Internet of Things and Cyber-Physical Systems 3 (2023) 213–248

Contents lists available at ScienceDirect

Internet of Things and Cyber-Physical Systems

journal homepage: www.keaipublishing.com/en/journals/internet-of-things-and-cyber-physical-systems

Web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions

Partha Pratim Ray

Sikkim University, India

ARTICLE INFO

Keywords:
Web3
Decentralization
Blockchain
Digital transformation
DApps
Zero-Trust architecture

ABSTRACT

Web3, the next generation web, promises a decentralized and democratized internet that puts users in control of their data and online identities. However, Web3 faces significant challenges, including scalability, interoperability, regulatory compliance, and energy consumption. To address these challenges, this review paper provides a comprehensive analysis of Web3, including its key advancements and implications, as well as an overview of its major applications in Decentralized Applications (DApps), Decentralized Finance (DeFi), Non-fungible Tokens (NFTs), Decentralized Autonomous Organizations (DAOs), and Supply Chain Management and Provenance Tracking. The paper also discusses the potential social and economic impact of Web3, as well as its integration with emerging technologies such as artificial intelligence (AI), the Internet of Things (IoT), and smart cities. This article then discusses importance of zero-trust architecture for Web3. Ultimately, this review highlights the importance of Web3 in shaping the future of the internet and provides insights into the challenges and opportunities that lie ahead.

1. Introduction

The Internet, as we know it today, has come a long way since its inception. In the past few decades, it has evolved from a simple information-sharing platform to an interactive, global network that connects billions of people and devices [1–5]. This article aims to provide a comprehensive understanding of the Internet's evolution and discuss Web3, the next stage in this ongoing transformation [6–8]. Web3, the next generation web, is an emerging decentralized architecture that leverages blockchain technology to offer enhanced security, privacy, and autonomy to its users [9–12]. The Web3 ecosystem is rapidly evolving with a wide range of dApps, DeFi platforms, NFTs, and DAOs emerging as key components. However, despite the immense potential of Web3, the existing challenges such as scalability, regulatory compliance, and environmental sustainability need to be addressed for its widespread adoption [13–15].

The motivation behind this review paper is to provide a comprehensive overview of the Web3 ecosystem, its current state, potential opportunities and challenges, and future perspectives. The primary objective is to analyze the recent advancements in Web3 and explore their implications for various industries and sectors. Additionally, this review paper aims to identify the key challenges hindering the widespread adoption of Web3 and propose potential solutions to address them. We present a detailed background on the evolution of the interest in this context as follows [16–20].

1.1. Background on the evolution of the internet

In the beginning at late 1960s, the development of the Advanced Research Projects Agency Network (ARPANET) by the United States Department of Defense as the first-ever computer network, enabling communication among connected computers. At the 1970s, Ray Tomlinson invents email, transforming electronic communication and paving the way for later messaging platforms. In 1980s, introduction of the Internet Protocol Suite (TCP/IP) was done by Vint Cerf and Bob Kahn, which allowed multiple networks to communicate with each other, leading to the creation of the modern Internet. Tim Berners-Lee proposed the World Wide Web (WWW) while working at CERN, laying the foundation for the web as we know it today. In 1990s, popularization of web browsers took place like Mosaic and Netscape Navigator, making the Internet more accessible to non-technical users. Launch of Amazon and eBay, made the beginning of e-commerce and revolutionizing the way people shop. Rapid growth and expansion of the Internet embarked to include applications such as email, file sharing, and the World Wide Web, marking the beginning of Web 1.0. We saw the launch of Google, which quickly becomes the dominant search engine due to its superior search

E-mail address: ppray@cus.ac.in.

https://doi.org/10.1016/j.iotcps.2023.05.003
Received 16 April 2023; Received in revised form 3 May 2023; Accepted 6 May 2023
Available online 9 May 2023

algorithm and simple user interface. In 2020s, the broadband Internet becomes more widely available, enabling faster connections and allowing for richer online experiences, such as streaming media. We witnessed the launch of Wikipedia, the collaborative online encyclopedia, showcasing the power of user-generated content and knowledge sharing. We also saw the launch of MySpace, the pioneering social networking platform, which sets the stage for the rise of social media, Facebook, which quickly gains popularity and eventually becomes the largest social networking platform, connecting billions of users worldwide, YouTube, revolutionizing the way people consume and share video content, and giving rise to a new generation of content creators, Twitter, the microblogging platform that allows users to share short messages (tweets) and follow real-time news and events. We also witnessed the rise of smartphones, with the launch of the iPhone in 2007, followed by the release of the first Android device in 2008, greatly increases mobile Internet access and usage at the mis of 2000s. In 2010s, we noticed the proliferation of cloud computing services, enabling individuals and businesses to store and access data remotely, and use software applications without the need for local installations. The rise of messaging apps (e.g., WhatsApp, Telegram, WeChat) further revolutionized communication and paves the way for new business models and services. The emergence of IoT technologies, connecting everyday objects to the Internet, and laid the foundation for smart homes, smart cities, and Industry 4.0. In 2020s, we saw an increased focus on data privacy and security, leading to the implementation of privacy regulations such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States. During 2020–2021, the COVID-19 pandemic accelerated digital transformation across industries, highlighting the importance of the Internet in enabling remote work, online education, telemedicine, and contactless transactions. Also, the growing awareness and adoption of blockchain technology and cryptocurrencies, with Bitcoin and Ethereum gaining mainstream acceptance, and the rise of DeFi platforms took place. Th world saw the NFT boom, as digital artists, musicians, and content creators begin to utilize blockchain technology to verify the uniqueness and ownership of digital assets. We found the emergence of DAOs, which leveraged blockchain technology and smart contracts to enable decentralized decision-making and governance. The same was empowered by the launch of Ethereum 2.0, aiming to improve the scalability, security, and sustainability of the Ethereum blockchain, further paving the way for the development of Web3 applications. Later, the rise of the Metaverse, a collective virtual shared space, with platforms such as Decentraland, Somnium Space, and CryptoVoxels gaining traction, and major tech companies investing in the concept continued for the development of Web3 technologies and protocols, such as Polkadot, Cosmos, and Avalanche, focused on improving interoperability and scalability within the blockchain ecosystem. Currently, an ongoing growth of the Web3 ecosystem, with an increasing number of dApps, NFT marketplaces, and DeFi platforms being developed and adopted by users, signaling a shift towards a more decentralized, secure, and user-centric Internet is being noticed.

As we move further into the 2020s, the Internet continues to evolve at a rapid pace, with cutting-edge technologies like blockchain, AI, and the IoT pushing the boundaries of what's possible. The emerging Web3 paradigm is poised to address the limitations of Web 2.0 and create a more equitable, secure, and interconnected digital world. The promise of Web3 is increasingly tangible, as developers, entrepreneurs, and users around the globe work together to shape the future of the Internet. The transition from Web1 to Web2 involves many events as discussed above [21–26].

1.2. Key characteristics of the Web 2.0 era

Here are some possible additions and improvements to the key characteristics of the Web 2.0 era [27–29]:

- User-generated content: Web 2.0 platforms allowed users to create, share, and interact with content in new ways, such as blogs, social media, wikis, and video-sharing sites. This gave rise to new forms of online collaboration, expression, and community-building, and challenged the traditional gatekeepers and intermediaries of the media and entertainment industries.
- Social networking: Web 2.0 platforms also enabled users to connect and communicate with each other in new ways, such as social networking sites like Facebook, Twitter, and LinkedIn. This created new opportunities for personal and professional networking, social activism, and collective intelligence, but also raised concerns about privacy, security, and online harassment.
- Personalization and recommendation: Web 2.0 platforms also used data analytics and algorithms to personalize and recommend content and services to users, based on their preferences, behaviors, and social networks. This created new opportunities for targeted advertising, content discovery, and user engagement, but also raised concerns about filter bubbles, echo chambers, and algorithmic bias.
- Mobility and ubiquity: Web 2.0 platforms also expanded the reach and accessibility of the internet, by enabling users to access and interact with content and services from anywhere and anytime, through mobile devices, tablets, and other portable gadgets. This created new opportunities for on-demand and location-based services, but also raised concerns about digital addiction, distraction, and disconnection.
- Cloud computing and SaaS: Web 2.0 platforms also adopted cloud computing and software-as-a-service (SaaS) models, which allowed users to access and use software and computing resources over the internet, without having to install or maintain them locally. This created new opportunities for cost savings, scalability, and collaboration, but also raised concerns about data security, vendor lock-in, and technological dependence.
- Overall, the key characteristics of the Web 2.0 era represented a significant shift from the static and one-way nature of Web 1.0, to the dynamic and interactive nature of Web 2.0. This shift empowered users to create, share, and interact with content and services in new ways, and challenged the traditional models of media, entertainment, and communication. However, the Web 2.0 era also posed new challenges and risks, such as privacy, security, and algorithmic bias, that needed to be addressed in the evolution of the internet and the digital economy.

As the next stage of internet evolution, Web3 promises to revolutionize the digital landscape by fostering greater decentralization, user empowerment, and innovation across various sectors, from finance and governance to data privacy and digital identity management. By leveraging cutting-edge technologies and paradigms, Web3 seeks to create a more equitable, secure, and interconnected online ecosystem for all users. In Ref. [30], metaverse is associated with Web3 for use of simple business and economics purpose. It includes NFTs and merging metaverse economy. This article lacks in technical detailing about Web3 and its use in terms of other aspects. An article [31] focuses to examine the research on Web3.0 that has been published from 2003 to 2022. It used a technique called Latent Dirichlet Allocation (LDA) to identify seven research themes and their corresponding key phrases. The research themes are interrelated and contribute to understanding various solutions, applications, and use cases, such as metaverse and NFT. Additionally, we propose an agenda for future research based on the innovative work in Blockchain, decentralized networks, smart contracts, and algorithms. A study examines the elusive goal of Web3, which is to create a “Universal Trust Machine” that would be owned by everyone and no one in a truly decentralized paradigm [32]. To do so, the study first explains the challenge of generating trust without a middleman, drawing from Robert Axelrod's seminal research on the evolution of cooperation in the iterated prisoner's dilemma. The study then presents the infrastructural and social challenges that the Universal Trust Machine would

have to overcome to encourage long-term cooperation in a decentralized setting. Various reputation systems are presented as promising techniques for promoting trustworthy behavior in a decentralized network through indirect reciprocity. The study also discusses the emerging Distributed Ledger technologies that offer secure transaction facilitating and privacy-preserving techniques as a good complement to the limitations of current reputation systems. Finally, the study concludes by discussing a future roadmap for creating the desired Universal Trust Machine. The major focus of this work remains in the trust factor no other aspects are discussed at all. In Ref. [33], the types of creative practitioners who are utilizing web3 technologies are detailed. By examining empirical data and conducting a review of research literature and media coverage, it is demonstrated that income is being earned by artists who previously struggled to monetize their work through web3 technologies. In fact, many of these practitioners come from traditionally marginalized backgrounds or practices. Differentiation is made between creative professionals who use blockchain technologies generally, those who integrate blockchain technologies into their creative processes, proxy users who collaborate with others that engage with the technologies on their behalf, and non-users of blockchain technologies. Despite the increased activity surrounding non-fungible tokens (NFTs) in 2021, the adoption and usage of web3 technologies in Australia is still in its early stages. A divided response among creative practitioners towards these technologies is revealed by our survey. In Ref. [34], a comprehensive survey of Web3 is presented, with a focus on current technologies, challenges, opportunities, and outlook. Several major Web3 technologies are introduced, and the type of Web3 applications is illustrated in detail. It is explained that decentralized organizations are less trusted and more truthful than centralized organizations, thanks to blockchain and smart contracts. Decentralized finance is emphasized as a global and inclusive system for unbanked people. The relationship between the Metaverse and Web3, as well as the differences and similarities between Web 3.0 and Web3, are also discussed. Maslow's hierarchy of needs theory inspired a novel hierarchy of needs theory within Web3. Finally, several future research directions of Web3 are worth considering. However, it lacks in in-depth understanding, challenges and future direction. An article [35] derived from the current state-of-the-art literature, four essential elements, including appropriate decentralization, good user experience, appropriate translation and synchronization to the real world, and a viable economy, are introduced, which are required for the appropriate implementation of a metaverse and its applications. The development of the Metaverse is dependent on decentralization, and blockchain can play a significant part in the future of Web3. Additionally, this paper sheds light on the most relevant open issues and challenges currently facing the Web3/metaverse and its applications, with the hope of encouraging the development of appropriate solutions. A paper [36] reviews and outlines the conceptual map, research issues, and technical opportunities of decentralized AI and edge intelligence, going beyond centralized and distributed AI. The complementarity and metasynthesis between centralized and decentralized AI are also explained. Decentralized AI and edge intelligence are assessed for their potential to enable and promote smart blockchain, Web3, metaverse, and decentralized science disciplines in terms of discipline, technical, practical, and broader aspects. The next major generational evolution of the web, Web3, is introduced in Ref. [37]. The fundamental evolution of the internet and the web over the past three decades is reviewed, including a brief presentation of important publications in Business Horizons related to the emergence of Web3. The implications of recent developments on organizations, consumers, and the public are discussed. Although it is uncertain to what extent Web3 will be widely adopted, these technologies are already creating both exhilarating and terrifying implications for e-commerce, digital media, online social networking, online marketplaces, search engines, supply chain management, and finance, among other areas. The consideration and management of technical, organizational, and regulatory interoperability for Web3 to deliver on its promises of value are proposed. Failure to consider these interoperability components may destroy economic value, consumer confidence, or social issues online. Furthermore, the importance of researchers focusing on these interoperability issues and their potential impact on the positive and negative aspects of Web3 technologies is emphasized to help us understand and shape our Web3 future. The competing economic and philosophical approaches to the future of the internet are explored in Ref. [38]. On one hand, the most successful internet advertising firms (Facebook and Google) and their video game competitors (Roblox, Microsoft's Minecraft, Epic Games, and Valve) are driving the internet, while on the other hand, Web3 advocates are focused on cryptocurrencies, nonfungible tokens, DeFi, and DAOs. This article reviews three core areas for the development of the metaverse within the context of U.S. law: the regulatory environment, the transactional essentials, and the limits on governmental intrusion into the metaverse.

Research Gaps of Existing Review Papers:

- Lack of understanding about the potential impact of Web3 on various industries and sectors
- Limited research on the technical, organizational, and regulatory interoperability needed for Web3 to deliver on its promises
- Uncertainty regarding the degree to which Web3 will be widely adopted and its implications for e-commerce, digital media, online social networking, online marketplaces, search engines, supply chain management, and finance, among other areas
- Limited research on the types of creative practitioners utilizing Web3 technologies and their impact
- Insufficient research on the factors that will help in the development, successful adoption, and sustainable use of the Web3/metaverse and its applications
- Limited understanding of the potential impact of decentralized AI and edge intelligence on smart blockchain, Web3, metaverse, and decentralized science disciplines

The major contributions of this review paper include following that aims to resolve above research gaps:

- A detailed analysis of the Web3 ecosystem and its components, highlighting the opportunities and challenges associated with each.
- Moreover, it provides insights into the potential impact of Web3 on various industries and sectors, as well as its future prospects, including the metaverse, AI, and the integration with the IoT and smart cities.
- Then, it presents various zero-trust architectures.
- Finally, this review paper proposes potential solutions to address the key challenges hindering the widespread adoption of Web3, including scalability, regulatory compliance, and environmental sustainability.

This paper is organized as follows. Section 2 presents key features of Web3. Section 3 deals with existing technologies that support Web3. Section 4 discuss about various applications and use cases. Section 5 presents zero-trust architecture for web3. Section 6 presents the key challenges of Web3. Section 7 discusses about future directions about Web3. Section 8 concludes this review paper. Table 1 presents the abbreviations and key terms used in this paper.

2. Key features of Web3

2.1. Decentralization

Decentralization is the process of distributing and dispersing power, authority, and control away from a central authority or location. In the context of the internet and Web3, decentralization refers to the shift from centralized servers, data centers, and intermediaries to distributed networks, peer-to-peer protocols, and user-centric models. Decentralization promotes a more open, transparent, and equitable digital ecosystem, reducing the risk of censorship, downtime, data breaches, and single

Table 1
Abbreviations and key terms.

Abbreviations	Full Form
AI	Artificial Intelligence
AML	Anti-Money Laundering
AR	Augmented Reality
ARPANET	Advanced Research Projects Agency Network
ASIC	Application-Specific Integrated Circuits
ASP	Adaptive Security Platform
AWS	Amazon Web Services
CCPA	California Consumer Privacy Act
CMS	Content Management System
DAG	Directed Acyclic Graph
DAOs	Decentralized Autonomous Organizations
DApps	Decentralized Applications
dCDNs	Decentralized Content Delivery Networks
dDNS	Decentralized Domain Name Systems
DeE	Decentralized Energy Systems
DeFi	Decentralized Finance
DeG	Decentralized Gaming
DeH	Decentralized Healthcare
DeSM	Decentralized Social Media
DEXs	Decentralized Exchanges
DID	Decentralized Identity
DIF	Decentralized Identity Foundation
DL	Deep Learning
DLT	Distributed Ledger Technology
EAA	Enterprise Application Access
EVM	Ethereum Virtual Machine
GDPR	General Data Protection Regulation
GPU	Graphics Processing Units
IBC	Inter-Blockchain Communication
ICO	Initial Coin Offerings
ICP	Interchain Communication Protocol
ILP	Interledger Protocol
IoT	Internet Of Things
IPFS	Interplanatory File System
IPLD	Interplanetary Linked Data
KYC	Know Your Customer
MFA	Multi-Factor Authentication
ML	Machine Learning
NFTs	Non-Fungible Tokens
NLP	Natural Language Processing
P2P	Peer-to-Peer
PDS	Personal Data Store
PoS	Proof of Stake
PoW	Proof of Work
SaaS	Software-as-a-Service
SDP	Software-Defined Perimeter
SSI	Self-Sovereign Identity
STO	Security Token Offerings
UEBA	User and Entity Behavior Analytics
UX	User Experience
W3C	World Wide Web Consortium
WWW	World Wide Web
ZTNA	Zero-Trust Network Access

points of failure. Decentralized systems can foster increased innovation and collaboration by empowering users and communities to contribute to the development and management of platforms, applications, and digital assets. In Ref. [39], a five layered Web3 technology stack is presented as shown in Fig. 1. Level 0 comprises of P2P internet overlay networks (e.g., Devp2p, Libp2p) and platform neural computation description languages. Level 2 includes zero-trust interaction platforms and/or protocols as well as transient data messaging tools along with data distribution protocols such as IPFS. Level3 uses state channels, encrypted storage, plasma protocols heavy computations, oracles, storage incentives and distributed secret management tools. Level 3 consists of protocol-extension APIs such as Web3.js, Solidity, Rust and ether.js. Lever 4 uses protocol extensible user interface cradle for example Metamask.

2.2. Blockchain

Blockchain technology is a key enabler of decentralization in Web3, providing a secure, transparent, and tamper-proof foundation for distributed networks and applications. Blockchain is a distributed ledger technology (DLT) that uses cryptographic hashing, consensus algorithms, and a network of nodes to create an immutable, shared record of transactions and data. By removing the need for central authorities and intermediaries, blockchain technology allows for the creation of decentralized applications, platforms, and digital assets that can operate securely and efficiently without relying on a single point of control. Smart contracts, which are self-executing agreements encoded on a blockchain, can automate processes and facilitate decentralized decision-making, governance, and resource allocation. Key features of blockchain technology includes following [40–43].

- Immutability: The use of cryptographic hashing and consensus mechanisms ensures that once data is recorded on a blockchain, it cannot be easily altered or tampered with.
- Transparency: All transactions and data on a blockchain are visible to all participants in the network, promoting trust and accountability.
- Security: The decentralized nature of blockchain networks makes them resistant to attacks, as there is no single point of failure or control that can be exploited.
- Interoperability: Blockchain technology enables the creation of cross-chain solutions and bridges, allowing users to seamlessly interact with multiple blockchain networks and digital assets.
- Distributed ledger: Blockchain is a distributed ledger technology that maintains a decentralized record of transactions across a network of computers, ensuring that no single entity can control or manipulate the system.
- Consensus mechanisms: Blockchain networks use various consensus mechanisms, such as proof-of-work, proof-of-stake, and delegated

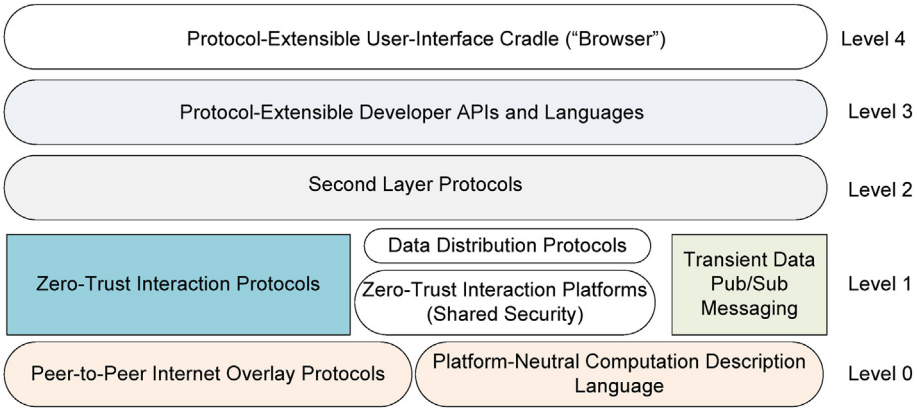

Fig. 1. Web3 technology stack.

proof-of-stake, to validate and confirm transactions, ensuring the security and integrity of the system.
- Cryptography: Blockchain technology relies on cryptographic techniques, such as public-key cryptography and hash functions, to secure transactions and user data.
- Smart contracts: Blockchain networks support the development of smart contracts, programmable scripts that execute automatically based on predefined conditions, enabling the creation of self-executing agreements and applications.

Fig. 2 presents the Web3 architecture with help of blockchain applications, platforms, solutions and protocols [44]. The architecture shows how blockchain platforms and protocols can support JSON RPC aware front-end for the efficient access of information by the users. The major activity is performed from the user's web browser after successful signing in. L2 scaling solutions and decentral controller together work on the smart contracts for providing efficient decentralized services with support from the decentralized file systems.

2.3. Role of blockchain in fostering decentralization

- Trustless environment

Blockchain and DLT eliminate the need for trusted third parties, as they provide a secure, transparent, and tamper-proof platform for recording transactions and managing digital assets. The consensus mechanisms used in blockchain networks, such as proof-of-work and proof-of-stake, ensure that no single participant can manipulate the system, fostering trust among users. By eliminating the need for intermediaries, blockchain and DLT reduce transaction costs and enable more efficient and direct peer-to-peer interactions [45,46]. Decentralized networks minimize single points of failure, making them more resilient to attacks and system failures. Trustless environments enable new business models and applications that were not possible with centralized systems, such as DeFi and DAOs. The decentralized nature of blockchain and DLT ensures that data and digital assets are owned and controlled by users, promoting data privacy and user empowerment.

The decentralized architecture of blockchain and DLT makes them more resistant to cyberattacks, as compromising the entire system requires taking control of a majority of the network nodes. The immutability of blockchain records ensures that once data is added to the ledger, it cannot be altered, providing a secure and auditable record-keeping system. Cryptographic techniques, such as public-key cryptography and hash functions, protect user data and transactions, ensuring the integrity and confidentiality of the network [47]. The transparent nature of blockchain and DLT allows for continuous monitoring and auditing of the network, enabling early detection of potential security threats. Decentralized networks can mitigate the risks associated with central points of control, such as insider threats and regulatory capture. Blockchain and DLT enable secure and verifiable digital identity solutions, reducing the risk of identity theft and fraud.

- Improved governance

Decentralized networks enable more democratic and inclusive decision-making processes, as users can participate in governance through voting and consensus mechanisms. Blockchain and DLT can facilitate decentralized governance models, such as DAOs, which enable

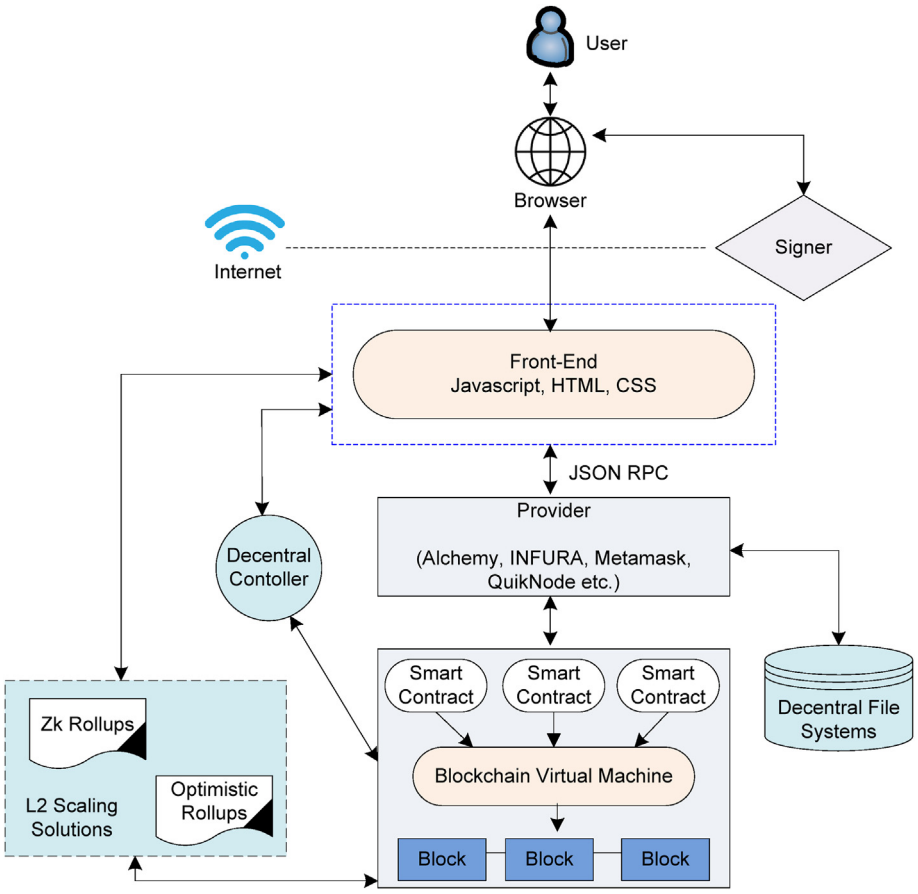

Fig. 2. Web3 architecture on top of blockchain platforms and protocols.

- Enhanced security

users to directly influence the direction and development of the network. Transparent and auditable record-keeping on blockchain networks ensures that decisions and resource allocations are visible to all participants, fostering trust and accountability [48]. Decentralized governance models can adapt more quickly to changes in the environment or user needs, as decision-making is not bottlenecked by centralized authorities. Blockchain and DLT enable token-based governance models, where users can stake or delegate their tokens to influence decision-making and network upgrades. Decentralized governance models can mitigate the risk of regulatory capture and centralized control, fostering a more open and equitable digital ecosystem.

- Increased transparency and auditability

Blockchain technology enables a high degree of transparency by providing a public and verifiable record of all transactions on the network. The decentralized nature of blockchain and DLT ensures that all network participants can access and verify transaction data, promoting accountability and trust [49]. The transparent record-keeping of blockchain and DLT allows for real-time auditing of network activity, enabling users and regulators to monitor system performance and compliance. Increased transparency can also help prevent fraud, corruption, and other malicious activities by making it easier to track and trace transactions and assets. Transparency on blockchain networks can improve market efficiency by providing users with accurate and up-to-date information about as set prices, trading volumes, and other relevant data. Blockchain-based platforms can foster transparent supply chains, enabling stakeholders to track and verify the provenance of goods, ensuring product quality and sustainability.

- Interoperability and cross-chain solutions

Decentralization in Web3 is further enhanced by the interoperability between different blockchain networks, allowing them to communicate and interact seamlessly. Cross-chain solutions, such as Polkadot, Cosmos, and Avalanche, are developed to bridge different blockchain networks, enabling the transfer of assets and data between them and expanding the possibilities for dApp development [50]. Interoperability fosters a more open and collaborative digital ecosystem, where users can access services and assets across various blockchain networks without the need for intermediaries. Interoperability enables the development of multi-chain applications that leverage the unique features and capabilities of different blockchain networks, providing users with more advanced and versatile services. Decentralized exchanges and cross-chain liquidity pools can facilitate seamless trading and asset management across different blockchain networks, reducing friction and promoting a more efficient and interconnected digital economy. Interoperability standards and protocols, such as the ICP and the TokenBridge, facilitate seamless communication and asset transfers between different blockchains.

- DApps

Blockchain technology enables the development of dApps that run on distributed networks, removing the need for centralized servers and intermediaries. dApps can be built on various blockchain platforms, such as Ethereum, Binance Smart Chain, and Solana, each offering unique features and capabilities for developers to leverage [51]. Decentralized applications can provide users with more secure, transparent, and efficient digital services, as they are less prone to censorship, downtime, and data breaches. The use of smart contracts in dApps enables the creation of self-executing agreements and automated processes, reducing friction and improving user experiences. dApps have numerous applications across various industries, including DeFi, gaming, social media, and supply chain management. The development of dApp ecosystems and marketplaces, such as DappRadar and State of the DApps, fosters innovation and collaboration in the Web3 space, promoting the growth of the decentralized application landscape.

- DeFi

Decentralization in Web3 has led to the emergence of DeFi, which aims to create a more open, transparent, and inclusive financial system by leveraging blockchain technology and smart contracts [52]. DeFi platforms provide users with various financial services, such as lending, borrowing, trading, and asset management, without the need for traditional financial intermediaries like banks and brokerages. Decentralized exchanges (DEXs), such as Uniswap and SushiSwap, enable users to trade digital assets directly with one another, reducing transaction costs and increasing market efficiency. DeFi protocols, such as Aave, Compound, and MakerDAO, provide decentralized lending and borrowing services, allowing users to access credit and earn interest on their digital assets. DeFi platforms can foster financial inclusion by providing users with access to financial services regardless of their geographical location or socio-economic status, as long as they have an internet connection and a compatible digital wallet. DeFi platforms often employ innovative tokenomics and governance models, such as liquidity mining and yield farming, to incentivize user participation and promote the growth of the ecosystem.

- Digital Identity and privacy

Decentralization in Web3 allows for the creation of secure and self-sovereign digital identity solutions, giving users control over their personal data and online interactions. Blockchain-based digital identity platforms, such as uPort and Civic, enable users to create and manage their digital identities, sharing only the necessary information with service providers and other parties [53]. Decentralized identity solutions can improve privacy by reducing the need for centralized data storage, which is often susceptible to data breaches and unauthorized access. Web3 digital identity systems can facilitate seamless and secure authentication and authorization processes, reducing the reliance on traditional username-password schemes and improving user experiences. Digital identity solutions in Web3 can be used across various applications, including finance, healthcare, education, and e-commerce, providing users with secure and interoperable identity management tools. Decentralized identity platforms can empower users to monetize their data and engage in data-sharing agreements on their terms, fostering a more equitable and user-centric digital ecosystem.

- DAOs

Web3 enables the creation of DAOs, which are self-governing entities that operate based on predefined rules encoded in smart contracts. DAOs can be used to facilitate decentralized governance, decision-making, and resource allocation processes, empowering users to participate in the development and management of projects and platforms [54]. Blockchain technology and smart contracts enable the automation of various processes within DAOs, reducing the need for manual intervention and administrative overhead. DAOs often employ token-based governance models, allowing users to influence decision-making and network upgrades by staking or delegating their tokens. DAOs have numerous applications across various industries, including finance, supply chain management, content creation, and social networking, providing users with more equitable and inclusive organizational structures. The development of DAO platforms and frameworks, such as Aragon, DAOstack, and Colony, fosters innovation and collaboration in the Web3 space, promoting the growth of the decentralized organization landscape.

- Decentralized data storage and management

Web3 promotes the decentralization of data storage and management, reducing reliance on centralized servers and data centers and

improving data privacy and security [55,56]. Decentralized data storage platforms, such as Filecoin, Storj, and IPFS, enable users to store and share data across a distributed network of nodes, ensuring data redundancy and resilience. Decentralized data management solutions can improve data privacy by allowing users to control access to their data, sharing it only with authorized parties. Decentralized data storage can reduce the risk of data breaches and unauthorized access by eliminating central points of failure and control. Decentralized data management platforms can enable more efficient and secure data exchange between various parties, fostering collaboration and innovation in areas such as research, healthcare, and finance. Decentralized data storage and management solutions can also contribute to a more sustainable digital ecosystem by reducing the energy consumption and environmental impact of centralized data centers.

- Scalability and Layer-2 solutions

Scalability is a crucial aspect of Web3 development, as decentralized applications and platforms require high throughput and low latency to handle growing user bases and increasing transaction volumes [57,58]. Many blockchain networks, such as Ethereum, are actively working on improving their scalability through upgrades, such as Ethereum 2.0, which introduces a proof-of-stake consensus mechanism and sharding to increase the network's capacity. Layer-2 solutions, such as Optimism, zkSync, and Polygon (previously Matic), provide scalability enhancements to existing blockchain networks by offloading some transactions and computations off the main chain, while still retaining the security and decentralization benefits. Layer-2 solutions employ various techniques, including optimistic rollups, zero-knowledge rollups, and state channels, to improve transaction throughput, reduce latency, and lower transaction fees. Scalable blockchain networks and Layer-2 solutions can support the development of more complex and resource-intensive decentralized applications, such as gaming, virtual reality, and decentralized social networks. Improved scalability in Web3 can contribute to a more accessible and user-friendly digital ecosystem, where users can interact with decentralized applications and platforms without experiencing bottlenecks or high transaction fees.

- Decentralized Web Infrastructure

Web3 aims to create a decentralized web infrastructure that can support the next generation of internet applications, with a focus on data privacy, security, and user control [59–61]. Decentralized Domain Name Systems (dDNS), such as Handshake and ENS, can provide users with more control over their domain names, reducing reliance on centralized domain registrars and promoting a more equitable and censorship-resistant internet. Decentralized Content Delivery Networks (dCDNs), such as Theta Network and Livepeer, can enable more efficient and resilient content distribution by leveraging the computing resources of a distributed network of nodes. Decentralized web hosting platforms, such as Dfinity's Internet Computer and Skynet, can support the development and deployment of decentralized applications and websites, without the need for centralized servers or hosting providers. Decentralized web infrastructure can contribute to a more open, accessible, and user-centric internet, where individuals and communities have greater control over their digital assets and online interactions. By creating a more decentralized web infrastructure, Web3 can foster innovation, collaboration, and user empowerment, paving the way for a more equitable, secure, and interconnected digital ecosystem.

2.4. Potential of Web3 in decentralization

- The potential of Web3 for social and environmental impact:

Web3 has the potential to drive social and environmental impact by promoting greater accountability, transparency, and sustainability in various industries and sectors [62]. Decentralized finance, for example, can offer new opportunities for financial inclusion, wealth creation, and poverty reduction, particularly in underbanked and underserved communities. Non-fungible tokens can enable new forms of ownership, expression, and value creation in the arts, music, and other creative industries, empowering artists and creators to monetize their work and engage with their audiences directly. Web3 can also address various environmental challenges, such as carbon emissions and energy consumption, by promoting more efficient, decentralized, and sustainable models for data storage, processing, and communication.

- The role of privacy and security in Web3

Privacy and security are critical aspects of Web3, enabling users to maintain control over their personal data, assets, and identities, and protecting them from various threats, such as cyberattacks, fraud, and theft. Web3 leverages various privacy-enhancing technologies, such as zero-knowledge proofs, homomorphic encryption, and multi-party computation, to enable secure and private data storage, sharing, and processing. Web3 also employs robust security measures, such as consensus algorithms, cryptographic hashing, and smart contract audits, to ensure the integrity and trustworthiness of decentralized platforms, applications, and digital assets. Privacy and security in Web3 require ongoing research, development, and innovation, as new threats and challenges emerge, and the ecosystem evolves and expands.

- The role of governance in Web3

Governance is a critical aspect of Web3, enabling decentralized platforms, applications, and organizations to make collective decisions, allocate resources, and enforce rules and policies [63]. Decentralized governance models, such as DAOs and other community-driven mechanisms, leverage blockchain technology and smart contracts to enable transparent, democratic, and decentralized decision-making processes. Governance in Web3 can address various challenges and issues, such as security, scalability, interoperability, and user participation, by fostering collaboration, innovation, and consensus-based solutions. Effective governance in Web3 requires a balance between decentralization and coordination, empowering users and communities while also ensuring the long-term sustainability and growth of the ecosystem.

- The importance of user experience in Web3

User experience (UX) is a critical aspect of Web3 adoption, as many users may find the decentralized and self-custodial nature of Web3 platforms and applications confusing or intimidating [64]. Web3 can improve UX by designing interfaces that are intuitive, user-friendly, and accessible, and by providing educational resources and support to help users navigate the ecosystem. Web3 can also leverage emerging technologies, such as virtual and augmented reality, to create immersive and engaging user experiences that enhance the value and appeal of decentralized platforms and applications. By prioritizing UX in Web3 development, we can reduce barriers to adoption and promote greater user participation and engagement in the ecosystem.

- The role of interoperability in Web3

Interoperability is a critical aspect of Web3, enabling different platforms, applications, and systems to communicate and interact with each other seamlessly. Interoperability can facilitate greater collaboration, innovation, and user adoption across the ecosystem, enabling users to access and use different services and assets without being restricted by network effects or other constraints [65]. Web3 can promote interoperability through cross-chain communication standards, such as the Inter-Blockchain Communication (IBC) protocol, and tokenization standards, such as ERC-20 and ERC-721. Interoperability in Web3 can

contribute to a more diverse and vibrant digital landscape, where users have more choice, control, and freedom over the platforms and services they use.

- The role of Web3 in the metaverse

The metaverse is a virtual universe that encompasses various digital environments, such as social media, gaming, and virtual reality [66]. Web3 can play a critical role in the metaverse by providing the infrastructure, tools, and standards necessary to enable interoperable and decentralized digital experiences. Web3 can facilitate the creation of decentralized virtual worlds, digital assets, and social platforms that enable greater user control, ownership, and participation. Web3 can also promote new forms of value creation, such as virtual real estate, digital art, and gaming assets, that can be traded and monetized across different platforms and environments.

- The potential of Web3 for decentralized finance

DeFi is a rapidly growing sector of Web3 that aims to provide financial services and products through decentralized platforms and protocols [67]. DeFi can offer various advantages over traditional finance, such as greater accessibility, transparency, and efficiency, by leveraging blockchain technology and decentralized governance models. DeFi platforms enable various financial activities, such as lending, borrowing, trading, and investing, using digital assets as collateral or value exchange. DeFi platforms can enable greater financial inclusion, particularly in underbanked and underserved communities, by providing access to financial services and products that were previously unavailable or restricted.

- The potential of Web3 for decentralized identity

Decentralized identity (DID) is a new paradigm for identity management that aims to give individuals greater control over their personal data and identity [68]. DID leverages blockchain technology and cryptographic techniques to create a decentralized, tamper-proof, and privacy-preserving identity infrastructure. DID can enable users to authenticate themselves, authorize access to their data, and manage their digital identities across different platforms and services. DID can address various challenges and issues with centralized identity management, such as data breaches, identity theft, and lack of user control and consent.

- The potential of Web3 for decentralized social media

Decentralized social media (DeSM) is a new paradigm for social media that aims to give users greater control over their data, privacy, and community governance [69]. DeSM leverages blockchain technology and decentralized governance models to create a user-centric, transparent, and decentralized social media ecosystem. DeSM platforms can enable users to own and control their data, monetize their content, and participate in community decision-making and resource allocation. DeSM platforms can address various challenges and issues with centralized social media, such as data breaches, censorship, and algorithmic bias.

- The potential of Web3 for decentralized gaming

Decentralized gaming (DeG) is a new paradigm for gaming that aims to provide users with greater ownership, control, and value exchange over their gaming assets and experiences [70]. DeG leverages blockchain technology and decentralized governance models to create a user-centric, transparent, and decentralized gaming ecosystem. DeG platforms can enable users to own and control their gaming assets, monetize their achievements, and participate in community decision-making and resource allocation. DeG platforms can address various challenges and issues with centralized gaming, such as lack of ownership, value extraction, and community governance.

- The potential of Web3 for decentralized energy systems

Decentralized energy systems (DeE) are a new paradigm for energy production, distribution, and consumption that aim to provide users with greater control, sustainability, and cost-effectiveness over their energy use [71]. DeE leverages blockchain technology and decentralized governance models to create a user-centric, transparent, and decentralized energy ecosystem. DeE platforms can enable users to produce, store, and trade energy using decentralized renewable sources, such as solar and wind power, without relying on centralized utilities or fossil fuels. DeE platforms can also enable greater efficiency, reliability, and resilience in energy systems, by leveraging smart contracts, peer-to-peer energy trading, and microgrids.

- The potential of Web3 for decentralized healthcare

Decentralized healthcare (DeH) is a new paradigm for healthcare that aims to provide users with greater control, privacy, and efficiency over their health data and services. DeH leverages blockchain technology and decentralized governance models to create a user-centric, transparent, and decentralized healthcare ecosystem. DeH platforms can enable users to own and control their health data, share it securely and selectively with healthcare providers, and participate in research and clinical trials. DeH platforms can also enable greater innovation, collaboration, and patient-centered care, by leveraging smart contracts, tokenization, and decentralized clinical trials [72].

2.5. *Interoperability*

Web3's interoperability is crucial for enabling cross-platform and cross-chain communication. It allows different decentralized applications to interact and exchange value with each other, regardless of their underlying blockchain or protocol. Here are some of the key features and benefits of Web3's interoperability.

- Standardized data formats and APIs

Standardized data formats and APIs are crucial for enabling interoperability between different applications and networks, by providing a common language and interface for data exchange. These data formats and APIs can include JSON-RPC, RESTful APIs, GraphQL, and other standardized formats and protocols. For example, the Ethereum JSON-RPC API is a widely used API for interacting with Ethereum nodes and smart contracts, and provides a standardized format for data exchange between different applications and platforms [73].

- Cross-chain asset wrapping and bridging

Cross-chain asset wrapping and bridging are critical for enabling interoperability between different blockchain networks and assets, by creating a standard way to represent and transfer assets across different networks. These wrapping and bridging mechanisms can include token standards such as ERC-20 and ERC-721, and interoperability protocols such as the Wrapped Bitcoin (WBTC) protocol. For example, the WBTC protocol allows Bitcoin to be wrapped as an ERC-20 token on the Ethereum network, enabling Bitcoin holders to use their Bitcoin assets on the Ethereum network [74].

- Interoperable identity and authentication

Interoperable identity and authentication systems are essential for enabling cross-platform and cross-chain user identity and access management, by providing a common way to verify and authenticate users across different networks and applications [75]. These identity and

authentication systems can include decentralized identity protocols such as Decentralized Identity Foundation (DIF) and decentralized authentication mechanisms such as OAuth. For example, the DIF provides a standard for decentralized identity management, enabling users to control their digital identities across different networks and platforms.

- Interoperable DeFi protocols

Interoperable DeFi protocols are crucial for enabling cross-platform and cross-chain DeFi applications and services, by providing a common way to interact and exchange value across different DeFi networks and protocols [76]. These DeFi protocols can include lending and borrowing protocols such as Aave and Compound, and liquidity protocols such as Uniswap and Curve. For example, the Aave protocol provides a lending and borrowing platform that can be accessed by different applications and networks, enabling users to borrow and lend assets across different DeFi protocols.

- Cross-chain and cross-network governance

Cross-chain and cross-network governance models are essential for enabling interoperability between different networks and protocols, by creating a common way to coordinate and govern the actions and decisions of different stakeholders and communities. These governance models can include DAOs and other decentralized governance frameworks that enable community-driven decision-making and coordination [77]. For example, the MakerDAO protocol uses a DAO-based governance model to manage its stablecoin ecosystem, enabling different stakeholders and communities to participate in the decision-making process and contribute to the growth and development of the protocol. Overall, Web3's interoperability is a critical feature for enabling cross-platform and cross-chain communication and value exchange. By leveraging standardized protocols, data formats, and APIs, as well as interoperable asset wrapping, identity and authentication systems, DeFi protocols, and governance models, Web3 can create a more open, inclusive, and connected digital ecosystem, enabling greater innovation, collaboration, and value creation.

- Interoperable decentralized storage

Interoperable decentralized storage is important for enabling cross-platform and cross-chain data storage and retrieval, by creating a common way to access and store data across different networks and protocols [78]. These decentralized storage solutions can include IPFS, Filecoin, and other decentralized storage protocols that allow users to store and access data in a decentralized and censorship-resistant manner. For example, IPFS provides a distributed file storage system that allows users to store and access files across different nodes and networks, and can be used by various decentralized applications and services.

- Interoperable messaging and communication

Interoperable messaging and communication systems are important for enabling cross-platform and cross-chain communication and collaboration, by creating a common way to communicate and share information across different networks and protocols [79]. These messaging and communication systems can include decentralized messaging protocols such as Whisper and Matrix, and social networking protocols such as ActivityPub. For example, Matrix is an open-source messaging protocol that allows users to communicate and share information across different networks and platforms, and can be integrated with various decentralized applications and services.

- Cross-chain and cross-network identity verification

Cross-chain and cross-network identity verification is crucial for enabling interoperability between different networks and protocols, by creating a common way to verify and authenticate user identities and access rights across different networks and platforms [80]. These identity verification systems can include decentralized identity verification protocols such as uPort and Civic, and blockchain-based identity verification systems such as Ontology and NEO. For example, uPort is a decentralized identity verification platform that allows users to control and manage their digital identities across different networks and platforms, and can be used by various decentralized applications and services [80].

- Interoperable decentralized marketplaces

Interoperable decentralized marketplaces are important for enabling cross-platform and cross-chain commerce and trade, by creating a common way to buy and sell goods and services across different networks and protocols [81]. These decentralized marketplaces can include open marketplaces such as OpenBazaar and Splyt, and protocol-based marketplaces such as the 0x protocol. For example, the 0x protocol is a decentralized exchange protocol that enables users to trade assets across different networks and platforms, and can be used by various decentralized marketplaces and services.

- Cross-chain and cross-network data analytics

Cross-chain and cross-network data analytics is essential for enabling interoperability between different networks and protocols, by creating a common way to analyze and visualize data across different networks and platforms [82]. These data analytics solutions can include decentralized data analytics platforms such as Ocean Protocol and Kylin Network, and blockchain-based data analytics solutions such as DEXTools and Dune Analytics. For example, Ocean Protocol is a decentralized data marketplace that allows users to share and monetize data across different networks and platforms, and can be used by various decentralized data analytics applications and services.

- Cross-network and cross-protocol smart contract interoperability

Cross-network and cross-protocol smart contract interoperability is important for enabling interoperability between different networks and protocols, by creating a common way to exchange and execute smart contracts across different chains and platforms [83]. These smart contract interoperability solutions can include interoperability protocols such as Polkadot's Substrate and Cosmos' IBC, and cross-chain bridge solutions such as ChainBridge and Wanchain. For example, Polkadot's Substrate framework provides a modular, customizable framework for building interoperable blockchains that can share logic and state across different chains and networks.

- Interoperable governance and dispute resolution mechanisms

Interoperable governance and dispute resolution mechanisms are important for enabling cross-network and cross-protocol coordination and decision-making, by creating a common way to resolve disputes and coordinate governance activities across different networks and protocols [84]. These governance and dispute resolution mechanisms can include decentralized arbitration and dispute resolution platforms such as Kleros and Aragon Court, and decentralized governance frameworks such as MolochDAO and Colony. For example, Kleros is a decentralized arbitration platform that provides a standardized dispute resolution protocol that can be used across different networks and protocols.

- Cross-chain and cross-protocol staking and validation

Cross-chain and cross-protocol staking and validation is important for enabling cross-network and cross-protocol consensus and security, by creating a common way to validate and secure different chains and

networks using a common set of validators and stakers. These staking and validation solutions can include interoperability protocols such as Cosmos' Stargate and Polkadot's Nominated Proof-of-Stake, and cross-chain and cross-protocol validator solutions such as the Sentinel Network [85]. For example, the Sentinel Network provides a cross-chain validator network that can be used to secure various chains and protocols, including Ethereum, Binance Smart Chain, and Polkadot.

- Interoperable cross-chain and cross-protocol NFTs

Interoperable cross-chain and cross-protocol NFTs are important for enabling cross-network and cross-protocol ownership and exchange of NFTs, by creating a common way to represent and exchange NFTs across different networks and platforms. These interoperable NFT solutions can include cross-chain and cross-protocol NFT standards such as ERC-1155 and NEP-171, and interoperability protocols such as ChainGuardian and Anyswap. For example, ChainGuardian is an interoperable NFT platform that allows users to mint, buy, and sell NFTs across different chains and protocols, using its own cross-chain NFT standard [86].

- Interoperable DAOs

Interoperable DAOs are important for enabling cross-network and cross-protocol coordination and decision-making among different decentralized communities and stakeholders, by creating a common way to govern and coordinate different DAOs across different networks and protocols [87]. These interoperable DAO solutions can include cross-chain and cross-protocol DAO frameworks such as Aragon and Colony, and DAO interoperability protocols such as DAOstack's ArcHives and Gnosis' SafeSnap. For example, Aragon is a decentralized governance framework that allows users to create and manage interoperable DAOs that can operate across different networks and protocols. Overall, Web3's interoperability is a constantly evolving and expanding field that requires ongoing innovation and collaboration among different stakeholders and communities. By leveraging a.

- Cross-chain and cross-network asset transfer

Cross-chain and cross-network asset transfer is important for enabling interoperability between different networks and protocols, by creating a common way to transfer assets and value across different chains and platforms. These asset transfer solutions can include cross-chain and cross-protocol bridges such as ThorChain and RenVM, and cross-network asset wrapping and tokenization solutions such as Polkadot's XCMP and Cosmos' IBC. For example, ThorChain is a cross-chain liquidity protocol that enables users to swap assets across different chains and protocols, using its own native asset wrapping and bridging mechanism [88].

- Cross-chain and cross-protocol identity verification and reputation systems

Cross-chain and cross-protocol identity verification and reputation systems are important for enabling interoperability between different networks and protocols, by creating a common way to verify and authenticate user identities and assess their reputation across different chains and platforms [89]. These identity verification and reputation systems can include decentralized identity verification and reputation protocols such as BrightID and HOPR, and blockchain-based identity verification and reputation systems such as Ontology's ONT ID and Polkadot's Kusama Identity Service (Kusama ID). For example, BrightID is a decentralized identity verification platform that allows users to verify their identities across different networks and protocols, using a trust-based reputation system.

- Cross-chain and cross-protocol gaming and virtual world interoperability

Cross-chain and cross-protocol gaming and virtual world interoperability is important for enabling cross-platform and cross-chain gaming and virtual world experiences, by creating a common way to exchange and interact with virtual assets and environments across different chains and networks. These gaming and virtual world interoperability solutions can include interoperable gaming protocols such as Enjin and Animoca Brands, and cross-chain and cross-protocol virtual world platforms such as Somnium Space and Decentraland. For example, Somnium Space is a virtual world platform that allows users to create, own, and trade virtual assets and environments across different networks and protocols, using its own interoperable virtual asset standard [90].

- Cross-chain and cross-protocol privacy and security solutions

Cross-chain and cross-protocol privacy and security solutions are important for enabling secure and private communication and transactions across different networks and protocols, by creating a common way to ensure privacy and security across different chains and platforms. These privacy and security solutions can include privacy-focused protocols such as the Secret Network and Oasis Network, and cross-chain and cross-protocol security solutions such as CertiK and Chainlink. For example, the Secret Network is a privacy-focused blockchain that allows users to communicate and transact securely across different chains and protocols, using its own privacy-preserving smart contract platform. Overall, Web3's interoperability is a vital aspect of its development and growth, as it allows for greater connectivity, collaboration, and innovation across different networks and protocols. By leveraging a range of interoperable protocols, systems, and solutions, Web3 can create a more open and inclusive digital ecosystem, enabling greater value creation and impact for users and communities around the world [91].

- Cross-chain and cross-protocol stablecoin interoperability

Cross-chain and cross-protocol stablecoin interoperability is important for enabling seamless and efficient value transfer across different networks and protocols, by creating a common way to exchange and use stablecoins across different chains and platforms [92]. These stablecoin interoperability solutions can include cross-chain and cross-protocol stablecoin platforms such as Terra and MakerDAO, and interoperability protocols such as the Interledger Protocol (ILP). For example, Terra is a stablecoin platform that enables cross-chain and cross-protocol stablecoin transfer and use, using its own native stablecoins pegged to various fiat currencies.

- Cross-chain and cross-protocol insurance and risk management

Cross-chain and cross-protocol insurance and risk management is important for enabling secure and efficient management of risk and uncertainty across different networks and protocols, by creating a common way to insure and protect assets and activities across different chains and platforms. These insurance and risk management solutions can include cross-chain and cross-protocol insurance protocols such as Nexus Mutual and Opyn, and interoperable risk management platforms such as BarnBridge. For example, Nexus Mutual is a decentralized insurance platform that allows users to insure their assets and activities across different networks and protocols, using its own native risk management and governance system [93].

- Cross-chain and cross-protocol energy and environmental interoperability

Cross-chain and cross-protocol energy and environmental interoperability is important for enabling more sustainable and efficient use of energy and natural resources across different networks and protocols, by creating a common way to manage and exchange energy and environmental assets and data across different chains and platforms [94]. These

energy and environmental interoperability solutions can include cross-chain and cross-protocol energy platforms such as Power Ledger and WePower, and interoperable environmental data platforms such as Ocean Protocol and ClimateChain. For example, Power Ledger is a decentralized energy platform that enables cross-chain and cross-protocol energy trading and management, using its own native energy token and trading platform.

- Cross-chain and cross-protocol healthcare and medical data interoperability

Cross-chain and cross-protocol healthcare and medical data interoperability is important for enabling secure and efficient sharing and management of healthcare and medical data across different networks and protocols, by creating a common way to store, share, and access medical data across different chains and platforms [95]. These healthcare and medical data interoperability solutions can include decentralized medical data platforms such as Medicalchain and Solve.Care, and cross-chain and cross-protocol healthcare data interoperability solutions such as the Health Nexus. For example, Medicalchain is a decentralized medical data platform that enables secure and transparent storage and sharing of medical data across different networks and protocols, using its own native medical data standard and interoperability protocol.

- Cross-chain and cross-protocol education and learning interoperability

Cross-chain and cross-protocol education and learning interoperability is important for enabling more accessible and inclusive education and learning experiences across different networks and protocols, by creating a common way to share and access edu cational content and credentials across different chains and platforms [96]. These education and learning interoperability solutions can include decentralized education platforms such as BitDegree and LearnX, and cross-chain and cross-protocol educational credentialing and verification systems such as the Learning Ledger. For example, BitDegree is a decentralized education platform that enables cross-chain and cross-protocol education content sharing and access, using its own native educational content standard and interoperability protocol.

- Cross-chain and cross-protocol payment interoperability

Cross-chain and cross-protocol payment interoperability is important for enabling efficient and secure payment processing across different networks and protocols, by creating a common way to exchange and use digital currencies across different chains and platforms [97]. These payment interoperability solutions can include cross-chain and cross-protocol payment gateways such as Utrust and PayPal, and interoperability protocols such as Ripple's ILP. For example, Utrust is a cross-chain payment gateway that enables merchants and users to accept and use a variety of digital currencies across different networks and protocols, using its own native payment processing and conversion system.

- Cross-chain and cross-protocol data and analytics interoperability

Cross-chain and cross-protocol data and analytics interoperability is important for enabling more accurate and comprehensive data analysis and decision-making across different networks and protocols, by creating a common way to access and analyze data and analytics across different chains and platforms [98]. These data and analytics interoperability solutions can include cross-chain and cross-protocol data and analytics platforms such as Chainlink and Ocean Protocol, and interoperability protocols such as the Streamr Network. For example, Chainlink is a decentralized oracle network that enables cross-chain and cross-protocol data and analytics integration and analysis, using its own native data and analytics standard and interoperability protocol.

- Cross-chain and cross-protocol social and community interoperability

Cross-chain and cross-protocol social and community interoperability is important for enabling more connected and collaborative digital communities and social networks across different networks and protocols, by creating a common way to interact and engage with different communities and social networks across different chains and platforms [99]. These social and community interoperability solutions can include cross-chain and cross-protocol social network platforms such as HUMAN Protocol and Nodle Network, and interoperability protocols such as the W3C Social Web Working Group. For example, HUMAN Protocol is a decentralized identity verification and human intelligence task platform that enables cross-chain and cross-protocol interaction and engagement across different networks and protocols, using its own native social and community interaction and engagement standard and interoperability protocol. Cross-chain and cross-protocol decentralized storage and.

- Computing Interoperability

Cross-chain and cross-protocol decentralized storage and computing interoperability is important for enabling more secure and efficient storage and computing of data and applications across different networks and protocols, by creating a common way to store and process data and applications across different chains and platforms [100]. These decentralized storage and computing interoperability solutions can include cross-chain and cross-protocol storage and computing platforms such as IPFS and Substrate, and interoperability protocols such as the Cosmos IBC protocol. For example, InterPlanetary File System (IPFS) is a decentralized storage and content-addressed distribution protocol that enables cross-chain and cross-protocol storage and distribution of data and applications, using its own native storage and computing standard and interoperability protocol. Overall, Web3's interoperability is a crucial factor in enabling the next stage of internet evolution, as it allows for greater connectivity, collaboration, and innovation across different networks and protocols. By leveraging a range of interoperable protocols, systems, and solutions, Web3 can create a more open and inclusive digital ecosystem, enabling greater value creation and impact for users and communities around the world.

- Cross-chain and cross-protocol DeFi interoperability

Cross-chain and cross-protocol DeFi interoperability is important for enabling more accessible and inclusive financial services and products across different networks and protocols, by creating a common way to access and use different DeFi platforms and applications across different chains and platforms [101]. These DeFi interoperability solutions can include cross-chain and cross-protocol DeFi platforms such as Aave and Compound, and interoperability protocols such as the Ethereum Layer 2 solutions. For example, Aave is a decentralized lending and borrowing protocol that enables cross-chain and cross-protocol access and use of its lending and borrowing services, using its own native interoperability solutions.

- Cross-chain and cross-protocol governance and decision-making interoperability

Cross-chain and cross-protocol governance and decision-making interoperability is important for enabling more transparent and democratic decision-making and governance across different networks and protocols, by creating a common way to participate and vote in different governance and decision-making processes across different chains and platforms [102]. These governance and decision-making interoperability solutions can include cross-chain and cross-protocol governance and decision-making platforms such as Aragon and DAOstack, and

interoperability protocols such as the Cosmos IBC protocol. For example, Aragon is a decentralized governance and decision-making platform that enables cross-chain and cross-protocol participation and voting in different governance and decision-making processes, using its own native interoperability solutions.

- Cross-chain and cross-protocol content and media interoperability

Cross-chain and cross-protocol content and media interoperability is important for enabling more accessible and diverse content and media experiences across different networks and protocols, by creating a common way to share, distribute, and access different types of content and media across different chains and platforms [103]. These content and media interoperability solutions can include cross-chain and cross-protocol content and media platforms such as Livepeer and Arweave, and interoperability protocols such as the InterPlanetary Linked Data (IPLD). For example, Livepeer is a decentralized video infrastructure platform that enables cross-chain and cross-protocol distribution and streaming of video content, using its own native content and media standard and interoperability protocol.

- Cross-chain and cross-protocol digital identity and reputation interoperability

Cross-chain and cross-protocol digital identity and reputation interoperability is important for enabling more secure and trustworthy digital identity and reputation systems across different networks and protocols, by creating a common way to verify, authenticate, and assess digital identities and reputations across different chains and platforms [104]. These digital identity and reputation interoperability solutions can include cross-chain and cross-protocol digital identity and reputation protocols such as Sovrin and uPort, and interoperability protocols such as the World Wide Web Consortium (W3C) Verifiable Credentials. For example, Sovrin is a decentralized digital identity platform that enables cross-chain and cross-protocol verification and authentication of digital identities, using its own native digital identity and reputation standard and interoperability protocol.

- Standardization and governance

Standardization and governance are important considerations for ensuring the compatibility and interoperability of different protocols, systems, and solutions in Web3 [105]. Standardization refers to the process of defining common standards and protocols that different systems can use to interact and exchange data and assets, while governance refers to the rules and mechanisms for managing and coordinating these standards and protocols. In Web3, there are several initiatives and organizations working on standardization and governance, such as the Interwork Alliance, the Web3 Foundation, and the W3C.

- Scalability and performance

Scalability and performance are critical factors for enabling seamless and efficient interoperability across different networks and protocols in Web3. Scalability refers to the ability of a system to handle increasing amounts of data, traffic, and transactions, while performance refers to the speed and reliability of the system in processing and executing these data, traffic, and transactions [106]. In Web3, there are several scalability and performance solutions being developed and implemented, such as sharding, Layer 2 solutions, and Proof-of-Stake consensus mechanisms.

- Security and privacy

Security and privacy are crucial considerations for ensuring the safety and integrity of data, assets, and interactions in Web3's interoperable digital ecosystem. Security refers to the protection against cyber-attacks, hacks, and fraud, while privacy refers to the protection of personal and sensitive information from unauthorized access and use. In Web3, there are several security and privacy solutions being developed and implemented, such as multi-signature wallets, zero-knowledge proofs, and decentralized identity and access management [107].

- User experience and adoption

User experience and adoption are key factors for driving the adoption and mainstreaming of Web3's interoperability solutions and applications. User experience refers to the ease and intuitiveness of using and interacting with Web3's interoperable systems and solutions, while adoption refers to the level of adoption and usage of these systems and solutions by different user groups and communities. In Web3, there are several user experience and adoption initiatives being pursued, such as user-friendly wallets and interfaces, educational and awareness campaigns, and incentives and rewards programs. Overall, Web3's interoperability is a powerful enabler of the next stage of internet evolution, offering a more connected, collaborative, and innovative digital ecosystem that can drive greater value creation and impact for users and communities around the world. By addressing the challenges and considerations of interoperability, Web3 can unlock its full potential and create a more open and inclusive digital future. Fig. 3 presents interoperable layered Web3 architecture [108]. This architecture is five-layered approach that pass data from lowest layer to the highest applications layer. The intermediate layers such as network, consensus and incentives support the whole Web3 activities. Several decentralized miners and millions of nodes generate and validate data via blockchains, crypto-analysers, NFTs, and wallets. Such decentralized data is then processed in next higher layer of network where privacy, trust, network security, propagation protocols, P2P protocols, and validation protocols act upon. Later, various consensus algorithms including PoW, PoS, PoC, PoET, PBFT and Delegated PoS are used to provide decentralized incentives in terms of rewards, and transaction fees. Finally, metaverse aware crypto applications are run at the backend.

2.6. *User-centricity and data privacy*

Web3's user-centricity and data privacy are crucial aspects of its next-generation internet evolution. By putting users in control of their own data and identity, Web3 is creating a more secure, transparent, and personalized digital ecosystem. Here are some additional insights and bulleted points to further improve the section on user-centricity and data privacy.

- Self-sovereign identity

SSI is a key feature of Web3's user-centricity and data privacy, enabling users to have full control and ownership of their identity and personal data. SSI allows users to create and manage their own digital identity, which can be used across different platforms and networks without relying on a centralized authority or intermediary. SSI is based on decentralized and cryptographic technologies, such as blockchain, which enable secure and trustless identity verification and authentication [109]. SSI can enhance privacy and security, as users can choose which data to share and with whom, and can revoke access at any time. SSI can also improve user experience, as users can have a seamless and consistent identity across different platforms and networks. Some examples of SSI projects and initiatives include the Sovrin Foundation, the Decentralized Identity Foundation, and the W3C Verifiable Credentials Working Group.

- Data ownership and control

Web3's user-centricity and data privacy also enable users to have greater ownership and control over their personal data, which can be

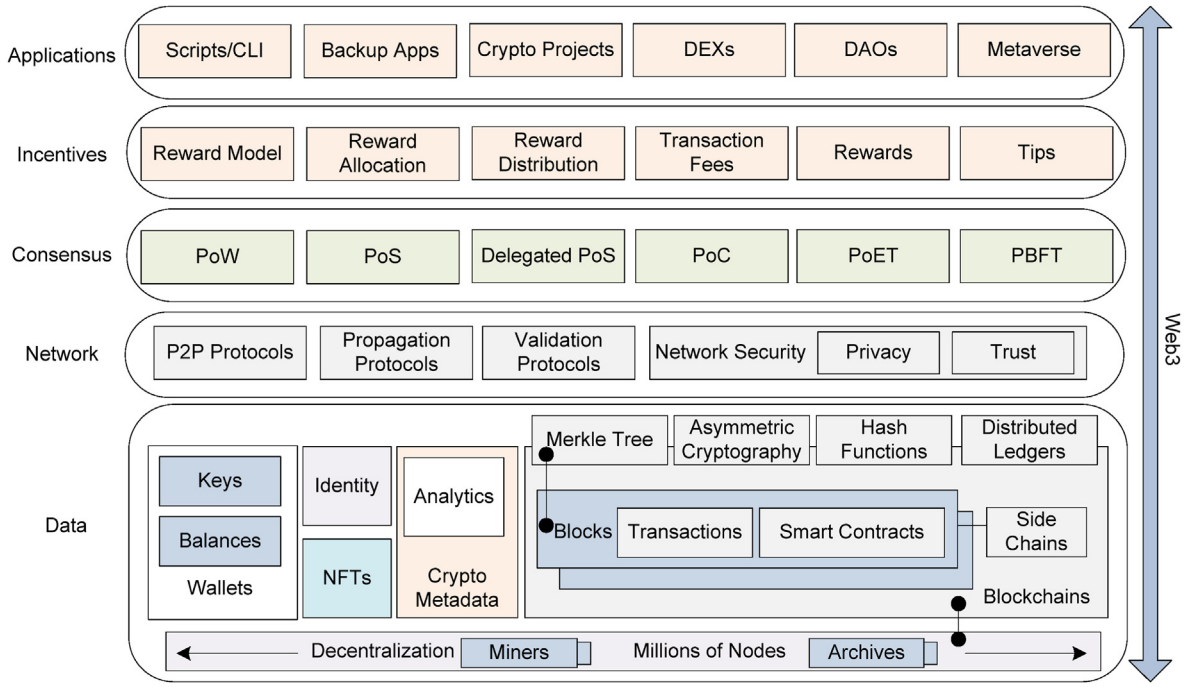

Fig. 3. Interoperable Web3 layered architecture.

used for various purposes, such as identity verification, authentication, and authorization [110]. With Web3, users can choose which data to share and with whom, and can also monetize their data through decentralized data marketplaces and other incentive mechanisms. Decentralized storage systems, such as IPFS and Filecoin, can also enable secure and efficient storage and retrieval of user data, without relying on centralized servers or databases. Data ownership and control can enhance privacy and security, as users can prevent unauthorized access and use of their data, as well as reduce the risk of data breaches and hacks. Data ownership and control can also foster innovation and collaboration, as users can share and collaborate on data in a more open and transparent way, without relying on centralized intermediaries or gatekeepers. Some examples of Web3-based data ownership and control initiatives include Ocean Protocol, Data Union, and MyData.

- Privacy-preserving technologies

Web3's user-centricity and data privacy also rely on various privacy-preserving technologies and mechanisms, such as zero-knowledge proofs, homomorphic encryption, and differential privacy. Zero-knowledge proofs enable secure and private verification and authentication of data and transactions, without revealing any sensitive information [111]. Homomorphic encryption enables computation and processing of encrypted data, without decrypting it, thus preserving privacy and security. Differential privacy enables statistical analysis and processing of data, while protecting individual privacy and confidentiality. Privacy-preserving technologies can enhance privacy and security, while also enabling data sharing and collaboration in a more trustworthy and efficient way. Some examples of Web3-based privacy-preserving technologies and initiatives include Zcash, Enigma, and NuCypher.

- Challenges and opportunities

While Web3's user-centricity and data privacy present many opportunities and benefits, they also pose challenges and risks, such as the potential for misuse, abuse, or manipulation of data and identity. To address these challenges, Web3 needs to develop and implement robust governance, regulation, and security frameworks that can ensure the responsible and ethical use of user data and identity [112,113]. Web3 also needs to address the issue of data interoperability and portability, as users may want to move their data across different platforms and networks without losing control or privacy. Moreover, Web3 needs to ensure that privacy-preserving technologies are user-friendly and accessible, and do not create additional barriers or complexity for users. Finally, Web3 needs to promote awareness and education on user-centricity and data privacy, and engage with users and communities in a transparent and participatory way. Some opportunities and benefits of Web3's user-centricity and data privacy include empowering users and communities, fostering innovation and collaboration, promoting diversity and inclusion, and enhancing privacy and security in the digital ecosystem. Self-sovereign identity and data ownership and privacy are key features of Web3, that aim to empower users to have full control and ownership of their digital identity and data, and to protect their privacy from unauthorized access and exploitation. These features are enabled by various technologies and mechanisms, such as DIDs, verifiable credentials, identity wallets, data wallets, zero-knowledge proofs, and decentralized storage. Self-sovereign identity and data ownership and privacy offer various benefits and challenges, and require robust security, governance, and ethical frameworks, as well as engagement with various stakeholders and communities in a transparent and participatory way.

2.7. Tokenomics and digital assets

Web3 is closely linked to the concept of tokenomics and the use of digital assets [114–117]. Tokenomics refers to the study of how tokens are designed, issued, distributed, and utilized within a given blockchain network or ecosystem. Digital assets, in this context, are tokens or coins that represent various assets, such as cryptocurrencies, NFTs, and security tokens.

- Cryptocurrencies

Cryptocurrencies are digital currencies that use cryptography to secure transactions and control the creation of new units. Bitcoin, which was introduced in 2009, was the first cryptocurrency to gain widespread attention. Since then, numerous other cryptocurrencies have emerged,

including Ethereum, Litecoin, Ripple, and many more. Cryptocurrencies offer a range of benefits, including low transaction fees, fast settlement times, and increased privacy. Some other insights into cryptocurrencies are.

- Cryptocurrencies are decentralized, which means that they are not controlled by any single entity or organization.
- Cryptocurrencies have a finite supply, which makes them a deflationary asset.
- Cryptocurrencies can be used for a variety of purposes, including payments, investments, and store of value.

- Tokenomics and digital assetsNFTs

NFTs are digital tokens that represent unique assets, such as artwork, music, videos, and other creative works. NFTs are created using blockchain technology, which ensures that each token is unique and can be verified as authentic. NFTs have gained popularity in recent years, with high-profile sales of digital art and other collectibles reaching millions of dollars. NFTs offer new opportunities for artists, creators, and collectors to monetize their work and build communities around their content. Some other insights into NFTs are.

- NFTs are unique, which means that they cannot be replicated or duplicated.
  •NFTs can be used to represent a wide range of assets, including digital art, music, videos, and more.
- NFTs have the potential to revolutionize the way that creators monetize their work, by providing a direct connection between creators and fans.

- Tokenomics and digital assetsDeFi

DeFi refers to financial services and applications that are built on blockchain networks and operate without intermediaries. DeFi includes a range of services, including lending and borrowing, asset management, insurance, and more. DeFi is enabled by smart contracts, which allow for automated and trustless transactions between parties. DeFi has gained traction in recent years, with total value locked in DeFi protocols reaching billions of dollars. DeFi offers new opportunities for financial inclusion, transparency, and innovation. Some other insights into DeFi are.

- DeFi is built on open-source technology, which means that anyone can participate in DeFi networks and protocols.
- DeFi allows for peer-to-peer transactions without the need for intermediaries, which can result in lower fees and faster settlement times.
- DeFi has the potential to disrupt traditional financial services, by providing more accessible and transparent alternatives to traditional banking and investing.

2.8. Key features of tokenomics and digital assets

- Programmability

Digital assets are programmable, meaning that they can be designed to perform specific functions or execute specific instructions. This feature allows for the creation of smart contracts, which are self-executing contracts that can be programmed to automatically trigger specific actions when certain conditions are met. Smart contracts enable a wide range of applications, including DeFi, supply chain management, and identity verification [118].

- Liquidity

Digital assets can be traded on DEXs and other trading platforms, allowing for greater liquidity and price discovery. This feature allows investors and traders to buy and sell digital assets quickly and easily, without the need for intermediaries or centralized exchanges. Decentralized exchanges are also more resistant to hacking and fraud, as they do not hold custody of users' assets.

- Transparency

Blockchain technology provides a high level of transparency, making it possible to track the ownership and movement of digital assets. This feature allows for greater accountability and trust in transactions, as all parties can view the transaction history of a given asset. This transparency is especially important in the case of public blockchains, where all transaction data is publicly available.

- Security

Digital assets are secured using cryptography and distributed ledger technology, making them resistant to fraud and hacking. This feature ensures that digital assets are protected from unauthorized access or manipulation, as each transaction must be verified by multiple participants on the blockchain network. Additionally, the use of public and private keys adds an extra layer of security to digital asset ownership.

- Interoperability

Digital assets can be designed to be interoperable, meaning they can be used across different blockchain networks and ecosystems. This feature allows for greater flexibility in the use of digital assets, as they can be easily transferred between different platforms and networks. Interoperability is especially important as the number of blockchain networks and platforms continues to grow.

- Community Governance

Digital assets can be used to incentivize participation and engagement in decentralized networks and communities, allowing for community-driven governance and decision-making. This feature is especially important in decentralized networks, where there is no central authority to make decisions. By incentivizing community participation, digital assets can help ensure the long-term sustainability and growth of decentralized networks.

- Token Economics

Tokenomics involves the study of how digital assets are designed, issued, and used within a given blockchain ecosystem. Token economics can have a significant impact on the value and utility of digital assets. Factors such as token supply, distribution, and usage can all affect the value of digital assets, making token economics a crucial consideration in the design of blockchain networks and applications.

- Cryptocurrencies

Digital assets can include cryptocurrencies, which are decentralized digital currencies that use cryptography to secure transactions and control the creation of new units. Cryptocurrencies offer a range of benefits, including low transaction fees, fast settlement times, and increased privacy.

- NFTs

NFTs are digital tokens that represent unique assets, such as artwork, music, videos, and other creative works. NFTs are created using blockchain technology, which ensures that each token is unique and can be

verified as authentic. NFTs have gained popularity in recent years, with high-profile sales of digital art and other collectibles reaching millions of dollars. NFTs offer new opportunities for artists, creators, and collectors to monetize their work and build communities around their content [119].

- DeFi

DeFi refers to financial services and applications that are built on blockchain networks and operate without intermediaries. DeFi includes a range of services, including lending and borrowing, asset management, insurance, and more. DeFi is enabled by smart contracts, which allow for automated and trustless transactions between parties. DeFi has grown significantly in recent years, with billions of dollars in assets locked in various DeFi protocols. DeFi offers several benefits, including greater accessibility, lower transaction fees, and increased transparency and security.

- Tokenization

Tokenization refers to the process of representing real-world assets, such as real estate, commodities, and securities, as digital tokens on a blockchain. Tokenization can help to increase liquidity and accessibility for these assets, as well as reduce costs and streamline the process of buying and selling them.

- Governance Tokens

Governance tokens are digital tokens that are used to participate in the governance of a decentralized network or platform. Governance tokens allow holders to vote on proposals and decisions related to the network or platform, and can also be used to earn rewards or incentives for participating in governance [120].

- Staking

Staking involves holding digital assets in a specific wallet or account, known as a staking pool, to help secure the network and earn rewards. Staking is a key feature of many blockchain networks, as it helps to ensure the security and stability of the network by incentivizing participants to hold and use the network's digital assets.

- Cross-chain Interoperability

Cross-chain interoperability refers to the ability of digital assets to be used across multiple blockchain networks and ecosystems. This feature is becoming increasingly important as the number of blockchain networks and platforms continues to grow, and can help to promote greater liquidity and accessibility for digital assets [121].

- Privacy-enhancing Technologies

Privacy-enhancing technologies, such as zero-knowledge proofs and secure multi-party computation, are increasingly being used to improve the privacy and security of digital assets and transactions. These technologies allow for private transactions and data sharing on a blockchain, while still maintaining the integrity and security of the network.

3. Web3 technologies and protocols

Web3 technologies and protocols are essential for the growth and development of decentralized applications and networks. These technologies enable the creation of secure, transparent, and decentralized systems that allow for greater trust and innovation. In this section, we will explore some of the key Web3 technologies and protocols, including blockchain platforms and smart contracts, decentralized storage solutions, decentralized identity management, and interoperability protocols. We will examine how these technologies are used in Web3 applications, and how they are driving the evolution of the internet towards a more decentralized and user-centric future.

3.1. Blockchain platforms and smart contracts

- Ethereum: Ethereum is a decentralized blockchain platform that supports smart contracts and decentralized applications. It is the most widely used blockchain platform for developing decentralized applications and is home to the largest DeFi ecosystem [122].
- Polkadot: Polkadot is a next-generation blockchain platform that allows for interoperability between different blockchains. It enables cross-chain communication and allows developers to create specialized blockchains, called parachains, to meet specific use cases [123].
- Cardano: Cardano is a blockchain platform that uses a proof-of-stake consensus mechanism to validate transactions. It aims to offer a more energy-efficient and sustainable alternative to proof-of-work blockchains, like Bitcoin [124].
- Solana: Solana is a high-performance blockchain platform that uses a proof-of-stake consensus mechanism. It is designed to handle high transaction volumes and is known for its fast processing times and low transaction fees [125].
- Binance Smart Chain: Binance Smart Chain is a blockchain platform that is built on top of the Binance Chain. It supports smart contracts and is designed to be compatible with the Ethereum Virtual Machine (EVM), enabling developers to port their Ethereum-based applications to Binance Smart Chain [126].
- Cosmos: Cosmos is a blockchain platform that allows for the creation of independent blockchains that can communicate and transact with each other. It allows for the creation of interconnected blockchain networks, known as the “Internet of Blockchains” [127].
- Tezos: Tezos is a blockchain platform that uses a self-amending protocol to enable upgrades and improvements to the network without hard forks. It uses a proof-of-stake consensus mechanism and supports smart contracts [128].
- Avalanche: Avalanche is a blockchain platform that uses a consensus mechanism called Avalanche to enable high transaction throughput and low latency. It supports smart contracts and enables the creation of interoperable subnets [129].
- Nervos: Nervos is a blockchain platform that uses a layered architecture to enable scalability and interoperability between different blockchain networks. It supports smart contracts and allows for the creation of decentralized applications [130].
- IOTA: IOTA is a blockchain platform that uses a directed acyclic graph (DAG) structure, known as the Tangle, to enable fast and feeless transactions. It is designed to be used for the IoT and supports smart contracts [131].
- Hedera Hashgraph: Hedera Hashgraph is a blockchain platform that uses a consensus mechanism called Hashgraph to enable fast and secure transactions. It is designed to be used for enterprise applications and supports smart contracts [132].
- Near Protocol: Near Protocol is a blockchain platform that uses a sharding mechanism to enable scalability and high transaction throughput. It supports smart contracts and is designed to be developer-friendly [133].
- Algorand: Algorand is a blockchain platform that uses a proof-of-stake consensus mechanism to enable fast and secure transactions. It supports smart contracts and is designed to be scalable and energy-efficient [134]. Table 2 presents comparison of blockchain platforms and smart contracts.

3.2. Decentralized storage solutions

Decentralized storage solutions are an essential component of Web3 technology. They enable secure and efficient storage and sharing of data

Table 2
Comparison of blockchain platforms and smart contracts.

Blockchain Platform	Consensus Mechanism	Scalability	Interoperability	Smart Contract Support	Governance	Data Privacy and Security	Decentralized Applications
Ethereum	Proof of Work (transitioning to Proof of Stake)	Medium	Limited	Fully Turing-Complete	Decentralized	Limited	Wide
Polkadot	Nominated Proof of Stake	High	Yes	Cross-chain messaging and interoperability	Decentralized	High	Wide
Cardano	Proof of Stake	High	Limited	High assurance and security for smart contracts	Decentralized	High	Wide
Solana	Proof of History, Tower BFT	High	Limited	High throughput and low latency	Decentralized	High	Wide
Binance Smart Chain	Proof of Stake	High	Yes	Interoperability with Binance Chain	Centralized	Limited	Wide
Cosmos	Tendermint Consensus	High	Yes	Interoperability between blockchain networks	Decentralized	Limited	Wide
Tezos	Liquid Proof of Stake	High	Limited	Self-amendment and formal verification	Decentralized	High	Wide
Avalanche	Avalanche Consensus	High	Limited	High throughput and low latency	Decentralized	High	Wide
Nervos	Proof of Work, Proof of Stake	High	Yes	High security and scalability	Decentralized	High	Wide
IOTA	Tangle Consensus	High	Limited	Scalability and feeless transactions	Decentralized	High	Narrow
Hedera Hashgraph	Hashgraph Consensus	High	Yes	High throughput and low latency	Centralized	High	Narrow
Near Protocol	Proof of Stake	High	Limited	High throughput and low latency	Decentralized	Limited	Wide
Algorand	Pure Proof of Stake	High	Limited	High security and decentralization	Decentralized	High	Wide

on a decentralized network. Here are some list of decentralized storage solutions.

- Swarm: Swarm is a decentralized storage platform that enables users to store and share data on a peer-to-peer network. It uses a unique incentivization mechanism to ensure the availability and durability of stored data [135].
- Arweave: Arweave is a blockchain-based storage platform that uses a proof-of-access consensus mechanism to ensure the permanent storage of data. It allows users to store data permanently on the blockchain without the need for ongoing storage fees [136].
- Sia: Sia is a decentralized storage platform that allows users to rent out their unused storage space to others. It uses smart contracts to automate storage agreements and provides users with a highly secure and efficient storage solution [137].
- Filecoin: Filecoin is a decentralized storage platform that combines blockchain technology with traditional cloud storage. It provides users with secure and reliable storage services that are both cost-effective and scalable [138].
- Storj: Storj is a decentralized storage platform that uses a distributed network of nodes to store data. It allows users to rent out their unused storage space and provides them with a highly secure and efficient storage solution [139].
- MaidSafe: MaidSafe is a decentralized storage platform that uses a peer-to-peer network to store and share data. It uses a unique consensus mechanism, called the Safe Network, to ensure the secure and efficient storage of data [140].
- Bluzelle: Bluzelle is a decentralized storage platform that uses a unique consensus mechanism, called swarming, to ensure the availability and durability of stored data. It allows users to store data securely and efficiently on a decentralized network [141]. Table 3. Presents comparison of decentralized storage solutions.

3.3. Decentralized identity management

- Sovrin: Sovrin is a decentralized identity management platform that uses a global public utility for identity verification. It allows users to have full control over their digital identity and personal data and provides a highly secure and privacy-preserving solution [142,143].
- Civic: Civic is a decentralized identity management platform that uses blockchain technology to verify user identity. It provides a secure and efficient way to verify identity for various use cases, such as online purchases, travel, and government services [144].
- BrightID: BrightID is a decentralized identity management platform that uses social connections to verify user identity. It allows users to prove their uniqueness and establish trust without revealing any personally identifiable information [144].
- HATDEX: HATDEX is a decentralized identity management platform that uses a Personal Data Store (PDS) to allow users to control and manage their personal data. It enables users to share their data with trusted third parties without compromising their privacy [145].

Table 3
Comparison of decentralized storage solutions.

Blockchain Platform	Consensus Mechanism	Scalability	Interoperability	Smart Contract Support	Governance	Data Privacy and Security	Decentralized Applications
Swarm	Proof of custody	Medium	Yes	Yes	DAO	Private keys and encryption	Yes
Arweave	Proof of access	High	Yes	No	DAO	Encryption and data sharding	Yes
Sia	Proof of storage	High	No	No	DAO	Private keys and encryption	No
Filecoin	Proof of replication	High	Yes	Yes	DAO	Proofs and encryption	Yes
Storj	Proof of replication	High	Yes	No	DAO	Encryption and erasure coding	Yes
MaidSafe	PARSEC consensus	High	No	No	DAO	Self-encryption and data sharding	Yes
Bluzelle	Tendermint	High	Yes	Yes	DAO	Byzantine fault tolerance	Yes
Stori	Proof of replication	High	No	No	DAO	Encryption and replication	Yes

- 3Box: 3Box is a decentralized identity management platform that uses a decentralized database to store and manage user profiles and data. It allows users to control their data and share it with trusted third parties while maintaining their privacy [146].
- SelfKey: SelfKey is a decentralized identity management platform that uses blockchain technology to enable users to verify their identity and access various services. It provides a highly secure and efficient way to manage digital identity and personal data [147].
- DID: It is a type of decentralized identity management tool that allows users to create and control their own digital identities on a decentralized network. They provide a secure and privacy-preserving way to verify identity and enable users to share their data with trusted third parties [148].
- uPort: uPort is a decentralized identity management platform that uses blockchain technology to provide users with a secure and efficient way to manage their digital identity and personal data. It allows users to create and control their own identity and data and share it with trusted third parties [149].
- ION: ION is a decentralized identity management platform that uses the Bitcoin blockchain to enable users to create and control their own digital identity. It provides a highly secure and privacy-preserving way to verify identity and share data with trusted third parties [150]. Table 4 presents comparison of decentralized identity management solutions.

3.4. Interoperability protocols

Interoperability protocols are critical for enabling communication and interaction between different blockchain networks and decentralized applications. Here are some examples of interoperability protocols.

- Chainlink: Chainlink is an interoperability protocol that provides secure and reliable communication between blockchain networks and external data sources. It enables decentralized applications to access real-world data in a trustless and decentralized manner [151].
- Wanchain: Wanchain is a cross-chain interoperability protocol that allows for communication and transfer of assets between different blockchain networks. It uses a unique architecture that supports both public and private blockchains and enables the creation of new decentralized applications [152].
- Arkane Network: Arkane Network is an interoperability protocol that provides a unified API for interacting with multiple blockchain networks. It allows developers to build decentralized applications that can interact with various blockchain networks without the need for extensive knowledge of each network's unique architecture [153].
- Polkastarter: Polkastarter is an interoperability protocol that enables cross-chain swapping of assets between different blockchain networks. It provides a highly secure and efficient way to exchange assets and enables the creation of new DeFi applications [154].
- Ren Protocol: Ren Protocol is a cross-chain interoperability protocol that enables the transfer of assets between different blockchain networks in a trustless and decentralized manner. It uses a unique architecture that ensures the privacy and security of asset transfers [155].
- Polygon: Polygon (formerly known as Matic Network) is an interoperability protocol that provides a highly scalable and efficient solution for building decentralized applications on the Ethereum network. It allows for faster and cheaper transactions and enables the creation of new use cases for decentralized applications [156]. Table 5 presents comparison of interoperability protocols.

Key Lessons Learned.

- Web3 technologies and protocols are crucial for the growth and development of decentralized applications and networks, promoting secure, transparent, and decentralized systems.
- Various blockchain platforms and smart contracts, such as Ethereum, Polkadot, Cardano, Solana, Binance Smart Chain, Cosmos, Tezos, Avalanche, Nervos, IOTA, Hedera Hashgraph, Near Protocol, and Algorand, provide different consensus mechanisms, scalability, interoperability, and governance structures.
- Decentralized storage solutions, including Swarm, Arweave, Sia, Filecoin, Storj, MaidSafe, and Bluzelle, offer secure and efficient storage and sharing of data on decentralized networks.
- Decentralized identity management platforms, such as Sovrin, Civic, BrightID, HATDEX, 3Box, SelfKey, DID, uPort, and ION, allow users to control their digital identities and personal data, providing privacy-preserving solutions.
- Interoperability protocols, including Chainlink, Wanchain, Arkane Network, Polkastarter, Ren Protocol, and Polygon, enable communication and interaction between different blockchain networks and decentralized applications, fostering cross-chain functionality and the growth of decentralized applications.

4. Applications and use cases

Decentralized applications, or dApps, are software applications that run on a decentralized network, such as a blockchain. These applications are built to provide the same functionality as traditional centralized applications, but with a focus on decentralization, transparency, and security. Here are some of the popular decentralized applications as follows.

Table 4
Comparison of decentralized identity management solutions.

Decentralized Identity Management Tool	Interoperability	Smart Contract Support	Governance	Data Privacy and Security	Decentralized Application	User Experience	Community Size
Sovrin	Yes	No	Sovrin Foundation	Zero-knowledge proofs	Yes	Good	Medium
Civic	Yes	No	Civic Technologies	Secure multiparty computation	Yes	Good	Large
BrightID	Yes	No	BrightID community	Public key cryptography	Yes	Good	Medium
HATDEX	Yes	No	HAT community	End-to-end encryption	Yes	Good	Small
3Box	Yes	Yes	3Box community	End-to-end encryption	Yes	Good	Small
SelfKey	Yes	Yes	SelfKey Foundation	End-to-end encryption	Yes	Good	Medium
DID	Yes	Yes	Decentralized	Various cryptographic methods	Yes	Good	Medium
uPort	Yes	Yes	uPort community	Public key cryptography	Yes	Good	Medium
ION	Yes	No	Microsoft	Public key cryptography	Yes	Good	Large

Table 5
Comparison of interoperability protocols.

Interoperability Tool	Consensus Mechanism	Scalability	Interoperability	Smart Contract Support	Governance	Data Privacy and Security	Decentralized Application	Liquidity Provider
Chainlink	Proof of Stake	High	Multi-chain	Yes	Community	Confidentiality	Yes	Uniswap
Wanchain	Proof of Stake	High	Cross-chain	Yes	Community	Privacy-preserving	Yes	WanSwap
Arkane	Proof of Stake	High	Multi-chain	Yes	Community	Confidentiality	Yes	QuickSwap
Polkastarter	Proof of Stake	High	Multi-chain	Yes	Community	Confidentiality	Yes	Uniswap
Ren Protocol	Byzantine Fault Tolerance (BFT)	High	Cross-chain	Yes	Community	Privacy-preserving	Yes	Curve.fi
Polygon	Proof of Stake	High	Multi-chain	Yes	Community	Confidentiality	Yes	QuickSwap

4.1. DApps

- Decentralized Social Media Platforms

Decentralized social media platforms aim to address the concerns of privacy, data ownership, and censorship faced by centralized social media platforms. Some popular examples of decentralized social media platforms are as follows.

- o Steemit: A social media platform where users are rewarded for their contributions to the network in the form of cryptocurrency [157].
- o Mastodon: A decentralized micro-blogging platform that allows users to create their own instances of the network, giving them control over their data and moderation policies [158].
- o Peepeth: A decentralized Twitter-like platform that is built on the Ethereum blockchain and focuses on promoting ethical behavior and positive interactions [159].

- Decentralized Marketplaces for Goods and Services

Decentralized marketplaces aim to eliminate intermediaries and provide a platform for direct peer-to-peer transactions. Here are some examples:

- o OpenBazaar: A decentralized marketplace that allows users to buy and sell goods and services without any fees or restrictions [160].
- o Bitify: A decentralized marketplace for buying and selling digital products and services, such as software licenses and website templates [161].
- o Origin Protocol: A decentralized platform for creating and managing online marketplaces, built on the Ethereum blockchain [162].

- Decentralized Prediction Markets

Decentralized prediction markets allow users to bet on the outcome of real-world events, such as elections and sports matches. These markets are designed to incentivize accurate predictions and provide a platform for people to share information and opinions. Some examples include:

- o Augur: A decentralized platform for creating and trading prediction markets. It is built on the Ethereum blockchain and allows users to create markets on any topic [163].
- o Gnosis: A platform that enables the creation of decentralized prediction markets for various use cases, such as insurance and financial forecasting [164].

- Decentralized gaming platforms

Decentralized gaming platforms are built on blockchain technology and enable peer-to-peer gaming without the need for intermediaries. Examples of decentralized gaming platforms include:

- o Axie Infinity: a blockchain-based game that enables players to collect, breed, and battle creatures called Axies [165].
- o Decentraland: a virtual world that is owned and operated by its users, where users can buy, sell, and build virtual assets [166].

- Decentralized voting systems

Decentralized voting systems are designed to ensure fair and transparent elections. These systems operate on a blockchain network, where votes are recorded and stored in a tamper-proof manner. Examples of decentralized voting systems include:

- o Horizon State: a platform that enables secure and transparent voting for various use cases, such as corporate governance and community decision-making [167].
- o Agora: a blockchain-based platform that enables secure and transparent voting for national elections [168].

- Decentralized education platforms

Decentralized education platforms are designed to provide accessible and affordable education to users worldwide. These platforms operate on a blockchain network, where users can access educational content and earn certifications. Examples of decentralized education platforms include:

- o BitDegree: a platform that enables users to access educational content and earn digital certifications for completing courses [169].
- o TeachMePlease: a decentralized platform that enables users to access educational content and interact with teachers from around the world [170].

- Decentralized healthcare platforms

Decentralized healthcare platforms are designed to provide secure and transparent healthcare services to users worldwide. These platforms operate on a blockchain network, where users can access healthcare services and share their medical data in a secure manner. Examples of decentralized healthcare platforms include:

- o MedCredits: a platform that enables patients to connect with doctors for virtual consultations and second opinions [171].
- o Patientory: a blockchain-based platform that enables patients to Another example of a dApp is the Brave browser, which integrates the Basic Attention Token (BAT) to provide a more private and secure browsing experience. Users can earn BAT by opting into viewing ads, which can be used to support their favourite content creators or exchanged for other cryptocurrencies [172].

In addition, decentralized education platforms like ODEM offer a peer-to-peer marketplace for educators and students to connect and exchange knowledge, without the need for traditional intermediaries like universities. Decentralized healthcare platforms like Solve.Care aim to streamline healthcare administration by using blockchain technology to automate administrative tasks, reduce costs, and improve patient outcomes. For example, patients can use the platform to schedule

appointments, manage medical records, and receive remote care. Table 6 presents comparison of DApps in various applications.

4.2. DeFi

DeFi refers to a financial system built on top of blockchain technology that is designed to be open, transparent, and accessible to anyone. DeFi applications aim to eliminate intermediaries and replace them with smart contracts that are self-executing and enforceable. The following are some of the key use cases of DeFi:

- DEXs

These are platforms that allow users to trade cryptocurrencies in a peer-to-peer (P2P) manner without the need for intermediaries. DEXs use smart contracts to execute trades automatically, and users retain control of their funds throughout the process. Examples include Uniswap, PancakeSwap, and SushiSwap.

  - o Uniswap: DEX platform for ERC-20 tokens on Ethereum [173].
  - o PancakeSwap: DEX platform for BEP-20 tokens on Binance Smart Chain [174].
  - o SushiSwap: It is a decentralized exchange platform built on the Ethereum blockchain that allows users to trade cryptocurrencies and earn rewards in its native token SUSHI [175].

- Decentralized lending and borrowing platforms

These platforms allow users to lend or borrow cryptocurrency without the need for intermediaries. Loans are issued through smart contracts, and interest rates are determined by supply and demand. Examples include Aave, Compound, and MakerDAO.

  - o Aave: Decentralized lending and borrowing platform on Ethereum [176].
  - o Compound: Decentralized lending and borrowing platform on Ethereum [177].
  - o MakerDAO: It is a decentralized autonomous organization that governs the Maker protocol, which allows users to generate the stablecoin DAI by locking up collateral in exchange for a loan [178].

- Decentralized stablecoins

Stablecoins are cryptocurrencies that are pegged to a stable asset, such as the US dollar or gold. Decentralized stablecoins are issued through smart contracts and aim to provide price stability in the volatile cryptocurrency market. Examples include DAI, USDT, and USDC.

  - Dai: Decentralized stablecoin pegged to the US dollar on Ethereum [179].
  - USDT (Tether): It is a stablecoin cryptocurrency pegged to the US dollar and backed 1:1 by assets held in reserve, designed to maintain a stable value equivalent to one USD [180].
  - USDC: It is a stablecoin that is pegged to the US dollar and operates on the Ethereum blockchain, with the aim of providing a more stable cryptocurrency for use in everyday transactions and financial activities [181].

- Decentralized insurance platforms:

These platforms offer insurance services to users through smart contracts, eliminating the need for intermediaries. Insurance policies are automatically executed when specific conditions are met, such as a flight delay or a natural disaster. Examples include Nexus Mutual and Etherisc.

Table 6
Comparison of DApps in various use cases.

Name	Functionality	Scalability	Interoperability	Smart Contract Support	Governance	Data Privacy and Security	Decentralized Application
Steemit	Decentralized social media platform	High	Low	Yes	Decentralized autonomous organization based	Privacy of user data with encryption and IPFS	Yes
Mastodon	Decentralized microblogging platform	High	Low	No	Decentralized moderation by instance admins	User data privacy with encryption	Yes
Peepeth	Decentralized microblogging platform	High	Low	Yes	User-owned moderation	User data privacy with encryption	Yes
OpenBazaar	Decentralized marketplace for goods and services	High	Low	Yes	Decentralized governance by token holders	User data privacy with encryption	Yes
Bitify	Decentralized marketplace for goods and services	High	Low	No	Decentralized moderation by token holders	User data privacy with encryption	Yes
Origin Protocol	Decentralized marketplace for goods and services	High	Medium	Yes	Decentralized autonomous organization based	User data privacy with encryption and IPFS	Yes
Augur	Decentralized prediction markets	Medium	Medium	Yes	Decentralized autonomous organization based	User data privacy with encryption	Yes
Gnosis	Decentralized prediction markets and trading platform	Medium	Medium	Yes	Decentralized autonomous organization based	User data privacy with encryption	Yes
Axie Infinity	Decentralized gaming platform	High	Low	Yes	Decentralized autonomous organization based	User data privacy with encryption	Yes
Decentraland	Decentralized virtual reality platform	High	Low	Yes	Decentralized autonomous organization based	User data privacy with encryption	Yes
HorizonState	Decentralized voting system for communities and groups	High	Low	Yes	Decentralized governance by token holders	User data privacy with encryption	Yes
Agora	Decentralized voting system for communities and groups	High	Low	Yes	Decentralized autonomous organization based	User data privacy with encryption	Yes
BitDegree	Decentralized education platform	High	Low	Yes	Decentralized governance by token holders	User data privacy with encryption	Yes
teachMePlease	Decentralized education platform	High	Low	No	Decentralized moderation by community	User data privacy with encryption	Yes
MedCredits	Decentralized healthcare platform	High	Low	Yes	Decentralized autonomous organization based	User data privacy with encryption	Yes
Patientory	Decentralized healthcare platform	High	Low	Yes	Decentralized moderation by healthcare providers	User data privacy with encryption	Yes

- Nexus Mutual: Decentralized insurance platform for smart contract risks on Ethereum [182].
- Etherisc: Decentralized insurance platform for various insurance products on Ethereum [183].

- Decentralized asset management platforms:

These platforms allow users to manage their cryptocurrency portfolios through smart contracts. Users can set up automated investment strategies or follow the strategies of professional traders. Examples include Melon, Enzyme, and Set Protocol.

- Melon: Decentralized asset management platform on Ethereum [184].
- Set Protocol: Platform for creating and managing tokenized portfolios on Ethereum [185].
- Enzyme: It is a decentralized asset management platform that enables developers to create, scale, and monetize on-chain investment strategies [186].

- Decentralized derivatives platforms:

These platforms allow users to trade derivatives, such as options and futures, without intermediaries. Derivatives are issued through smart contracts, and the terms are automatically enforced. Examples include dYdX and Synthetix.

- dYdX: It is a DEX that provides margin trading and lending for cryptocurrencies, allowing traders to earn interest on their deposits and access leveraged positions [187].
- Synthetix: Synthetix is a decentralized finance platform on the Ethereum blockchain that enables the creation of synthetic assets, including cryptocurrencies, commodities, and fiat currencies, that can be traded without the need for an intermediary [188]. Table 7 presents comparison of DeFi platforms.

4.3. NFTs

- Digital art marketplaces: NFTs have enabled the creation of digital art that is unique, verifiable, and ownable. Platforms like SuperRare, Nifty Gateway, and OpenSea allow artists to mint and sell their digital artworks as NFTs, with ownership recorded on the blockchain. Examples include SuperRare,

  Nifty Gateway, Async Art.

- SuperRare - Platform for buying and selling rare digital art [189].
- Nifty Gateway - Marketplace for limited edition NFT drops by popular artists and brands [190].
- Async Art - Platform for creating and selling programmable and dynamic NFTs [191].

- Collectibles and memorabilia platforms: NFTs have also revolutionized the way collectibles and memorabilia are bought and sold. NBA Top Shot is a popular platform where users can buy, sell, and trade NFT-based collectibles in the form of moments from NBA games. Examples include CryptoKitties, NBA Top Shot, Crypto Collectibles.
  - CryptoKitties - Game for collecting and breeding unique digital cats [192].

Table 7
Comparison of DeFi platforms.

Name	Functionality	Scalability	Interoperability	Smart Contract Support	Governance	Data Privacy and Security	Decentralized Application
Uniswap	Decentralized exchange for swapping ERC-20 tokens	High	Low	Yes	Token holders	Public data on-chain	Yes
PancakeSwap	Decentralized exchange for swapping BEP-20 tokens	High	Low	Yes	Token holders	Public data on-chain	Yes
SushiSwap	Decentralized exchange for swapping ERC-20 tokens	High	Low	Yes	Token holders	Public data on-chain	Yes
Aave	Decentralized lending and borrowing platform for crypto	High	Low	Yes	Token holders	Public data on-chain	Yes
Compound	Decentralized lending and borrowing platform for crypto	High	Low	Yes	Token holders	Public data on-chain	Yes
MakerDAO	Decentralized platform for creating and managing DAI	High	Low	Yes	Token holders	Public data on-chain	Yes
DAI	Decentralized stablecoin	High	Low	Yes	Token holders	Public data on-chain	Yes
USDT	Decentralized stablecoin	High	Low	Yes	Token holders	Public data on-chain	Yes
USDC	Decentralized stablecoin	High	Low	Yes	Token holders	Public data on-chain	Yes
Nexus Mutual	Decentralized platform for buying and selling insurance	High	Low	Yes	Token holders	Private data off-chain	Yes
Etherisc	Decentralized insurance platform	High	Low	Yes	Token holders	Private data off-chain	Yes
Melon	Decentralized asset management platform	High	Low	Yes	Token holders	Public data on-chain	Yes
Enzyme	Decentralized asset management platform	High	Low	Yes	Token holders	Public data on-chain	Yes
Set Protocol	Decentralized asset management platform	High	Low	Yes	Token holders	Public data on-chain	Yes
Augur	Decentralized platform for prediction markets	High	Low	Yes	Token holders	Public data on-chain	Yes
Gnosis	Decentralized platform for prediction markets	High	Low	Yes	Token holders	Public data on-chain	Yes
Synthetix	Decentralized platform for synthetic assets	High	Low	Yes	Token holders	Public data on-chain	Yes
dYdX	Decentralized platform for margin trading	High	Low	Yes	Token holders	Public data on-chain	Yes

- NBA Top Shot - Platform for buying and trading officially licensed NBA NFTs [193].
- Crypto Collectibles - Marketplace for buying and selling a wide variety of NFTs.

- Gaming and virtual world assets: NFTs are being used in the gaming industry to create rare and unique in-game assets that can be bought, sold, and traded. Decentraland is a virtual world built on the Ethereum blockchain that uses NFTs as the basis for its in-game assets. Examples include Axie Infinity, Decentraland, The Sandbox.
  - The Sandbox - Virtual world and gaming platform built on blockchain technology [194].
- Music and other creative content ownership and licensing: NFTs are being used to enable artists to sell and manage the ownership of their creative content. Audius is a music streaming platform that uses NFTs to enable artists to monetize their work and manage their copyright ownership. Examples include Audius, Ujo, Mycelia.
  - Audius - Music streaming platform with a focus on artist control and ownership [195].
  - Ujo - Platform for connecting artists with fans and enabling direct payments for their work [196].
  - Mycelia - Platform for enabling fair and transparent payment and distribution systems for music [197]. Table 8. Presents comparisons NFTs.

4.4. DAOs

DAOs are organizations that operate autonomously and are governed by smart contracts on a blockchain. DAOs are designed to be decentralized, transparent, and democratic, with decision-making power distributed among their members. Table 9 presents comparisons of DAOS.

- Decentralized Governance Structures for Companies and Organizations

DAOs can be used as decentralized governance structures for companies and organizations, enabling members to have a say in the decision-making process. This can include anything from voting on company policies to electing board members. Examples of DAOs in this category include Aragon, MolochDAO, and MakerDAO.

- o Aragon: Governance platform for decentralized organizations [198].
- o MolochDAO: Community-run DAO for funding Ethereum-based projects [199].
- o MakerDAO: Decentralized platform for creating stablecoins [200].

- Decentralized Investment Funds and Venture Capital

DAOs can also be used as decentralized investment funds and venture capital firms. Members can pool their funds together and make investment decisions collectively, without the need for intermediaries such as banks or traditional venture capitalists. Examples of DAOs in this category include The LAO, MetaCartel Ventures, and dYdX.

- o The LAO: Decentralized autonomous organization for investing in Ethereum-based projects [201].
- o MetaCartel Ventures: DAO for investing in Ethereum-based projects [202].

- Decentralized Decision-Making Processes for Communities and Groups

Finally, DAOs can be used as decentralized decision-making processes for communities and groups, enabling members to make decisions together and allocate resources more effectively. Examples of DAOs in this category include DAOstack, Colony, and Giveth.

- o DAOstack: Platform for creating decentralized autonomous organizations [203].
- o Colony: Decentralized platform for creating and managing organizations [204].
- o Giveth: Decentralized platform for charitable donations [205].

4.5. Supply chain management and provenance tracking

- Decentralized tracking of goods and products: With the use of blockchain technology, supply chain management can be made more transparent and efficient. Decentralized tracking allows companies to track their products from the source to the final destination, giving them more control over their supply chain. Examples include VeChain (VET), Ambrosus (AMB), Waltonchain (WTC), Provenance (PRO), TE-FOOD (TONE).
  - o VeChain: A blockchain platform for supply chain management and business processes [206].
  - o Ambrosus: A blockchain platform for supply chain management, food safety, and quality assurance [207].
  - o Waltonchain: A blockchain platform for supply chain management and IoT integration [208].
  - o Provenance: A blockchain platform for supply chain management, transparency, and sustainability [209].
  - o TE-FOOD: A blockchain platform for supply chain management and food traceability [210].
- Decentralized verification of product authenticity and quality: By using decentralized solutions such as blockchain, companies can ensure that their products are authentic and of high quality. Decentralized verification can also help to prevent counterfeiting and fraud, which is a major problem in many industries. Examples include CertiK (CTK), Everledger (EVE), Devery (EVE).
  - o CertiK: A blockchain platform for secure smart contract development and auditing [211].
  - o Everledger: A blockchain platform for tracking and verifying the provenance of diamonds and other luxury goods [212].
  - o Devery: A blockchain platform for product verification and tracking [213].
- Decentralized tracing of product origins and histories: Decentralized tracing allows companies to track the origin of their products,

Table 8
Comparison of NFTs.

Platform	Functionality	Scalability	Interoperability	Smart Contract Support	Decentralized Application
SuperRare	Digital art marketplace	High	Ethereum	Yes	Yes
Nifty Gateway	Digital art marketplace and NFT platform	High	Ethereum	Yes	Yes
Async Art	Programmable digital art marketplace	High	Ethereum	Yes	Yes
CryptoKitties	Collectibles platform for digital cats	High	Ethereum	Yes	Yes
NBA Top Shot	Collectibles platform for basketball highlights	High	Flow	Yes	Yes
Crypto Collectibles	Collectibles platform for various items	High	Ethereum	Yes	Yes
The Sandbox	Virtual world platform with NFT assets	High	Ethereum	Yes	Yes
Audius	Decentralized music streaming platform	High	Ethereum	Yes	Yes
Ujo	Music platform for creators and fans	High	Ethereum	Yes	Yes
Mycelia	Music rights platform	High	Ethereum	Yes	Yes

Table 9
Comparison of DAOs.

Name	Functionality	Scalability	Interoperability	Smart Contract Support	Governance	Data Privacy and Security	Decentralized Application
Aragon	Creation and management of DAOs and decentralized companies	Good	Yes	Yes	On-chain voting	Transparent	Yes
MolochDAO	Crowdfunding and management of DAOs	Good	Yes	Yes	On-chain voting	Transparent	Yes
MakerDAO	Creation and management of stablecoin DAI	Good	Yes	Yes	On-chain voting	Transparent	Yes
The LAO	Investment fund for blockchain startups	Good	Yes	Yes	On-chain voting	Transparent	Yes
metaCartel Ventures	Startup accelerator for blockchain-based projects	Good	Yes	Yes	On-chain voting	Transparent	Yes
DAOstack	Creation and management of DAOs and decentralized companies	Good	Yes	Yes	On-chain voting	Transparent	Yes
Colony	Decentralized project management platform	Good	Yes	Yes	On-chain voting	Transparent	Yes
Giveth	Decentralized platform for charitable giving	Good	Yes	Yes	On-chain voting	Transparent	Yes

including the source of raw materials, production facilities, and transportation methods. This information can be used to ensure that products are ethically sourced and produced, and can also help to prevent issues such as foodborne illness. Examples include OriginTrail (TRAC), Skuchain, Ambrosus (AMB).
  - o OriginTrail: A blockchain platform for supply chain data management and sharing [214].
  - o Skuchain: A blockchain platform for supply chain management and document verification [215].
- Decentralized monitoring of supply chain conditions and sustainability efforts: By using blockchain-based solutions, companies can monitor the conditions of their supply chain and ensure that their products are produced in an environmentally sustainable manner. Decentralized monitoring can also help to ensure that workers are treated fairly and that supply chain practices are ethical. Examples include Sweetbridge (SWT), Provenance (PRO), Ambrosus (AMB).
  - o Sweetbridge: It is a blockchain-based lending and borrowing platform that aims to streamline supply chain financing by connecting asset owners and lenders [216].

Table 10 presents comparison of supply chain management and provenance tracking. Table 11. Presents comparison of various applications and use cases classifications.

Key Lessons Learned:

- Decentralization and transparency: Decentralized applications and platforms can offer greater transparency, security, and trust compared to their centralized counterparts. This is particularly important in industries where data integrity, provenance, and authenticity are crucial.
- Elimination of intermediaries: Blockchain technology enables direct peer-to-peer transactions, reducing the need for intermediaries and, in turn, lowering transaction costs and improving efficiency.
- User empowerment and control: Decentralized platforms empower users by giving them more control over their data, assets, and decision-making processes. This can lead to increased privacy, security, and a more equitable distribution of resources and power.
- Incentivization and tokenization: Many decentralized platforms make use of tokens and cryptocurrencies to incentivize user participation, creating new economic models and monetization opportunities for users, content creators, and service providers.
- Cross-industry applicability: The use cases mentioned above demonstrate that blockchain technology and decentralized applications have potential applications across various industries, including finance, healthcare, education, supply chain management, and more.
- Challenges and limitations: Despite the potential benefits, there are challenges and limitations to consider when implementing decentralized solutions, such as scalability, energy consumption, regulatory compliance, and user adoption.
- Collaboration and interoperability: As the decentralized ecosystem grows, it is essential to ensure collaboration and interoperability among different platforms, protocols, and technologies. This will enable seamless integration and help to maximize the potential benefits of decentralization.

5. Zero-trust architecture for Web3

The rise of Web3 and dApps has brought about a new paradigm shift in how we think about security and trust online. With Web3, the Internet is transformed into a more decentralized, secure, and transparent environment, powered by blockchain technology [217–222]. To ensure the

Table 10
Comparison of supply chain management and provenance tracking.

Name	Consensus Mechanism	Scalability	Interoperability	Smart Contract Support	Governance	Data Privacy and Security	Decentralized Application
VeChain (VET)	Proof of Authority	High	Yes	Yes	Foundation	Yes	Yes
Ambrosus (AMB)	Proof of Authority	High	Yes	Yes	DAO	Yes	Yes
Waltonchain (WTC)	Proof of Work and Stake	High	Yes	Yes	Foundation	Yes	Yes
Provenance (PRO)	Proof of Authority	High	Yes	Yes	DAO	Yes	Yes
TE-FOOD (TONE)	Proof of Authority	High	Yes	Yes	Foundation	Yes	Yes
CertiK (CTK)	Proof of Stake	High	Yes	Yes	DAO	Yes	Yes
Everledger (EVE)	Not disclosed	High	No	Yes	Private	Yes	Yes
Devery (EVE)	Proof of Authority	High	No	Yes	DAO	Yes	Yes
OriginTrail (TRAC)	Proof of Stake	High	Yes	Yes	DAO	Yes	Yes
Skuchain	Not disclosed	High	No	Yes	Private	Yes	Yes
Sweetbridge (SWT)	Not disclosed	High	Yes	Yes	DAO	Yes	Yes

Table 11
Comparison of various applications and use cases classifications.

Parameter	Decentralized Applications	Decentralized Finance	Non-fungible Tokens	Decentralized Autonomous Organizations	Supply Chain Management and Provenance Tracking
Functionality	Social media, marketplaces, gaming, voting, education, healthcare	Decentralized exchanges, lending, stablecoins, insurance, asset management, prediction markets, derivatives	Digital art, collectibles, virtual world assets, creative content ownership and licensing	Decentralized governance, investment funds, decision-making processes	Decentralized tracking, verification, tracing, monitoring
Scalability	Varies depending on the specific dApp	Varies depending on the specific DeFi platform	Varies depending on the specific NFT marketplace or platform	Varies depending on the specific DAO	Varies depending on the specific supply chain use case
Interoperability	Varies depending on the specific dApp and blockchain protocols used	Varies depending on the specific DeFi platform and blockchain protocols used	Varies depending on the specific NFT marketplace or platform and blockchain protocols used	Varies depending on the specific DAO and blockchain protocols used	Varies depending on the specific supply chain use case and blockchain protocols used
Smart Contract Support	Yes	Yes	Yes	Yes	Yes
Governance	Decentralized decision-making processes	Decentralized decision-making processes	Decentralized decision-making processes	Decentralized decision-making processes	Decentralized decision-making processes
Data Privacy and Security	Varies depending on the specific dApp and platform	Varies depending on the specific DeFi platform and protocol	Varies depending on the specific NFT marketplace or platform	Varies depending on the specific DAO and platform	Varies depending on the specific supply chain use case and platform
Decentralized Application	Yes	Yes	Yes	Yes	Yes

security of this ecosystem, the concept of zero-trust architecture has become increasingly important. Zero-trust architecture is a security model that assumes no user, device, or service can be trusted by default. Instead, trust must be continuously verified through multiple layers of authentication, authorization, and encryption. The concept of zero trust has its origins in traditional IT environments, but it is now being adopted and adapted to the Web3 ecosystem.

5.1. Key principles of zero-trust architecture

Zero-trust architecture is built upon a set of fundamental principles that help create a secure and resilient environment. These principles ensure that security measures are consistently applied and adapted to address the evolving threat landscape. The key principles of zero-trust architecture include [223–230]:

- Never Trust, Always Verify

This principle emphasizes the need to assume that any user, device, or application could be a potential threat. Instead of relying on trust based on network location or previous interactions, every access request must be authenticated, authorized, and validated before granting access.

- Least Privilege Access

Grant users, devices, and applications the minimum level of access required to perform their tasks. This approach minimizes the potential damage in case of a security breach by limiting the attacker's ability to move laterally within the network or escalate privileges.

- Micro-segmentation

Divide the network into smaller segments, each with its own security policies and access controls. This approach prevents unauthorized access to sensitive data or resources and limits the potential damage in case of a breach.

- Multi-factor Authentication (MFA)

Require users to provide multiple forms of verification to confirm their identity before granting access. MFA reduces the risk of unauthorized access due to compromised credentials, as it requires the attacker to bypass multiple layers of authentication.

- Context-aware Access Controls

Make access decisions based on contextual information, such as user role, device posture, location, and risk factors. This approach ensures that access controls adapt to the current situation and take into account potential threats or vulnerabilities.

- Continuous Monitoring and Validation

Monitor user activities, device health, and application behavior in real-time to detect potential threats or anomalies. Regularly validate security controls, policies, and configurations to ensure their effectiveness in addressing evolving threats.

- Data Protection

Secure sensitive data at rest, in transit, and during processing by implementing encryption, tokenization, and other data protection techniques. Implement strong access controls and monitoring to prevent unauthorized access to sensitive data.

- User and Entity Behavior Analytics (UEBA)

Analyze user and entity behavior to identify patterns and detect anomalies that may indicate potential threats or malicious activities. UEBA enables organizations to proactively respond to potential security incidents and minimize the potential damage.

- Visibility and Analytics

Gain comprehensive visibility into user activities, device health, and application behavior across the entire environment. Use analytics to identify trends, detect potential threats, and inform decision-making regarding security policies and controls.

- Integration and Automation

Integrate security tools, processes, and solutions to enable seamless communication and collaboration. Leverage automation to streamline security operations, reduce human error, and enhance the organization's

ability to respond to potential threats.

5.2. Benefits of zero-trust architecture in Web3

Implementing a zero-trust architecture in the Web3 ecosystem offers numerous advantages that can help organizations build secure and resilient decentralized applications, networks, and services [231–235]. Some key benefits of employing zero-trust principles in the Web3 context include [236–251]:

- Enhanced Security

By adopting the "never trust, always verify" principle, Web3 applications can proactively counter threats and minimize the risk of unauthorized access, data breaches, and other security incidents.

- Reduced Attack Surface

Micro-segmentation and least privilege access help limit an attacker's ability to move laterally within the network, reducing the overall attack surface and containing the potential damage from a security breach.

- Adaptability

Zero-trust architecture allows organizations to adapt to the dynamic and evolving nature of the Web3 ecosystem. By considering context and risk factors in access decisions, zero-trust architecture ensures that security measures remain relevant and effective in various situations.

- Decentralized Identity Management

Implementing zero-trust principles in Web3 enables the integration of decentralized identity solutions, improving user privacy and control over personal data while maintaining robust access control mechanisms.

- Data Protection and Privacy

Zero-trust architecture emphasizes data protection throughout its lifecycle, ensuring that sensitive information is secured at rest, in transit, and during processing. This is particularly important in Web3, where data is often distributed across multiple nodes and platforms.

- Scalability and Flexibility

Zero-trust principles can be applied to various aspects of the Web3 environment, including user and device authentication, smart contract security, and access control mechanisms for decentralized applications. This flexibility enables organizations to scale security measures as their Web3 infrastructure grows and evolves.

- Interoperability

Zero-trust architecture promotes the integration and collaboration of security tools and processes, which is crucial in the Web3 ecosystem, where multiple technologies and platforms coexist. This interoperability enables organizations to build comprehensive and consistent security measures across their decentralized infrastructure.

- Automated Security

Implementing automation in zero-trust architecture helps streamline security operations, enhance responsiveness to potential threats, and reduce the risk of human error. This is particularly beneficial in the Web3 context, where the rapid pace of innovation demands efficient and effective security measures.

- Visibility and Analytics

Gaining comprehensive visibility into user activities, device health, and application behavior across the Web3 environment enables organizations to identify trends, detect potential threats, and inform decision-making regarding security policies and controls.

- Proactive Threat Mitigation

Continuous monitoring, real-time threat detection, and user and entity behavior analytics help organizations proactively respond to potential security incidents, minimizing the potential damage and reducing the likelihood of successful attacks in the Web3 ecosystem.

5.3. Zero-trust architecture platforms

Various zero-trust architectures have been proposed and implemented in both traditional IT environments and the emerging Web3 landscape. This section provides an overview of some of the most prominent zero-trust architectures, highlighting their key features and potential applicability to Web3.

- Google's BeyondCorp

BeyondCorp is a zero-trust security model developed by Google to shift access controls from the network perimeter to individual devices and users. It eliminates the traditional concept of a trusted internal network, instead focusing on device and user authentication. BeyondCorp's approach to device and user-centric security can be adapted to the Web3 environment. By focusing on user and device authentication, Web3 applications can leverage BeyondCorp's principles to provide secure access to decentralized services and resources [252].

- Forrester's Zero Trust eXtended (ZTX) Framework

Forrester's ZTX framework is an evolution of the zero-trust model, extending its principles to cover data, networks, devices, people, and workloads. The ZTX framework emphasizes the importance of data security and aims to protect data throughout its entire lifecycle. Web3 applications and platforms can benefit from the ZTX framework's comprehensive approach to security. By incorporating its data-centric principles, Web3 applications can ensure the privacy and integrity of user data, both on-chain and off-chain [253].

- NIST SP 800-207: Zero Trust Architecture

NIST SP 800-207 provides guidelines for implementing zero-trust architectures within organizations. The document outlines the key components of a zero-trust architecture, including policies, governance, and technologies, and offers recommendations for implementing these components. The NIST guidelines can serve as a valuable resource for organizations building and deploying Web3 applications. By following the recommendations provided in NIST SP 800-207, Web3 developers can create secure and resilient decentralized systems that adhere to zero-trust principles [254]. Fig. 4 presents the zero-trust network view for NIST SP 800-207 where various components interact with each other via data and control wise plane structure. Continuous diagnostics mitigation (CDM), public key infrastructure (PKI), and security information and event management (SIEM) provide important role in this architecture.

Cloudflare's Zero Trust Platform offers a suite of tools and services designed to help organizations implement a zero-trust architecture. This includes features such as access management, device posture enforcement, and secure application delivery. As Web3 applications often rely on cloud infrastructure and services, Cloudflare's Zero Trust Platform can provide additional security layers to protect these applications. By leveraging Cloudflare's tools, Web3 developers can enforce access

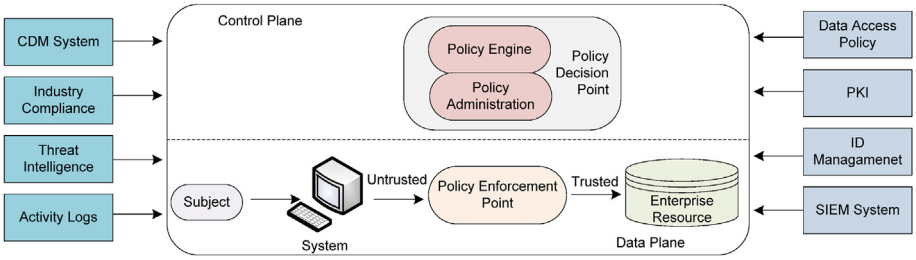

Fig. 4. Zero-Trust view of network of NIT SP 800-207.

- Cloudflare's Zero Trust Platform

controls, secure data in transit, and monitor network activity for potential threats [255].

- Microsoft's Zero Trust Model

Microsoft's Zero Trust Model focuses on the protection of identities, devices, applications, and data, aiming to prevent breaches and limit their impact. It emphasizes the principles of verify explicitly, use least privilege access, and assume breach, providing a comprehensive approach to security. Microsoft's Zero Trust Model can be adapted to the Web3 context by applying its principles to decentralized identities, dApps, and data storage. By incorporating these principles, Web3 developers can enhance security, prevent unauthorized access, and mitigate potential breaches [256].

- Cisco's Zero Trust Architecture

Cisco's Zero Trust Architecture is a security framework that covers workforce, workloads, and workplace. It aims to provide secure access to applications and data based on dynamic trust levels, user context, and device security posture. Cisco's Zero Trust Architecture can be applied to Web3 by focusing on the security of decentralized applications, user identities, and device access. Implementing the dynamic trust assessment and context-aware access control mechanisms can further enhance the security of Web3 platforms and dApps [257].

- Okta's Zero Trust Framework

Okta's Zero Trust Framework is centered on identity and access management, with a focus on ensuring that the right people have the right access to the right resources at the right time. It provides a comprehensive suite of tools for user authentication, authorization, and access management. The Okta Zero Trust Framework can be integrated into Web3 applications by leveraging decentralized identity solutions and blockchain-based access control mechanisms. By adopting Okta's focus on identity-driven security, Web3 developers can ensure that access to resources and data is tightly controlled and managed [258].

- Palo Alto Networks' Prisma Access

Palo Alto Networks' Prisma Access is a cloud-based security platform that enables organizations to implement zero-trust network access (ZTNA) for remote users and devices. It offers features such as multi-factor authentication, micro-segmentation, and context-aware access controls. Prisma Access can be applied to the Web3 ecosystem by securing remote access to decentralized applications and services. By incorporating ZTNA principles, Web3 developers can create secure remote access solutions that protect user data and maintain the privacy and integrity of the decentralized network [259].

- Akamai's Zero Trust Security Solutions

Akamai's zero-trust security solutions include the Enterprise Application Access (EAA) and Enterprise Threat Protector (ETP) products. These solutions focus on secure application access, device posture enforcement, and threat intelligence to protect against potential security risks. Akamai's solutions can be applied to Web3 by securing access to decentralized applications, ensuring device integrity, and leveraging threat intelligence to proactively identify and mitigate potential risks. This can help create a more secure Web3 ecosystem by protecting users, devices, and applications [260].

- Illumio's Adaptive Security Platform (ASP)

Illumio's ASP is a micro-segmentation and zero-trust security solution that helps organizations protect critical applications and data. It offers visibility into application dependencies, real-time threat monitoring, and automated policy enforcement to maintain a strong security posture. Illumio's ASP can be adapted to the Web3 environment by implementing micro-segmentation and automated policy enforcement in the context of decentralized networks and applications. This can help secure the Web3 ecosystem by isolating potentially compromised components and preventing unauthorized access to sensitive data [261].

- Zscaler's Zero Trust Exchange

Zscaler's Zero Trust Exchange is a cloud-based security platform that enables organizations to implement zero-trust access controls for users, devices, and applications. It offers features such as multi-factor authentication, application segmentation, and secure web gateways to protect against cyber threats. Zscaler's Zero Trust Exchange can be applied to Web3 by implementing zero-trust access controls for decentralized applications and services. By leveraging its authentication, segmentation, and gateway features, Web3 developers can create a more secure environment for users, devices, and applications [262].

- AppGate's Software-Defined Perimeter (SDP)

AppGate's SDP is a network security solution that provides secure remote access to applications and data based on user context and device posture. It utilizes the principles of zero-trust to minimize the attack surface and prevent unauthorized access. AppGate's SDP can be adapted for the Web3 ecosystem by creating secure access solutions for decentralized applications and services based on user context and device posture. This can help protect user data and ensure the privacy and integrity of the decentralized network [263].

- VMware's Zero Trust Security Model

VMware's zero-trust security model is built around the concepts of “never trust, always verify” and “least privilege.” It provides a comprehensive approach to securing applications, networks, data, and endpoints by employing micro-segmentation, identity and access management, and endpoint security. VMware's zero-trust security model can be applied to

Web3 by utilizing its principles to secure decentralized applications, networks, and data. By implementing micro-segmentation, identity management, and endpoint security, developers can create a more secure and resilient Web3 ecosystem [264].

- Unisys' Stealth Security Platform

Unisys' Stealth Security Platform is a zero-trust solution that provides dynamic isolation, encryption, and secure communication between users, devices, and applications. It aims to protect critical assets and data by preventing unauthorized access and reducing the attack surface. The Unisys Stealth Security Platform can be adapted for the Web3 environment by employing dynamic isolation, encryption, and secure communication techniques to protect decentralized networks and applications. This can help enhance security and privacy while preventing unauthorized access to sensitive data [265].

- Guardicore's Centra Security Platform

Guardicore's Centra Security Platform is a micro-segmentation and zero-trust security solution that helps organizations protect their critical assets and data. It offers visibility into application dependencies, real-time threat detection, and policy enforcement to maintain a strong security posture. Guardicore's Centra Security Platform can be adapted for the Web3 environment by implementing micro-segmentation and policy enforcement techniques in the context of decentralized networks and applications. This can help secure the Web3 ecosystem by isolating potentially compromised components and preventing unauthorized access to sensitive data [266].

- Waverley Labs' Software-Defined Perimeter Framework

Waverley Labs' SDP Framework is a zero-trust network access solution that provides secure remote access to applications and data based on user context, device posture, and other factors. It aims to minimize the attack surface and prevent unauthorized access. Waverley Labs' SDP Framework can be adapted for the Web3 ecosystem by creating secure access solutions for decentralized applications and services based on user context and device posture. This can help protect user data and ensure the privacy and integrity of the decentralized network [267]. Table 12. Presents comparisons of existing solutions for zero-trust architecture and solution models.

5.4. Challenges of Web3

Implementing zero-trust architecture in the Web3 environment comes with its own set of challenges that organizations must address to ensure effective security measures [268–273]. These challenges include:

- Decentralized Trust Models

Research is being conducted to develop decentralized trust models that leverage blockchain technology to create a more secure and transparent trust infrastructure [274]. These models could potentially replace or complement traditional centralized trust providers, reducing the risk of single points of failure and fostering a more resilient Web3 ecosystem.

- Enhanced Privacy and Anonymity

Current research focuses on enhancing privacy and anonymity in Web3 by integrating zero-knowledge proofs, homomorphic encryption, and secure multi-party computation. These technologies enable secure data processing and sharing without revealing sensitive information, thus upholding the principles of zero-trust architecture.

- Scalability and Performance

As the Web3 ecosystem grows, scalability and performance become critical challenges. Researchers are exploring various approaches, such as sharding, off-chain computation, and layer 2 solutions, to improve transaction throughput and network capacity without sacrificing security [275].

- Adaptive Risk Assessment

Adaptive risk assessment techniques are being investigated to assess and adjust trust levels dynamically based on the behavior of users, devices, and services. This enables a more nuanced approach to access control, which considers contextual factors and historical data to provide tailored access privileges [276].

- Integration with Web3 Applications and Services

Ensuring seamless integration between zero-trust security measures and the variety of Web3 applications, protocols, and services can be challenging, as these solutions may have unique requirements and security considerations [277].

- Managing Decentralized Identities

Implementing zero-trust principles in Web3 requires the integration of decentralized identity solutions, which may involve dealing with interoperability issues, scalability challenges, and evolving standards [278].

5.5. Future scope of Web3

As the Web3 ecosystem evolves, new challenges and opportunities will emerge. The following subsections outline some of the key areas for future research and development in the context of zero-trust architecture for Web3 [279–283].

- Advanced Decentralized Trust Models

Building upon current research in decentralized trust models, future work will focus on creating more sophisticated and adaptable trust mechanisms that can better handle the complexity and dynamism of the Web3 environment. This could involve the integration of ML and AI to enhance trust assessment and decision-making processes.

- Quantum-Resistant Cryptography

As quantum computing advances, traditional cryptographic algorithms will become increasingly vulnerable to attack. Future research will need to develop and implement quantum-resistant cryptographic algorithms to ensure the long-term security of zero-trust architectures in Web3.

- Interoperability and Standardization

Interoperability between various Web3 platforms and dApps is crucial for a seamless user experience and to foster a more cohesive ecosystem. Future research should focus on developing standardized protocols and frameworks that facilitate secure cross-platform communication and data exchange while adhering to zero-trust principles.

- Security Automation and Orchestration

As the complexity of Web3 networks grows, manual security management will become increasingly untenable. Future work will explore the development of automated security systems that can detect, respond to, and mitigate threats in real-time, leveraging advanced analytics, ML, and AI to optimize security orchestration.

Table 12
Comparisons of zero-trust architecture and models.

Example	Overview	Applicability to Web3	Key Features	Benefits	Potential Challenges
Google's BeyondCorp	Focuses on device and user authentication, shifting access controls from the network perimeter to individual devices and users.	Can be adapted to the Web3 environment by focusing on user and device authentication in decentralized services and resources.	- Device and user authentication - User and device - centric security	- Improved security - Reduced reliance on network perimeters	- Complex implementation - Management of device security
Forrester's ZTX	Extends zero-trust principles to data, networks, devices, people, and workloads, emphasizing data security throughout its lifecycle.	Web3 applications can benefit from ZTX's comprehensive approach by incorporating its data-centric principles.	- Data-centric security - Covers all aspects of the IT environment	- Comprehensive protection - Data lifecycle security	- May require significant organizational changes - Adapting to decentralized environments
NIST SP 800-207	Provides guidelines for implementing zero-trust architectures, including policies, governance, and technologies.	Offers valuable resources for organizations building and deploying Web3 applications with zero-trust principles.	- Detailed guidelines - Recommendations for implementation	- Clear guidance for implementation - Best practices for zero-trust architectures	- Not tailored specifically for Web3 - May require interpretation for specific use cases
Cloudflare's Zero Trust Platform	Offers tools and services for access management, device posture enforcement, and secure application delivery.	Provides additional security layers for Web3 applications relying on cloud infrastructure and services.	- Access management - Device posture enforcement - Secure application delivery	- Improved access control - Enhanced security for cloud services	- Reliance on Cloudflare infrastructure - Integration with decentralized applications
Microsoft's Zero Trust Model	Focuses on protection of identities, devices, applications, and data, aiming to prevent breaches and limit impact.	Can be adapted to the Web3 context by applying its principles to decentralized identities, dApps, and data storage.	- Identity protection - Device security - Application and data protection	- Comprehensive security approach - Prevention and mitigation of breaches	- Adapting principles to decentralized networks - Integration with existing Web3 solutions
Cisco's Zero Trust Architecture	Covers workforce, workloads, and workplace, providing secure access based on dynamic trust levels, user context, and device security posture.	Can be applied to Web3 by focusing on the security of decentralized applications, user identities, and device access.	- Workforce, workloads, and workplace security - Dynamic trust assessment - Context-aware access controls	- Secure access to applications and data - Adaptable to changing trust levels	- Adapting to decentralized environments - Integration with Web3 applications and networks
Okta's Zero Trust Framework	Centers on identity and access management, ensuring the right people have the right access to the right resources at the right time.	Can be integrated into Web3 applications by leveraging decentralized identity solutions and blockchain-based access control mechanisms.	- Identity-driven security - Access management and control	- Enhanced access control - Scalable identity management	- Integration with decentralized identity systems - Adapting to blockchain-based access control
Palo Alto Networks' Prisma Access	Provides zero-trust network access for remote users and devices with features such as multi-factor authentication, micro-segmentation, and context-aware access controls.	Can be applied to Web3 by securing remote access to decentralized applications and services.	- Multi-factor authentication - Micro-segmentation - Context-aware access controls	- Secure remote access - Protection of user data and	- Adapting to decentralized networks - Integration with Web3 applications and services
Akamai's Zero Trust Security Solutions	Provides secure application access, device posture enforcement, and threat intelligence to protect against potential security risks.	Can be applied to Web3 by securing access to decentralized applications, ensuring device integrity, and leveraging threat intelligence.	- Secure application access - Device posture enforcement - Threat intelligence	- Enhanced application security - Proactive threat mitigation	- Adapting to the decentralized environment - Integration with existing Web3 solutions
Illumio's ASP	Offers micro-segmentation, identity and access management, and endpoint security to help protect critical applications and data.	Can be adapted to Web3 by implementing micro-segmentation and automated policy enforcement in decentralized networks and applications.	- Micro-segmentation - Real-time threat monitoring - Automated policy enforcement	- Improved network security - Isolation of compromised components	- Adapting micro-segmentation to decentralized networks - Implementing policy enforcement in Web3 applications
Zscaler's Zero Trust Exchange	Enables zero-trust access controls for users, devices, and applications with features such as multi-factor authentication, application segmentation, and secure web gateways.	Can be applied to Web3 by implementing zero-trust access controls for decentralized applications and services.	- Multi-factor authentication - Application segmentation - Secure web gateways	- Enhanced access control - Improved application security	- Adapting to decentralized application environments - Integration with Web3 services
VMware's Zero Trust Security Model	Built around the concepts of "never trust, always verify" and "least privilege," it provides a comprehensive approach to securing applications, networks, data, and endpoints.	Can be applied to Web3 by utilizing its principles to secure decentralized applications, networks, and data.	- Micro-segmentation - Identity and access management - Endpoint security	- Comprehensive security approach - Least privilege access control	- Adapting principles to decentralized networks - Integrating with existing Web3 solutions
	Provides dynamic isolation, encryption, and secure	Can be adapted for the Web3 environment by employing dynamic	- Dynamic isolation - Encryption	- Enhanced security and privacy	

(*continued on next page*)

Table 12 (*continued*)

Example	Overview	Applicability to Web3	Key Features	Benefits	Potential Challenges
Unisys' Stealth Security Platform	communication between users, devices, and applications to protect critical assets and data.	isolation, encryption, and secure communication techniques to protect decentralized networks and applications.	- Secure communication	- Reduced attack surface	- Integration with decentralized networks - Adapting encryption techniques to Web3
Guardicore's Centra Security Platform	Offers micro-segmentation, real-time threat detection, and policy enforcement to maintain a strong security posture.	Can be adapted for the Web3 environment by implementing micro-segmentation and policy enforcement techniques in the context of decentralized networks and applications.	- Micro-segmentation - Real-time threat detection - Policy enforcement	- Improved network security - Isolation of compromised components	- Adapting micro-segmentation to decentralized networks - Implementing policy enforcement in Web3 applications
Waverley Labs' SDP Framework	Provides secure remote access to applications and data based on user context, device posture, and other factors, aiming to minimize the attack surface and prevent unauthorized access.	Can be adapted for the Web3 ecosystem by creating secure access solutions for decentralized applications and services based on user context and device posture.	- Context-aware access controls - Device posture enforcement - Secure remote access	- Enhanced access control - Protection of user data and privacy	- Adapting to decentralized application environments - Integration with Web3 services

- Decentralized Access Control Mechanisms

Research in decentralized access control mechanisms will become more crucial as the Web3 ecosystem grows. Future work should focus on designing novel access control schemes that can adapt to the unique requirements of decentralized systems, incorporating aspects such as decentralized governance, reputation systems, and consensus mechanisms.

- Privacy-Preserving Technologies

With increasing concerns over data privacy, future research will need to explore the integration of advanced privacy-preserving technologies, such as zero-knowledge proofs, secure multi-party computation, and differential privacy, into Web3 zero-trust architectures. This will enable users to maintain control over their data while still benefiting from the functionality and security of decentralized systems.

- Innovative Solutions for Decentralized Networks

As the adoption of Web3 technologies grows, new security solutions specifically designed for decentralized networks will emerge, incorporating zero-trust principles to address the unique challenges of these environments.

- Cross-Platform Interoperability

With the increasing variety of platforms and protocols in the Web3 ecosystem, the need for interoperable security solutions will grow. Future developments in zero-trust architecture will likely focus on providing seamless integration across multiple platforms, protocols, and services.

- Enhanced Decentralized Identity Managements

As decentralized identity management becomes more prevalent in the Web3 ecosystem, zero-trust architecture will need to evolve to accommodate these solutions effectively, ensuring robust access control while maintaining user privacy and data security.

- Automated and Intelligent Security

The rapid pace of innovation in the Web3 environment demands efficient and effective security measures. Future developments in zero-trust architecture will likely involve leveraging AI, ML, and automation to streamline security operations, enhance threat detection, and enable proactive threat mitigation.

Key Lessons Learned.

- The importance of zero-trust architecture: Emphasizing continuous authentication, authorization, and validation in the Web3 environment is crucial for securing decentralized networks, applications, and services.
- Implementing key principles: Organizations can enhance their Web3 security by adopting principles such as never trust, always verify, least privilege access, micro-segmentation, and multi-factor authentication.
- Benefits of zero-trust architecture in Web3: Adopting this approach offers numerous advantages, including enhanced security, reduced attack surface, adaptability, decentralized identity management, and data protection.
- Challenges in implementation: Organizations must overcome challenges related to decentralized trust models, enhanced privacy and anonymity, scalability, adaptive risk assessment, and integration with Web3 applications and services.
- Future research and development: To capitalize on the opportunities presented by Web3, focus on advanced decentralized trust models, quantum-resistant cryptography, interoperability and standardization, security automation and orchestration, decentralized access control mechanisms, privacy-preserving technologies, and innovative solutions for decentralized networks is necessary.
- Continuous adaptation: Embracing zero-trust architecture and adapting to the evolving Web3 landscape will enable organizations to build more secure and resilient decentralized systems, ultimately contributing to a more transparent, decentralized, and user-centric Internet.

6. Opportunities and challenges

Decentralized technologies have the potential to revolutionize many industries and address various social and economic challenges. However, as with any emerging technology, there are also challenges that need to be addressed. In this section, we will discuss some of the opportunities and challenges associated with decentralized technologies [284–289].

6.1. Potential for social and economic impact

Decentralized technologies have the potential to transform various aspects of society and the economy. Here are some of the potential opportunities and benefits, as well as the challenges and risks, that come with the adoption of these technologies.

6.1.1. Opportunities and benefits

- Greater financial inclusion: Decentralized financial systems can potentially provide access to financial services for people who are

currently underserved by traditional financial institutions. For example, decentralized lending platforms can offer loans to people without a credit history or collateral, and decentralized exchanges can allow anyone to trade cryptocurrencies without the need for a bank account.

- Lower transaction costs: Decentralized systems can potentially reduce transaction costs for businesses and individuals by eliminating intermediaries and reducing the need for trust. For example, decentralized marketplaces can connect buyers and sellers directly, reducing fees and commissions, while decentralized payment systems can enable low-cost cross-border transactions.
- Greater transparency and accountability: Decentralized systems can potentially increase transparency and accountability by providing a tamper-proof record of transactions and enabling real-time tracking of goods and services. For example, blockchain-based supply chain systems can provide greater visibility into the origin and journey of products, making it easier to verify their authenticity and sustainability.
- Enhanced privacy and security: Decentralized systems can potentially enhance privacy and security by using cryptography and distributed architectures to protect user data and prevent hacks and breaches. For example, decentralized identity systems can enable users to control their own personal data and provide verifiable proof of identity without relying on a central authority.
- Increased innovation and competition: Decentralized systems can potentially spur innovation and competition by enabling anyone to build and launch applications without the need for permission from a centralized authority. For example, decentralized app stores can provide a level playing field for developers and allow for the creation of new types of applications that were not possible before.

6.1.2. Challenges and risks

- Regulatory uncertainty: The regulatory environment around decentralized technologies is still evolving, and there is a risk that new laws and regulations could stifle innovation or limit the potential benefits of these technologies.
- Lack of user adoption: Decentralized technologies may face resistance from users who are unfamiliar with the technology or who prefer to use traditional systems. This could limit the potential impact of these technologies and slow their adoption.
- Technical limitations: Decentralized technologies are still in their early stages of development, and there are technical limitations that may need to be overcome in order to fully realize their potential. For example, scalability and interoperability issues could limit the usefulness of decentralized systems in certain applications.
- Energy consumption: Some decentralized systems, such as blockchain networks, require significant amounts of energy to operate. This could be a barrier to adoption in some cases, especially if the energy consumption is not offset by the benefits provided by the system.
- Cybersecurity risks: Decentralized systems are not immune to cyberattacks, and there is a risk that a security breach could compromise user data or the integrity of the system. This could undermine trust in the system and limit its adoption.

6.2. Scalability issues and possible solutions

The decentralized nature of blockchain technology presents unique challenges in terms of scalability. As the number of users and transactions increase, the blockchain can become congested, leading to slower transaction times and higher fees.

To address these issues, developers have proposed various solutions, including:

- Layer 2 Scaling Solutions
  - Layer 2 scaling solutions involve processing transactions off-chain, which reduces the load on the blockchain and improves transaction speed. These solutions include:
    - Payment channels: These are off-chain channels that enable two parties to transact without the need to record every transaction on the blockchain. The most well-known example of a payment channel is the Lightning Network for Bitcoin.
    - Sidechains: These are separate blockchains that are interoperable with the main blockchain, allowing for faster and more efficient transactions. One example is the Liquid Network for Bitcoin.
    - State channels: Similar to payment channels, state channels allow parties to transact off-chain, but also enable more complex interactions, such as gaming or voting.
- Sharding

Sharding involves splitting the blockchain into smaller partitions or shards, each of which can process transactions independently. This can significantly increase transaction throughput and reduce the load on the blockchain.

- Proof-of-Stake

Proof-of-stake (PoS) is an alternative consensus mechanism to the current proof-of-work (PoW) used by many blockchains. PoS is designed to be more energy-efficient and allows for faster transaction processing.

- Interoperability

Interoperability is the ability for different blockchains to communicate and transact with each other seamlessly. This can increase scalability by allowing for more efficient use of resources across multiple blockchains. Despite these proposed solutions, scalability remains a major challenge for blockchain technology, and further research and development are needed to ensure its continued growth and adoption.

6.3. Legal, regulatory, and compliance considerations

The growth of decentralized technologies has raised important questions around the legal, regulatory, and compliance implications. As these technologies continue to evolve and expand, it is essential to consider the potential legal and regulatory challenges that could impact their development and adoption. This section examines some of the key legal and regulatory considerations that must be taken into account.

- Regulatory Landscape

The regulatory landscape for decentralized technologies varies greatly around the world. While some countries have embraced the technology and established supportive regulatory frameworks, others have taken a more cautious approach, imposing stringent regulations or outright bans. The decentralized nature of these technologies creates additional complexities for regulators, as it is often difficult to identify and regulate the parties involved.

- Securities Laws

One of the key regulatory challenges for decentralized technologies is determining whether they are subject to securities laws. In some cases, the tokens or assets used in decentralized applications may be considered securities under existing regulatory frameworks, which could trigger compliance requirements such as registration with regulatory authorities and disclosure requirements.

- Anti-Money Laundering (AML) and Know Your Customer (KYC) Requirements

Decentralized technologies also present challenges for compliance with AML and KYC requirements. While these requirements are intended to prevent financial crimes such as money laundering and terrorist financing, they can be difficult to enforce in decentralized ecosystems, where it may be challenging to identify the parties involved in a transaction.

- Intellectual Property Rights

Another key legal consideration for decentralized technologies is the protection of intellectual property rights. While blockchain technology is often associated with open-source development, it is important to ensure that intellectual property rights are respected and protected. The use of decentralized technologies may also raise questions around ownership and control of data and other digital assets.

- Data Privacy and Protection

The use of decentralized technologies also raises important questions around data privacy and protection. While blockchain technology offers inherent security features such as immutability and encryption, it is still essential to ensure that personal data and other sensitive information is protected in compliance with applicable privacy regulations. The legal, regulatory, and compliance landscape for decentralized technologies is complex and rapidly evolving. It is important for individuals and organizations involved in these technologies to remain up-to-date on the latest developments and to engage with regulators and other stakeholders to ensure that these technologies can be developed and used in a responsible and compliant manner.

6.4. Environmental and energy concerns

The environmental impact of blockchain technology is an increasingly important topic of discussion, as the energy consumption required for many blockchain networks has been a growing concern. Additionally, the use of certain materials in the production of blockchain hardware can also have negative environmental implications. This section explores some of the environmental and energy concerns associated with blockchain technology.

- Energy Consumption

The energy consumption required for certain blockchain networks, such as Bitcoin, has raised concerns about their environmental impact. The process of mining Bitcoin and other cryptocurrencies requires a significant amount of computational power, which in turn requires a large amount of energy. This has led to concerns about the carbon footprint of these networks. Possible solutions to address the energy consumption issue include the development of more energy-efficient consensus algorithms, such as Proof-of-Stake, and the use of renewable energy sources to power blockchain networks.

- Electronic Waste

The production of blockchain hardware, such as Application-Specific Integrated Circuits (ASICs) and Graphics Processing Units (GPUs), requires the use of certain materials that can have negative environmental impacts. Additionally, the short lifecycle of these devices can lead to a significant amount of electronic waste. Possible solutions to address the electronic waste issue include the development of more durable hardware and the implementation of more efficient recycling programs.

- Smart Contracts and Environmental Sustainability

Smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code, have the potential to facilitate more sustainable business practices [290]. For example, smart contracts can be used to automate supply chain management and ensure compliance with environmental regulations. They can also enable the tracking of environmental impact data in a more efficient and transparent manner. However, there are also concerns about the energy consumption required for the execution of smart contracts, as well as the potential for unintended consequences if smart contracts are not designed with environmental sustainability in mind. Overall, the environmental and energy concerns associated with blockchain technology highlight the importance of developing more sustainable and eco-friendly solutions. By addressing these issues, blockchain technology has the potential to not only revolutionize various industries but also contribute to a more sustainable future.

7. Future perspectives

The potential of Web3 technologies is vast and constantly evolving, offering exciting opportunities for innovation and collaboration. In this section, we will explore some of the emerging trends and future perspectives of Web3 [291-302, 303].

7.1. The metaverse: a Web3-enabled digital universe

The concept of the Metaverse has been around for some time, but with the advent of Web3 technologies, it is now becoming a reality. The Metaverse is a fully immersive, virtual world where users can interact with each other and with digital objects in a way that feels just as real as the physical world. With the help of Web3 technologies such as blockchain, decentralized storage, and smart contracts, the Metaverse has the potential to be a truly decentralized and democratic space where users have complete control over their data and identities. The Metaverse is already being explored by companies such as Decentraland, Somnium Space, and The Sandbox, and we can expect to see more innovation and growth in this space in the coming years.

- The concept of the metaverse

The concept of the metaverse refers to a virtual universe that is shared by millions of people in real-time, enabling them to interact with each other and digital objects in a 3D space. The metaverse is envisioned as a fully immersive and interconnected virtual world that can be accessed from anywhere and at any time. It is essentially a convergence of the physical and virtual worlds, where users can engage with each other in a variety of ways, from playing games to attending concerts and even shopping.

- Web3-enabled metaverse platforms

Web3-enabled metaverse platforms are built on blockchain technology, allowing for decentralized ownership, control, and governance of virtual assets and properties. These platforms enable the creation of unique digital identities for users, and they allow users to own and trade digital assets such as virtual real estate, avatars, and in-game items. Some popular examples of Web3-enabled metaverse platforms include Decentraland, Somnium Space, and The Sandbox.

- Potential applications and opportunities for the metaverse

The metaverse has the potential to revolutionize a wide range of industries, from gaming and entertainment to e-commerce and education. Here are some potential applications and opportunities for the metaverse:

o Gaming and entertainment: The metaverse can provide a fully immersive gaming experience, where users can interact with each

other and the virtual environment in real-time. It can also offer new forms of entertainment, such as virtual concerts and events.
- o E-commerce: The metaverse can provide a new platform for e-commerce, allowing users to buy and sell virtual goods and services, as well as real-world products and services in a virtual environment.
- o Education and training: The metaverse can provide a new platform for education and training, allowing users to learn and practice new skills in a fully immersive and interactive environment.
- o Virtual real estate: The metaverse allows for the creation and ownership of virtual real estate, which can be used for a variety of purposes, such as gaming, entertainment, and e-commerce.
- o Social interaction: The metaverse can provide a new way for people to interact with each other, bridging the gap between physical and virtual worlds, and enabling new forms of socialization and community building.

7.2. AI and ML in Web3

AI and ML are already being integrated into Web3 technologies to enhance their capabilities and offer new opportunities for innovation. AI and ML can be used to improve decentralized applications such as prediction markets, fraud detection, and personalized content recommendations. With the help of AI and ML, Web3 technologies can become more efficient, secure, and scalable. However, there are also concerns about the potential risks and challenges of AI and ML in the context of Web3, such as bias, privacy violations, and the need for transparent governance models.

- AI and ML in DeFi

AI and ML technologies have the potential to enhance various aspects of DeFi, such as prediction of market trends, risk assessment, and fraud detection. These technologies can also enable the automation of processes such as trading, lending, and borrowing, leading to improved efficiency and accuracy. For instance, AI-powered algorithms can analyze vast amounts of financial data and make informed decisions in real-time, providing traders with valuable insights and enabling them to make better investment decisions.

- AI and ML in DAOs

AI and ML can also facilitate decentralized decision-making processes and governance structures. These technologies can assist in the creation of algorithms that automate decision-making, eliminate biases, and improve the efficiency of voting mechanisms. For instance, DAOs can use AI algorithms to analyze various proposals and make recommendations to the community. This approach can lead to more informed and transparent decision-making processes and increase community engagement in governance.

- Potential applications and opportunities for AI and ML in Web3

The integration of AI and ML in Web3 has the potential to enhance various applications and use cases across different sectors. For example, in healthcare, AI and ML can help analyze and process medical data, leading to better diagnoses and treatment plans. In supply chain management, these technologies can assist in tracking products and ensuring authenticity, providing greater transparency and security. Additionally, AI and ML can improve the accuracy and efficiency of predictive models, allowing for more effective risk management in various industries. Overall, the integration of AI and ML in Web3 can lead to a more robust and efficient decentralized ecosystem.

7.3. Integration with IoT and smart cities

The IoT and smart cities are rapidly expanding, and there is great potential for integration with Web3 technologies. IoT devices can benefit from the security and transparency offered by blockchain, while smart contracts can enable automated and decentralized decision-making processes in smart city infrastructures. Web3 technologies can also facilitate the sharing and tracking of data in a way that is secure, transparent, and decentralized. With the integration of IoT and smart cities, Web3 technologies can offer new opportunities for innovation and sustainable development.

- Use cases for Web3 and IoT integration

The integration of Web3 and IoT has the potential to unlock a new era of innovation and interconnectedness, where smart devices and sensors can interact with decentralized networks and applications. Some of the use cases for Web3 and IoT integration include:

- o Supply chain management: IoT sensors can be used to track the movement of goods and products in real-time, while Web3 networks can provide secure and transparent data management.
- o Energy management: Smart homes and buildings equipped with IoT devices can interact with Web3 networks to optimize energy consumption and reduce waste.
- o Smart agriculture: IoT sensors can be used to monitor soil conditions, crop growth, and weather patterns, while Web3 networks can provide data management and predictive analytics.

- Decentralized data management and security for IoT devices

The integration of Web3 and IoT also presents significant opportunities for decentralized data management and security. By leveraging blockchain technology and decentralized networks, IoT devices can securely store and share data without relying on centralized servers or intermediaries. This can provide greater privacy, security, and control over personal data, as well as reduce the risk of data breaches or hacks.

- Potential opportunities and challenges for Web3 and smart cities

The integration of Web3 and smart cities has the potential to transform urban environments, making them more efficient, sustainable, and interconnected. Some of the potential opportunities for Web3 and smart cities include:

- o Improved urban planning and management: Web3-enabled platforms can provide better data management and analytics for city planners, allowing them to optimize city services and resources.
- o Increased citizen participation and engagement: Decentralized governance structures can enable greater citizen participation and decision-making in the management of city services and infrastructure.
- o Greater transparency and accountability: Web3 networks can provide greater transparency and accountability in the management of public funds and resources.

However, there are also challenges and potential risks associated with the integration of Web3 and smart cities, such as data privacy concerns, regulatory barriers, and the need for interoperability and standardization across different platforms and networks.

7.4. Potential for innovation and collaboration

Web3 technologies are still in the early stages of development, and there is immense potential for innovation and collaboration in this space. The open and decentralized nature of Web3 technologies enables new forms of collaboration and co-creation, where individuals and communities can work together to build new applications and services that are free from centralized control. Web3 technologies also offer new

opportunities for funding and investment, such as decentralized funding models like Initial Coin Offerings (ICOs) and Security Token Offerings (STOs). With the potential for innovation and collaboration in Web3, we can expect to see new business models, products, and services emerge in the coming years.

- Collaborative decentralized development and open-source software

Web3 technologies are built on open-source software and collaborative decentralized development. The decentralized nature of Web3 allows for a more collaborative approach to software development, where different individuals or teams can contribute to the development process. Open-source software and decentralized development can lead to more secure, transparent, and community-driven solutions.

- Opportunities for Web3 to disrupt traditional industries

Web3 has the potential to disrupt traditional industries by introducing decentralized alternatives to centralized systems. DeFi is a prime example of this, where Web3 solutions are disrupting traditional financial institutions and intermediaries. Other industries, such as supply chain management, healthcare, and gaming, could also see disruption from Web3 technologies.

- Potential for Web3 to drive social impact and sustainability efforts

Web3 technologies can enable more transparent and secure data management, which could lead to greater social impact and sustainability efforts. For example, supply chain management and provenance tracking using Web3 technologies can enable greater transparency and accountability in product sourcing and manufacturing, leading to more sustainable practices. Web3 technologies can also enable greater financial inclusion through DeFi solutions, which can provide access to financial services for individuals who are traditionally underserved by traditional financial institutions.

8. Conclusion

In conclusion, Web3 technology represents a fundamental shift towards a more decentralized and democratized internet. The various subsections of this article have provided insights into the potential of Web3 in various areas such as decentralized applications, finance, non-fungible tokens, decentralized autonomous organizations, supply chain management, and more. Web3 has the potential to create new opportunities for social and economic impact, and drive innovation and collaboration in various industries. However, there are also challenges such as scalability issues, legal and regulatory considerations, and environmental concerns that need to be addressed. Despite these challenges, the potential of Web3 technology cannot be overlooked. With the concept of the metaverse, integration with IoT and smart cities, and the potential for AI and ML, Web3 is poised to play a critical role in shaping the future of the internet. As we move towards a more decentralized and democratized internet, it is important for individuals, organizations, and governments to recognize the potential of Web3 technology and work towards its development and adoption. Only through collective efforts can we ensure that the benefits of Web3 are fully realized, and the potential of a decentralized and democratized internet is realized.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] R. Aria, N. Archer, M. Khanlari, B. Shah, Influential factors in the design and development of a sustainable web3/metaverse and its applications, Future Internet 15 (4) (2023) 131.
[2] K. Nabben, Web3 as 'self-infrastructuring': the challenge is how, Big Data Soc. 10 (1) (2023), 20539517231159002.
[3] A. Murray, D. Kim, J. Combs, The promise of a decentralized internet: what is Web3 and how can firms prepare? Bus. Horiz. 66 (2) (2023) 191–202.
[4] D. Tennakoon, Y. Hua, V. Gramoli, Smart redbelly blockchain: reducing congestion for Web3, in: Proceedings of the 37th IEEE International Parallel & Distributed Processing Symposium (IPDPS), 2023.
[5] J. Sadowski, K. Beegle, Expansive and extractive networks of Web3, Big Data Soc. 10 (1) (2023), 20539517231159629.
[6] L.W. Cong, K. Tang, Y. Wang, X. Zhao, Inclusion and Democratization through Web3 and Defi? Initial Evidence from the Ethereum Ecosystem (No. W30949), National Bureau of Economic Research, 2023.
[7] C. Ferraro, M.A. Wheeler, J.I. Pallant, S.G. Wilson, J. Oldmeadow, Not so 'trustless' after all: trust in Web3 technology and opportunities for brands, Bus. Horiz. (2023).
[8] S. Fan, T. Min, X. Wu, W. Cai, Altruistic and profit-oriented: making sense of roles in Web3 community from airdrop perspective, arXiv preprint arXiv:2303.08457 (2023).
[9] M. Lacity, E. Carmel, A.G. Young, T. Roth, The quiet corner of Web3 that means business, MIT Sloan Manag. Rev. 64 (3) (2023).
[10] G. Wang, R. Qin, J. Li, F.Y. Wang, Y. Gan, L. Yan, A novel DAO-based parallel enterprise management framework in Web3 era, IEEE Trans. Comput. Soc. Syst. (2023).
[11] R. Madhwal, J. Pouwelse, The Universal Trust Machine: a survey on the Web3 path towards enabling long term digital cooperation through decentralised trust, arXiv preprint arXiv:2301.06938 (2023).
[12] J. Goldston, T.J. Chaffer, J. Osowska, C.V. Goins II, Digital inheritance in Web3: a case study of soulbound tokens and the social recovery pallet within the Polkadot and Kusama ecosystems, arXiv preprint arXiv:2301.11074 (2023).
[13] J.A. Khan, K. Ozbay, AFFIRM: privacy-by-design blockchain for mobility data in Web3 using information centric fog networks with collaborative learning, in: 2023 International Conference on Computing, Networking and Communications (ICNC), IEEE, 2023, February, pp. 456–462.
[14] A. Cassatt, Web3 Marketing: A Handbook for the Next Internet Revolution, John Wiley & Sons, 2023.
[15] J.E. Longshak, The emergence of Web3 and metaverse technologies: implications for library and information services, in: Global Perspectives on Sustainable Library Practices, IGI Global, 2023, pp. 84–113.
[16] P. Sharma, D. Sachdeva, D. Jain, A. Sharma, Y. Sharma, S. Tayal, Web3 and Blockchain Introduction in Blogging to Maintain User Anonymity in SmartCity, 2023. SSRN 4392685.
[17] U. Vidovič, V. Keršič, M. Turkanović, Integrating Web3 features into moodle, in: Blockchain and Applications, 4th International Congress, Springer International Publishing, Cham, 2023, January, pp. 434–443.
[18] Q. Stokkink, C.U. Ileri, D. Epema, J. Pouwelse, Web3 Sybil Avoidance Using Network Latency, Computer Networks, 2023, 109701.
[19] Almajed, R., Abualkishik, A. Z., Ibrahim, A., & Mourad, N. Forecasting NFT Prices on Web3 Blockchain Using Machine Learning to Provide SAAS NFT Collectors.
[20] L.W. Cong, K. Grauer, D. Rabetti, H. Updegrave, The Dark Side of Crypto and Web3: Crypto-Related Scams, 2023. SSRN 4358572.
[21] Stöger, F., Zhou, A., Duan, H., & Perrig, A. Demystifying Web3 Centralization: the Case of Off-Chain NFT Hijackin.
[22] R. Tateishi, S. Hosono, Decentralized ID and RBAC-based policy agent for establishing Web3, in: Abstracts of Annual Conference of Japan Society for Management Information Annual Conference of Japan Society for Management Information 2022, THE JAPAN SOCIETY FOR MANAGEMENT INFORMATION (JASMIN), 2023, January, pp. 45–48.
[23] E. Blondell, Exploring the Security Implications of a Decentralized Internet: Vulnerabilities in Web3 and Blockchain-Based Networks, 2023.
[24] L. Yang, X. Dong, Y. Zhang, Q. Qu, W. Tong, Y. Shen, Generic-NFT: A Generic Non-fungible Token Architecture for Flexible Value Transfer in Web3, 2023.
[25] R. Ge, Research on the Development Technology of B-Learning System Based on Web3. 0, 2023.
[26] N. Brähler, The evolution of branding in Web3: towards headless brands? J. Brand Strategy 11 (4) (2023) 298–305.
[27] T. Schrepel, The Complex Relationship between Web2 Giants and Web3 Projects, Amsterdam Law & Technology Institute Working Paper, 2023, p. 1, 2023.
[28] de Vos, M., Ishmaev, G., & Pouwelse, J. Descan: Censorship-Resistant Indexing and Search for Web3. Available at SSRN 4333335.
[29] M. Davar, I. Bratu, Web3 and beyond: arbitration or consumer rights: the victor is, Arbitration: The International Journal of Arbitration, Mediation Dispute Manag. 89 (1) (2023).
[30] P.P. Momtaz, Some very simple economics of web3 and the metaverse, FinTech 1 (3) (2022) 225–234.
[31] C. Guan, D. Ding, J. Guo, Web3. 0: a review and research agenda, in: 2022 RIVF International Conference on Computing and Communication Technologies (RIVF), IEEE, 2022, December, pp. 653–658.
[32] R. Madhwal, J. Pouwelse, The Universal Trust Machine: a survey on the Web3 path towards enabling long term digital cooperation through decentralised trust, arXiv preprint arXiv:2301.06938 (2023).

[33] E. Rennie, I. Holcombe-James, A. Kushnir, T. Webster, B. Morgan, Developments in Web3 for the Creative Industries, 2022.
[34] S. Wan, H. Lin, W. Gan, J. Chen, P.S. Yu, Web3: the next internet revolution, arXiv preprint arXiv:2304.06111 (2023).
[35] R. Aria, N. Archer, M. Khanlari, B. Shah, Influential factors in the design and development of a sustainable web3/metaverse and its applications, Future Internet 15 (4) (2023) 131.
[36] L. Cao, Decentralized ai: edge intelligence and smart blockchain, metaverse, web3, and desci, IEEE Intell. Syst. 37 (3) (2022) 6–19.
[37] A. Park, M. Wilson, K. Robson, D. Demetis, J. Kietzmann, Interoperability: our exciting and terrifying Web3 future, Bus. Horiz. (2022).
[38] Jon M. Garon, "Legal implications of a ubiquitous metaverse and a Web3 future.", Marquette Law Rev. 106 (2022) 163.
[39] https://techblog.geekyants.com/an-introduction-to-terminologies-and-layers-in-web3. April, 2023.
[40] A. Murray, D. Kim, J. Combs, The promise of a decentralized internet: what is Web3 and how can firms prepare? Bus. Horiz. 66 (2) (2023) 191–202.
[41] S. Fan, T. Min, X. Wu, W. Cai, Altruistic and profit-oriented: making sense of roles in Web3 community from airdrop perspective, arXiv preprint arXiv:2303.08457 (2023).
[42] W. Ding, J. Hou, J. Li, C. Guo, J. Qin, R. Kozma, F.Y. Wang, DeSci based on Web3 and DAO: a comprehensive overview and reference model, IEEE Trans. Comput. Soc. Syst. 9 (5) (2022) 1563–1573.
[43] J. Wickström, M. Westerlund, E. Raj, Decentralizing machine learning operations using Web3 for IoT platforms, in: 2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), IEEE, 2022, December, pp. 238–245.
[44] April, 2023, https://thenewstack.io/web3-architecture-and-how-it-compares-to-traditional-web-apps/.
[45] Y. Zhang, Balance analysis of digital industry development based on Web3. 0, Highlights Bus. Econ. Manag. 1 (2022) 362–367.
[46] G. Yu, X. Wang, Q. Wang, T. Bi, Y. Dong, R.P. Liu, A. Reeves, Towards Web3 applications: easing the access and transition, arXiv preprint arXiv:2210.05903 (2022).
[47] T. Jesperson, G. Jensen, C. Winter, A. Arbuckle, & Ray Siemens with the INKE Research Group, Open, Collaborative Commons: Web3, Blockchain, and Next Steps for the Canadian Humanities and Social Sciences Commons, 2022.
[48] R. Qin, W. Ding, J. Li, S. Guan, G. Wang, Y. Ren, Z. Qu, Web3-Based Decentralized Autonomous Organizations and Operations: Architectures, Models, and Mechanisms, IEEE Transactions on Systems, Man, and Cybernetics, Systems, 2022.
[49] T.J. Chaffer, J. Goldston, On the existential basis of self-sovereign identity and soulbound tokens: an examination of the "self" in the age of Web3, J. Strat. Innov. Sustain. 17 (3) (2022) 1.
[50] G. Yu, Q. Wang, T. Bi, S. Chen, S. Xu, Leveraging architectural approaches in Web3 applications–A DAO perspective focused, arXiv preprint arXiv:2212.05314 (2022).
[51] Y. Zhang, P. Li, P. Cong, H. Zou, X. Wang, X. He, Web 3.0: developments and directions of the future internet architecture?, in: Web Services–ICWS 2022: 29th International Conference, Held as Part of the Services Conference Federation, SCF 2022 Cham: Springer Nature Switzerland, Honolulu, HI, USA, 2022, December, pp. 104–121. December 10–14, 2022, Proceedings.
[52] L. Yang, X. Dong, Y. Zhang, Q. Qu, W. Tong, Y. Shen, Generic-NFT: A Generic Non-fungible Token Architecture for Flexible Value Transfer in Web3, 2023.
[53] M. Unzeelah, Z.A. Memon, Fighting against fake news by connecting machine learning approaches with Web3, in: 2022 International Conference on Emerging Trends in Smart Technologies (ICETST), IEEE, 2022, September, pp. 1–6.
[54] M.L. Stewart, Focusing Limited Web3 Startup Resources for Higher Impact Product Development (Doctoral Dissertation, The George Washington University, 2023.
[55] D. Sheridan, J. Harris, F. Wear, J. Cowell Jr., E. Wong, A. Yazdinejad, Web3 Challenges and Opportunities for the Market, 2022 arXiv preprint arXiv: 2209.02446.
[56] T. McConaghy, Ocean Protocol: tools for the Web3 data economy, in: Handbook on Blockchain, Springer International Publishing, Cham, 2022, pp. 505–539.
[57] C. Guan, D. Ding, J. Guo, Web3. 0: a review and research agenda, in: 2022 RIVF International Conference on Computing and Communication Technologies (RIVF), IEEE, 2022, December, pp. 653–658.
[58] C. Guan, D. Ding, J. Guo, Web3. 0: a review and research agenda, in: 2022 RIVF International Conference on Computing and Communication Technologies (RIVF), IEEE, 2022, December, pp. 653–658.
[59] A. Newitz, Web3 is a fantasy, but it can still hurt you, New Sci. 253 (3376) (2022) 28.
[60] T. Taulli, How to Create a Web3 Startup, Springer Books, 2022.
[61] J. Potts, D.W. Allen, C. Berg, A.M. Lane, T. MacDonald, The Exchange Theory of Web3 Governance (Or 'blockchains without Romance'), 2022 (SSRN).
[62] M.M. Mirza, A. Ozer, U. Karabiyik, Mobile cyber forensic investigations of Web3 wallets on android and iOS, Appl. Sci. 12 (21) (2022), 11180.
[63] J.J. O'Hare, A. Fairchild, U. Ali, Money & trust in digital society, Bitcoin and stablecoins in ML enabled metaverse telecollaboration, arXiv preprint arXiv: 2207.09460 (2022).
[64] A. Ioniță, The politics for digital transformation: a prescriptive approach, Section: History, Political Sciences, International Relations 64 (2022).
[65] S. Gilbert, Crypto, Web3, and the Metaverse, Bennett Institute for Puplic Policy, Cambridge University, March, 2022.
[66] R. Belk, M. Humayun, M. Brouard, Money, possessions, and ownership in the metaverse: NFTs, cryptocurrencies, Web3 and wild markets, J. Bus. Res. 153 (2022) 198–205.
[67] M. de Vega, A. Masanto, R. Leslie, A. Yeoh, A. Page, T. Litre, Nillion: A Secure Processing Layer for Web3, 2022.
[68] N. Kshetri, A typology of metaverses, Computer 55 (12) (2022) 150–155.
[69] J. Tan, M. Langenkamp, A. Weichselbraun, A. Brody, L. Korpas, Constitutions of Web3. Metagov working paper. https://constitutions. metagov. org, 2022.
[70] G. Sagar, V. Syrovatskyi, Blockchain: the foundation of Web3, in: Technical Building Blocks: A Technology Reference for Real-World Product Development, Apress, Berkeley, CA, 2022, pp. 325–384.
[71] A. Park, M. Wilson, K. Robson, D. Demetis, J. Kietzmann, Interoperability: our exciting and terrifying Web3 future, Bus. Horiz. (2022).
[72] F. Honecker, J. Dreyer, R. Tönjes, Comparison of distributed tamper-proof storage methods for public key infrastructures, Future Internet 14 (11) (2022) 336.
[73] A.R. Chopra, N.K.C. Nair, R. Rahayani, VA3: a web 3.0 based I2I power transaction platform, in: 2022 7th IEEE Workshop on the Electronic Grid (eGRID), IEEE, 2022, November, pp. 1–5.
[74] J.M. Garon, Legal implications of a ubiquitous metaverse and a Web3 future, Marquette Law Rev. 106 (2022) 163.
[75] J. Sadowski, K. Beegle, Expansive and extractive networks of Web3, Big Data Soc. 10 (1) (2023), 20539517231159629.
[76] R. Blythman, M. Arshath, J. Smékal, H. Shaji, S. Vivona, T. Dunmore, Libraries, integrations and hubs for decentralized AI using IPFS, arXiv preprint arXiv: 2210.16651 (2022).
[77] T. Taulli, Taxes and regulations: how to navigate the Web3 world, in: How to Create a Web3 Startup: A Guide for Tomorrow's Breakout Companies, Apress, Berkeley, CA, 2022, pp. 151–163.
[78] C. Connors, D. Sarkar, Comparative study of blockchain development platforms: features and applications, arXiv preprint arXiv:2210.01913 (2022).
[79] Y.P. Gupta, A. Chawla, T. Pal, M.P. Reddy, D.S. Yadav, 3d networking and collaborative environment for online education, in: 2022 10th International Conference on Emerging Trends in Engineering and Technology-Signal and Information Processing (ICETET-SIP-22), IEEE, 2022, April, pp. 1–5.
[80] C. Catalini, A. de Gortari, N. Shah, Some simple economics of stablecoins, Annu. Rev. Fin. Econ. 14 (2022).
[81] G. Chen, M. Liu, Y. Zhang, Z. Wang, S.M. Hsiang, C. He, Using images to detect, plan, analyze, and coordinate a smart contract in construction, J. Manag. Eng. 39 (2) (2023), 04023002.
[82] I. Holcombe-James, E. In Rennie, I. Holcombe-James, A. Kushnir, T. Webster, B.A. Morgan, Developments in Web3 for the Creative Industries, 2022.
[83] H. Harsono, The utilization of WEB3 native resources to create a centralized base of authoritarian power, J. Int. Aff. 75 (1) (2022) 153–168.
[84] Patel, A., Thakar, D., Patel, D., Dave, A., Patel, D. M., & Shukla, B. Web 3.0: The Risks and Benefits of Web 3.0 no Web 2.0, Web 1.0. Journal homepage: www. ijrpr. com ISSN, 2582, 7421.
[85] L. Cao, Decentralized ai: edge intelligence and smart blockchain, metaverse, web3, and desci, IEEE Intell. Syst. 37 (3) (2022) 6–19.
[86] I. Seddon, E. Rosenberg, S.K. Houston, Future of virtual education and telementoring, Curr. Opin. Ophthalmol. 34 (3) (2023) 255–260.
[87] K. Nabben, Entering the Field of Web3:'Infrastructuring'and How to Do it, 2022. SSRN 4290516.
[88] T. Vardanega, M. Duranton, Digels", digital genius loci engines to guide and protect users in the "next web, HiPEAC Vision 2023 (2023) 18.
[89] R. Aria, N. Archer, M. Khanlari, B. Shah, Influential factors in the design and development of a sustainable web3/metaverse and its applications, Future Internet 15 (4) (2023) 131.
[90] M. Kovacova, J. Horak, M. Higgins, Behavioral analytics, immersive technologies, and machine vision algorithms in the Web3-powered Metaverse world, Ling. Phil. Invest. 21 (2022) 57–72.
[91] L. Cao, Decentralized ai: edge intelligence and smart blockchain, metaverse, web3, and desci, IEEE Intell. Syst. 37 (3) (2022) 6–19.
[92] R. Belk, M. Humayun, M. Brouard, Money, possessions, and ownership in the metaverse: NFTs, cryptocurrencies, Web3 and wild markets, J. Bus. Res. 153 (2022) 198–205.
[93] A. Murray, D. Kim, J. Combs, The promise of a decentralized internet: what is Web3 and how can firms prepare? Bus. Horiz. 66 (2) (2023) 191–202.
[94] A. Park, M. Wilson, K. Robson, D. Demetis, J. Kietzmann, Interoperability: our exciting and terrifying Web3 future, Bus. Horiz. (2022).
[95] Yu Xia, Research on the Integration of Network Information Resources in University Libraries under the Background of Web3. 0, Collection, 2018, p. 51.
[96] S. Voshmgir, Token Economy: How the Web3 Reinvents the Internet, vol. 2, Token Kitchen, 2020.
[97] Z. Liu, Y. Xiang, J. Shi, P. Gao, H. Wang, X. Xiao, Y.C. Hu, Make web3. 0 connected, IEEE Trans. Dependable Secure Comput. 19 (5) (2021) 2965–2981.
[98] Q. Wang, R. Li, Q. Wang, S. Chen, M. Ryan, T. Hardjono, Exploring web3 from the view of blockchain, arXiv preprint arXiv:2206.08821 (2022).
[99] L.W. Cong, K. Tang, Y. Wang, X. Zhao, *Inclusion and Democratization through Web3 and Defi? Initial Evidence from the Ethereum ecosystem*(No. W30949), National Bureau of Economic Research, 2023.
[100] J.M. Garon, Legal implications of a ubiquitous metaverse and a Web3 future, Marquette Law Rev. 106 (2022) 163.
[101] P.P. Momtaz, Some very simple economics of web3 and the metaverse, FinTech 1 (3) (2022) 225–234.
[102] J. Sadowski, K. Beegle, Expansive and extractive networks of Web3, Big Data Soc. 10 (1) (2023), 20539517231159629.

[103] D. Tennakoon, Y. Hua, V. Gramoli, Smart redbelly blockchain: reducing congestion for Web3, in: Proceedings of the 37th IEEE International Parallel & Distributed Processing Symposium (IPDPS), 2023.
[104] J. Popp, A.C. Cuțitoi, Immersive visualization systems, spatial simulation and environment mapping algorithms, and decision intelligence and modeling tools in the web3-powered metaverse world, J. Self Govern. Manag. Econ. 10 (3) (2022) 56–72.
[105] J. Bambacht, J. Pouwelse, Web3: a decentralized societal infrastructure for identity, trust, money, and data, arXiv preprint arXiv:2203.00398 (2022).
[106] G. Korpal, D. Scott, Decentralization and Web3 Technologies, 2022.
[107] J. Wu, K. Lin, D. Lin, Z. Zheng, H. Huang, Z. Zheng, Financial Crimes in Web3-Empowered Metaverse: Taxonomy, Countermeasures, and Opportunities, 2022 *arXiv preprint arXiv:2212.13452*.
[108] https://www.zdnet.com/article/how-decentralization-and-web3-will-impact-the-enterprise/. April, 2023.
[109] L.V. Kiong, Web3 Made Easy: A Comprehensive Guide to Web3: Everything You Need to Know about Web3, Blockchain, DeFi, Metaverse, NFT and GameFi, Liew Voon Kiong, 2022.
[110] W.M. Lee, W.M. Lee, Using the web3. Js APIs. *Beginning Ethereum smart contracts programming: with Examples in Python*, Solidity, and JavaScript (2019) 169–198.
[111] R. Qin, W. Ding, J. Li, S. Guan, G. Wang, Y. Ren, Z. Qu, Web3-Based Decentralized Autonomous Organizations and Operations: Architectures, Models, and Mechanisms, IEEE Transactions on Systems, Man, and Cybernetics, Systems, 2022.
[112] J. Potts, E. Rennie, Web3 and the creative industries: how blockchains are reshaping business models, in: A Research Agenda for Creative Industries, Edward Elgar Publishing, 2019, pp. 93–111.
[113] A. Clarke, A. Craig, B. Hagen, C. Youngblood, C. Jaquier, D. Perillo, S. Howley, Mainframe: the Web3 Communications Layer, 2018.
[114] Huixia Yin, Research on Web3.0 and its educational application, Inform. Technol. Inform. (6) (2018) 163–165.
[115] Bingjie Zhang, *Research on Innovation of Library Information Consultation Service under Web3. 0 Environment*(Master's Thesis, Liaoning Normal University, 2018.
[116] Zhiqiang Pan, *Research on the Construction of Third-Party Real Estate E-Commerce Platform Based on Web3. 0*(Master's Thesis, Hefei University of Technology, 2018.
[117] Guowei Gao, Qi Guo, Construction of Government Knowledge Service System under Web3. 0, vol. 14, Reform and Opening, 2018.
[118] Yan Zhao, Construction of University Library Information Service Platform Based on Web3. 0, vol. 11, Henan Library Journal, 2018.
[119] Yan Lai, Research on apparel online marketing strategy——comment on "apparel online marketing in the Web3. 0 era: theory and practice", Printing and Dyeing Auxiliaries 35 (3) (2018), 70-70.
[120] W. Ding, J. Hou, J. Li, C. Guo, J. Qin, R. Kozma, F.Y. Wang, DeSci based on Web3 and DAO: a comprehensive overview and reference model, IEEE Trans. Comput. Soc. Syst. 9 (5) (2022) 1563–1573.
[121] R. Aria, N. Archer, M. Khanlari, B. Shah, Influential factors in the design and development of a sustainable web3/metaverse and its applications, Future Internet 15 (4) (2023) 131.
[122] https://ethereum.org/en/. April, 2023.
[123] https://polkadot.network/. April, 2023.
[124] https://cardano.org/. April, 2023.
[125] https://solana.com/. April, 2023.
[126] https://www.binance.com/en. April, 2023.
[127] https://cosmos.network/. April, 2023.
[128] https://tezos.com/. April, 2023.
[129] https://www.avax.com/. April, 2023.
[130] https://www.nervos.org/. April, 2023.
[131] https://www.iota.org/. April, 2023.
[132] https://hedera.com/. April, 2023.
[133] https://near.org/. April, 2023.
[134] https://algorand.com/. April, 2023.
[135] https://www.ethswarm.org/. April, 2023.
[136] https://www.arweave.org/. April, 2023.
[137] https://sia.tech/. April, 2023.
[138] https://filecoin.io/. April, 2023.
[139] https://www.storj.io/. April, 2023.
[140] https://maidsafe.net/. April, 2023.
[141] https://bluzelle.com/. April, 2023.
[142] https://sovrin.org/. April, 2023.
[143] https://www.civic.com/. April, 2023.
[144] https://www.brightid.org/. April, 2023.
[145] https://angel.co/hatdex. April, 2023.
[146] https://3boxlabs.com/. April, 2023.
[147] https://selfkey.org/. April, 2023.
[148] https://www.w3.org/TR/did-core/. April, 2023.
[149] https://www.uport.me/. April, 2023.
[150] https://identity.foundation/ion/. April, 2023.
[151] https://chain.link/. April, 2023.
[152] https://www.wanchain.org/. April, 2023.
[153] https://wallet.venly.io/. April, 2023.
[154] https://polkastarter.com/. April, 2023.
[155] https://medium.com/renproject/introducing-ren-2-0-43025b3d5d6. April, 2023.
[156] https://polygon.technology/. April, 2023.
[157] https://steemit.com/. April, 2023.
[158] https://mastodon.social/. April, 2023.
[159] https://peepeth.com/. April, 2023.
[160] https://openbazaar.org/. April, 2023.
[161] https://bitify.com/. April, 2023.
[162] https://www.originprotocol.com/. April, 2023.
[163] https://augur.net/. April, 2023.
[164] https://www.gnosis.io/. April, 2023.
[165] https://axieinfinity.com/. April, 2023.
[166] https://decentraland.org/. April, 2023.
[167] https://horizonstate.com/product/blockchain/. April, 2023.
[168] https://www.agora.vote/. April, 2023.
[169] https://www.bitdegree.org/crypto/tutorials/what-is-blockchain. April, 2023.
[170] https://dscpl.medium.com/teachmeplease-main-services-and-features-dd1936a51ebb. April, 2023.
[171] https://tracxn.com/d/companies/medcredits.io. April, 2023.
[172] https://patientory.com/. April, 2023.
[173] https://uniswap.org/. April, 2023.
[174] https://pancakeswap.finance/. April, 2023.
[175] https://www.sushi.com/. April, 2023.
[176] https://aave.com/. April, 2023.
[177] https://compound.finance/. April, 2023.
[178] https://makerdao.com/. April, 2023.
[179] https://www.coinbase.com/price/dai. April, 2023.
[180] https://tether.to/. April, 2023.
[181] https://www.circle.com/en/usdc. April, 2023.
[182] https://nexusmutual.io/. April, 2023.
[183] https://etherisc.com/. April, 2023.
[184] https://medium.com/enzymefinance/melon-v1-0-zahreddino-60105f51988d. April, 2023.
[185] https://www.gemini.com/cryptopedia/set-protocol-erc20-set-token-tokensets-asset-tokenization. April, 2023.
[186] https://enzyme.finance/. April, 2023.
[187] https://dydx.exchange/. April, 2023.
[188] https://synthetix.io/. April, 2023.
[189] https://superrare.com/. April, 2023.
[190] https://www.niftygateway.com/. April, 2023.
[191] https://async.art/. April, 2023.
[192] https://www.cryptokitties.co/. April, 2023.
[193] https://nbatopshot.com/. April, 2023.
[194] https://www.sandbox.game/en/. April, 2023.
[195] https://blog.ujomusic.com/tagged/blockchain. April, 2023.
[196] http://myceliaformusic.org/. April, 2023.
[197] https://aragon.org/. April, 2023.
[198] https://molochdao.com/. April, 2023.
[199] https://makerdao.com/. April, 2023.
[200] https://www.thelao.io/. April, 2023.
[201] https://metacartel.xyz/. April, 2023.
[202] https://daostack.io/. April, 2023.
[203] https://colony.io/. April, 2023.
[204] https://giveth.io/. April, 2023.
[205] https://www.vechain.org/. April, 2023.
[206] https://ambrosus.io/. April, 2023.
[207] https://www.waltonchain.org/. April, 2023.
[208] https://provenance.io/. April, 2023.
[209] https://te-food.com/. April, 2023.
[210] https://www.certik.com/. April, 2023.
[211] https://everledger.io/. April, 2023.
[212] https://devery.io/. April, 2023.
[213] https://origintrail.io/. April, 2023.
[214] https://www.skuchain.com/. April, 2023.
[215] https://sweetbridge.com/. April, 2023.
[216] J.J.D. Rivera, T.A. Khan, W. Akbar, A. Muhammad, W.C. Song, ZT&T: secure blockchain-based tokens for service session management in Zero Trust Networks, in: 2022 6th Cyber Security in Networking Conference (CSNet), IEEE, 2022, October, pp. 1–7.
[217] Y. Liu, X. Hao, W. Ren, R. Xiong, T. Zhu, K.K.R. Choo, G. Min, A blockchain-based decentralized, fair and authenticated information sharing scheme in zero trust internet-of-things, IEEE Trans. Comput. (2022).
[218] J. Wickström, M. Westerlund, E. Raj, Decentralizing machine learning operations using Web3 for IoT platforms, in: 2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), IEEE, 2022, December, pp. 238–245.
[219] W. Powell, China, Trust and Digital Supply Chains: Dynamics of a Zero Trust World, Taylor & Francis, 2022.
[220] S. Silva, Web 3.0 and cybersecurity–short paper, ARIS2-Adv. Res. Inform. Syst. Sec. 2 (2) (2022) 39–49.
[221] J.A. Khan, K. Ozbay, AFFIRM: privacy-by-design blockchain for mobility data in Web3 using information centric fog networks with collaborative learning, in: 2023 International Conference on Computing, Networking and Communications (ICNC), IEEE, 2023, February, pp. 456–462.
[222] A. Gupta, H.U. Khan, S. Nazir, M. Shafiq, M. Shabaz, Metaverse security: issues, challenges and a viable ZTA model, Electronics 12 (2) (2023) 391.
[223] H.S. Hassan, R. Hassan, E.K. Gbashi, E-Voting system based on Ethereum blockchain technology using ganache and remix environments, Eng. Technol. J. 41 (4) (2023) 1–16.
[224] X. Cheng, M. Xu, R. Pan, D. Yu, C. Wang, X. Xiao, W. Lyu, Meta computing, arXiv preprint arXiv:2302.09501 (2023).
[225] N.F. Syed, S.W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, R. Doss, Zero Trust Architecture (Zta): A Comprehensive Survey, IEEE Access, 2022.

[226] Y. He, D. Huang, L. Chen, Y. Ni, X. Ma, A survey on zero trust architecture: challenges and future trends, Wireless Commun. Mobile Comput. 2022 (2022).
[227] L. Alevizos, V.T. Ta, M. Hashem Eiza, Augmenting zero trust architecture to endpoints using blockchain: a state-of-the-art review, Sec. Priv. 5 (1) (2022) e191.
[228] Z. Adahman, A.W. Malik, Z. Anwar, An analysis of zero-trust architecture and its cost-effectiveness for organizational security, Comput. Secur. 122 (2022), 102911.
[229] L. Meng, D. Huang, J. An, X. Zhou, F. Lin, A continuous authentication protocol without trust authority for zero trust architecture, China Commun. 19 (8) (2022) 198–213.
[230] K. Ramezanpour, J. Jagannath, Intelligent Zero Trust Architecture for 5G/6G Networks: Principles, Challenges, and the Role of Machine Learning in the Context of O-RAN, Computer Networks, 2022, 109358.
[231] X. Chen, W. Feng, N. Ge, Y. Zhang, Zero trust architecture for 6G security, arXiv preprint arXiv:2203.07716 (2022).
[232] P. Phiayura, S. Teerakanok, A comprehensive framework for migrating to zero trust architecture, IEEE Access 11 (2023) 19487–19511.
[233] M.A. Alipour, S. Ghasemshirazi, G. Shirvani, Enabling a Zero Trust Architecture in a 5G-Enabled Smart Grid, 2022 arXiv preprint arXiv:2210.01739.
[234] L. Wang, H. Ma, Z. Li, J. Pei, T. Hu, J. Zhang, A data plane security model of SR-BE/TE based on zero-trust architecture, Sci. Rep. 12 (1) (2022), 20612.
[235] F. Tang, C. Ma, K. Cheng, Privacy-preserving authentication scheme based on zero trust architecture, Digital Commun. Network. (2023).
[236] C. Katsis, F. Cicala, D. Thomsen, N. Ringo, E. Bertino, NEUTRON: a graph-based pipeline for zero-trust network architectures, in: Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy, 2022, April, pp. 167–178.
[237] L. Alevizos, M.H. Eiza, V.T. Ta, Q. Shi, J. Read, Blockchain-enabled intrusion detection and prevention system of APTs within zero trust architecture, IEEE Access 10 (2022) 89270–89288.
[238] S. Sarkar, G. Choudhary, S.K. Shandilya, A. Hussain, H. Kim, Security of zero trust networks in cloud computing: a comparative review, Sustainability 14 (18) (2022), 11213.
[239] H. Liu, M. Ai, R. Huang, R. Qiu, Y. Li, Identity authentication for edge devices based on zero-trust architecture, Concurrency Comput. Pract. Ex. 34 (23) (2022), e7198.
[240] E.S. Hosney, I.T.A. Halim, A.H. Yousef, An artificial intelligence approach for deploying zero trust architecture (ZTA), in: 2022 5th International Conference on Computing and Informatics (ICCI), IEEE, 2022, March, pp. 343–350.
[241] J. Zhang, J. Zheng, Z. Zhang, T. Chen, K. Qiu, Q. Zhang, Y. Li, Hybrid isolation model for device application sandboxing deployment in Zero Trust architecture, in: Applied Cryptography and Network Security Workshops: ACNS 2022 Satellite Workshops, AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, SiMLA, Rome, Italy, June 20–23, 2022, Proceedings, Springer International Publishing, Cham, 2022, September, pp. 104–123.
[242] H.A. Kholidy, A. Karam, J. Sidoran, M.A. Rahman, M. Mahmoud, M. Badr, A.F. Sayed, Toward zero trust security in 5G open architecture network slices, in: MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM), IEEE, 2022, November, pp. 577–582.
[243] V.B. Kondaveety, H. Lamkuche, S. Prasad, A zero trust architecture for next generation automobiles, in: AIP Conference Proceedings, vol. 2519, AIP Publishing LLC, 2022, October, 030088, 1.
[244] J.B. Michael, G.C. Dinolt, F.B. Cohen, D. Wijesekera, Can you trust zero trust? Computer 55 (8) (2022) 103–105.
[245] A. Levine, B.A. Tucker, Zero trust architecture: risk discussion, Digital Threats: Res. Pract. 4 (1) (2023) 1–6.
[246] D. Leahy, C. Thorpe, Zero trust container architecture (ZTCA): a framework for applying zero trust principals to docker containers, in: International Conference on Cyber Warfare and Security vol. 17, 2022, March, pp. 111–120, 1.
[247] J. Iggbom, Zero-trust architecture is creating a passwordless society, Netw. Secur. 2022 (7) (2022).
[248] C.A. Iordache, A.V. Dragomir, C.V. Marian, Public institutions updated enhanced biometric security, zero trust architecture and multi-factor authentification, in: 2022 International Symposium on Electronics and Telecommunications (ISETC), IEEE, 2022, November, pp. 1–4.
[249] S. Li, M. Iqbal, N. Saxena, Future industry internet of things with zero-trust security, Inf. Syst. Front (2022) 1–14.
[250] K. Ishide, S. Okada, M. Fujimoto, T. Mitsunaga, ML detection method for malicious operation in hybrid zero trust architecture, in: 2022 IEEE International Conference on Computing (ICOCO), IEEE, 2022, November, pp. 264–269.
[251] https://cloud.google.com/beyondcorp. April, 2023.
[252] https://www.forcepoint.com. April, 2023.
[253] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf. April, 2023.
[254] https://www.cloudflare.com. April, 2023.
[255] https://www.microsoft.com/en-us/security/business/zero-trust. April, 2023.
[256] https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/zt-arch-guide.html. April, 2023.
[257] https://www.okta.com/resources/whitepaper/zero-trust-with-okta-modern-approach-to-secure-access/. April, 2023.
[258] https://docs.paloaltonetworks.com/prisma/prisma-access. April, 2023.
[259] https://www.akamai.com/our-thinking/zero-trust/where-to-start-with-zero-trust-security. April, 2023.
[260] https://www.illumio.com/sites/default/files/2020-04/Illumio_FAQ.pdf. April, 2023.
[261] https://www.zscaler.com. April, 2023.
[262] https://www.appgate.com/support/software-defined-perimeter-support/sdp-v5-5. April, 2023.
[263] https://techzone.vmware.com/understanding-zero-trust. April, 2023.
[264] https://public.support.unisys.com/st3/docs/Stealth-5.2/82059239-015.pdf. April, 2023.
[265] https://www.guardicore.com/wp-content/uploads/2020/07/Guardicore_Centra_Datasheet_32.pdf. April, 2023.
[266] https://www.waverleylabs.com/wp-content/uploads/2020/06/Software-Defined-Perimeter-and-Zero-Trust.pdf. April, 2023.
[267] S. Voshmgir, Token Economy: How the Web3 Reinvents the Internet, vol. 2, Token Kitchen, 2020.
[268] Galdeman, A., Chiatante, M. P., Zignani, M., & Gaito, S. Disentangling the Growth of Web3 Blockchain-Based Networks by Graph Evolution Rules.
[269] K. Kanai, T. Yamazaki, S. Miyata, H. Kanemitsu, A. Mine, S. Mori, H. Nakazato, Research and development of Co-creating digital twins using Web3 technologies to accelerate beyond 5G. IEICE technical report, IEICE Tech. Rep. 122 (269) (2022) 1–6.
[270] de Vos, M., Ishmaev, G., & Pouwelse, J. Descan: Censorship-Resistant Indexing and Search for Web3. Available at SSRN 4333335.
[271] A. Kushnir, E. Rennie, I. Holcombe-James, A. Kushnir, T. Webster, B.A. Morgan, R. Doi, Developments in Web3 for the Creative Industries, 2022.
[272] A. Grasser, A. Parger, Blockchain architectures, the potential of Web3 for decentralized participatory architecture: collaborative objects on the blockchain, in: 40th Conference on Education and Research in Computer Aided Architectural Design in Europe: eCAADe 2022, 2022, September, pp. 431–440.
[273] G. Sagar, V. Syrovatskyi, Blockchain: the foundation of Web3, in: Technical Building Blocks: A Technology Reference for Real-World Product Development, Apress, Berkeley, CA, 2022, pp. 325–384.
[274] T. Zhang, Teaching and training system based on WEB3. 0 technology, in: 2022 Second International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE), IEEE, 2022, December, pp. 1–4.
[275] Y. Zhang, Balance analysis of digital industry development based on Web3. 0, Highlight. Bus. Econ. Manag. 1 (2022) 362–367.
[276] B. Blau, S. Vikram, Entering a New Era of Decentralized Customer Experience (DCX) Web3 Unlocks the New Market Category of Decentralized Customer Experience with Unforeseen Value across Industries, 2022. SSRN 4219848.
[277] S.N. Jelil, Non-Fungible Tokens, Crypto-Assets and Web3: What's in it for Conservation Science?, 2022. SSRN 4282312.
[278] D. Bucher, D. Hall, New ways of data governance for construction? Decentralized data marketplaces as Web3 concept just around the corner, in: Proceedings of the 29th EG-ICE International Workshop on Intelligent Computing in Engineering, Aarhus University, 2022, June.
[279] I.M. Purcarea, Digital twins, Web3, metaverse, value innovation and E-commerce retail, Romanian Distribution Committee Magazine 13 (3) (2022) 41–47.
[280] M. Davar, I. Bratu, Web3 and beyond: arbitration or consumer rights: the victor is, Arbitration: The International Journal of Arbitration, Mediation Dispute Manag. 89 (1) (2023).
[281] Nwogugu, M. C. ESG-In-DeFi and Problems Inherent in Regulation of DeFi, Web3, CryptoCurrencies, DCCs/DFPCs, and NFTs/Fractional-NFTs. Web3, CryptoCurrencies, DCCs/DFPCs, and NFTs/Fractional-NFTs (Revised, 2022).
[282] C. Chen, L. Zhang, Y. Li, T. Liao, S. Zhao, Z. Zheng, J. Wu, When Digital Economy Meets Web 3.0: Applications and Challenges, IEEE Open Journal of the Computer Society, 2022.
[283] H. Xu, Y. Sun, Z. Li, Y. Sun, L. Zhang, X. Zhang, deController: a Web3 native cyberspace infrastructure perspective, IEEE Commun. Mag. (2023).
[284] Q. DuPont, A Progressive Web3: from Digital Polycentric Governance to Social Coproduction, 2023. SSRN 4320959.
[285] A. Broustail, La diffusion libre de l'information à l'heure du web3 et des blockchains, I2D-Information, donnees documents 1 (1) (2022) 104–107.
[286] M. Campbell-Verduyn, M. Huetten, From peer-regulated divisions to unity in Web3: implications of blockchain mutations for internet governance, Glob. Coop. Res.: A Quarterly Magazine 2022 (2/3) (2022).
[287] J. Isselmann, Non-Fungible Tokens (NFTs) & Web3: New Product Worlds for the Financial Market, Information Systems & Management, 2023, pp. 1–12.
[288] B. Cant, J. Hatchell, Walk before you run: why healthcare needs web 2.5 before it can adopt Web3, Blockchain in Healthcare Today 6 (1) (2023).
[289] A. Kushnir, E. Rennie, I. Holcombe-James, A. Kushnir, T. Webster, B.A. Morgan, R. Doi, Developments in Web3 for the Creative Industries, 2022.
[290] J.R. Jensen, O. Ross, Retooling DAOs with Web3 social media. Jensen, johannes rude and ross, omri, retooling DAOs with Web3 social media (october 6, 2022), AMPLIFY 35 (10) (2022).
[291] K. Sandberg, S. Chamberlin, Web3 and Sustainability, 2023.
[292] Stöger, F., Zhou, A., Duan, H., & Perrig, A. Demystifying Web3 Centralization: the Case of Off-Chain NFT Hijacking.
[293] A. Grasser, A. Parger, Blockchain architectures, the potential of Web3 for decentralized participatory architecture: collaborative objects on the blockchain, in: 40th Conference on Education and Research in Computer Aided Architectural Design in Europe: eCAADe 2022, 2022, September, pp. 431–440.
[294] G. Sagar, V. Syrovatskyi, Blockchain: the foundation of Web3, in: Technical Building Blocks: A Technology Reference for Real-World Product Development, Apress, Berkeley, CA, 2022, pp. 325–384.
[295] E. Blondell, Exploring the Security Implications of a Decentralized Internet: Vulnerabilities in Web3 and Blockchain-Based Networks, 2023.

[296] T. Jesperson, G. Jensen, C. Winter, A. Arbuckle, & Ray Siemens with the INKE Research Group, Open, Collaborative Commons: Web3, Blockchain, and Next Steps for the Canadian Humanities and Social Sciences Commons, 2022.
[297] S. Krishnan, eCommerce in the Web3 Era, 2022.
[298] T. Dowdy, Speech markets & Web3: refreshing the first amendment for non-fungible tokens (NFTs), U. Cin. L. Rev. 91 (2022) 206.
[299] D. Zhang, S. Chadwick, L. Liu, The Metaverse: Opportunities and Challenges for Marketing in Web3, 2022. SSRN 4278498.
[300] L.W. Cong, K. Grauer, D. Rabetti, H. Updegrave, The Dark Side of Crypto and Web3: Crypto-Related Scams, 2023. SSRN 4358572.
[301] N. Brähler, The evolution of branding in Web3: towards headless brands? J. Brand Strategy 11 (4) (2023) 298–305.
[302] T. Taulli, The Web3 team: the roles needed for startup success, in: How to Create a Web3 Startup: A Guide for Tomorrow's Breakout Companies, Apress, Berkeley, CA, 2022, pp. 63–80.