading and then fragment them. When each fragment has passed review, it can be transmitted to the network. When it comes to downloading, users simply retrieve all the fragments and reassemble them to obtain the complete file.

3.2.3. Sia

Sia [44], similar to Storj, is a decentralized storage platform in which users can lease their hardware capacity for storage needs. Through smart contracts, users and storage providers establish file contracts that outline storage details and associated fees. These contracts define the time period for data storage and the compensation for both valid and invalid proofs. The key data element in the file contract is the Merkle root hash of the file [45], which, along with its size, is used to verify proof of storage. Additionally, users utilize Sia network tokens (Siacoin) to engage with storage providers based on the actual storage capacity and usage time. Table 3 presents a comparison of Filecoin, Storj, and Sia.

Table 3. Filecoin vs. Storj vs. Sia

Solution	Platform	Token for Rewarding	Consensus Mechanism	File Structure	Gas
Filecoin	Blockchain with IPFS	Filecoin	PoRep and PoSt	Merkle Directed Acyclic Graph	Yes
Storj	Ethereum with Distributed Hash Table	Storj (ERC-20 token)	-	Encrypted file sharding	No
Sia	Blockchain	Siacoin	PoW	Encrypted file sharding	Yes

3.3. Self-Sovereign Identity

SSI [46] is a framework for digital identity authentication that empowers individuals with complete control and sovereignty over their identity information. The interaction between the entities in this framework is illustrated in Figure 7. When a user possesses certain attributes, the Issuer issues an identity that the user can autonomously manage and control. The Verifier can authenticate the user's identity by establishing a trusted relationship with the Issuer. In the SSI model, individuals have ownership of their identity information and can independently create, manage, and control their digital identities without relying on centralized identity verification agencies or third-party trust intermediaries. Key characteristics of SSI include:

1. Decentralized Identification [47]: individuals use decentralized identifiers (DID) to establish unique identities within the network; DID is a globally unique identifier that can be implemented through blockchain technology or other distributed ledger technologies, ensuring secure and tamper-proof identity verification.
2. User Control: in the SSI model, individuals have complete autonomy over their identity information; they have the freedom to determine when, where, and with whom their identifiable information is shared, providing enhanced safeguards for personal privacy and data protection.
3. Decentralized Identity Verification [48]: SSI relies on a decentralized identity certificates (VC) without the need for centralized identity verification agencies; this approach ensures greater independence, privacy, and control over one's personal identity credentials.
4. Data Ownership: in the SSI model, individuals retain full ownership of their identity data, possessing the freedom to store their identity data in decentralized storage systems and the authority to grant or revoke access to this data for other entities; this allows individuals to exercise enhanced control over their personal information, enabling them to make informed decisions regarding its use and disclosure.

By adopting SSI, Web3 can establish a more open, transparent, secure, and protected network environment. At the same time, individuals can better realize their autonomy and sovereign identity in the digital world.

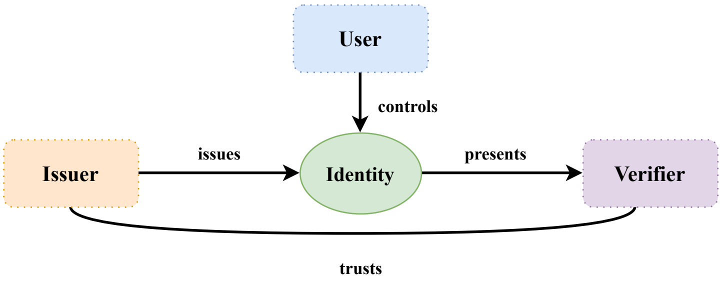

Figure 7. Self-Sovereign Identity actors [49].

3.4. NFTs

The term non-fungible token (NFT) refers to an irreplaceable and negotiable encrypted digital proof of ownership based on a blockchain [50], mainly involving smart contracts and digital signature technology [51]. Unlike traditional assets such as Bitcoin, each NFT has its own unique identifier and characteristics. Thus, each NFT is unique and distinct from any other. Moreover, NFTs are indivisible, meaning that NFT works can only be traded and circulated in the form of a whole. An NFT is created by digital content creators or publishers through smart contracts on a blockchain. During the creation process, they can specify the attributes, metadata, and other relevant information of the NFT to ensure its uniqueness and recognizability. The first official NFT standard was ERC721, which was proposed in 2018. This standard was the new standard of the Ethereum blockchain at that time; since then, ERC1155 has emerged, which has flexibility and functional characteristics that ERC721 does not [52]. Currently, there is a multitude of NFT projects. To elucidate the specific characteristics of different NFTs, Table 4 presents a comprehensive comparison among various NFTs.

Table 4. A comparison of various NFTs.

Project	Creation Methods	Language of Smart Contract	Main Platform	Field
ERC-721 NFT	ERC721	Solidity	Ethereum	Artworks, games, digital collectibles
ERC-1155 NFT	ERC1155	Solidity	Multi chain support, Ethereum compatible	Mass distribution of digital assets
Binance Smart Chain NFT	Standards of Binance Smart Chain	Solidity	Binance Smart Chain	Simple tokenization projects, digital collectibles
Flow (Dapper Labs)	Flow Protocol	Cadence	NBA Top Shot	Games, virtual assets

NFTs have had a significant impact on Web3, offering the following benefits: (1) by associating unique NFTs with digital assets, the ownership and transaction of digital content become more transparent, secure, and traceable; (2) users have the flexibility to transfer their NFTs across various platforms and utilize them in diverse application scenarios; (3) creators can directly publish and sell their works as digital assets through NFTs, enabling them to gain economic rewards; (4) NFTs provide a means to ensure authenticity and source traceability of digital content by linking it with specific a NFT.

4. Application Prospect

Drawing upon the literature analysis in Section 2, we have consolidated the diverse applications of Web3, specifically focusing on Decentralized Autonomous Organizations (DAOs), Decentralized Finance (DeFi), and the Metaverse. The subsequent sections provide comprehensive descriptions of the roles and functionalities associated with each of these application types.

4.1. Decentralized Autonomous Organization

A groundbreaking organizational structure, the DAO concept [22] is built on foundational technologies such as blockchain, AI, big data, and IoT. It operates through token-based incentives and collaborative governance, embodying characteristics of trust, consensus, openness, decentralization, and transparency. As the fundamental organizational form of Web3, DAOs enables their members to manage their own data, effectively mitigating misuse of user information by centralized entities. In practice, a DAO functions as an organic and transparent community in which participants share common objectives. Each member enjoys the right to partake in decision-making processes, collectively shaping the organization's trajectory and benefiting from equitable incentives.

Decentralized organizational forms such as DAOs have a long history in real-world contexts. Early manifestations of DAOs can be observed in Cyber Movement Organizations (CMOs) [53] and Distributed Artificial Intelligence (DAI) [54]. CMOs refer to social groups that engage in discussions around specific events within a short timeframe, while DAI involves distributed nodes collaborating to solve complex problems. Although these studies provided early insights into decentralized organization, the development of DAOs has significantly benefited from the emergence of blockchain technology. DAOs emerged shortly after Bitcoin was introduced, and was first conceptualized and defined by Vitalik Buterin. Subsequently, following the advent of Ethereum smart contracts, the inaugural DAO project, known as "The DAO", came into existence in 2016.

The underlying architecture of DAO is illustrated in Figure 8. The foundation of the DAO project lies in the blockchain, forming its fundamental layer. The middle layer represents the technology stack protocol of the DAO project, providing functionalities such as distributed ledger database and APIs for front-end access. The upper layer encompasses the applications built on top of the DAO project, enabling developers to implement code based on the business logic of the application. Each layer acts as a support for the layers above it, creating a cohesive structure. Additionally, [55] proposed a comprehensive five-layer DAO reference model (Figure 9) that provides a comprehensive framework for understanding and implementing DAOs.

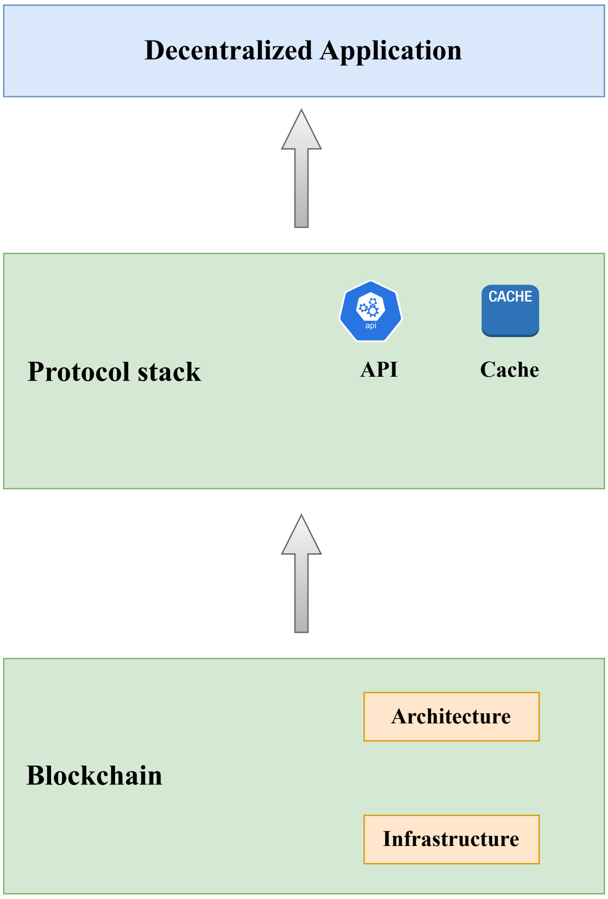

Figure 8. The underlying architecture of a DAO.

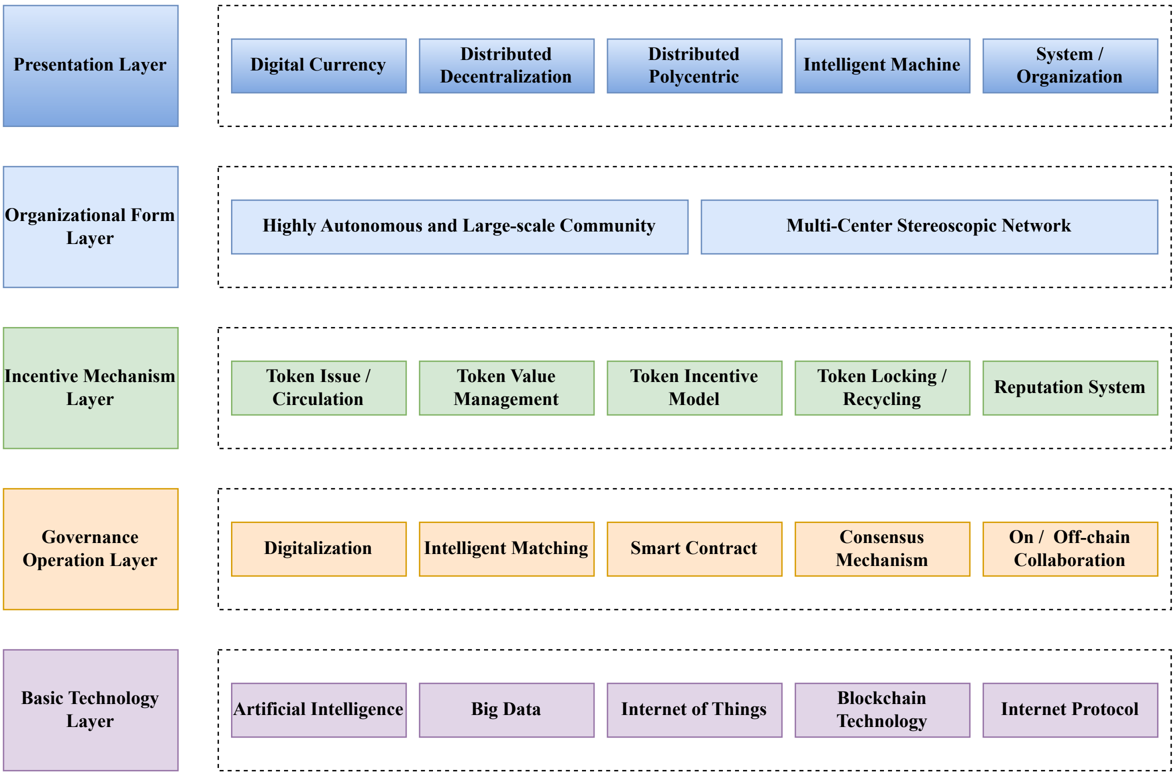

Figure 9. The five-layer architecture reference model of a DAO [55].

Based on the characteristics of DAOs and their model architecture, the working method can be summarized as follows:

1. Establishment: the establishment of a DAO usually starts with an initial stage in which the creator or initiator develops and publishes the governance agreement, smart contracts, and associated rules and conditions. These rules may encompass voting mechanisms, governance processes, token economics, and other aspects.
2. Participant joining: anyone can freely choose to participate in the DAO and become a member by holding DAO tokens. By purchasing tokens, participating in pledges, or making other contributions, members acquire rights and privileges within the DAO and gain the ability to participate in decision-making progresses.
3. Decision-making: DAO decision-making is achieved through members' votes. Each member has the opportunity to vote for or against specific proposals based on their token holdings or other designated stake. These proposals can encompass crucial decisions, including funding allocations, changes to governance rules, project development directions, and more. The collective voting process ensures that decision are made in a democratic and transparent manner, reflecting the consensus and preferences of the DAO community.
4. Smart contract execution: governance protocols and regulations for DAOs are commonly implemented as smart contracts and carried out on the blockchain. Decisions automatically executed according to the voting results of members, ensuring transparency, accuracy, and tamper-resistance in a process that becomes trustless and immutable. This obviates the need for intermediaries and provide a reliable framework for decision-making.
5. Governance and operation: DAO members can submit proposals, discuss issues, participate in voting, and supervise the operation of the DAO during the process of participating in governance and operation. The governance and operation of the DAO can be achieved through regular voting, community discussions, governance committees, etc.

6. Distribution and rewards: DAOs can motivate and reward members' contributions through the token economic model. According to the rules of the DAO, members may receive token rewards, dividends, governance rights, or other forms of rewards to encourage participation and contribution.
7. Audit and supervision: because the smart contracts and decisions of the DAO are open and transparent, members and other relevant parties can audit and supervise the activities of the DAO to ensure its compliance, fairness, and transparency.

4.2. Decentralized Finance

DeFi [56] refers to a revolutionary financial system and application ecosystem built on blockchain technology. It aims to democratize access to traditional financial services and introduce innovative financial products through open-source protocols and decentralized networks. With DeFi, individuals can seamlessly access a broad spectrum of financial services, including borrowing, insurance, wealth management, and cryptocurrency derivatives without the need for intermediaries, eliminating costly fees [57]. Leveraging the power of blockchains and smart contracts, DeFi protocols serve as advanced applications that leverage distributed transaction records, resulting in enhanced transaction processing capabilities. This transformative technology enables faster, more secure, and more transparent financial transactions, providing individuals with greater control over their financial assets and fostering financial inclusion on a global scale.

In recent years, the landscape of DeFi has evolved into a sophisticated ecosystem [58]. As shown in Figure 10, the DeFi infrastructure can be categorized into three key layers. Each layer performs a vital function in facilitating the DeFi ecosystem's operations and compatibility.

- The infrastructure layer primarily consists of the blockchain and its underlying protocols, which serve as the foundational infrastructure for the upper layers. This layer establishes a reliable and secure environment for transactions, ensuring that transaction status transitions are confirmed through the consensus mechanism. It provides a trustworthy storage mechanism for transactions, guaranteeing the integrity and immutability of the data.
- The asset layer is primarily comprised of the native protocol of the blockchain and other asset protocols that are compatible with the underlying blockchain infrastructure. These protocols play a crucial role in determining the standards and rules for handling different types of assets within the ecosystem. They facilitate the generation, transfer, and administration of diverse digital assets, including cryptocurrencies, tokens, and both fungible and non-fungible assets.
- The protocol layer establishes standardized protocols for transactions, lending, and cryptocurrency derivatives within the DeFi ecosystem. It sets the rules and frameworks for executing these financial activities in a decentralized and trustless manner. Additionally, developers have created various user application interfaces that interact with smart contracts through web browsers, enabling users to access and utilize the services provided by these protocols.

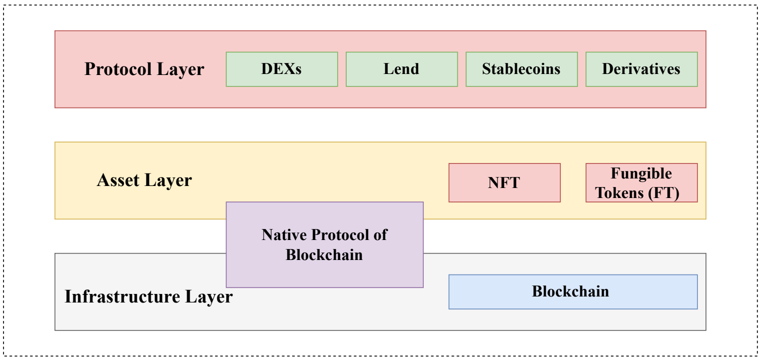

Figure 10. The architecture of DeFi.

Using the characteristics of Web3, DeFi has created a new financial and economic system. Decentralized Exchange (DEX) [59] in DeFi enables users to trade their own digital assets without the participation of traditional financial institutions. Because Web3 provides DeFi with the basis of a decentralized identity and credit system, users can use their own digital identities for authentication and isomorphic smart contracts to build their own credit history without the need for credit evaluation by traditional financial institutions.

4.3. Metaverse

The current internet is plagued by issues such as data monopolies and privacy breaches. It has become evident that data hegemony poses significant problems, while Web3 stands against such dominance. Smart contracts pave the way for a new form of governance that enables global collaboration. With the fundamental concepts of co-creation, sharing, and co-governance, the term "Metaverse" [60] refers to a computer-generated virtual space comprising digital environments and virtual reality. Its initial reference can be traced back to the science fiction novel "Avalanche" [61], published in 1992. In 2021, Mark Zuckerberg garnered significant attention by announcing his company's rebranding as Meta, marking the inception of the Metaverse era. Within the Metaverse, virtual assets take center stage; users have the ability to create, purchase, sell, and own various virtual assets, including digital artworks, virtual land, game props, and more. Furthermore, users can engage, collaborate, and socialize with others through their avatars in a virtual social environment offered by Metaverse. Notably, transactions involving virtual assets within the Metaverse often incorporate cryptocurrencies and smart contracts, establishing a self-governed economic system [62].

Metaverse and Web3 share a close relationship, with the Metaverse being a significant application field of Web3. Web3 encompasses decentralized infrastructure, smart contracts, and cryptocurrencies, providing a decentralized, transparent, and programmable environment for the Metaverse. The decentralized technology of Web3 ensures the genuine ownership of virtual assets and empowers users with autonomy and control over the Metaverse. Furthermore, Web3's self-identity and tokenized asset technology enable users within the Metaverse to truly express their identities and possess and trade virtual assets. Users can engage with other participants through their digital identities and conduct virtual asset transactions. Ultimately, the Metaverse leverages Web3-based smart contracts and DApps to realize diverse functions and application scenarios within the virtual world.

5. Challenges and Future Research Opportunities

5.1. SWOT Analysis

In this section, we undertake an assessment of Web3, delving into its challenges and prospects for future research. To gain a comprehensive understanding of the current state and potential of Web3, we have employed the SWOT analysis method, which systematically evaluates Strengths, Weaknesses, Opportunities, and Threats. SWOT analysis [63] is a widely recognized strategic management tool that enables a nuanced comprehension of the overall landscape and critical issues faced by Web3.

In conducting the SWOT analysis, we drew insights from various pertinent research articles and industry reports. These papers offer extensive research findings and perspectives on Web3, aiding in the identification of key factors associated with Web3 and providing valuable support for our analysis. We obtained Table 5, which offers insights into the present state and future development directions of Web3.

Web3 draws its strengths primarily from the decentralized and tamper-resistant features enabled by blockchain technology [17]. These attributes grant Web3 enhanced security and user control, fostering equal user participation and data ownership [64]. As outlined in [65], Web3 excels in standardizing information across diverse public platforms, facilitating seamless interoperability among various applications. Moreover, the emergence of Web3 has catalyzed the development of novel business models and provided valuable insights into identity authentication and community management solutions [14,22].

Table 5. SWOT analysis of Web3.

	(+) Positive Impact	**(−) Negative Impact**
Internal factors	Strengths (S) (1) Decentralization and immutability (2) User data ownership empowerment (3) Equal access for users (4) Trust in trustless networks (5) Information standardization across diverse public platforms (6) Automated execution of smart contracts (7) Seamless interoperability among various platforms and applications (8) New business models (9) A agile solution for community governance (10) A solution for identity authentication	Weaknesses (W) (1) Scalability and latency (2) Unfriendly user interface (3) High gas price (4) Digital divide (5) Supervision lacking and social instability (6) Numerous node dependencies of the front-end (7) Difficulty in restoring stored data on external pages (8)Additional learning costs (9) The significant resource consumption of PoW
External factors	Opportunities (O) (1) Blockchain Innovation (2) Social trust crisis (3) Elimination of necessity of trust (4) An increasingly complete developer ecosystem (5) The escalating demand for data privacy (6) Integration with Quality 4.0	Threats (T) (1) Cross site tracking of users (2) Regulatory challenges (3) Vulnerability of smart contract

Nevertheless, Web3 encounters notable weaknesses. Scalability is a significant concern, with current technology struggling to efficiently handle large-scale transactions and applications [66,67]. Improving user experience remains a hurdle, necessitating a more streamlined interface and workflow for ordinary users to adapt seamlessly to Web3 applications [68,69]. Additionally, inherent flaws in blockchain technology contribute to unsatisfactory energy and gas consumption by PoW [1].

Looking ahead, Web3 is poised for numerous opportunities. The ongoing advancements in blockchain technology and the evolving Web3 development environment play pivotal roles in its progression [70]. Simultaneously, research in Quality 4.0 and the escalating demand for data privacy offer promising avenues for Web3 [71].

However, it is crucial to acknowledge the looming threats faced by Web3. Addressing regulatory and compliance issues is imperative to ensure the legality and adherence of Web3 technology. Security vulnerabilities and technological competition demand ongoing attention [11]. Continual efforts to enhance Web3 security and compete effectively with other technological platforms are essential for maintaining a leading position.

In summary, Web3, as the next-generation internet evolution, holds immense potential and opportunities; however, it is not without its share of challenges and risks. The subsequent sections delve into the challenges and research prospects confronting Web3, spanning application, security, and regulatory aspects.

5.2. Application

Achieving the goal of replacing Web 2.0 with Web3 is indeed challenging, despite the advantages of decentralization and returning data ownership to users. Web 2.0 has become deeply ingrained in people's daily lives and work, leading to user habits and dependencies that are not easily changed. Currently, many Web3 applications lack a user-friendly interface and intuitive interaction design, which presents a barrier for users who may require technical knowledge and face learning costs [70].

From a technological standpoint, Web3 relies on various underlying technologies. The progression and ongoing evolution of these technologies, including blockchain and distributed storage, remain ongoing. Blockchain technology, in particular, faces scalability and performance challenges that necessitate more mature solutions to support large-scale users and applications. Additionally, the Web3 ecosystem consists of multiple blockchains and protocols, lacking standardization and interoperability. The interaction of data and assets across different chains poses technical and protocol challenges that need to be addressed for seamless cross-chain integration. While Web3 has the potential to revolutionize the digital landscape, it is crucial to address these user experience and technological hurdles in order to facilitate widespread adoption and realize the full potential of Web3 as a successor to Web 2.0.

5.3. Security

Although Web3 offers many innovations and potential, it faces data privacy and security issues as well. Because Web3 is a complex ecosystem employing emerging technologies such blockchain and decentralized storage, this complexity amplifies the system's attack surface and the potential for vulnerabilities.

1. Smart Contracts: as the core component of Web3, smart contracts are bound to have a huge impact on the security of specific Web3 projects. Due to the inability to modify smart contracts after deployment, any vulnerabilities or errors may result in user funding or system paralysis [72]. CeriK, a blockchain security audit firm, reported that in the first half of 2022 Web3 initiatives incurred losses exceeding USD 2 billion from cyberattacks and vulnerabilities, primarily within the domain of smart contracts. Vulnerabilities in smart contracts are mainly caused by programming errors or insufficient security audits, such as re-entrancy [73], gas-related vulnerabilities [74], permission bugs [75], and integer overflow/underflow [76]. Therefore, enhancing the security of smart contracts stands as the focus of Web3-related research.
2. Data Issues: the data problem for Web3 consists of two aspects: on the one hand, DApps in Web3 usually store data on a blockchain or distributed storage system. While this provides data transparency and tamper resistance, all data are publicly visible. This means that users' personal data may not be anonymized unless additional privacy protection measures are taken [68]. On the other hand, owing to the inherent limitations in storing extensive data on the blockchain, Web3 applications usually need to interact with traditional internet applications and external data sources. Linking off-chain data (such as personally identifiable information) with on-chain data (such as transaction records) can threaten user privacy. Without proper privacy protection measures, sensitive information may be disclosed.

5.4. Legality

The rapid development of Web3 technologies and applications outpaces the ability of existing legal and regulatory frameworks to adapt [1]. Many countries and regions lack clear legal regulations on emerging concepts such as digital assets, DeFi, and smart contracts in Web3 applications. This legal vacuum leads to legal risks and uncertainties, making it difficult for Web3 applications to operate in compliance. In terms of governance, Web3 technology involves DeFi applications, cryptocurrencies, and digital assets. However, financial businesses are usually subject to strict regulatory requirements such as such as international compliance issues, tax issues, etc. Web3 applications need to ensure compliance with applicable financial regulatory requirements to prevent money laundering, liquidity risk, and malicious activity. At the same time, the decentralized content sharing and creation platform in Web3 applications may involve intellectual property and copyright issues. Unlike traditional centralized platforms, content uploading and distribution on decentralized platforms are difficult to trace. What is more, copyright protection and rights protection have become more difficult. Protecting intellectual property rights and resolving copyright disputes are important challenges facing Web3 applications.

5.5. Opportunities

In addressing the application challenges of Web3, future research endeavors may focus on constructing a more robust software architecture, drawing insights from established methodologies such as [77,78]. This approach aims to instill heightened security features, thereby fostering user confidence in utilizing their digital wallets for transactions within the Web3 ecosystem. Furthermore, prioritizing a user-friendly interface and interactive design is paramount, as it serves to mitigate entry barriers for non-technical users and facilitate seamless navigation of Web3 applications. Performance enhancements can be achieved through the strategic implementation of cross-chain technology [79], elevating interoperability and scalability. This involves interconnecting diverse blockchains to facilitate cross-chain transfer and transactions of digital assets while concurrently optimizing load distribution across multiple chains to amplify overall throughput and performance.

In the realm of smart contracts, proactive measures include the identification and mitigation of potential vulnerabilities through rigorous security audits and formal verification processes [80]. Addressing the evolving landscape of Web3 technologies and applications necessitates proactive efforts from governments and regulators to formulate comprehensive legal frameworks. This entails the establishment of regulations governing digital assets and cryptocurrencies as well as regulatory guidelines for smart contracts and DeFi, among other aspects. Providing unambiguous legal provisions and guidance for Web3 is imperative to ensure compliance and mitigate uncertainties.

Furthermore, active collaboration between the Web3 community and pertinent stakeholders with regulatory bodies is essential. Establishing mechanisms for ongoing dialogue and cooperation can foster mutual understanding, address concerns, and ensure that Web3 applications operate within a compliant regulatory framework. Through sustained communication and collaboration with regulatory agencies, a more nuanced comprehension of regulatory requirements can be achieved, paving the way for the resolution of uncertainties and the seamless operation of Web3 applications within established compliance parameters.

Web3 exhibits promising applications in the context of Industry 4.0, particularly within the domain of Quality 4.0. Preceding Quality 4.0, the evolutionary stages encompassed Quality Control, Quality Assurance, and Total Quality Management [81]. Quality 4.0 represents an innovative paradigm in quality management [82], focusing on the enhancement of product and service quality through intelligent and automated quality management processes. However, as highlighted in [83], the implementation of Quality 4.0 is encumbered by challenges such as data security, traceability, and auditable transactions. Blockchain technology presents a transformative solution by meticulously recording crucial nodes in the product lifecycle, spanning raw material procurement, production processes, and distribution channels. The immutability inherent in blockchain ensures that consumers can precisely trace the origin and manufacturing journey of products, thereby validating their authenticity and adherence to quality standards. This robust traceability mechanism acts as a deterrent against the circulation of counterfeit and substandard products, fostering heightened product quality and consumer trust. Moreover, the utilization of hash functions and elliptic curve encryption algorithms in blockchains bolsters security within the digital manufacturing process. This suggests a viable application of blockchains to maintain security and achieve data traceability in digital manufacturing. Therefore, the integration of Quality 4.0 with Web3 emerges as a meaningful endeavor. On one front, the digital information pertaining to Quality 4.0 can be inscribed into smart contracts, seamlessly aligning with the Web3 architecture elucidated in Section 1. Simultaneously, the construction of a decentralized transactional framework targeting digital manufacturers and users facilitates user interaction with Quality 4.0 through token transactions. This amalgamation not only enhances the accessibility of Quality 4.0 data, it introduces novel transactional avenues that align with the principles of decentralization and user empowerment inherent in the Web3 paradigm.

6. Conclusions

This paper serves as a holistic exploration of the promising realm of Web3, with a deep dive into its core characteristics, namely, decentralization, SSI verification, user-centric data control, and the emergence of a collaborative sharing economy. It begins with an insightful introduction to the foundational technologies underpinning these features, embracing blockchain's secure ledgers, innovative data storage solutions, the groundbreaking SSI framework, and the revolutionary NFT. Moreover, to provide a tangible understanding of

Web3's practical applications, we offer three compelling case studies as testaments to its real-world viability. These instances encompass the domains of DeFi, digital art curation, and supply chain traceability. Through these, we unveil how Web3 stands poised to revolutionize industries, render conventional intermediaries obsolete, and empower users with a new level of control over their digital lives. The Web3 landscape is not without its challenges and opportunities, and we thoroughly dissect these in our discussion. The ever-present issues of scalability, interoperability, and regulatory compliance are addressed alongside the exciting prospects of global financial inclusion, enhanced data security, and a reinvention of the internet as we know it. It is our fervent aspiration that this review offer a guiding light for future researchers navigating the complexities and boundless potential of Web3. By sharing our insights, we aim to inspire innovation, collaboration, and an unceasing quest to propel the frontier of Web3 technologies into new and uncharted territories.

Author Contributions: Conceptualization, M.L., Y.L. (Yiwei Lai) and J.Y.; methodology, M.L. and Y.L. (Yiwei Lai); validation, Y.L. (Yiwei Lai), J.Y. and Y.L. (Yibei Li); formal analysis, M.L., J.Y. and S.L.; investigation, Y.L. (Yiwei Lai) and Y.L. (Yibei Li); resources, M.L., Y.L. (Yibei Li) and S.L.; writing—original draft preparation, Y.L. (Yiwei Lai); writing—review and editing, Y.L. (Yiwei Lai); visualization, J.Y. and S.L.; supervision, M.L. and J.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this review.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wang, Q.; Li, R.; Wang, Q.; Chen, S.; Ryan, M.; Hardjono, T. Exploring web3 from the view of blockchain. *arXiv* **2022**, arXiv:2206.08821.
2. Hasan, R.; Anwar, Z.; Yurcik, W.; Brumbaugh, L.; Campbell, R. A survey of peer-to-peer storage techniques for distributed file systems. In Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05)-Volume II, Las Vegas, NV, USA, 4–6 April 2005; Volume 2, pp. 205–213.
3. Jain, A.; Farkas, C. Secure resource description framework: An access control model. In Proceedings of the Eleventh ACM Symposium on Access Control Models and Technologies, Lake Tahoe, CA, USA, 7–9 June 2006; pp. 121–129.
4. Nakamoto, S.; Bitcoin, A. A peer-to-peer electronic cash system. *Bitcoin* **2008**, *4*, 15.
5. Benet, J. Ipfs-content addressed, versioned, p2p file system. *arXiv* **2014**, arXiv:1407.3561.
6. Cai, W.; Wang, Z.; Ernst, J.B.; Hong, Z.; Feng, C.; Leung, V.C. Decentralized applications: The blockchain-empowered software system. *IEEE Access* **2018**, *6*, 53019–53033. [CrossRef]
7. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, W.; Chen, X.; Weng, J.; Imran, M. An overview on smart contracts: Challenges, advances and platforms. *Future Gener. Comput. Syst.* **2020**, *105*, 475–491. [CrossRef]
8. Karantias, K. SoK: A Taxonomy of Cryptocurrency Wallets. Available online: https://eprint.iacr.org/2020/868 (accessed on 6 December 2023).
9. Filipčić, S. Web3 & DAOs: An overview of the development and possibilities for the implementation in research and education. In Proceedings of the 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 23–27 May 2022; pp. 1278–1283.
10. Keizer, N.V.; Yang, F.; Psaras, I.; Pavlou, G. The case for AI based Web3 reputation Systems. In Proceedings of the 2021 IFIP Networking Conference (IFIP Networking), Espoo and Helsinki, Finland, 21–24 June 2021; pp. 1–2.
11. Borgen, K.A.T. Web3 for sensitive data, enterprise, government, private, and permissioned use. In Proceedings of the 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain), Irvine, CA, USA, 7–11 June 2022; pp. 1–6.
12. Wood, G. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.
13. Khan, J.A.; Ozbay, K. AFFIRM: Privacy-by-Design Blockchain for Mobility Data in Web3 using Information Centric Fog Networks with Collaborative Learning. In Proceedings of the 2023 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 20–22 February 2023; pp. 456–462.
14. Chen, C.; Zhang, L.; Li, Y.; Liao, T.; Zhao, S.; Zheng, Z.; Huang, H.; Wu, J. When digital economy meets web 3.0: Applications and challenges. *IEEE Open J. Comput. Soc.* **2022**, *3*, 233–245. [CrossRef]
15. Guan, C.; Ding, D.; Guo, J. Web3. 0: A Review And Research Agenda. In Proceedings of the 2022 RIVF International Conference on Computing and Communication Technologies (RIVF), Ho Chi Minh City, Vietnam, 20–22 December 2022; pp. 653–658.

16. Weyl, E.G.; Ohlhaver, P.; Buterin, V. Decentralized Society: Finding Web3's Soul. Available at SSRN 4105763. 2022. Available online: https://www.microsoft.com/en-us/research/publication/decentralized-society-finding-web3s-soul/ (accessed on 6 December 2023).
17. Wan, S.; Lin, H.; Gan, W.; Chen, J.; Yu, P.S. Web3: The Next Internet Revolution. *arXiv* **2023**, arXiv:2304.06111.
18. Kumar, A.; Krishnamurthi, R.; Nayyar, A.; Sharma, K.; Grover, V.; Hossain, E. A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes. *IEEE Access* **2020**, *8*, 118433–118471. [CrossRef]
19. Belk, R.; Humayun, M.; Brouard, M. Money, possessions, and ownership in the Metaverse: NFTs, cryptocurrencies, Web3 and Wild Markets. *J. Bus. Res.* **2022**, *153*, 198–205. [CrossRef]
20. Wang, X.; Yang, J.; Han, J.; Wang, W.; Wang, F.Y. Metaverses and DeMetaverses: From digital twins in CPS to parallel intelligence in CPSS. *IEEE Intell. Syst.* **2022**, *37*, 97–102. [CrossRef]
21. Schlatt, V.; Sedlmeir, J.; Feulner, S.; Urbach, N. Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. *Inf. Manag.* **2022**, *59*, 103553. [CrossRef]
22. Qin, R.; Ding, W.; Li, J.; Guan, S.; Wang, G.; Ren, Y.; Qu, Z. Web3-based decentralized autonomous organizations and operations: Architectures, models, and mechanisms. *IEEE Trans. Syst. Man Cybern. Syst.* **2022**, *53*, 2073–2082. [CrossRef]
23. Subramanian, H.; Subramanian, S. Improving diagnosis through digital pathology: Proof-of-concept implementation using smart contracts and decentralized file storage. *J. Med. Internet Res.* **2022**, *24*, e34207. [CrossRef] [PubMed]
24. Buldas, A.; Draheim, D.; Gault, M.; Laanoja, R.; Nagumo, T.; Saarepera, M.; Shah, S.A.; Simm, J.; Steiner, J.; Tammet, T.; et al. An ultra-scalable blockchain platform for universal asset tokenization: Design and implementation. *IEEE Access* **2022**, *10*, 77284–77322. [CrossRef]
25. Vidal-Tomás, D. The illusion of the metaverse and meta-economy. *Int. Rev. Financ. Anal.* **2023**, *86*, 102560. [CrossRef]
26. George, W.; Al-Ansari, T. Review of Blockchain Applications in Food Supply Chains. *Blockchains* **2023**, *1*, 34–57. [CrossRef]
27. Liu, Z.; Xiang, Y.; Shi, J.; Gao, P.; Wang, H.; Xiao, X.; Wen, B.; Li, Q.; Hu, Y.C. Make web3. 0 connected. *IEEE Trans. Dependable Secur. Comput.* **2021**, *19*, 2965–2981. [CrossRef]
28. Yang, T.; Zhang, Y.; Xiao, S.; Zhao, Y. Digital signature based on ISRSAC. *China Commun.* **2021**, *18*, 161–168. [CrossRef]
29. Dai, H.N.; Zheng, Z.; Zhang, Y. Blockchain for Internet of Things: A survey. *IEEE Internet Things J.* **2019**, *6*, 8076–8094. [CrossRef]
30. Buterin, V. A next-generation smart contract and decentralized application platform. *White Pap.* **2014**, *3*, 1–2.
31. Kiayias, A.; Russell, A.; David, B.; Oliynykov, R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In Proceedings of the A37th Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2017; Springer: Berlin/Heidelberg, Germany, 2017; pp. 357–388.
32. Xu, G.; Liu, Y.; Khan, P.W. Improvement of the DPoS consensus mechanism in blockchain based on vague sets. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4252–4259. [CrossRef]
33. Castro, M.; Liskov, B. Practical byzantine fault tolerance. In Proceedings of the OsDI, New Orleans, LA, USA, 22–25 February 1999; Volume 99, pp. 173–186.
34. Zhang, T.Y.; Feng, T.T.; Cui, M.L. Smart contract design and process optimization of carbon trading based on blockchain: The case of China's electric power sector. *J. Clean. Prod.* **2023**, *397*, 136509. [CrossRef]
35. Jiang, Z.; Zheng, Z.; Chen, K.; Luo, X.; Tang, X.; Li, Y. Exploring smart contract recommendation: Towards efficient blockchain development. *IEEE Trans. Serv. Comput.* **2022**, *16*, 1822–1832. [CrossRef]
36. Dimakis, A.G.; Ramchandran, K.; Wu, Y.; Suh, C. A survey on network codes for distributed storage. *Proc. IEEE* **2011**, *99*, 476–489. [CrossRef]
37. Benisi, N.Z.; Aminian, M.; Javadi, B. Blockchain-based decentralized storage networks: A survey. *J. Netw. Comput. Appl.* **2020**, *162*, 102656. [CrossRef]
38. Wang, M.; Duan, M.; Zhu, J. Research on the security criteria of hash functions in the blockchain. In Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts, Incheon, Republic of Korea, 4 June 2018; pp. 47–55.
39. Guidi, B.; Michienzi, A.; Ricci, L. Evaluating the decentralisation of filecoin. In Proceedings of the 3rd International Workshop on Distributed Infrastructure for the Common Good, Quebec City, QC, Canada, 7 November 2022; pp. 13–18.
40. Damgård, I.; Ganesh, C.; Orlandi, C. Proofs of replicated storage without timing assumptions. In Proceedings of the Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 355–380.
41. Moran, T.; Orlov, I. Simple proofs of space-time and rational proofs of storage. In Proceedings of the Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 381–409.
42. de Figueiredo, S.; Madhusudan, A.; Reniers, V.; Nikova, S.; Preneel, B. Exploring the Storj Network: A Security Analysis. In Proceedings of the 36th Annual ACM Symposium on Applied Computing, New York, NY, USA, 4 March 2021; SAC '21; pp. 257–264. [CrossRef]
43. Zhang, X.; Grannis, J.; Baggili, I.; Beebe, N.L. Frameup: An incriminatory attack on Storj: A peer to peer blockchain enabled distributed storage system. *Digit. Investig.* **2019**, *29*, 28–42. [CrossRef]
44. Vorick, D.; Champine, L. Sia: Simple decentralized storage. *Retrieved May* **2014**, *8*, 2018.
45. Merkle, R.C. Protocols for public key cryptosystems. In *Secure Communications and Asymmetric Cryptosystems*; Routledge: Abingdon, UK, 2019; pp. 73–104.

46. Soltani, R.; Nguyen, U.T.; An, A. A survey of self-sovereign identity ecosystem. *Secur. Commun. Netw.* **2021**, *2021*, 8873429. [CrossRef]
47. Reed, D.; Sporny, M.; Longley, D.; Allen, C.; Grant, R.; Sabadello, M.; Holt, J. *Decentralized Identifiers (Dids) v1. 0.*; Draft Community Group Report; W3C: Wakefield, MA, USA,2020.
48. Sporny, M.; Longley, D.; Chadwick, D. *Verifiable Credentials Data Model v1.1.*; W3C Recommendation; W3C: Wakefield, MA, USA, 2022.
49. Mühle, A.; Grüner, A.; Gayvoronskaya, T.; Meinel, C. A survey on essential components of a self-sovereign identity. *Comput. Sci. Rev.* **2018**, *30*, 80–86. [CrossRef]
50. Chohan, U.W. Non-fungible tokens: Blockchains, scarcity, and value. *Crit. Blockchain Res. Initiat. (CBRI) Work. Pap.* **2021**. Available online: https://www.semanticscholar.org/paper/Non-Fungible-Tokens%3A-Blockchains%2C-Scarcity%2C-and-Chohan/a37918195898f80d083fdc3a6d83ed79d9f01ded (accessed on 6 December 2023). [CrossRef]
51. Roy, A.; Karforma, S. A Survey on digital signatures and its applications. *J. Comput. Inf. Technol.* **2012**, *3*, 45–69.
52. Balduf, L.; Florian, M.; Scheuermann, B. Dude, where's my NFT: Distributed infrastructures for digital art. In Proceedings of the 3rd International Workshop on Distributed Infrastructure for the Common Good, Quebec City, QC, Canada, 7 November 2022; pp. 1–6.
53. Aragón, P.; Volkovich, Y.; Laniado, D.; Kaltenbrunner, A. When a movement becomes a party: Computational assessment of new forms of political organization in social media. In Proceedings of the International AAAI Conference on Web and Social Media, Cologne, Germany, 17–20 May 2016; Volume 10, pp. 12–21.
54. Ferber, J.; Weiss, G. *Multi-Agent Systems: An Introduction to Distributed Artificial Intelligence*; Addison-Wesley Reading: Boston, MS, USA, 1999; Volume 1.
55. Wang, S.; Ding, W.; Li, J.; Yuan, Y.; Ouyang, L.; Wang, F.Y. Decentralized autonomous organizations: Concept, model, and applications. *IEEE Trans. Comput. Soc. Syst.* **2019**, *6*, 870–878. [CrossRef]
56. Kitzler, S.; Victor, F.; Saggese, P.; Haslhofer, B. Disentangling decentralized finance (DeFi) compositions. *ACM Trans. Web* **2023**, *17*, 1–26. [CrossRef]
57. Wu, Z.; Liu, J.; Wu, J.; Zheng, Z.; Luo, X.; Chen, T. Know Your Transactions: Real-time and Generic Transaction Semantic Representation on Blockchain & Web3 Ecosystem. In Proceedings of the ACM Web Conference 2023, Austin, TX, USA, 30 April–4 May 2023; pp. 1918–1927.
58. Schär, F. Decentralized finance: On blockchain-and smart contract-based financial markets. *FRB St. Louis Rev.* **2021**, *103*, 153–174. [CrossRef]
59. Wang, Y.; Chen, Y.; Wu, H.; Zhou, L.; Deng, S.; Wattenhofer, R. Cyclic arbitrage in decentralized exchanges. In Proceedings of the WWW'22: The ACM Web Conference 2022, Lyon, France, 25–29 April 2022; pp. 12–19.
60. Chen, Z.; Wu, J.; Gan, W.; Qi, Z. Metaverse security and privacy: An overview. In Proceedings of the 2022 IEEE International Conference on Big Data (Big Data), Osaka, Japan, 17–20 December 2022; pp. 2950–2959.
61. Lin, H.; Wan, S.; Gan, W.; Chen, J.; Chao, H.C. Metaverse in education: Vision, opportunities, and challenges. In Proceedings of the 2022 IEEE International Conference on Big Data (Big Data), Osaka, Japan, 17–20 December 2022; pp. 2857–2866.
62. Wei, L.; Wang, X.; Wang, T.; Duan, Z.; Hong, Y.; He, X.; Huang, H. Recommendation Systems for the Metaverse. *Blockchains* **2023**, *1*, 19–33. [CrossRef]
63. Puyt, R.W.; Lie, F.B.; Wilderom, C.P. The origins of SWOT analysis. *Long Range Plan.* **2023**, *56*, 102304. [CrossRef]
64. Ferraro, C.; Wheeler, M.A.; Pallant, J.I.; Wilson, S.G.; Oldmeadow, J. Not so trustless after all: Trust in Web3 technology and opportunities for brands. *Bus. Horiz.* **2023**, *66*, 667–678. [CrossRef]
65. Fang, Z.; Zhao, L.; Xiao, M.; Zhou, Y. The Honeycomb Theory of Web3. 0. In Proceedings of the 2008 IEEE International Symposium on Service-Oriented System Engineering, Jhongli, Taiwan, 18–19 December 2008; pp. 263–268.
66. Ding, W.; Hou, J.; Li, J.; Guo, C.; Qin, J.; Kozma, R.; Wang, F.Y. DeSci based on Web3 and DAO: A comprehensive overview and reference model. *IEEE Trans. Comput. Soc. Syst.* **2022**, *9*, 1563–1573. [CrossRef]
67. Xu, H.; Sun, Y.; Li, Z.; Sun, Y.; Zhang, L.; Zhang, X. deController: A Web3 native cyberspace infrastructure perspective. *IEEE Commun. Mag.* **2023**, *61*, 68–74. [CrossRef]
68. Park, A.; Wilson, M.; Robson, K.; Demetis, D.; Kietzmann, J. Interoperability: Our exciting and terrifying Web3 future. *Bus. Horiz.* **2023**, *66*, 529–541. [CrossRef]
69. Murray, A.; Kim, D.; Combs, J. The promise of a decentralized internet: What is Web3 and how can firms prepare? *Bus. Horiz.* **2023**, *66*, 191–202. [CrossRef]
70. Sadowski, J.; Beegle, K. Expansive and extractive networks of Web3. *Big Data Soc.* **2023**, *10*, 20539517231159629. [CrossRef]
71. Winter, P.; Lorimer, A.H.; Snyder, P.; Livshits, B. What's in your wallet? privacy and security issues in web 3.0. *arXiv* **2021**, arXiv:2109.06836.
72. Li, H.; Dang, R.; Yao, Y.; Wang, H. A Review of Approaches for Detecting Vulnerabilities in Smart Contracts within Web 3.0 Applications. *Blockchains* **2023**, *1*, 3–18. [CrossRef]
73. Xue, Y.; Ma, M.; Lin, Y.; Sui, Y.; Ye, J.; Peng, T. Cross-contract static analysis for detecting practical reentrancy vulnerabilities in smart contracts. In Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering, Virtual, 21–25 December 2020; pp. 1029–1040.

74. Ghaleb, A.; Rubin, J.; Pattabiraman, K. eTainter: Detecting gas-related vulnerabilities in smart contracts. In Proceedings of the 31st ACM SIGSOFT International Symposium on Software Testing and Analysis,Virtual, 18–22 June 2022; pp. 728–739.
75. Liu, Y.; Li, Y.; Lin, S.W.; Artho, C. Finding permission bugs in smart contracts with role mining. In Proceedings of the 31st ACM SIGSOFT International Symposium on Software Testing and Analysis, Virtual, 18–22 June 2022; pp. 716–727.
76. Gao, J.; Liu, H.; Liu, C.; Li, Q.; Guan, Z.; Chen, Z. Easyflow: Keep ethereum away from overflow. In Proceedings of the 2019 IEEE/ACM 41st International Conference on Software Engineering: Companion Proceedings (ICSE-Companion), Montreal, QC, Canada, 25–31 May 2019; pp. 23–26.
77. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Choo, K.K.R. P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking. *Comput. Secur.* **2020**, *88*, 101629. [CrossRef]
78. Yazdinejadna, A.; Parizi, R.M.; Dehghantanha, A.; Khan, M.S. A kangaroo-based intrusion detection system on software-defined networks. *Comput. Netw.* **2021**, *184*, 107688. [CrossRef]
79. Robinson, P. Survey of crosschain communications protocols. *Comput. Netw.* **2021**, *200*, 108488. [CrossRef]
80. Bhargavan, K.; Delignat-Lavaud, A.; Fournet, C.; Gollamudi, A.; Gonthier, G.; Kobeissi, N.; Kulatova, N.; Rastogi, A.; Sibut-Pinote, T.; Swamy, N.; et al. Formal verification of smart contracts: Short paper. In Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security, Vienna, Austria, 24 October 2016; pp. 91–96.
81. Tambare, P.; Meshram, C.; Lee, C.C.; Ramteke, R.J.; Imoize, A.L. Performance measurement system and quality management in data-driven Industry 4.0: A review. *Sensors* **2021**, *22*, 224. [CrossRef]
82. Javaid, M.; Haleem, A.; Singh, R.P.; Suman, R. Significance of Quality 4.0 towards comprehensive enhancement in manufacturing sector. *Sensors Int.* **2021**, *2*, 100109. [CrossRef]
83. AlKhader, W.; Jayaraman, R.; Salah, K.; Sleptchenko, A.; Antony, J.; Omar, M. Leveraging blockchain and NFTs for quality 4.0 implementation in digital manufacturing. *J. Manuf. Technol. Manag.* **2023**, *34*, 1208–1234. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.