Huawei Huang
Jiajing Wu
Zibin Zheng *Editors*

From Blockchain to Web3 & Metaverse

Springer

From Blockchain to Web3 & Metaverse

Huawei Huang • Jiajing Wu • Zibin Zheng
Editors

From Blockchain to Web3 & Metaverse

Springer

Editors

Huawei Huang
School of Software Engineering
Sun Yat-sen University
Zhuhai, Guangdong, China

Jiajing Wu
School of Software Engineering
Sun Yat-sen University
Zhuhai, Guangdong, China

Zibin Zheng
School of Software Engineering
Sun Yat-sen University
Zhuhai, Guangdong, China

ISBN 978-981-99-3647-2 ISBN 978-981-99-3648-9 (eBook)
https://doi.org/10.1007/978-981-99-3648-9

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Paper in this product is recyclable.

Acknowledgments

We would like to express our sincere appreciation to all those who have contributed to the completion of this book on from blockchain to Web3.

First, we extend our gratitude to the contributors who have shared their valuable expertise and insights on this complex and rapidly evolving topic. Their contributions have been instrumental in creating a comprehensive and up-to-date resource on the subject. We are also grateful to the editorial team at Springer for their guidance and support throughout the publishing process. Their professionalism, expertise, and commitment to excellence have been crucial in making this book a reality.

Finally, we express our appreciation to the readers of this book. We hope that the book will be a valuable resource for researchers, engineers, policymakers, and others working in the area of blockchain and Web3. We also hope that the book will inspire further research and innovation in this exciting and important field.

We acknowledge that the subject of blockchain and its applications is complex and rapidly evolving, and that there are many potential conflicts of interest that may arise in the course of researching, writing, and publishing a book on this topic. We have made every effort to disclose any conflicts of interest that we are aware of, and we welcome feedback and input from readers and other stakeholders on any potential biases or conflicts that may be present in the work. This book is partially supported by the National Key R&D Program of China (No. 2022YFB2702304), the National Natural Science Foundation of China under project (62032025, 62272496, 62172453, 6197332), Technology Program of Guangzhou, China (No. 202103050004), Fundamental Research Funds for the Central Universities, Sun Yat-sen University (Grant No. 23lgbj019).

Contents

Acronyms

AI	Artificial Intelligence
AIGC	Artificial Intelligence-Generated Content
AML	Anti-money Laundering
AR	Augmented Reality
BC	Blockchain
BTC	Bitcoin
CEX	Centralized Exchange
CNN	Convolutional Neural Network
DAO	Decentralized Autonomous Organization
DEX	Distributed Exchange
DeFi	Decentralized Finance
DID	Decentralized Identity
DFS	Distributed File System
DLT	Distributed Ledger Technology
DRL	Deep Learning-based Reinforcement Learning
DT	Digital Twin
ETH	Ethereum
FL	Federated Learning
ICO	Initial Coin Offerings
IoT	Internet of Things
IPFS	InterPlanetary File System
KYC	Know Your Customer
MEC	Multi-access Edge Computing
MEV	Miner Extractable Value
ML	Machine Learning
NFT	Non-fungible Token
NLP	Natural Language Process
PoS	Proof of Stake
PoW	Proof of Work
P2E	Play to Earn
P2P	Peer to Peer

PGC	Professional Generated Content
QoS	Quality of Service
TPS	Transaction Per Second
UGC	User Generated Content
VR	Virtual Reality
Web3	The Third Iteration of Internet
XR	Extended Reality
3D	Three Dimensional
6G	The Sixth-generation Communications Network

Chapter 1
An Introduction to Web3 and Metaverse

Qinglin Yang, Huawei Huang, Kaixin Lin, and Jiajing Wu

Abstract This chapter briefly explains metaverse, Web3, and their relationship. To better understand Web3 and metaverse, we introduce some crucial concepts, such as blockchains, smart contracts, digital assets and tokens, decentralized applications, and DID. Finally, we also discuss the typical applications related to Web3 and metaverse such as games, virtual world metaverse, social network projects, DAOs, and DeFi.

Keywords Metaverse · Web3 · Blockchain · Smart contract · Digital assets · Decentralized autonomous organizations

1.1 Introduction

Metaverse, literally a combination of the prefix "meta" (meaning *beyond*) and the suffix "verse" (abbreviation of "universe"), describes a world consisting of both virtuality and reality beyond the physical world built by human beings using digital technologies. Although there is no standard definition of "metaverse" in academic research, we can understand from the literal meaning how the most essential connotation of metaverse defines it. It is believed that the corresponding ground support of metaverse is the comprehensive innovation combining the Internet, augmented reality (AR), virtual reality (VR), extended reality (XR), Internet of Things (IoT), artificial intelligence (AI), networking, cloud computing, and other related technologies. In the context of *metaverse*, people can acquire a completely new experience with high realism and deep immersion.

Q. Yang · H. Huang (✉) · J. Wu
School of Software Engineering, Sun Yat-sen University, Zhuhai, Guangdong, China
e-mail: huanghw28@mail.sysu.edu.cn; wujiajing@mail.sysu.edu.cn

K. Lin
School of Computer Science and Engineering, Sun Yat-sen University, Zhuhai, Guangdong, China
e-mail: linkx26@mail2.sysu.edu.cn

H. Huang et al. (eds.), *From Blockchain to Web3 & Metaverse*,
https://doi.org/10.1007/978-981-99-3648-9_1

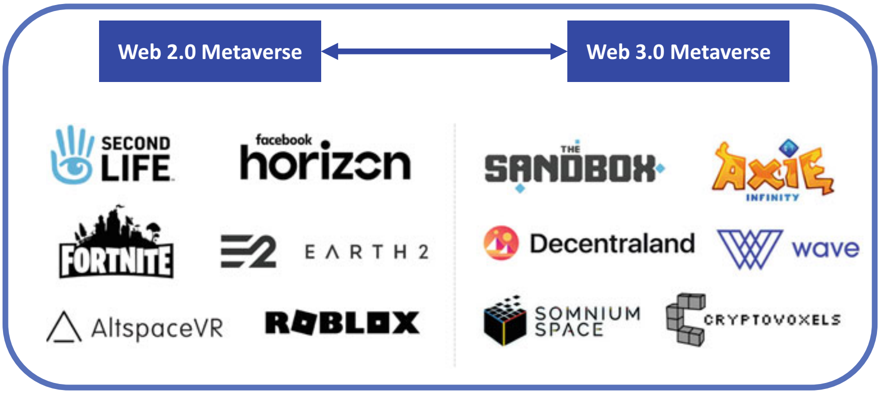


Fig. 1.1 Different styles of metaverses, empowered by Web2.0 and Web3.0, respectively

In 1992, when the concept of *metaverse* was first introduced, it was described as a virtual world where people who were not part of the elite could spend most of their free time. The movie “Ready Player One” is regarded as a good interpretation of the metaverse.

In the past decade, the industry has become to consider how to establish a metaverse and what features a metaverse has. For example, the industry has reached a common agreement that blockchain and Web3 are the fundamental technologies of the metaverse [1].

A key consideration when building the metaverse is whether it is centralized (centrally owned and controlled by large technology companies) or decentralized (jointly owned by general users of the metaverse community). Typically, as shown in Fig. 1.1, the former is referred to as the centralized metaverse, or “Web2-style closed metaverse,” while the latter is referred to as the decentralized metaverse, or “Web3-empowered open metaverse.”

1.2 Introduction to Web3

The concept of “Web3” refers to the third generation of the Internet that has been launched globally in recent years. Compared with the second generation of the Internet (i.e., Web2.0), which enables users to “read and write,” Web3 enables users to “read, write, and own.” In the context of “Web3,” users themselves hold the ownership of digital assets and their related authorities, which are fundamental for the current decentralized Internet.

1.2.1 Definition of Web3

The literal meaning of Web3 is translated as the third-generation Internet. There is currently no standard definition. One can describe it as a collection of decentralized Internet technologies based on blockchain technologies. In this collection, new technologies and paradigms are included, as well as new organizational forms (i.e., decentralized autonomous organization, DAO) and corresponding values and worldviews.

The term Web3 was first proposed by Tim Berners-Lee, the inventor of HTTP, during the period of the Internet bubble. It refers to an integrated communication framework, in which Internet data can span various applications and systems to achieve machine-readable [2]. In fact, the concept of Web3 we are discussing today is completely different from the concept proposed by Tim Berners-Lee. The currently so-called Web3 was redefined by Gavin Wood, the co-founder of Ethereum and the founder of Polkadot in 2014, in an article called "DApp: What is Web3.0" [3]. This blog redefines the term "Web3" originally proposed by Tim Berners-Lee. Essentially, Gavin Wood's definition of Web3 refers to blockchain technology that enables innovative interaction patterns between parties based on a trustless interactive system. The *trustless interactive system* mentioned here actually indicates a system supported by blockchain technologies.

Here is a brief introduction to Tim Berners-Lee. He is a computer scientist from Britain and the inventor of the World Wide Web (WWW). He was awarded the Turing Award in 2016. As we can see from his definition of Web3, this concept has a considerable sense of history because his original definition is only associated with a "communication framework," in which the machine's readability is across various applications and systems.

In fact, the concept of Web3 that we discuss today is completely different from Tim Berners-Lee's original definition. So, what does Web3 mean now? In a blog post titled "DApp: What is Web3.0?" [3], Gavin Wood, the co-founder of Ethereum and creator of Polkadot in 2014, redefined the term proposed by Tim Berners-Lee. Gavin Wood's definition of Web3 refers to blockchain technology that enables innovative interaction modes among parties based on a trustless interaction system. Such the "trustless interaction system" referred to here is actually a system supported by blockchain technologies.

Let's take a look at some other perspectives of Web3. A traditional investment partner believes that Web3 refers to a decentralized online ecosystem based on blockchain technologies. Many people believe that Web3 represents the next stage of the Internet, with the current Web3 industry resembling the Internet around the year 2000. This is because the Web3 industry has gradually introduced some prototype products, such as *Metamask*, considered as a decentralized version of "Alipay," which is a decentralized wallet tool with a fox logo; Audius, seen as a decentralized music sharing platform; and OpenSea, the world's largest NFT trading platform. These decentralized applications have attracted tens of millions of users worldwide, and the companies behind them are gradually becoming some of the most influential companies globally.

1.2.2 From Web1.0 to Web3.0

Now, let's review the development and evolution path from Web1.0 to Web3.0.

Web1.0 originated around 1990. At that time, representative applications were portal websites accessible only through desktop browsers, such as Wikipedia. Popular domestic portal websites at that time include old-school sites like Yahoo and Sina.com. It can be seen that the biggest feature of websites in the Web1.0 era was "readable" or "read-only." Users could only passively obtain information from these websites, as there was no channel provided for users to interact with them.

In the Web2.0 era, websites and applications underwent some new changes. The biggest change was the shift from a "readable" mode to a "readable and writable" mode. For example, a new generation of applications, such as blogs, Twitter, WeChat, and TikTok, allows users to create their own content, and these platforms also provide a variety of ways for users to interact with the platform or with other users. Therefore, the most significant feature of Web2.0 is "readable and writable."

With Web3, a new character has emerged on top of the "readable and writable" mode, which is "ownership." This "ownership" means that users have control over the content data they generate. In other words, users have sovereignty over their own data, unlike in Web2.0, where the ownership of user-generated data is controlled by platforms and oligarchs. It can be seen that the transition from Web1.0 to Web3.0 involves a transformation in the underlying logic. As a result, there is the potential for profound changes in the front-end and back-end ecosystems. The main reasons for this are as follows: Web1.0 and Web2.0 are considered information Internet, while Web3 can be seen as a value Internet. Web1.0 and Web2.0 essentially focus on transmitting information and consuming data or information, while Web3 is about transmitting value and creating wealth. Here "creating wealth" means that users' own data can generate revenue. However, the question is whether the wealth created can return to the hands of the users themselves. This issue also poses a new requirement for Web3 developers and entrepreneurs: they need to use technical means to ensure that the value created by users themselves is protected and ultimately passed on to the users. Therefore, some developers who are eager to embrace Web3 believe that all current Web2.0-style applications are worth re-developing in the context of Web3, thus upgrading them to corresponding dApps.

1.2.3 Technological Development Stack of Web3

This subsection introduces the technological development stack of Web3 and compares it with the development stack of the traditional "client-server" mode.

First, let's review the traditional "client-server" technological development stack. The front end is the client's browsers or Apps, which exploit HTML, CSS, or JavaScript to implement the front-end presentation. The back end, on the other hand,

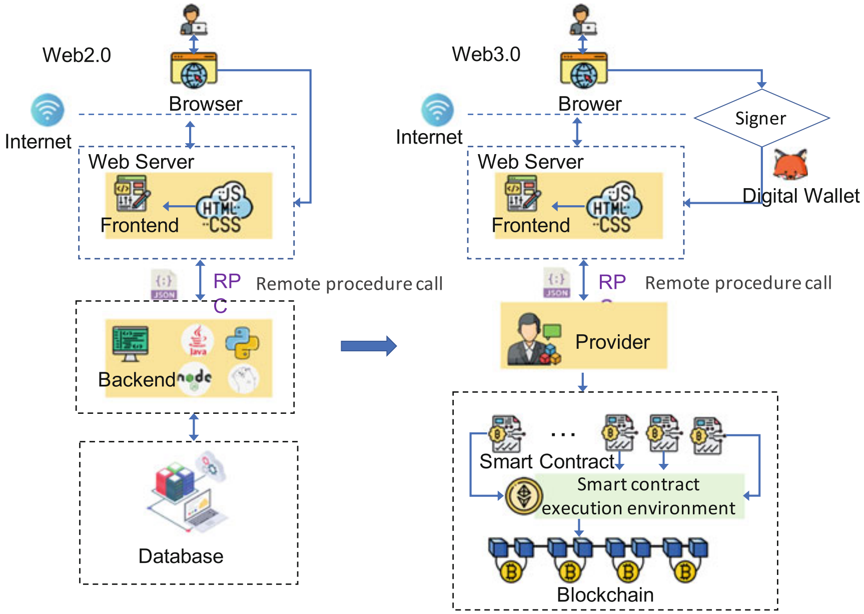


Fig. 1.2 Comparison between the development stacks of Web2 and Web3

is the server. So, what does the technological development stack look like for Web3-style Apps, also known as decentralized Apps (abbr. as dApps)?

In fact, as depicted in Fig. 1.2, the front end of the Web3 technological development stack is the same as the front end of the traditional Web2 client-server technological development stack, except that the back end changes from the traditional database into a blockchain. Then, there will be a Web3 service provider in the middle layer, that is, a Web3 service provider that provides some functions related to Web3, such as Web3 wallet and identity management tools. An example of such a wallet is Metamask [4].

We further analyze the technological development stack for Web3-style applications. First, for the front end, developers can create mobile dApps or develop front-end presentation pages that interact with Web3 wallets. Then, for the back end, if interaction with a large amount of off-chain data is required, this data can be stored in IPFS, which is a secure, distributed storage product [5].

If some Web3 dApps have more complex business requirements, they might need to rely on smart contracts for implementation. In this case, the relevant smart contracts need to be deployed on a blockchain that supports smart contracts, such as Ethereum. These contracts also need to interact with the Web3 identity management tools in the middle layer.

In summary, as shown in Fig. 1.2, the left-hand-side part is the user's front end, the right-hand-side part is the back-end blockchain, and the middle layer shows the Web3-style wallet management tools or identity management tools. Some complex applications may interact with multiple smart contracts.

1.2.4 Implication of Web3

Web3 relies on blockchain technologies to ensure users' rights to own their data. Web3's decentralized feature delivers richer, deeply personalized, next-generation Internet services.

After 30 years of development, the Internet is now at a critical point in time, evolving from Web2.0 to Web3.0. It is essential for researchers and practitioners to seize the opportunities of this era and promote forward-looking research and practices during the construction of the next-generation Internet, in order to enjoy the benefits that Web3 brings.

Internationally, plenty of Web3-related applications have emerged in the market. These applications mainly include decentralized applications (abbr. as dApps) running on top of blockchains and exploiting non-fungible tokens (NFTs). Users can freely trade virtual assets on trading platforms such as OpenSea. Currently, various dApps running on the Ethereum platform have applications mainly focused on finance, gaming, and social domains. Most NFTs are related to digital arts. However, behind the thriving development, there are also some hidden crises. For example, many so-called Web3 applications cannot achieve complete decentralization. Users are still using dApps through centralized front ends. Some research has found that many NFT art pieces have not genuinely issued digital assets on the blockchain. The sellers of these NFTs can arbitrarily change their pointers to other virtual art pieces. Despite this, the importance of Web3 is indisputable. For instance, in late 2021, the US Congress even held hearings to discuss the social value of Web3.

1.3 Introduction to Metaverse

1.3.1 Definition of Metaverse

The metaverse is a virtual shared space that combines elements of the Internet, virtual reality (VR), augmented reality (AR), and digital worlds. It is often portrayed as a collective, immersive environment where users can interact with other digital objects through avatars. The metaverse concept envisions a seamless blend of digital and physical spaces, enabling social interaction, entertainment, work, and commerce to take place in a single, interconnected environment. As the metaverse continues to develop, it is expected to integrate various technologies such as blockchain, artificial intelligence, and advanced networking infrastructure to create a more sophisticated, immersive, and interactive experience for users.

1.3.2 Three Early Stages of Metaverse

In this subsection, we briefly outline the three stages of the early development of metaverse, i.e., the *conception forming* period, the *technique shaping* period, and the *rapid development* period.

1.3.2.1 Conception Forming Period

Firstly, let's take a look at the conception forming period of the metaverse. The term *Meta* appeared in Neal Stephenson's science fiction *Snow Crash* in 1992. The metaverse depicted in Snow Crash is described as "put on headphones and goggles, find the connection terminal, and you can enter a virtual space parallel to the real world, simulated by computers, in the form of a virtual avatar." Snow Crash portrays a massive virtual reality world where everyone has a digital avatar. Through using avatars, users can engage in activities and compete with each other to improve their social status in the metaverse.

Surprisingly, in 1993, a Japanese video game company called Sega proposed its first-ever prototype of VR headset. This headset could only support popular arcade games at that time. Although this headset did not succeed to market as a product due to technological reasons, their concept far exceeded the products that should have been available at that time.

Another representative headset product that supports games is called *Virtual Boy*, launched by Nintendo in 1995. However, the device had limited usability, being fixed in one place. Users need to bring their eyes closer to see the game displayed inside the headset, which exploited parallax principles to create a 3D effect.

By the late 1990s, many 3D games emerged, particularly the rise of first-person shooter games, such as *Doom* in 1993, *Tomb Raider* in 1996, and *EverQuest* in 1999. A common feature of these games is that players have a human-like avatar to help them experience immersive 3D game environments.

1.3.2.2 Technique Shaping Period

Next, let's introduce the technique shaping period of the metaverse. A milestone that marked the beginning of this period was the 1999 sci-fi film *The Matrix*. This fascinating movie showed people perfectly entering a virtual metaverse world through brain-computer interface technology. In 2003, *Second Life* became the first phenomenal virtual world game. By 2006, *Roblox* was released, and by 2019, it had attracted over 100 million monthly active users. In 2017, *Fortnite* was nominated as the Best Multiplayer Game. By January 2018, it had gained over 45 million players worldwide. The 2018 film *Ready Player One* showcased a game scene called the *Oasis*, which was an excellent model of the metaverse.

1.3.2.3 Rapid Development Period

After a lengthy technique shaping period, the metaverse entered a rapid development phase. Since the first wave of the metaverse concept, Roblox went public in the United States on March 11, 2021, and the metaverse quickly entered people's vision. Tech giants also began to lay out their plans for the metaverse, especially Facebook, which changed its name to Meta and went all-in on the metaverse. This iconic event triggered the *metaverse fever* among major tech giants. Tech giants such as Facebook, Microsoft, Tencent, and ByteDance continued to invest heavily in the metaverse, expanding their commercial territories in multiple fields related to the metaverse, including VR/AR hardware, 3D game engines, content creation platforms, etc. As a result, some people call 2021 the *first year* of the metaverse. Since then, the entire Internet ecosystem has echoed the trend, and industries worldwide have responded, triggering the metaverse concept to explode completely. Subsequently, the emergence of NFT concepts has also directly fueled the metaverse boom. However, in the short term, NFTs mainly involve the digital authorities of virtual world arts and enable the circulation and the trading of digital collections.

1.3.3 Key Technologies for Metaverse

The following six key technologies play a crucial role in implementing the metaverse.

- **Virtual Reality (VR) and Augmented Reality (AR).** VR and AR are essential components of the metaverse, providing immersive experiences and seamless interactions between the digital and physical worlds. For example, VR creates entirely digital environments, while AR overlays digital elements upon the real world. These technologies enable users to feel like they are genuinely part of the metaverse, with realistic and interactive experiences.
- **3D Graphics and Real-Time Rendering.** High-quality 3D graphics and real-time rendering are crucial for creating visually stunning and believable metaverse environments. Advances in computer graphics, including ray tracing and realistic lighting, will contribute to the creation of highly detailed and immersive virtual worlds.
- **Artificial Intelligence (AI) and Machine Learning (ML).** AI and ML technologies will play a significant role in creating intelligent and interactive metaverse experiences. This includes natural language processing for more realistic communication between users and AI-driven characters, procedural content generation for creating diverse and dynamic environments, and machine learning algorithms that can analyze user behavior to optimize and personalize their experiences.
- **Blockchain and Decentralized Technologies.** Blockchain technology can be used to create decentralized metaverse platforms, ensuring secure digital asset

ownership, transfer, and trade. Blockchain-based solutions can provide a foundation for creating a digital economy within the metaverse, via exploiting cryptocurrencies, NFTs, and smart contracts.

- **Networking and Connectivity.** Robust networking infrastructure is essential for supporting the massive amounts of data and real-time interactions required by the metaverse. Technologies like 5G and edge computing will provide the low latency, high bandwidth, and reliable connectivity necessary for seamless experiences in the metaverse.
- **Interoperability and Standardization.** To create a truly connected metaverse, various platforms, systems, and digital assets must be able to interact and communicate with each other. Interoperability and standardization are critical for allowing users to move seamlessly between different virtual environments and enable users to exchange digital assets across various platforms.

By combining and advancing these technologies aforementioned, the metaverse can become a reality, providing users with immersive, interconnected, and interactive experiences across digital and physical spaces.

1.3.4 Hierarchical Structure of Metaverse Ecosystem

From the perspective of the hierarchical structure, metaverse ecosystem can be divided into several layers, i.e., foundation layer, hardware layer, software layer, content layer, application layer, and economic system, as illustrated in Fig. 1.3.

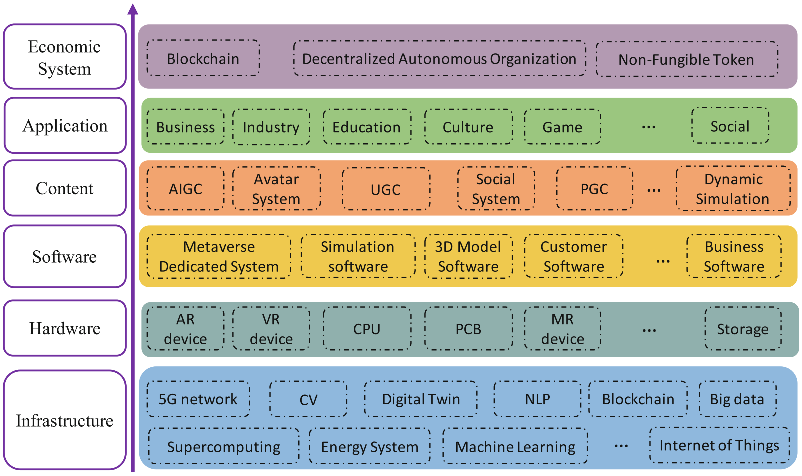


Fig. 1.3 Six-layer structure of metaverse ecosystem

- The foundation layer can provide basic infrastructures for metaverses, such as network infrastructure, 5G/6G communication, cloud computing/edge computing, blockchain, big data, Internet of Things technologies, supercomputing centers, and AI technologies.
- The hardware layer mainly involves human-computer interaction devices in the metaverse, such as AR/VR/XR devices, full-body motion-sensing devices, even biological chips, etc. The core components involved in the hardware layer include processors, gyroscopes, batteries, electroacoustic devices, displays, storage devices, sensors, printed circuit boards (PCBs), etc.
- The software layer can provide system software for the metaverse, such as the operating systems dedicated to the metaverse. In addition, application software such as 3D modeling software, synchronous simulation software, business software, and customer-oriented application software are also included.
- The content layer can generate core content for the metaverse. For example, AI technologies are enabling *user-generated content* (UGC), which helps create avatar systems, social systems, and personalized content. The core technologies involved in the content layer include 3D modeling, real-time rendering, dynamic simulation, spatial computing, holographic imaging, and decentralized technology.
- The application layer can support various industries at the social level, such as industry, commerce, and agriculture. Some typical scenarios include gaming, education, culture, sports, socializing, and so on.
- The top layer of the metaverse ecosystem is the economic system, which is mainly composed of four basic elements, i.e., digital creation, digital currency, digital assets (e.g., Non-Fungible Token), and digital markets.

1.3.5 Iconic Events of Metaverse

Since 2019, the development of the metaverse has witnessed several iconic events that have accelerated its growth. We pick up some of those most notable milestones (as depicted in Fig. 1.4) shown as follows:

- May 2019: The launch of Minecraft Earth [6]. Minecraft Earth is an augmented reality mobile game that allows players to build and explore in the real world using Minecraft elements, further blending virtual and physical spaces.
- April 2020: The first virtual Travis Scott concert is held in Fortnite, attracting over 12 million online viewers and showcasing the potential for large-scale virtual events in the metaverse.
- August 2020: Epic Games [7] announces the Unreal Engine V5, which promises to deliver new levels of realism and performance to virtual environments, making the creation of immersive metaverse experiences more accessible to developers.
- March 2021: Roblox Corporation [8] kicks off its initial public offering (IPO) through a direct listing of its stock.

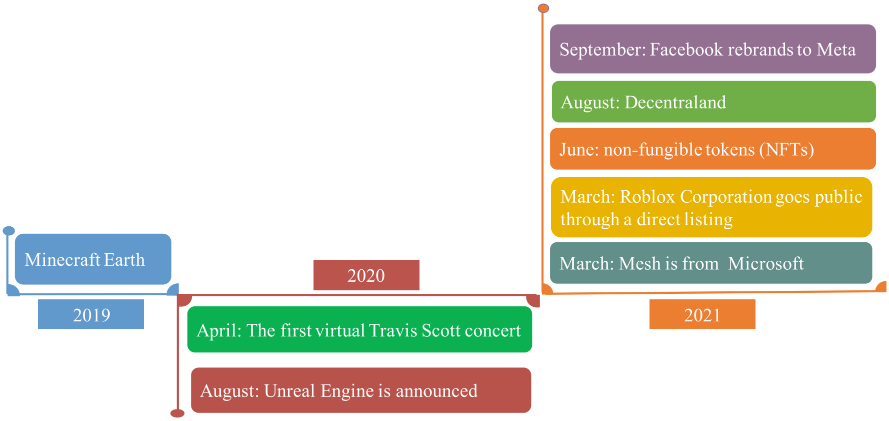

September: Facebook rebrands to Meta
August: Decentraland
June: non-fungible tokens (NFTs)
March: Roblox Corporation goes public through a direct listing
March: Mesh is from Microsoft
Minecraft Earth
2020
2019
2021
April: The first virtual Travis Scott concert
August: Unreal Engine is announced

Fig. 1.4 Iconic events that are related to metaverse

- March 2021: Microsoft announces Mesh [9], which is a mixed reality platform aimed at enabling shared experiences and collaboration in the metaverse.
- June 2021: The rise of non-fungible tokens (NFTs) gains mainstream attention, with many digital artists and creators using NFTs to monetize virtual assets and experiences in the metaverse.
- August 2021: Decentraland [10], which is a decentralized virtual world built on top of the Ethereum blockchain, hosts the first-ever Metaverse Fashion Week, showcasing the intersection of fashion, technology, and virtual spaces.
- September 2021: Facebook announces its rebranding to *Meta* and commits to investing $10 billion over the next several years to develop the metaverse, sparking widespread interest in the public (Fig. 1.4).

1.4 Fundamentals of Web3 and Metaverse

To better understand metaverse, in this section, we first introduce the technologies that implement the underlying logic of the metaverse, i.e., blockchain and smart contracts. In addition, the fuel for user activity in the economic system, i.e., crypto assets, is also introduced. An integrated overview of Web3, metaverse, and decentralized applications (abbreviated as dApps) is shown in Fig. 1.5.

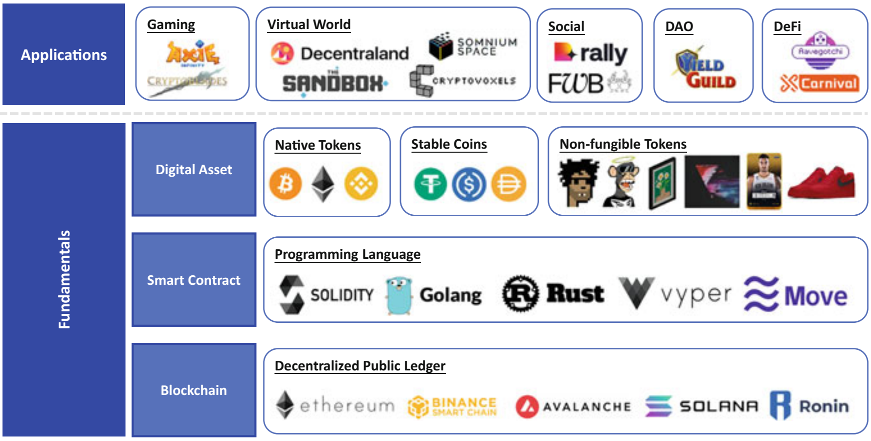


Fig. 1.5 A technical overview of Web3, metaverse, and popular dApps

1.4.1 Blockchains

Anu et al. [1] suggested that in Web3, application data is no longer stored in a private database but in a blockchain that can be written or read by anyone. Blockchain returns digital sovereignty to the users in a decentralized manner. As the underlying ledger of Bitcoin, a blockchain [11] is composed of blocks and chains. User-generated data is stored in a newly generated block that will be linked to previously generated blocks, all of which are strung together in a chronological order [12]. Each full node on the blockchain maintains a complete record of the blockchain data. Therefore, if one node makes an error or is attacked, the remaining millions of other consensus nodes can correct such errors [13, 14]. Generally, there are three types of blockchains, i.e., the public, the private, and the consortium blockchains [12]. One of the typical applications of the public blockchain is Bitcoin.

1.4.2 Smart Contracts

Szabo introduced the concept of smart contracts in the mid-1990s [15], where he suggested embedding the logic of the contract into the code. With traditional contracts, a document outlines the terms of the relationship between two parties, which can be enforced by law. If party *A* violates the contract, party *B* can take party *A* to court for noncompliance. A smart contract [16] can be understood as an automatically executed contract with the terms of the agreement between the buyer and seller embedded within the code logic. Languages that currently support writing smart contracts include Solidity, Go, Java, and more.

1.4.3 Digital Assets and Tokens

Digital assets are intangible digital objects with verifiable and ownable digital values [1]. One of the main representatives of digital assets is *token*. A token is a digital asset implemented in a smart contract and is the medium for the storage and exchange of value in the metaverse [17]. The benefits of digital assets include a ubiquitous ledger, transparent updates, and payments that can be recorded and verified and do not require centralized settlement [18]. In the metaverse, the blockchain automatically records human interactions in a tamper-proof public ledger, and the block miners obtain tokens as a reward. Tokens can be divided into two types: fungible tokens and non-fungible tokens. A fungible token is one that is interchangeable with another token, while non-fungible tokens (NFTs) are not interchangeable.

Among various token standards, Ethereum Request for Comment 20 (ERC-20), which was born in 2015, is one of the representative standards for fungible tokens created using the Ethereum blockchain. Despite the fact that fungible tokens have the same price per unit of currency, their values are typically somewhat volatile. For example, Bitcoin (BTC) is approximately 10 times more volatile relative to the US dollar than between major national currencies [19]. Stable coins were therefore created to address this problem [20]. Most of these stablecoins solve the problem of the large price fluctuations of most cryptocurrencies denominated in US dollars by pegging their value to a fixed number of traditional monetary instruments [20]. One representative is USDT, which is pegged to the US dollar.

The functionality of fungible tokens is limited because each coin has the same price and cannot carry extra information. Therefore, the concept of non-fungible tokens is introduced in the ERC-721 standard. Each non-fungible token is unique, with a unique Token ID and a different value. Each non-fungible token tends to be linked to a URL that stores media data, such as images and videos. For example, the NFT CryptoPunks series [21], which currently has a total value of 1,063,845 Ether on the OpenSea platform, has a historical NFT trading price ranging from 0.001 Ether to several hundred Ether.

1.4.4 Typical Applications Related to Web3 and Metaverse

1.4.4.1 Games

The metaverse has the potential to add realism to games. Players can build their own territory in metaverse games at will and are even able to change the pattern and future direction of the games by holding game tokens. The most important feature of metaverse games is that the currency or circulating items in the games are cryptocurrencies, which means that the currency and items traded in the game are tied to fiat currency. As a result, the concept of “Play-to-Earn” is frequently mentioned in metaverse games, that is, earning in-game money in the real world. The play-to-earn model was started with a pet trading and fighting game called Axie Infinity [22]. Players can create virtual pets called "Axies" in this Ethereum-based game and then send the avatars to earn game tokens through competitions and battles. There is also CryptoBlade [23], a game based on the Coinan chain. In the game, users can use weapons to defeat enemies to earn Skill tokens, which in turn upgrade the character. As users level up in the game, they can make weapons with different power. The more powerful the weapons they have, the more Skill tokens they will get.

1.4.4.2 Virtual World Metaverses

Typical examples of virtual world metaverses include Decentraland [10], Cryptovoxels [24], The Sandbox [25], and Somnium Space [26]. In these virtual worlds, users can own a part of the world by purchasing scarce land NFTs. Since the land in the virtual world is represented by NFTs. This means that each virtual land is unique and ownership can be easily tracked. In addition, since the land within the platform acts as virtual assets, they support the owners to build them and create a digital world according to their will. Therefore, many users will move their real life to those virtual world buildings such as casinos, financial centers, and shopping malls in a metaverse.

1.4.4.3 Social Network Projects

Social projects related to the metaverse concepts are mainly specialized social applications for certain kinds of groups, such as Friends with Benefits [27] and Rally [28]. For example, Friends with Benefits is a Discord-based private club with over 2000 members, which requires not only a strict identity check (written application) but also nearly 10,000 dollars in tickets and a certain amount of the native tokens called FWB to build their own customized personal tokens on the platform. Rally is an incentive platform for creators and their communities to build their independent digital economies. Creators receive incentives for creating personal tokens, and fans can support their favorite creators by purchasing tokens with tokens RLY.

1.4.4.4 DAOs

Decentralized autonomous organizations (DAOs) are groups established on a mission to coordinate and collaborate through a set of shared rules implemented on the blockchain. For example, Yield Guild Games [29] is a DAO gaming guild founded in the Philippines and composed of players and investors. In Yield Guild Games, all participating members are investors and players. The investors are responsible for the NFT assets of the different games in their ecosystem and lend these assets to the community of gamers. Players are responsible for participating in the game to acquire game currency, while the guild can reinvest the available surplus to purchase virtual assets and land within the game.

1.4.4.5 DeFi

DeFi was introduced in 2020, and its rapid development in recent years has greatly boosted the demand for NFT. Digital art, domain names, and anything related to ownership can be minted into NFTs. Like artworks and collectibles, digital assets are more difficult to buy and sell due to their low liquidity in encrypted markets. However, the advent of DeFi has changed all that, bringing much-needed liquidity to NFTs. DeFi has flourished because it has democratized the access to financial services such as lending, savings, and insurance, which have attracted significant investment in DeFi ecosystem. In short, the emergence of DeFi is revolutionizing the traditional financial industry, and a large number of influential financial practitioners are paying close attention and getting involved.

XCarinval [30], for example, is a collateralized lending platform for metaverse assets, offering collateralized lending services including all types of NFT assets as well as long-tail assets, providing an effective value release for liquidity-starved assets. In addition, Aavegotchi [31] is a digital collection of NFTs combined with DeFi, where each Aavegotchi NFT token is both a collectible and an asset capable of generating income, and the properties of the NFTs depend on their value and rarity in the Aavegotchi universe.

1.4.5 Digital Identity in Web3 and Metaverse

To participate in activities in Web3 and metaverse, users and even each digital object must have their identities. Given the fundamental role of digital identity, we introduce its concept and other related ecological issues.

1.4.5.1 Introduction to Digital Identity

Digital identity refers to the representation of an individual's identity through digital information. It can be understood as a digital key that compresses a user's real identity information, which can be bound, queried, and verified in real time with the user's behavior information. For example, digital electronic identity (eID), issued based on the citizen's ID number, serves as a digital identity for citizens. eID can ensure the uniqueness of the digital markers issued to each citizen, thus reducing the dissemination of citizens' plaintext identity information on the Internet. eID can also enable the interoperability of citizens' digital identities across different applications.

Since eID offers us a stable service, why would the technology of decentralized identity (DID) be necessary?

To answer this question, we need to understand the following characteristics of DID:

- DID is easier to authenticate. It can eliminate passwords and cumbersome multi-factor authentication protocols, making it easier for organizations to quickly verify a user's identity.
- DID has better data security. Sensitive identity information (personal information and credentials) will be securely stored in the user's digital wallet and only shared with necessary parties when needed.
- DID can reduce the cost of enterprise data management. It allows users to store personal data, relieving the burden for enterprises.
- Regulatory compliance. Decentralized identity frameworks can relieve the responsibility of centralized organizations when building databases to store user information.
- DID enable users to visit multiple websites with a single DID.
- DID ensures the ownership and authority of user data. Decentralized identity is described as self-sovereign identity (SSI) because it hands over the authority of personal data to individuals. In the DID system, users can decide which information will be shared with third parties.

In Web3, users can autonomously manage their identity through decentralized digital identity technologies, truly achieving personal ownership of data and assets and enabling decentralized sharing across applications. With the development of identity authentication technologies, users' digital identities have gradually transitioned from centralized single-institution identities to multi-institutional alliance identities. Identity data has also gradually acquired a certain degree of portability. The centralized identity authentication model commonly uses the institutions that issue certificates in the public key infrastructure (PKI) system to authenticate user identities. Alliance identity refers to the interoperability of identity systems between different internet platforms. To truly achieve user autonomy over their own identities, a decentralized "digital identity system" is needed.

DID is a type of identifier defined by the W3C DID specification organization, which has global uniqueness, high availability, and encryption verifiability [32]. The first DID standard specification was published by the W3C in 2019 [33]. The DID system defined by the W3C consists of two layers, i.e., the *basic layer* and the *application layer*.

The basic layer of a DID system consists of DID identifiers in string form and DID documents in JSON object format. The DID identifier has global uniqueness and is used to represent the digital identity of an entity. Each DID identifier corresponds to a DID document, which mainly contains key information and verification methods related to DID verification, which is used to control the digital identity of the entity. Since personal information such as name and address is not stored in the DID document, identity recognition and verification cannot be achieved solely through the DID identifier. Instead, the verifiable claim (VC) in the DID application layer must be exploited.

The DID standard proposes a verifiable proof mechanism. Verifiable claims (VCs) are the key to building the DID system. This is because the uniqueness and trustworthiness of the DID system need to be established on a trusted distributed system, where the main participants include the *Issuer*, *Inspect Verifier (IV)*, *Holder*, and *Identifier Registry*. The *Issuer* is an entity that has user data and can issue VCs, such as government departments, public security agencies, and educational institutions. The IV can verify the VCs issued by the *Issuer* and provide services based on them. The *Holder* is any user who has VCs. The *Identifier Registry* is responsible for maintaining information on the blockchain.

Compared with traditional PKI-based identity systems, the blockchain-based DID digital identity systems have the features of ensuring data authenticity and credibility, thus protecting users' privacy and security, and high portability. In addition, by combining with decentralized public key infrastructure (DPKI) [34], a DID system has achieved the key characteristics of decentralization, self-sovereignty, and trustworthy data exchange in Web3. DID is the key technology to achieving decentralized identity management. In the future digital society, the new concept brought by the distributed digital identity system will inevitably spawn new business models.

1.4.5.2 Taxonomy of Constructing the DID Ecosystem

Figure 1.6 illustrates the layered DID ecosystem published by Amber Group [35] in November 2021. The layered ecosystem includes five layers. Layer-I refers to various identifiers and standards such as Decentralized Identity Foundation (DIF), W3C, etc. Layer-II consists of infrastructures that enable other upper layers. Layer-III defines digital credentials. In Layer-IV, a large number of Web3 applications, such as wallets, Web3 products, and other decentralized Apps, can provide the application scenarios for the DID technology. The DID ecosystem also includes a transversal Layer-X, which consists of blockchains and blockchain-based DeFi protocols such as Ethereum, Bitcoin, IPFS, polygon, etc.

We then discuss the categories of constructing the DID ecosystem. The development of the DID ecosystem can be mainly classified into four categories, i.e., (1) off-chain identity authentication, (2) chain-based identity aggregator, (3) chain-based credit rating, and (4) chain-based behavior authentication.

Category 1: Off-Chain Identity Authentication

The first category of DID ecosystem is "off-chain identity authentication," which aims to bind real-world identity information to on-chain addresses. BrightID [36] is a representative project for verifying real-world identity. Users need to make an appointment for a Zoom video conference and complete BrightID's unique identity verification through face recognition and verification officer review. Several projects

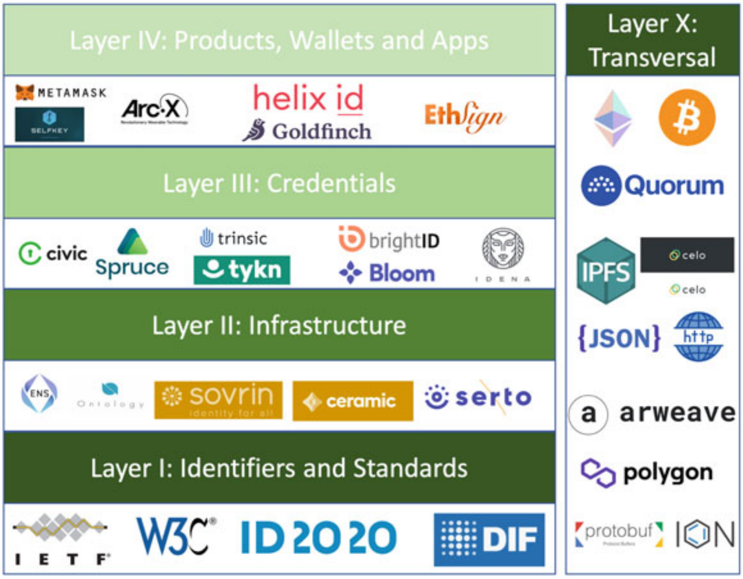


Fig. 1.6 DID layered ecosystem [35]

have adopted BrightID, such as Gitcoin, RabbitHole, Status, etc., to ensure the slogan for Web3 applications "one person, one ID."

In the following, we review several representative products that fall into the first category.

WeIdentity [37] is an open-source, blockchain-based solution for entity identity authentication and trusted data exchange led by WeBank. WeIdentity provides a series of basic and application interfaces for distributed identity trust and management, trusted data exchange protocols, and other functions. It realizes a set of distributed multicenter identity trust protocols and verifiable digital credential technology in accordance with the W3C DID specification, making distributed multicenter identity management possible. Institutions can also legally and compliantly exchange trusted data through user authorization.

Baidu's DID solution is structured into three layers, from bottom to top, i.e., *blockchain layer*, *decentralized Layer2 network*, and *trusted exchange layer*. The bottom layer uses decentralized storage and blockchain technology as its core, where distributed storage maintains the mapping between DID and public keys and the blockchain anchors the corresponding relationships of these identity data. The decentralized Layer2 [38] solves the problem of low throughput (measured by transaction per second, TPS) in current blockchain technology and provides a unified DID resolution service. In the trusted exchange layer, Baidu's DID solution enables secure identity authentication and data exchange among various participants in the ecosystem.

Microsoft's Microsoft DID is a distributed digital identity technology architecture based on Azure cloud services, capable of managing distributed digital identity across different blockchains. The solution can be divided into three parts, Sidetree [39], Identity Overlay Network (ION) [40], and DID, corresponding to the protocol layer, network layer, and application layer, respectively. The three parts are built in a hierarchical relationship. ION is the core of the entire solution, based on the Sidetree protocol, achieving good scalability while ensuring the decentralized nature of blockchain. Additionally, as a Layer2 solution, ION can achieve high TPS without being limited by the throughput of the underlying blockchain. The project registers distributed digital identity identifiers on different blockchains through the blockchain BaaS (blockchain as a service) service and can become a widely used intermediate layer to achieve the goal of interoperability of the Decentralized Identity Foundation (DIF). It also solves the problem of low efficiency in registering DID on public blockchains and provides developers with the basic module for managing user privacy data through the Identity Hub [41].

Sovrin [42] is a DID solution based on the HyperLedger blockchain. It allows for user-defined privacy protection, selectively disclosing personal data through paired pseudonymous identities, peer-to-peer private agents, and zero-knowledge proof encryption. In addition, to provide an economic incentive mechanism for VC issuers, owners, and verifiers, the Sovrin protocol uses a digital token called uPort. uPort [43] is a distributed digital identity management service based on Ethereum launched by Consensys. It enables users to perform identity verification, passwordless login, and digital signatures and interact with other applications on Ethereum. uPort aims to solve the common problem of blockchain user key management by providing users with a persistent and usable digital identity.

Category 2: Chain-Based Identity Aggregator

The second category of DID construction focuses on creating digital identities for "digital beings" and managing on-chain information aggregation. The service object of Web3 applications should be "digital beings" instead of real individuals. Each user in the real world can choose to build multiple digital identities in the Web3 world. Unipass [44] is one of the representatives of this category of projects, whose main product is chain-based identity aggregation management. Using a Unipass ID, users can bind email addresses, and multiple ETH addresses, and also build application layer protocols such as social graphs (e.g., CyberConnect) and information aggregation platforms (e.g., RSS3).

Category 3: Chain-Based Credit Rating

The third category of DID construction is "chain-based credit rating." This category aims to expand the DeFi lending scene and find a way to implement real-world credit mechanisms that can improve the efficiency of DeFi resource allocation. For example, ARCx [45] issues a DeFi Passport, which quantifies the credibility of its chain-based address based on the credit score of each DeFi Passport holder. The credit score is determined by analyzing the historical activities of the holder's Ethereum address, with a range set from 0 to 999, which determines the mortgage rate that the protocol provides to the user.

Category 4: Chain-Based Behavior Authentication
The last category of DID construction is “chain-based behavior authentication,” which dynamically updates users’ identity status and guides them to participate in activities or behaviors required by some cooperative parties and issues them with on-chain certification. RabbitHole [46] is the representative project of “learn to authenticate.” It decomposes each decentralized application into game tasks, guides users to interact with blockchain protocols and decentralized applications, and cultivates the usage habits of DeFi users. Users’ Web3 operations and behaviors will then receive authentication issued by RabbitHole.

1.4.5.3 Summary of DID

Research on DID reflects the importance of decentralized digital identities in the Web3 era. Various DID projects seamlessly integrate users’ digital identities into their daily lives, enabling users to include more data in their identities while protecting data privacy and authorizing users’ access and ownership of their data. Therefore, DID can be viewed as the identity center of the Web3 world. As users control the essentials of DID, they can decide when, with whom, and under what conditions to disclose their digital identity elements. Plenty of pioneering projects have been built upon DID and blockchain technologies. As one of the basic infrastructures of Web3, DID has shaped the Web3 ecosystem.

1.5 Brief Review of Related Works

The term “metaverse” was first used in the science fiction novel “Snow Crash” in 1992 [47]. In 2008, Hendaoui et al. [48] proposed an early concept of the metaverse, i.e., a 3D virtual social world. Schumacher et al. [49] discussed that the metaverse is an immersive Internet that provides a more advanced and efficient platform for social exchange and communication. Up to now, there have been a number of studies that have discussed metaverse from different aspects, as shown in Table 1.1.

In terms of the concept and definition of metaverse, Dionisio et al. [50] proposed four characteristics of the metaverse, including universality, realism, scalability, and interoperability. Lee et al. [14] summarized eight basic techniques for building a metaverse. Park et al. [51] discussed three components of the metaverse, namely, hardware, software, and content. Yang et al. [52] proposed that artificial intelligence and blockchain technology will play a great role in metaverse construction and further investigated the possibility of integrating artificial intelligence and blockchain technology with the metaverse. The concept of the metaverse is now clear, and therefore the number of metaverse applications has started to increase.

In terms of metaverse applications, Chen et al. [55] explored the advantages of using virtual reality to socialize in a metaverse compared to traditional social

Table 1.1 Related studies

Refs	Contribution	Keyword	Year
[48]	Metaverse is a 3D virtual social world	Metaverse concept	2008
[50]	Proposed four characteristics of metaverse	Metaverse concept	2013
[14]	Proposed eight basic techniques for building metaverse	Metaverse concept	2021
[51]	Discusses the three components of the metaverse	Metaverse concept	2022
[52]	Proposes the role of artificial intelligence and blockchain technology in the metaverse	Metaverse concept	2022
[49]	Metaverse is immersive Internet	Metaverse concept	2022
[52]	The convergence of artificial intelligence, blockchain technology, and metaverse	Metaverse concept	2022
[53]	Virtual classroom	Metaverse applications	2013
[54]	Virtual university	Metaverse applications	2021
[55]	Advantages of metaverse compared to traditional social media	Metaverse applications	2022
[56]	Metaverse applications in healthcare, social software, entertainment, and smart cities	Metaverse applications	2022
[14]	Protecting digital assets and user privacy	Metaverse security	2021
[57]	Metaverse unavoidable security issues	Metaverse security	2022
[58]	The existence of traditional and new types of attacks in the metaverse	Metaverse security	2022
[59]	Non-homogenized tokens are vulnerable to attacks	Metaverse security	2022
[60]	Related policies and corporate layout	Metaverse policies, regulations	2021
[61]	Protection of personal interests and intellectual property	Metaverse policies, regulations	2022
[62]	How existing laws apply to the metaverse	Metaverse policies, regulations	2022

media. Tarouco et al. [53] proposed a virtual classroom capable of teaching calculus that can help students learn efficiently. Duan et al. [54] implemented a blockchain-powered metaverse project based on the Chinese University of Hong Kong. Chen et al. [56] proposed that applications including healthcare, social software, entertainment, and smart city construction can be implemented in the world of the metaverse. In summary, metaverse applications have exploded in recent years, but there are still some issues with application security.

In terms of metaverse security, Wang et al. [57] pointed out that the metaverse is rather vulnerable to problems such as smart contract vulnerabilities, ransomware, scams, and phishing. In addition, Lee et al. [14] proposed that protecting digital assets and user privacy will become an important issue to be addressed.

Kadar [58] claimed that in metaverse frauds, there are not only traditional account-takeover attacks like phishing scams and hacking, but also account gang money laundering, rug pull, and other new attack methods. Kshetri et al. [59] found that non-fungible tokens, as one of the components of the metaverse, are very vulnerable to hacking. In conclusion, the current security of the metaverse is relatively weak, and there is a large amount of money flowing into it, which can easily attract the attention of criminals. The security of the metaverse is relatively weak, and there is a large flow of money, easy to attract the attention of criminals. However, the current regulatory strategy on metaverse security is not yet well developed, such that accountability for security incidents and crimes is more difficult.

In terms of policies related to metaverse, Ning et al. [60] summarized the policies and representative enterprises of a metaverse in various countries. Smaili et al. [61] argued that laws and regulations should be formulated and updated to protect personal interests and intellectual property rights in the metaverse. Tom et al. [62] raised issues such as possible intellectual property rights in the metaverse and suggested how existing laws and regulations can be applied to the metaverse.

Along with the development of blockchain and Web3, the economic system of the metaverse will become mature with decentralized and cross-platform characteristics [56]. The Web3-enabled metaverse economy has flourished in recent years and has attracted plenty of attention from the aspects of research, applications, and investments. However, this emerging metaverse ecology currently lacks clear regulations and supervision, making it become a hotbed of crimes. Financial crimes that frequently occur on the metaverse can cause huge economic losses to customers, institutions, and even countries and bring negative effects to the metaverse in the long run. Therefore, Chap. 7 elaborates on the financial crimes occurring in metaverse, such as frauds, money laundering, illegal services, code vulnerabilities, etc.

1.6 Conclusion

In this chapter, we mainly introduce the basics of Web3 and metaverse, including their definitions, applications, implications, and their fundamental enabling technologies as well. In particular, we discuss some essential technologies such as blockchains, smart contracts, digital assets, typical applications, and DID.

References

1. A. Banerjee, R. Byrne, I. D. Bode, and M. Higginson. (2022) Web3 beyond the hype. [Online]. Available: https://www.mckinsey.com/industries/financial-services/our-insights/web3-beyond-the-hype
2. V. Shannon, "A More Revolutionary Web," *The New York Times*, vol. 23, 2006.
3. G. Wood, "Dapps: What Web 3.0 Looks Like," https://gavwood.com/dappsweb3.html, September 6, 2022.
4. M. community, "A Crypto Wallet & Gateway to Blockchain Apps," https://metamask.io/, September 6, 2022.

5. L. Lukac, “A Technical Guide to IPFS–the Decentralized Storage of Web3,” https://www.freecodecamp.org/news/technical-guide-to-ipfs-decentralized-storage-of-web3, September 6, 2022.
6. MINECRAFT, “New game: Minecraft earth,” https://www.minecraft.net/zh-hans/article/new-game--minecraft-earth, Retrieved December 16, 2022.
7. E. Games, “The world’s most open and advanced real-time 3D creation tool,” https://www.unrealengine.com/en-US/, Retrieved December 16, 2021.
8. Roblox, “Reimagining the way people come together.” 2022. [Online]. Available: https://corp.roblox.com/
9. Microsoft, “Microsoft mesh,” https://www.microsoft.com/en-us/mesh, Retrieved December 16, 2022.
10. Decentraland, “Introduction,” https://docs.decentraland.org/decentraland/introduction/, Retrieved December 16, 2021.
11. S. Nakamoto. (2008) A peer-to-peer electronic cash system. [Online]. Available: https://bitcoin.org/bitcoin.pdf
12. A. A. Monrat, O. Schelén, and K. Andersson, “A survey of blockchain from the perspectives of applications, challenges, and opportunities,” *IEEE Access*, vol. 7, pp. 117 134–117 151, 2019.
13. W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. Leung, “Decentralized applications: The blockchain-empowered software system,” *IEEE Access*, vol. 6, pp. 53 019–53 033, 2018.
14. L.-H. Lee, T. Braud, P. Zhou, L. Wang, D. Xu, Z. Lin, A. Kumar, C. Bermejo, and P. Hui, “All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda,” *arXiv preprint arXiv:2110.05352*, 2021.
15. N. Szabo, “Formalizing and securing relationships on public networks,” *First Monday*, 1997.
16. W. Zou, D. Lo, P. S. Kochhar, X.-B. D. Le, X. Xia, Y. Feng, Z. Chen, and B. Xu, “Smart contract development: Challenges and opportunities,” *IEEE Transactions on Software Engineering*, vol. 47, no. 10, pp. 2084–2106, 2019.
17. T. Chen, Z. Li, Y. Zhu, J. Chen, X. Luo, J. C.-S. Lui, X. Lin, and X. Zhang, “Understanding ethereum via graph analysis,” *ACM Transactions on Internet Technology*, vol. 20, no. 2, pp. 1–32, 2020.
18. R. K. Lyons and G. Viswanath-Natraj, “What keeps stablecoins stable?” *Journal of International Money and Finance*, 2022.
19. D. Yermack, “Is bitcoin a real currency? an economic appraisal,” in *Handbook of digital currency*, 2015, pp. 31–43.
20. U. W. Chohan, “Are stable coins stable?” *Notes on the 21st Century (CBRi)*, 2019.
21. L. Labs, “Cryptopunks,” https://www.larvalabs.com/cryptopunks, September 6, 2022.
22. S. Mavis. (2021) Official Axie Infinity whitepaper. [Online]. Available: https://whitepaper.axieinfinity.com/
23. C. Group. (2022) Cryptoblades. [Online]. Available: https://www.cryptoblades.io/
24. N. Consulting. (2022) Cryptovoxels. [Online]. Available: https://www.voxels.com/
25. Pixowl. (2022) Sandbox. [Online]. Available: https://www.sandbox.game/en/
26. S. S. L. Company. (2022) Somnium space. [Online]. Available: https://somniumspace.com/
27. M. Bodge. (2022) Friends with benefits. [Online]. Available: https://www.fwb.help/
28. B. Morris. (2022) Rally. [Online]. Available: https://rally.io/
29. Y. G. Games. (2022) Yield guild. [Online]. Available: https://yieldguild.io/
30. X. Group. (2022) Top player of metaverse asset bank. [Online]. Available: https://xcarnival.fi/
31. P. Studios. (2022) Aavegotchi. [Online]. Available: https://www.aavegotchi.com/
32. W3C, “Decentralized identifiers (DIDs) v1.0,” https://www.w3.org/TR/did-core/, 19 July, 2022.
33. ——, “A primer for decentralized identifiers,” https://w3c-ccg.github.io/did-primer/, 11 November 2021.
34. J. Shi, X. Zeng, and R. Han, “A blockchain-based decentralized public key infrastructure for information-centric networks,” *Information*, vol. 13, no. 5, p. 264, 2022.
35. AMBER, “Decentralized identity: Passport to web3,” https://www.ambergroup.io/newsDetail?source=marketNews&id=40237.

36. BrightID, “Bright DAO is here!” https://www.brightid.org/, September 6, 2022.
37. WeIdentity, “Weidentity documents,” https://weidentity.readthedocs.io/zh_CN/latest/, September 6, 2022.
38. C. Sguanci, R. Spatafora, and A. M. Vergani, “Layer 2 blockchain scaling: A survey,” *arXiv preprint arXiv:2107.10881*, 2021.
39. DIF, “Sidetree v1.0.0,” https://identity.foundation/sidetree/spec/, September 6, 2022.
40. Wikipedia, “Microsoft ion,” https://en.wikipedia.org/w/index.php?title=Microsoft_ION&oldid=1055984592, September 6, 2022.
41. T. I. Hub, “Welcome to the identity hub,” https://docs.theidentityhub.com/doc/Index.html., September 6, 2022.
42. P. J. Windley, “Sovrin: An identity metasystem for self-sovereign identity,” *Frontiers in Blockchain*, p. 30, 2021.
43. N. Naik and P. Jenkins, “uPort open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain,” in *2020 IEEE International Symposium on Systems Engineering (ISSE)*. IEEE, 2020, pp. 1–7.
44. UNIPASS, “Your passport to studying overseas,” https://unipass.co.ke/.
45. ARCx, “Better borrowing,” https://arcx.money/, September 6, 2022.
46. RabbitHole, “Earn tokens by using crypto applications,” https://rabbithole.gg, September 6, 2022.
47. N. Stephenson, *Snow crash: A novel*. Spectra, 2003.
48. A. Hendaoui, M. Limayem, and C. W. Thompson, “3D social virtual worlds: Research issues and challenges,” *IEEE internet computing*, vol. 12, no. 1, pp. 88–92, 2008.
49. P. Schumacher, “The metaverse as opportunity for architecture and society: design drivers, core competencies,” *Architectural Intelligence*, vol. 1, no. 1, pp. 1–20, 2022.
50. J. D. N. Dionisio, W. G. B. III, and R. Gilbert, “3D virtual worlds and the metaverse: Current status and future possibilities,” *ACM Computing Surveys*, vol. 45, no. 3, pp. 1–38, 2013.
51. S.-M. Park and Y.-G. Kim, “A metaverse: Taxonomy, components, applications, and open challenges,” *IEEE Access*, vol. 10, pp. 4209–4251, 2022.
52. Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng, “Fusing blockchain and AI with metaverse: A survey,” *IEEE Open Journal of the Computer Society*, vol. 3, pp. 122–136, 2022.
53. L. Tarouco, B. Gorziza, Y. Corrêa, É. M. Amaral, and T. Müller, “Virtual laboratory for teaching calculus: An immersive experience,” in *2013 IEEE Global Engineering Education Conference (EDUCON)*, 2013, pp. 774–781.
54. H. Duan, J. Li, S. Fan, Z. Lin, X. Wu, and W. Cai, “Metaverse for social good: A university campus prototype,” in *Proceedings of the 29th ACM International Conference on Multimedia (MM)*, 2021, pp. 153–161.
55. B.-J. Chen and D.-N. Yang, “User recommendation in social metaverse with VR,” in *Proceedings of the 31st ACM International Conference on Information & Knowledge Management (CIKM)*, 2022, pp. 148–158.
56. C. Chen, L. Zhang, Y. Li, T. Liao, S. Zhao, Z. Zheng, H. Huang, and J. Wu, “When digital economy meets web 3.0: Applications and challenges,” *IEEE Open Journal of the Computer Society*, vol. 3, pp. 233–245, 2022.
57. Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, and X. Shen, “A survey on metaverse: Fundamentals, security, and privacy,” *IEEE Communications Surveys & Tutorials*, 2022.
58. T. Kadar. (2022) The metaverse fraud question: What are the risks? [Online]. Available: https://seon.io/resources/metaverse-fraud/
59. N. Kshetri, “Scams, frauds, and crimes in the nonfungible token market,” *Computer*, vol. 55, no. 4, pp. 60–64, 2022.
60. H. Ning, H. Wang, Y. Lin, W. Wang, S. Dhelim, F. Farha, J. Ding, and M. Daneshmand, “A survey on metaverse: the state-of-the-art, technologies, applications, and challenges,” *arXiv preprint arXiv:2111.09673*, 2021.

61. N. Smaili and A. de Rancourt-Raymond, “Metaverse: Welcome to the new fraud marketplace,” *Journal of Financial Crime*, 2022.
62. T. Ara, M. Radcliffe, M. Fluhr, and K. Imp. Intellectual property and technology news. [Online]. Available: https://www.dlapiper.com/en/us/insights/publications/2022/06/exploring-the-metaverse-ipt-news-june-2022/

Chapter 2
How to Enrich Metaverse? Blockchains, AI, and Digital Twin

Jing Li, Shuzhang Cai, Qinglin Yang, and Huawei Huang

Abstract Metaverse as the latest buzzword has attracted great attention from both industry and academia. Metaverse seamlessly integrates the real world with the virtual world and allows avatars to carry out rich activities including creation, display, entertainment, social networking, and trading. Thus, it is promising to build an exciting digital world and to transform a better physical world through the exploration of the metaverse. In this chapter, we dive into the metaverse by discussing how to enrich metaverse using the technologies of blockchains, artificial intelligence (AI), and digital twin. By investigating the state-of-the-art studies across the metaverse components, digital currencies, AI applications in the virtual world, and digital twin technologies, we present our outlook on building a promising future metaverse. Further exploitation and interdisciplinary research on how to enrich the metaverse will definitely require collaboration from both academia and industries. We wish that this chapter can help researchers, engineers, and educators build an open, fair, and rational future metaverse.

Keywords Blockchains · Artificial intelligence · Digital twin · AI-based generated content · User-generated content · Edge networks

J. Li
Department of Computing, The Hong Kong Polytechnic University, Hung Hom, Hong Kong
e-mail: jing5.li@polyu.edu.hk

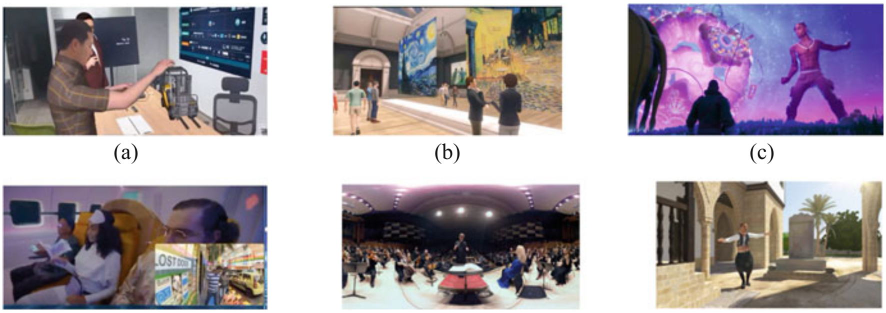
S. Cai
Naveen Jindal School of Management, The University of Texas at Dallas, Richardson, TX, USA

Q. Yang · H. Huang (✉)
School of Software Engineering, Sun Yat-sen University, Zhuhai, Guangdong, China
e-mail: yangqlin6@mail.sysu.edu.cn; huanghw28@mail.sysu.edu.cn

H. Huang et al. (eds.), *From Blockchain to Web3 & Metaverse*,
https://doi.org/10.1007/978-981-99-3648-9_2

2.1 Introduction

The concept of metaverse was proposed almost 30 years ago in the science fiction named *Snow Crash*, written by *Neal Stephenson* [2]. Metaverse has been one of the hottest buzzwords to attract the tech industry's attention due to the rapid advancements of blockchain, Internet of Things (IoT), VR/AR, artificial intelligence (AI), cloud/edge computing, etc. The sandbox game platform Roblox [3] is the company that firstly incorporates the term "metaverse" into their prospectus and proposes the key characteristics (e.g., identity, friends, immersive experience, low friction, civility, economy, anywhere, variety) of metaverse. The social company, Facebook, is renamed as *Meta* [4] to help bring metaverse to life and make people meet each other, learn, collaborate, and play in ways that go beyond what they can imagine. The video game Fortnite [5] that is released by Epic Games puts the players into a virtual world, such as a post-apocalyptic, zombie-infested world, experiencing new levels of photorealistic interaction [5–8] and watching virtual concert [9]. Metaverse seamlessly integrates the physical world with the virtual world and allows avatars to carry out rich activities including creation, display, entertainment, social, and trading. Nowadays, both academia and industries dive into the exploration of metaverse. For example, Jingteng Tech [10] has developed BeamLink, by which users can share photos and documents and have an interactive meeting collaboration, as shown in Fig. 2.1a. Furthermore, the optical sensors (e.g., depth and cameras) deployed with CNNs are commonly applied to capture the gestures and movements of dancers. The poses and movements of dancers, as shown in Fig. 2.1f, can be clustered as a high-dimensional feature space, which is further converted into dance performance in virtual environments [11] through techniques like *dynamic time wrapping* [12]. Compared to the physical world, autonomous avatars can understand human dancer's voice-to-motion mapping. Powered by deep learning, avatars can also mimic dance moves with high dance resemblance and emotional expressions.



(a) (b) (c)

(d) (e) (f)

Fig. 2.1 Scenarios that users can experience in metaverse. (**a**) Meeting collaboration. (**b**) Virtual exhibition. (**c**) Virtual concert. (**d**) Virtual-real symbiosis. (**e**) 360° Egocentric view. (**f**) Avatar's dance [1]

Given those potentials of metaverse, a problem is that researchers cannot accurately judge the shape and boundary of the future metaverse. They could only envision some of its possible characteristics, such as open space, decentralization, human-computer interaction experience, digital assets, and digital economy.

The avatars of human players, their creations, and consumption in metaverse truly affect the physical world and even change the behaviors of people in the physical world, through the influence of people's thoughts (e.g., choosing the entertainment method). This change has a profound social significance [13, 14] and thus forms the lifestyle of post-human society while reconstructing the digital economic system. The metaverse can be viewed as a complete and self-consistent economic system, a complete chain of the production and consumption of digital items. The economy of metaverse refers to the digital production-based economic behaviors, e.g., creation, exchange, and consumption in the digital world, are the fundamental components of the digital economy. The development of the economic system can be regarded as one of the most challenging tasks of metaverse. This is because the production and consumption of digital assets that can be traded in the virtual world is a phenomenon that traditional economists have not encountered [15]. Moreover, in a public, fair, and self-organized virtual world, the centralized economic system of the physical world cannot operate efficiently due to the high transaction volumes involved. Considering the interaction between the virtual world and the physical world, metaverse should enable the currency circulation to break the barrier of life, products, learning, working, etc. Therefore, the economic system of metaverse must be constructed in a decentralized manner such that the virtual assets of avatars could be traded efficiently in metaverse.

Blockchain as a decentralized ledger without a centralized authority has drawn enormous attention in diverse application fields in recent years. Blockchain is highly expected to bring a variety of opportunities to metaverse and trigger a new round of technological innovation and industrial transformation. On the other hand, recent advances in AI have brought promising solutions to overcoming the challenges of metaverse development, such as big data analytics, AI-empowered content generation, and intelligence deployment. Consequently, the integration of AI and blockchain becomes a promising trend to promote the benign evolution of the blockchain/AI-empowered metaverse ecosystem. Although the advent of blockchain and AI has spawned a large number of new technologies and applications, the fusion of blockchain and AI with metaverse also poses several emerging research challenges. For example, transaction volumes in metaverse systems are much higher than those in the physical world due to the features of digital products and markets. Blockchain-based non-fungible tokens (NFT) enable avatars to generate the content that can be traded with their digital certificates [16, 17].

We then review several representative survey articles here, to highlight the difference of our survey. Lim et al. [18] focus on the network demands [19] of metaverse from the perspective of edge intelligence [20] since metaverse is viewed as "the successor to the mobile Internet." Du et al. [21] propose a privacy-preserving targeted advertising strategy for the wireless edge metaverse to enable metaverse service providers to allocate network bandwidth to users so that the users can access metaverse from edge sites. Jiang et al. [22] introduce a kind of collaborative computing paradigm based on coded distributed computing to support the computation requirement of metaverse services [23]. The up-to-date survey [13] mainly reviews the state-of-the-art technologies as enablers to implement metaverse, such as high-speed networks (e.g., 5G) and edge computing, blockchain, and AI. The authors' findings demonstrate the gap between the up-to-date technologies and the demands of implementing metaverse. The other survey [24] focuses on metaverse analytics, search traffic, news frequency, and the topic concerning sustainable growth. Duan et al. [25] highlight the representative applications for social goods and propose a three-layer metaverse architecture from a macro perspective, which contains infrastructure, interaction, and ecosystem. In contrast, this chapter discusses how to enrich metaverse with blockchain, AI technologies, and digital twin.

2.2 How Blockchain and AI Enable Metaverse

2.2.1 An Open Metaverse Needs Blockchains

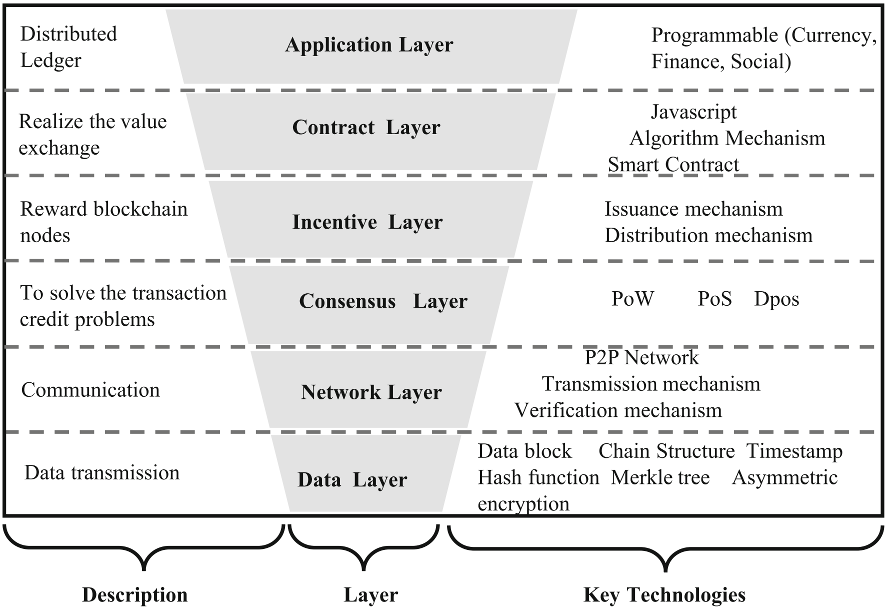
Metaverse is a decentralized virtual world based on blockchains. This means that the future metaverse will not be managed by a centralized entity, but is maintained by a large number of decentralized entities around the world. Therefore, metaverse technology is not subject to government review and is convenient for user experience [26].

Blockchains are used to record any type of data in publicly distributed ledgers [27]. From such ledgers, people can track the historical transactions of cryptocurrencies, NFTs, and other digital assets recorded in the chain. Given that the centralized token systems have suffered from severe hacking threats, centralized cryptocurrency exchanges (CEXes) may be stolen [28]. Therefore, the blockchain-based token system is more reliable than CEXes.

Blockchain is widely believed as one of the fundamental infrastructures of metaverse, because it can bridge isolated small sectors together and provide a stable economic system, which helps offer transparent, open, efficient, and reliable rules for metaverse. For example, hash algorithms and timestamp technologies as the major components in the data layer of blockchain could provide metaverse users the traceability and confidentiality of the data storing in the bottom layer of blockchains.

As illustrated in Fig. 2.2, the conventional blockchain architecture includes a data layer, network layer, consensus layer, incentive layer, contract layer, and application layer. The correlations between those layers and the metaverse are explained as follows:

- Data transmission and verification mechanism provide network support for various data transmission and verification of metaverse economic system.
- Consensus mechanisms solve the credit problem of metaverse transactions.



Description	Layer	Key Technologies
Distributed Ledger	Application Layer	Programmable (Currency, Finance, Social)
Realize the value exchange	Contract Layer	Javascript Algorithm Mechanism Smart Contract
Reward blockchain nodes	Incentive Layer	Issuance mechanism Distribution mechanism
To solve the transaction credit problems	Consensus Layer	PoW PoS Dpos
Communication	Network Layer	P2P Network Transmission mechanism Verification mechanism
Data transmission	Data Layer	Data block Chain Structure Timestamp Hash function Merkle tree Asymmetric encryption

Fig. 2.2 Layered architecture of the blockchain technology

- Distributed storage of blockchain ensures the security of virtual assets and the identities of metaverse users.
- Smart contract technology offers a trustworthy environment for all participating entities in the metaverse. It realizes the value exchange in the metaverse and ensures the transparent execution of system rules described in contract codes. Once deployed, the code of smart contracts cannot be modified anymore. All clauses depicted in those smart contracts must be completely executed.

The metaverse can exist without both blockchains and cryptocurrencies. However, an open and rational metaverse should be linked to open blockchains with high interoperability, in which virtual assets can be exchanged and circulated in a trustless and decentralized manner. Without the support of blockchain technology, it will be difficult to identify the value of the resources and goods trading in the metaverse, especially when those virtual elements have economic interactions with the real-world economy. Thus, it is undoubtedly worth exploring the blockchain technology in the metaverse.

2.2.2 High-Performance Blockchains Are the Foundation of Future Metaverse

Considering that the scalability of the metaverse keeps growing exponentially, it is not hard to imagine that the transactions originating from the future metaverse will be much more intensive than those in real-world scenarios. Thus, the future metaverse needs high-throughput and highly reliable blockchains, aiming to handle a giant number of transactions.

A lot of high-throughput blockchains have been proposed, such as Solana [29], Avalanche [30], Linera [31], Sui [32], Aptos [33], and BrokerChain [34]. Those blockchains claim to provide faster speeds, higher throughput, and lower fees than conventional blockchains such as Ethereum. Some of those new blockchains are also compatible with Ethereum assets and dApps. Given those advantages, we still believe that today's high-throughput blockchains will not be applicable to the requirement of the future metaverse. Therefore, researchers are encouraged to design new powerful blockchains that can achieve super high throughput such as at least 100 thousand *transactions per second* (TPS) and super high reliability.

This section introduces the application of AI technology in the field of generated content, compared with professional-generated content (PGC) and user-generated content (UGC).

2.2.3 Artificial Intelligence in Metaverse

Artificial intelligence is a research discipline proceeded based on the hypothesis that every aspect of learning can in principle be so precisely described [35]. The state-of-the-art AI studies focus on machine learning, deep learning, and reinforcement learning in the fields including computer vision, decision-making, and natural language process (NLP). Intuitively, the breakthroughs of artificial intelligence in the real world motivate people to realize metaverse. For example, machine learning provides technical support for all systems in metaverse to reach or exceed the level of human's learning. It shall significantly affect the operational efficiency and the intelligence of metaverse. Intelligent voice services provide technical support, such as voice recognition and communication, for metaverse users.

2.2.4 Representative AI Algorithms

Machine learning algorithms (e.g., linear regression [36], random forest [37], singular value decomposition [38]) enable machine to have the human ability by learning from experience and data. For example, support vector machine (Fig. 2.3) [39] is a kind of representative machine learning algorithm and is used for the

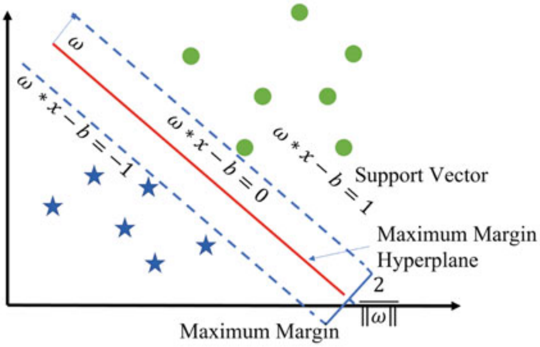


Fig. 2.3 Support vector machine

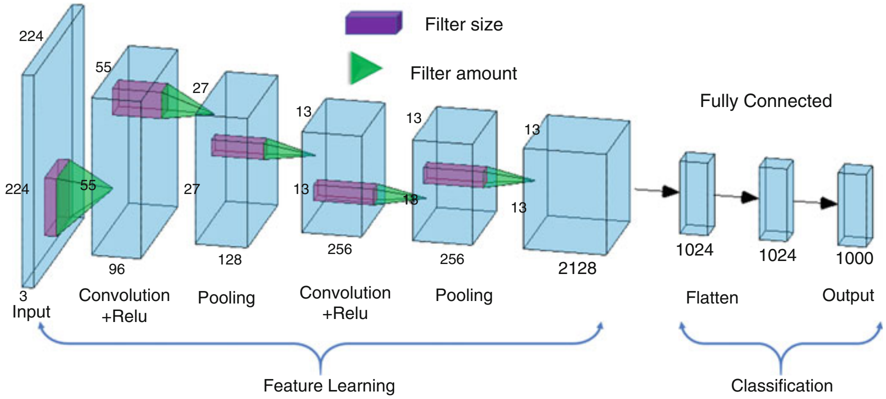


Fig. 2.4 Convolutional neural network

problem of pattern classification, regression, and learning a ranking function. The support vector classification aims to find an optimization hyperplane to separate the dataset D by minimizing the following object function:

$$L(\omega) = \sum_{i=1}^{|D|} \underbrace{\max\Big(0, 1 - y_i\Big[\omega^T x_i + b\,\Big]}_{\text{Loss function}} \underbrace{+\lambda\|\omega\|_2^2}_{\text{regularization}}\ , \qquad (2.1)$$

where ω denotes a weight vector, b denotes the threshold, and λ denotes a Lagrangian factor that determines the trade-off between margin maximization and regularization in the loss function. However, machine learning algorithms usually require selecting features manually, which limits its wide applications since a large amount of labeled data is needed.

The convolutional neural networks (CNNs or ConvNets (Fig. 2.4)) are a kind of representative deep neural network inspired by the biological neural network. The normal CNNs are based on the shared-weight architecture of the convolution kernels or filters that slide along input features and provide translation equivariant responses known as feature maps. CNNs are always composed of convolution layers, pooling layers, and fully connected layers [40]. The great amount of reduction in CNN is achieved by a technique called weight sharing between neurons. Given an image $X \in \mathbb{R}^{M \times N}$ and a filter $W \in \mathbb{R}^{m \times n}$, where $m << M, n << N$, the convolution can be written as follows:

$$y_{ij} = \sum_{u=1}^{m} \sum_{v=1}^{n} \omega_{uv} \cdot x_{i-u+1, j-v+1}, i \in [M], j \in [N], \tag{2.2}$$

where ω is the shared training parameters. Thus, CNNs are regarded as a kind of prevalent supervised learning that could perform well in many computer vision applications such as facial recognition, image search, augmented reality, and more.

However, reinforcement learning describes the sequential decision-making problem faced by an agent that must learn experience through trial-and-error by interacting with a dynamic environment [41]. The schematic of RL is demonstrated in Fig. 2.5. Considering the Markov decision processes (MDPs) [42] and deep neural network, deep reinforcement learning is promising to revolutionize the field of AI and represent a step toward establishing an autonomous system with a higher level of understanding of the visual world [43]. And there are two main approaches to solving RL problems: value functions and policy search. Value function methods are based on estimating the value (expected return) of being in a given state. The optimal policy π^* has a corresponding state-value function $V^*(s)$ and vice versa;

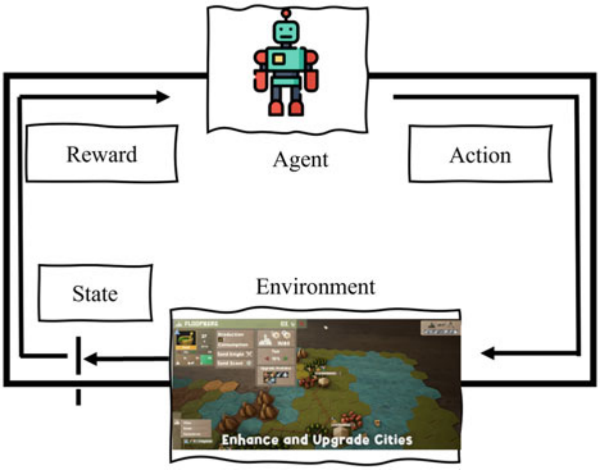


Fig. 2.5 Reinforcement learning

the optimal state-value function can be defined as:

$$V^*(\mathbf{s}) = \max_{\pi} \mathbb{E}[R|\mathbf{s},\ \pi].\ \forall \mathbf{s} \in \mathcal{S}, \tag{2.3}$$

where s denotes the state and π denotes the policy that agent follows. By contrast, policy search methods do not need to maintain a value function model but directly search for an optimal policy π^*. Until now, there have been developed many deep learning-based RL (DRL) algorithms, including deep Q-network (DQN), trust region policy optimization (TRPO), and asynchronous advantage actor-critic. These DRL algorithms can be applied to achieve over-human performance in some fields [43]. In the next section, we review the works on AI technologies that are related to the metaverse when it comes to the establishment of a metaverse environment and object creation in the metaverse.

2.2.5 Establishment of Metaverse Environment

Not only metaverse users, but the objects or things in the physical world also interact with the metaverse, evolving to persistently represent the structure, behaviors, and context of a unique physical asset (such as a component, a human, or a process) [44] in the virtual world. With the breakthroughs of digital transformation, the latest trend in every industry is to build digital twins with the ultimate goal of using them throughout the whole asset life cycle with real-time data [45]. Digital twins are instrumental not only during the conceptualization, prototyping, testing, and design optimization phase but also during the operational phase. The virtual world of metaverse generates a huge amount, variety, and velocity of data, such as structured data and unstructured data, which makes deep learning-based digital twin (DT) essential [46]. It can provide a better understanding of the underlying mechanics to all the stakeholders by the fusion of the virtual world with data sciences [47]. Ham et al. [48] propose a new participatory-sensing-to-digital twin city framework for community functioning in cities. The work fuses crowdsourced and unstructured visual data-based reality information with a three-dimensional (3D) virtual city to update the 3D city model that is fed into a computer-aided virtual environment (CAVE) for interacting and immersive visualization. To address the challenge of processing unstructured point clouds, epitomized by high-cost, movable objects, limited object classes, and high information inadequacy/redundancy, Xue et al. [49] present a novel unsupervised method, called Clustering of Symmetric Cross-sections of Objects (COSCO), to process urban LiDAR point clouds to a hierarchy of objects based on their characteristic cross sections. COSCO follows the Gestalt design principles, including proximity, connectivity, symmetry, and similarity (Table 2.1).

Lai et al. [50] propose a novel virtual environment for visual deep learning since the existing works have the drawbacks, such as small scenes or limited interactions with objects, which provides large-scale diversified indoor and outdoor

Table 2.1 A summary of AI applications in metaverse

Types	Description	Machine leaning models	Use cases
Virtual environments	3D computer vision [50]	DRL	Learning indoor navigation, Action recognition, Event detection, etc.
	Federated learning [51]	Parameter server-based	Augmented reality applications
	To reduce the executing latency and the drawbacks of AR [51]	Centralized FL in mobile edge computing	Collaborative learning
	Enabling cognitive smart cities using big data and machine learning [52]	Semi-supervised deep reinforcement learning	Smart city services
AI-based object	Recognizing Avatar faces [53]	Markov random field	Face recognition
	Detection and track [54]	Three-branch multistage CNN (Fig. 2.4)	Multi-people tracking
	NPC training [55]	RL (Fig. 2.5)	RL-DOT
	OpenAI Five [56]	Distributed learning framework and LSTM	Dota2
	Intelligent behavior avatar [57]	RL-based Bayesian networks graph	Play game tracking
	Learning-based interactive avatar control [58]	State-action	Animate and control avatars
	Human-computer interaction [59]	RL (Fig. 2.5)	Avatar moving
Virtual-real interaction	The trained controller in virtual environment can be transferred to the physical world [60–62]	LSTM and mixture density network	Robots training, Digital twin for human-machine interaction

scenes. Augmented reality (AR) devices could provide people with immersive and interactive experiences, while their applications are latency-sensitive. Hence, in the work [51], Chen et al. exploit to address the computation efficiency, low-latency objects recognition, and classification issues of AR applications by integrating mobile edge computing paradigm with federated learning. A city DT system depends on long-term and high-quality data to bring to perfection. Pang et al. [63] propose a federated learning-based DT framework to enable multiple city DTs to share the local strategy and status quickly while accumulating the insights from multiple data sources efficiently, thereby enhancing privacy protection settings.

Lee et al. [64] present a serious game for self-training fire evacuation drills, in which the avatar is synchronized with multiple trainees and can be placed in different remote physical locations with the option of real-time supervision. The proposed system architecture includes a wearable motion sensor and a head-mounted display to synchronize each user's expected motion with her/his avatar activity in the cyberspace of the metaverse environment. This system architecture provides an immersive and inexpensive environment for the easy-to-use user interface of a fire evacuation training system based on network experience. The model [54] explicitly deals with occluded body parts by hallucinating plausible solutions of not visible joint. Fabbri et al. propose a new end-to-end architecture that is a three-branch multistage CNN with four branches (visible heat-maps, occluded heat-maps, part affinity fields, and temporal affinity fields) fed by a time linker feature extractor.

To overcome the lack of surveillance data with tracking, body part, and occlusion annotations, they created the vastest computer graphics dataset for people tracking in urban scenarios by exploiting a photorealistic video game. During the initial stage of the metaverse, it still requires technological companies or governments to collaboratively establish the AI-based infrastructure regarding computational capacities, data, technologies, etc. However, scattered ownership of data is another barrier since companies often don't want to share commercially sensitive information, nor do governments [65]. To address this issue, federated learning (FL) has emerged as a kind of collaborative learning paradigm, allowing participants to train the shared model locally by transferring the training parameters instead of raw data. FL paradigm can protect the data privacy and reduce the communication overhead [66], especially for the large-scale scenarios with large models and massive data. With respect to the data privacy, there have been many research on applying FL in medical institutions [67], industries [65], banks [68], etc.

Mohammadi et al. [52] propose a semi-supervised deep reinforcement learning-based framework that utilizes a fusion of labeled (users' feedback) and unlabeled (without such users' feedback) data to converge toward better control policies instead of wasting the unlabeled data. The proposed framework is scalable to satisfy the demands of smart city services. Intuitively, this research on semi-supervised deep reinforcement learning-based can be mapped into the service of the metaverse, while the development of intelligent metaverse remains a challenge, such as integrating big and fast/streaming data analytics, big dataset shortage, and on-device intelligence.

2.2.6 *Intelligence for Metaverse*

After the descriptions of AI-based establishment of the virtual world, we shall argue the authoring tools in metaverse since AI-based authoring tools provide technical support for all systems and roles to reach the level of human learning. Authoring tools will greatly affect the operational efficiency and intelligence of metaverse.

2.2.6.1 Avatar and Non-player Characters

The notion *avatar* can be derived from Sanskrit. It identifies the god Vishnu's manifestations on earth. It was the first usage as a representation of a player in virtual worlds [69]. Avatars are not only used in games, but also as users' representations in e-commerce applications, virtual social environments, and geographically separated meetings [70].

Chen et al. [57] propose a novel method for personal intelligent behavior avatar to make the optimal strategic decision for the user through the interactions between the user and agents by integrating Bayesian networks and reinforcement learning in the virtual environment. To create a controllable and responsive avatar with large motion sets in computer games and virtual environments, Lee et al. [58] present a novel method of precomputing avatar behavior from unlabeled motion data in order to animate and control avatars at minimal runtime cost. Meanwhile, a reinforcement learning method [59] is applied to train a virtual character to move participants to a specified location. The virtual environment demonstrates an alleyway displayed through a wide field-of-view head-tracked stereo head-mounted display. This method opens up the door for many such applications where the virtual environment adapts to the responses of human participants with the aim of achieving particular goals.

Apart from the mentioned above, AI-driven non-player characters (NPCs) are computer-operated characters who act as enemies, partners, and support characters to provide challenges, offer assistance, and support the storyline. Whereas, from the game perspective, most of the human-looking NPCs are not intelligent enough to interact with players in specific game genres (e.g., real-time strategy, some modes of first-person shooting), which requires strong tactical decision-making abilities. Wang et al. [55] propose a reinforcement learning-based domination team for playing unreal tournament (UT) domination games that consists of a commander NPC and several solider NPCs. During each decision cycle in the running process, the commander NPC decides troop distribution and, according to that decision, sends action orders to other soldier NPCs. Each soldier NPC tries to accomplish its task in a goal-directed way, i.e., decomposing the final ultimate task (attacking or defending a domination point) into basic actions (such as running and shooting) that are directly supported by UT application programming interfaces (APIs). The RL agents as means of creating NPCs that could both progressively evolve behavioral patterns and adapt to the dynamic world by exploring their environment and learning optimal behaviors from interesting experiences [71, 72].

Berner et al. [56] develop a distributed training system and tools for continual training which allows researchers to train OpenAI Five for 10 months. By defeating the Dota-2 [73] world champion (Team OG), OpenAI Five demonstrates that self-play reinforcement learning can achieve superhuman performance on a difficult task. Rahmatizadeh et al. [60] attempt to address the challenging problem of behavior transfer from virtual demonstration to a physical robot through training a long short-term memory (LSTM) recurrent neural network to generate trajectories. During the training process, a mixture density network (MDN) is applied to calculate an error signal suitable for the multimodal nature of demonstrations. The learned controller in the virtual environment can be transferred to a physical robot (a Rethink Robotics Baxter) and successfully perform the manipulation tasks on a physical robot, which motivates the avatar to create AI objects that can impact the physical world. Similarly, the works [61, 62] exploit the interaction between the virtual environment and the physical world by CNNs.

2.2.6.2 AI-Driven Activities in Metaverse

In games (e.g., Epic [7], Roblox [3], and Decentraland [74]), the basic characteristics of metaverse can be perfectly explained and displayed. However, no game has fully achieved an ideal metaverse. Games conventionally have rules, objectives, and boundaries that enable them to shape specific gameplay. In contrast, metaverse does not require any specific gameplay. Some online social games are very similar to metaverse, such as *sims* [74]. Metaverse, however, differs from video games, because it involves many activities that are not necessarily for fun. Examples are reviewed as follows:

- Metaverse users can attend events (concerts, virtual exhibitions, remote education, meeting collaboration, etc.) without having to travel.
- Metaverse is virtual and real symbiosis, which means it can evolve in parallel even if people leave the virtual world anytime.

Being aware of the difference between video games and metaverse, we can exploit metaverse from the perspective of video games and extend it to the fields of manufacturing, education, creation, entertainment, social, and so on. Ando et al. [75] present a way how to infer the observed exhibits in a metaverse museum from a movement log based on Second Life. To use recommendation systems in metaverse museums, they need some pieces of information to infer which exhibits the user is visiting via performing this task efficiently and precisely by focusing on the avatar's states in the museum.

Yampolskiy et al. [53] propose a set of algorithms that are capable of verification and recognition of avatar faces with a high degree of accuracy. Lugrin et al. [76] propose a method for the AI-based simulation of object behavior so that interactive narrative can feature the physical environment inhabited by the player character as an *actor*. The prototype based on the top of the Unreal Tournament game engine relies on a *causal engine*, which essentially bypasses the native Physics engine to generate alternative consequences to player interventions. The evaluation method [77] can be applied to the human-centered evaluation of AI-based games, grounded in the analysis of player retellings of their play experiences in Civilization VI, Stellaris, and two distinct versions of the research game Prom Week. The reason is that it is difficult to understand through existing evaluation methods, such as the typical narrative structure that players tend to have in their minds when playing a specific game. The diversity of subjective experience narratives that might occur in a specific game.

Puder et al. [78] demonstrate that an open distributed environment can be viewed as a service market where services are freely offered and requested. Any infrastructure which pursues appropriate mechanisms for such an environment should contain mediator functionality (i.e., a trader) that matches service demands and service offers.

In the open and decentralized metaverse, DRL is expected as a promising alternative for automated trading in the metaverse ecosystem since DRL can enable the well-trained agent to make the decision automatically. Liu et al. [79, 80] believe that proper usage of AI will initiate a paradigm shift from the conventional trading routine to an automated machine learning approach. Therefore, Liu et al. [79] propose a DRL-based system to achieve efficiently automated trading in the ecosystem, named FinRL, which can solve dynamic decision-making problems and build a multi-factor model. In addition, Liu et al. [80] attempt to reduce the simulation-to-reality gap and data processing burden through an open-source library that includes hundreds of market environments for financial reinforcement learning.

2.2.7 User-Generated Content (UGC)

UGC is any type of digital content generated by metaverse users, including pictures, music, videos, etc. The generated content contains personal privacy data and potential economic value [81]. UGC is a promising alternative tool to identify the demand of users. It is mainly based on ordinary user-generated content, starting from users' needs, and everyone can publish content on the platform. When the content is approved by the system or manually, it can be displayed on the platform to the audience. Similar to the concept of *We Media*, users can create a variety of personal digital content, including blogs, podcasts, news, and videos. In metaverse, UGC tends to be heterogeneous which triggers the surging demand for the ownership of UGC [25]. However, the quality of user-generated content varies since there is no requirement for the skills of creating. The existing methods are inefficient for a large number of UGCs because much digital content is highly informal and duplicated. Timoshenko et al. [82] apply a deep learning-based approach to filter out noninformative content to avoid sampling repetitive content.

Although some researchers have focused on related research questions for UGC in the metaverse, there are still some challenges, e.g., ownership control, payment scheme, and incentive mechanism.

2.2.8 Professional-Generated Content (PGC)

PGC means the content is generated by experts or professional institutions that have professional content production capabilities. This manner can ensure the professionalism of the content. Therefore, PGC is generally checked by the platform. It is generally original content and pays more attention to copyrights. PGC can ensure the value and competitiveness of the content. For example, PGC video service is a user-friendly advertisement environment [83] with the characteristics of specialization and commercialization. However, PGC services have some drawbacks, including geographical restrictions, and a lack of professional user participation. The threshold for professional content creation is relatively high. That is why there are corresponding charges in some knowledge payment platforms.

For paid content, piracy is rampant. This phenomenon incurs a loss to both the platform and the payer of content. The platform needs a set of strict audit standards to ensure the quality of the content and must be able to produce high-quality content continuously. For PGC, platform procurement costs are higher than that of UGC.

2.2.9 Artificial Intelligence-Generated Content (AIGC)

Following the breakthroughs of artificial intelligence (AI), natural language generation (NLG) technologies can be applied to the digital content generated by the metaverse, such as news reports, poetry, and photo-generated. Nils et al. [84] adopt the NLG algorithm GPT-2 to generate poem samples by identifying the character of human poems. AIGC is a typical manner to produce digital assets [85]. In the future, with the development of the metaverse, the number of digital content consumers will far exceed that of digital content producers.

The AIGC enables metaverse to create massively qualified and customized content. Generally, AIGC consists of content creation in two ways [85], i.e., (1) AI generates digital content independently, and (2) users with assistant AI create digital content. For example, Epic Games create a large number of virtual roles (e.g., virtual conversational assistants) by AI algorithms in *MetaHuman* [86]. Singer et al. [87] propose an approach named *Make-A-Video*, for directly translating the tremendous recent progress in text-to-image (T2I) generation to text-to-video (T2V). With Make-A-Video, the generated videos inherit the vastness (i.e., diversity in aesthetic, fantastical depictions, etc.) of today's image generation models. However, Make-A-Video currently can only generate 5 seconds of 16 frames of silent clip per second. The picture can only describe one action or scene, and the pixels are only 768 × 768. Meanwhile, Ho et al. [88] present a text-conditional video generation system named *Imagen Video*, which is based on a cascade of video diffusion models. Given a text prompt, Imagen Video generates high-definition videos using a base video generation model and a sequence of interleaved spatial and temporal video super-resolution models. Feng et al. [89] propose a large-scale Chinese text-to-image diffusion model, named *ERNIE-ViLG 2.0*, which progressively upgrades the quality of generated images by (1) incorporating fine-grained textual and visual knowledge of key elements in the scene and (2) utilizing different denoising experts at different stages. Dong et al. [90] propose a method, called *DreamArtist*, which employs a learning strategy of contrastive prompt-tuning. DreamArtist introduces both positive and negative embeddings as pseudo-words and trains them jointly. With DreamArtist, everyone can be an artist who has productive imagination, specialized experiences, and fantastic inspirations. Wu et al. [91] investigate the explicit and implicit perceptions of AI-generated poetry and painting held by subjects from two societies (the USA and China).

It can be found that the aforementioned works focus on AI-generated content with respect to photos, videos, text, etc. While existing AI products are still far from human creation in terms of visuals and storylines, Meta and Google's new products are really impressive and raise the question of how AI will lead content production. However, skeptics and proponents continue to argue whether AI-generated content will ultimately satisfy the benchmark of content produced by human writers [92].

2.3 Fusing Blockchain and AI with Metaverse

As depicted in Fig. 2.6, AI technologies are applied to the digital creation and digital market. Meanwhile, blockchain can guarantee digital assets, digital currencies, and the digital market. On the other hand, in this survey, we emphasize the fusion of AI and blockchain technologies to establish an intelligent, open, fair, and promising future of metaverse.

As aforementioned, we have discussed the details of AI and blockchain and their impacts on the metaverse. The integration of AI and blockchain, namely, *blockchain intelligence* and *intelligent blockchain*, shall be explored due to their close interactions. For example, the decentralized AI as an integration of AI and

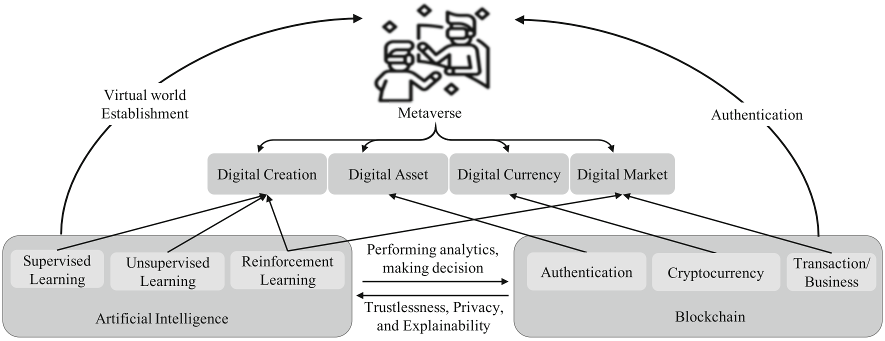


Fig. 2.6 Fusion of AI and blockchain in the metaverse

blockchain [93] enables to process and perform analytics or decision-making on trusted data without any support from trusted third parties. Hence, in this section, we shall discuss their integration and seek to answer the question: what contributions can intelligent systems make in metaverse [94].

2.3.1 Blockchain for AI

Blockchains can offer various components for AI, including datasets, algorithms, and computing power through trading from the decentralized marketplace. Blockchain encourages the innovation and adoption of AI to an unprecedented level in the context of metaverse. Several representative examples are reviewed as follows. Mamoshina et al. [95] propose a blockchain-based decentralized model that enables users to access their personal data in an AI-moderated healthcare data exchange. The proposed model allows users to upload their data directly to the system and grants access to their data using transparent pricing. Such transparent pricing is determined by a data value model, guaranteeing fair tracking of all data usage activities. Woods [96] analyzes the importance of fusing AI techniques and blockchain infrastructure, aiming to address the security risks faced by the Internet. The author finds that bots-bots and human-bots interactions have increased since 52% of the web traffic is generated by bots. Thus, bot-bot communications will exceed human-bot interactions according to the increasing bot traffic. In metaverse, each person will have multiple avatars. This fact inevitably leads to huge traffic due to massive interactions.

2.3.2 AI for Blockchain

To design a blockchain, developers have to tune a massive number of parameters and make trade-offs considering incentives, consensus, security, and many other aspects. AI technologies can be applied to deal with those problems and help blockchain systems achieve higher performance. In addition, with the breakthroughs of machine learning, a blockchain governed by a machine learning-based algorithm might enable the automatic detection of attacks and invoke appropriate defense mechanisms. For example, Salimitari et al. [97] propose a machine learning-based framework, which aims to offer a secure and robust consensus in blockchain-based IoT networks. The authors then present a two-stage consensus protocol for the AI-enabled blockchain that exploits an outlier detection algorithm in an IoT network.

2.4 How Digital Twin Enables Metaverse

Digital twin (DT) refers to the digital representation of the corresponding physical object. Based on data interaction technology, it can replicate the real-world product or process. As demonstrated in Fig. 2.7, DTs receive real-time data from physical objects, including states and sensory data, to facilitate high-fidelity DT modeling and updating. The dynamic interactions between physical objects and their DTs enable efficient simulations, analysis, predictions, and optimization in the virtual world, thereby feeding back to physical objects. Having been applied in intelligent manufacturing for more than a decade, it builds a bridge between the real world and the virtual world and thus can enrich the metaverse, if empowered by augmented reality (AR), virtual reality (VR), and the Internet of Things (IoT) techniques. As the metaverse steps from the conceptual to the practical stage, the digital twin can occupy a place in the promising future.

2.4.1 Taxonomy and Characteristics of Digital Twin

The innovation and application of DT have been going through rapid development, while its taxonomy somehow falls behind. By investigating the taxonomy and its corresponding characteristics, frontline researchers and practitioners may get a clear view of when, where, and how to adopt the DT technique in the metaverse.

Van et al. [98] propose a multidimensional taxonomy and examine the emerging DTs in the literature, from eight dimensions that shape a DT [99]. Among them, closely related to the metaverse are discussed below with the future prospects.

- **Data link**. The data exchange between the physical world and the digital twin can be one-directional or bidirectional. The former is to just extract the data from the prototype and create a digital counterpart, while the latter results in more intensive interaction. The bidirectional reliance between the DT and the multi-access edge computing (MEC) system in the metaverse is emphasized in [100]. Similarly, we can imagine expanding this bidirectional relationship to prototypes in the metaverse. This scheme will grant users the power to cause an impact on the real world from the metaverse.

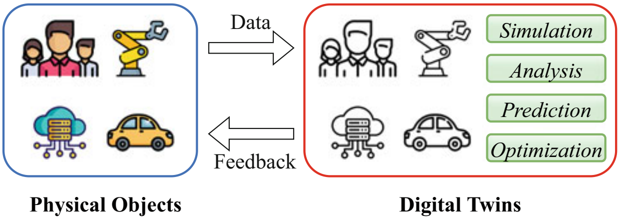


Fig. 2.7 Concept of digital twin technologies

- **Purpose**. Data processing is the major purpose for most DT, and the two others are data transferring and data repository. They are not mutually exclusive and can coexist in a specific system. In our context, they together comprise an interaction-intensive metaverse. Data processing and transferring are everywhere during the interaction and constitute the metaverse's core functions. Beyond the real world, data-related work such as simulations and forecasting can be done in the virtual world. Also, data collected in the physical world can be stored in the virtual world as a memento or backup. In this way, people can even experience it regardless of the dramatic change in the real world.
- **Conceptual elements**. It is the relation between digital units and their physical counterparts that can be directly bounded or independent. Reasonably, direct connections can make the DT in the metaverse have more fidelity, while a loose connection can allow one specific item to appear in many situations. This paradigm is incredible in reality and thus creates much more possibilities for the metaverse. Options of distinct experience are expected in the metaverse, and such an independence scheme depicts an imaginative picture of its future.
- **Model accuracy**. Either identical accuracy or partial accuracy regarding the detailed expression of a physical object—and this feature directly affects what the metaverse can provide. A more accurate representation provides a more sophisticated and comprehensive function set while requiring stronger computing power. As discussed above, for some functions like simulation or accurate prediction, it is essential to consider the model accuracy—and subsequent challenges of reliability as well.

Synchronization, interface, data input, and time of creation are other characteristics to categorize digital twin technologies. Such a comprehensive and explanatory taxonomy gives us a hint of the way to adopt DT technology and enrich the metaverse. Technologies such as IoT, edge computing, and 6G network lay the basis of DT's presence in the metaverse, and enriching the metaverse by the digital twin requires carefully made decisions and trade-offs in such a huge system. Hence, we need to figure out the advantages of digital twins afterward.

2.4.2 Advantages of Digital Twin

The DT technology brings plenty of benefits to the construction of metaverse [101], e.g., mitigating mistakes, uncertainty, inefficiencies, and costs within any procedure or system. This is the fundamental reason why the DT-enabled metaverse is regarded as the cornerstone of Industry 4.0 and improves the current business and industrial structures. The advantages of the DT technology include [102]:

- **Speed prototyping and product re-designing.** The design and analysis cycles for production are shortened, because of adopting simulations to investigate a variety of possibilities based on the DT technology [103, 104], thereby simplifying and fastening the whole prototyping or re-designing process. DTs may be utilized at a series of stages during the design process for production, from envisioning the idea of the product to testing the product. Because the DT is always in contact with its physical object, it is possible to compare performance over time with what was expected and what really occurred, allowing designers and engineers to reevaluate their original hypotheses.

- **Cost-effectiveness.** The total cost of prototyping goes down over time because a DT consumes virtual resources mostly in its construction [105]. Because physical materials and labor are required in traditional prototyping, product redesigning is time-consuming and pricey. Furthermore, when adopting DT technology, products can be rebuilt and undergo destructive tests without incurring any material costs.
- **Problem prediction.** With the DT technology and the real-time data flow from the physical objects, we can forecast the potential problems and mistakes that will arise in the physical object's life cycles and future states, giving us a chance to design the systems appropriately.
- **Optimizing solutions for maintenance.** Traditional methods of maintenance are usually reactive instead of proactive ones since they are based on either heuristic experience or worst situations [106]. However, DT has the ability to predict flaws and damage in the system or equipment used in production, allowing it to plan ahead for product maintenance. Through simulating various scenarios, DT optimizes the solution and maintenance approaches, and the maintenance procedure is significantly simplified. The continuous feedback loop between DT and its physical object can also be leveraged to continuously improve the performance of the system.
- **Accessibility.** With the help of their DTs, physical gadgets can be managed and controlled remotely. Meanwhile, virtual systems based on DTs can be widely disseminated and accessed remotely, in contrast to physical systems constrained by their actual locations [105].
- **Training.** Rather than conducting the conventional safety training programs in the physical world, DT can be utilized to create safety training programs, which are more effective and instructive [107]. DTs can be leveraged in the training of operators before they work on risky machinery or sites, with the aim of minimizing potential dangers. Exposing and training the operators on various procedures and scenarios will endow them with the confidence to handle similar conditions in real life.

2.4.3 Existing Applications and Expectations

Objects in the metaverse can vary from micro to macro scale, in different states, and there are tangible items as well as social relations [108]. In this section, we explore some applications, how they facilitate the construction of the metaverse, and what roles they may play in future practice.

Virtual city is a globally hot trend now. Collaborating with Unity, Orlando will find its digital twin of the metro region [109], in which visitors can take virtual tours and explore the city. Seoul launches a similar project [110] while even enabling users to receive government services and interact with others in that virtual world. And we can see Shanghai Digital Twin [111, 112], Singapore Digital Twin (called Virtual Singapore) [113], Dubai Digital Twin [114], etc. They are all in preparation for or as a procedure for creating a city-wide metaverse.

The cases aforementioned present an inspirational future of urban living in the metaverse—it is not necessarily an unfamiliar environment, but can be a replica of the cities we currently live in. Modern cities are principal places where people conduct production, business, and social and entertainment activities, which gives birth to those ambitious plans to cater to citizens; additionally, cities usually have most of the technical devices and resources; hence, it is reasonable to run the DT-supported metaverse of the early stage there.

From a micro-perspective, digital twin technologies can enable many sectors. For example, for supply chain management, the digital twin can enhance their connectivity, visibility, and resilience [115]. The traditional supply chain is complex and resource-consuming to get optimized, while the digital twin can be a tool to cost-effectively run the prediction and optimization. Furthermore, due to the broad accessibility, it can create 3D showrooms and products in the metaverse to empower retailing; can help users conveniently experience real-world products like cars or activities like skiing; can build a virtual workplace for remote-working staff to reduce the sense of distance; and can support a virtual concert so that fans can engage in it together in the metaverse.

2.4.4 Cutting-Edge Topics in Academia

At the same time, the digital twin also attracts the attention of academia to look deeply into it. In this part, we investigate the current research topics in general and present two state-of-the-art issues in academia for enabling the DT-based metaverse.

2.4.4.1 An Overview of Related Studies

The rapid advancement of the metaverse stimulates a flood of technical papers, while research fellows keep making headway on the DT. Therefore, some scholars turn their attention to applying DT in the metaverse. Li et al. [116] take the digital twin as one pillar technology of IoT, claim it is a fundamental technology that enhances user experience in the metaverse, and explore its applications in several scenarios such as healthcare, education, smart city, entertainment, real estate, and socialization.

The mainstream papers focus on specific technical problems amid the realization of the DT-supported metaverse and propose the mechanism design as a solution.

Lv et al. [117] propose a data storage solution called BlockNet, which utilizes the immutability of blockchain to strengthen the data reliability of digital twins, which makes up a step to a parallel metaverse. Aloqaily et al. [118] discuss DT-enabled metaverse and propose an integrated framework that brings digital twin and other advanced technologies (6G, blockchain, AI) together, to maintain continuous end-to-end metaverse services. To address the metaverse synchronization problem, Han et al. [101] develop a framework in which self-interested device owners dynamically select a VSP to maximize rewards and demonstrate that a hybrid protocol can lead to evolutionary stable states. Also, Han et al. study shareable digital twins in the metaverse, introduce the evolutionary game theory, and develop a dynamic hierarchical framework regarding the quality of shared DTs. Also, see [119] for the reliability and latency in digital twins-enabled metaverse, [120] for the synchronization and interoperability between digital twins and the metaverse at the edge, and [100] for the bidirectional reliance between the multi-access edge computing system and digital twins in the metaverse. Far et al. [121] present a review of the metaverse and highlight the security and privacy challenges of applying digital twin in the metaverse, with developing a three-layer architecture as a possible solution.

2.4.4.2 Digital Twin Edge Networks (DITENs) Toward 6G

The sixth-generation communications network (6G) is envisioned to support the burgeoning Internet of Everything (IoE) applications, including extended reality (XR), telemedicine, and autonomous systems [122], in order to give users an immersive experience in a digital world, i.e., metaverse. To achieve this, it is essential to incorporate a series of cutting-edge technologies into the 6G wireless network's design, such as artificial intelligence (AI) [123–127], Internet of Things (IoT) [128–133], and mobile edge computing (MEC) [134–138].

The cutting-edge network technologies toward 6G drive the development of digital twin (DT) technology [139]. Through taking advantage of advanced technologies for sensing, communication, and computing, the DT technology makes it possible to connect the physical world and metaverse to enable simulation, prediction, and analysis [101]. Especially, based on their intended purposes, DTs can be classified into three categories: monitoring DT, simulation DT, and operational DT [140]. The monitoring DT is deployed to keep track of the status of a physical system, and the simulation DT adopts simulation tools, along with machine learning (ML) technologies, to attempt to forecast the dynamics in the physical world. A cyber-physical system interacts with the system operators through the operational DT, which carries out a number of operations, like planning and optimization. The DT technique has been widely employed in a variety of applications, including the Internet of Things (IoT) and the upcoming 6G system toward metaverse.

The implementation of DTs is resource-intensive, which makes it difficult for end devices with limited resources to build and maintain DTs locally [141], while cloud computing and edge computing can help with dealing such a problem [142–146].

Under the context of traditional cloud computing, a cloud server gathers real-time data of physical objects and then builds the DTs for the physical objects with cloud computing-based DT modeling, which however causes significant communication overhead and long communication delay [147, 148]. Therefore, the concept of the digital twin edge network (DITEN) has emerged, where the DT technique is integrated with mobile edge computing (MEC) to serve a variety of applications [149]. Especially, the real-time data from physical objects is gathered by edge nodes in DITENs, e.g., base stations and access points. To maintain the synchronization between the physical objects and their DTs, the edge nodes constantly communicate with the physical objects. Thus, the effectiveness of networking schemes can be increased, while the costs of communication and computing decrease when optimizing the network schemes of the metaverse within the created DITEN.

Nowadays, DITENs have been investigated in a number of scenarios, including the IoT, autonomous vehicles, healthcare, and so on [150]. In particular, a DITEN enhances the system performance of metaverse in terms of service delay and reliability, empowered by DT modeling with high-fidelity, and the DITENs offer optimized decision-making functions to promote intelligent operations, such as accurate prediction, task offloading, and resource allocation.

2.4.4.3 Digital Twin as a Service

With the development of Industry 4.0, DT techniques enable to fill the gap between design and implementation within the metaverse [151]. It exists a trend for individualization in metaverse, and the paradigm of Digital Twin as a Service (DTaaS) emerges following the concept of service-oriented architecture (SOA) [152]. The function of the DTaaS is to serve as a DT-enabled service provider while providing capacities. The consumers of DT-enabled services are the users with service needs based on DTs.

Due to the precise and instant responses from DTs, the benefit of DTaaS is that it offers a straightforward and scalable paradigm in metaverse, catering to the significance of mass individualization [153]. Especially, DTaaS refers to a business model adopted by managed service providers that endow clients with the ability to create DTs, and the collected profits are maximized through operationalizing the virtual models. A DTaaS-based service provider might take the lead with a platform where clients are able to create digital twins of their products, services, and so on. A DTaaS-based service provider may also work with a valued consultant to construct a complete digital twin for customers after fully comprehending their company requirements. Digital twins can be created and maintained for clients by a top-notch team consisting of business consultants, engineers, and data architects.

2.5 Challenges and Open Issues

Through the previous review, we found that blockchain, AI, and digital twin technologies are fundamental technologies for the metaverse. Although those technologies are promising to build a scalable, reliable, and efficient metaverse, we are aware that the metaverse is still in its infant stage. Thus, this section discusses the related challenges and open issues.

2.5.1 Open Issues on Digital Economy in Metaverse

Different from the physical world, digital creation in the virtual world might be unlimited. The identity of digital objects determines value instead of undifferentiated labor in the conventional economy. In the field of digital creation, it is necessary to develop authoring tools to enable users to produce original content easily and gain rewards efficiently at a low cost. Those tools could improve the enthusiasm of content producers of the metaverse. The marginal benefits will increase in the metaverse instead of diminishing marginal benefits of production in the physical world. The difference in marginal benefits between the physical world and the virtual world demands a value conversion mechanism to bridge their gap.

In the future metaverse, people prefer to turn to their virtual cabinet to select a digital outfit, while companies begin to hype the virtual skins, virtual clothing, and even virtual estates with a high price which will block a large portion of players to join in the metaverse. Hence, it is necessary to propose particular governance mechanisms under the cooperation of worldwide companies. Furthermore, how to establish a digital currency system that enables the currency exchange between the metaverse and the physical world remains an open issue.

In addition, the transaction volume and frequency that occurred in the metaverse will become extremely much higher than what happened in the physical world. Thus, how to support such high-volume and high-frequency transactions remains a challenging problem in the future metaverse. Another issue related to the future metaverse might be the inflation caused by massive cryptocurrency supplements in a decentralized economy system built upon blockchain and AI technologies.

2.5.2 Artificial Intelligence Issues

The breakthroughs of artificial intelligence technologies, especially deep learning, enable academia and industries to make great progress in the automatic operation and design in the metaverse and perform better than conventional approaches. For example, the study [7] applies AI to generate vivid digital characters quickly that might be deployed by virtual service providers as conversational virtual assistants to populate the metaverse. However, existing deep learning models are usually very deep and have a massive amount of parameters, which incurs a high burden for resource-constrained mobile devices to deploy learning-based applications. However, current AI technologies are just at the stage where people tell the machine to do specific tasks instead of enabling the machine to learn automatically. Most learning tasks are only suitable for the closed static environment and have poor robustness and poor interpretability that cannot satisfy the requirement of availability, robustness, interpretability, and adaptability in an open and dynamic environment.

Meta-learning [154] is a promising learning paradigm that can observe how different machine learning approaches perform on a wide range of learning tasks. Learning from this experience, meta-data can learn new tasks much faster than others possible. Not only does meta-learning dramatically speed up and improve the design of machine learning pipelines or neural architectures, it also allows us to replace hand-engineered algorithms with novel approaches learned in a data-driven way. Therefore, meta-learning remains challenging to achieve auto-machine learning in future years.

2.5.3 Blockchain-Related Issues

Although blockchain technologies have achieved a lot of improvements, there are still challenges and open issues while fusing blockchain in metaverse. We post several questions in the following to inspire readers to deeply dive into the related technical studies.

- Can the existing real-world NFT platforms adapt to the high transaction volumes in the metaverse? NFTs are unique cryptographic tokens that are deployed on blockchains. Assigning non-reproducible features, NFTs digitalize real-world items like artworks and real estate. However, the current NFT platforms are in their initial stage. To meet the high-volume requirement of future metaverse applications, improving the service level of NFT platforms is an essential research and engineering topic.
- What rules does metaverse require for a healthy digital blockchain-empowered market and business? From the perspective of policy, the combination of decentralization and regulation might be a promising way for the digital blockchain-empowered market. DAO [155] is regarded as an efficient, decentralized, and promising paradigm that works with like-minded folks around the globe. The members of DAO have built-in treasuries that no one has the authority to access without the approval of the group. DAOs are executed through smart contracts, which are transparent codes verifiable by anyone. Thus, by exploiting DAOs, decisions can be governed by proposals and voting, to ensure everyone in the metaverse has a countable voice.

- Is the real-world blockchain-empowered application model able to be directly transplanted to metaverse? Nowadays, the overwhelming speculations over thousands of cryptocurrencies and the scams of *initial coin offering* (ICO) have brought notorious doubts to metaverse. Moreover, the existing blockchain-empowered application models cannot meet the stringent requirements of metaverse with its low latency and high-throughput performance. Hence, a high-performance and secure blockchain-empowered application model is needed for the various applications used in the future metaverse.
- Does metaverse need new blockchain platforms and new consensus mechanisms? The foundation of the blockchain is a consensus mechanism, such as PoW and PoS. However, the existing consensus mechanisms have shortcomings with regard to large amounts of hash computing and various security issues. The future decentralized applications demand a blockchain platform to fulfill the following desired characteristics, i.e., low latency, high throughput, fast transaction-sequential performance, offline payment of transactions, low transaction fees, modern free Internet business model, etc. Thus, new blockchain platforms and new consensus mechanisms are expected to appear in the future metaverse.

2.5.4 Governance for Metaverse

Currently, the concept of the metaverse is mainly used and propagated by companies such as Roblox and Meta (Facebook previously). Predictably, the most popular ecosystems soon are built and operated by these giant corporations. Tiny metaverse has only a few application scenarios. In contrast, the macro metaverse would include all scenarios required by users. To realize such a vision, large companies need to cooperate to create a huge unified metaverse. The problem is how to incentivize those giant companies to cooperate. Once the unified metaverse is set up, how do we make uniform rules that govern the whole unified metaverse?

On the other hand, the threats of market manipulation and money laundering will exist in the future metaverse. Thus, market governance will be viewed as more significant from the perspective of the jurisdiction in metaverse.

2.5.5 Blockchain-Empowered Applications for Metaverse

Various applications will boost the virtual economy in the metaverse, such as blockchain-empowered Apps for office work, social networks, NFT markets, game finance, etc. For instance, the blockchain-based game Axie Infinity [156] establishes a digital pet universe in which players can battle, raise, and trade fantasy creatures called Axies. The game allows players to deposit from an Ethereum wallet to a Ronin wallet via the Ronin Bridge. In short, the game allows the currency exchange between fiat and cryptocurrency since the players can buy ETH on a cryptocurrency exchange like Binance or Coinbase or with fiat on Ronin and send it to their address due to the legality of cryptocurrency in some countries. Although this blockchain-empowered game finance does not work in some countries, we believe that the future metaverse will embrace a much more open, fair, and rational physical world.

2.5.6 Security and Privacy for Metaverse

From the perspective of metaverse companies, developers, and metaverse users alike, a natural question is how to guarantee their security and privacy in metaverse which could mean violation of their privacy, potential identity theft, and other types of fraud [157].

For example, plenty of private properties in the metaverse, including digital assets, the identity of virtual objects, cryptocurrency payment records, and other private user data, are required to be protected. Thus, metaverse-oriented cryptography mechanisms are open proposals for privacy preservation in the metaverse.

2.6 Conclusion

Artificial intelligence, blockchain, and digital twin technologies are expected to play essential roles in the ever-expanding metaverse. For example, metaverse uses artificial intelligence and blockchain to create a digital virtual world where anyone can safely and freely engage in social and economic activities that are beyond the real world. Exploiting metaverse, the application of these latest AI and blockchain technologies will be accelerated as well.

By investigating the most related studies across metaverse components, digital currencies, AI technologies, the dApps used in the virtual world, and digital twin-empowered technologies, we wish to offer a thoughtful overview of how to enrich metaverse to experts from both academia and industries. We also envisioned critical challenges and open issues in constructing the fundamental elements of metaverse with the fusion of AI, blockchain, and digital twin. Further exploitation and interdisciplinary research on the metaverse entail collaboration from both academia and industries to strive for an open, fair, and rational future metaverse.

References

1. A. Aristidou, A. Shamir, and Y. Chrysanthou, “Digital dance ethnography: Organizing large dance collections,” *J. Comput. Cult. Herit.*, vol. 12, no. 4, Nov 2019. [Online]. Available: https://doi.org/10.1145/3344383
2. J. Joshua, “Information bodies: Computational anxiety in Neal Stephenson’s snow crash,” *Interdisciplinary Literary Studies*, vol. 19, no. 1, pp. 17–47, 2017.
3. J. Fennimore, “Roblox:5 fast facts you need to know,” https://heavy.com/games/2017/07/&\roblox-youtube-free-download-corporation-baszucki-cassel-nerfmodder/, Retrieved December 16, 2021.
4. Meta, “Introducing meta: A social technology company,” https://about.fb.com/news/2021/10/facebook-company-is-now-meta/, Retrieved December 16, 2021.
5. E. Games, “Fortnite,” *Epic Games*, 2017.
6. P. Ambrasaitė and A. Smagurauskaitė, “Epic games v. apple: Fortnite battle that can change the industry,” *Vilnius University Open Series*, pp. 6–25, 2021.
7. E. Games, “The world’s most open and advanced real-time 3D creation tool,” https://www.unrealengine.com/en-US/, Retrieved December 16, 2021.
8. M. Seymour, C. Evans, and K. Libreri, “Meet mike: epic avatars,” in *ACM SIGGRAPH 2017 VR Village*, 2017, pp. 1–2.
9. E. Kain, “Epic games pulls Travis Scott emote from ‘fortnite’ item shop,” https://www.forbes.com/sites/erikkain/2021/11/09/epic-games-pulls-travis-scott-emote-from-fortnite-item-shop/?sh=7f5cbabe4708, Retrieved December 16, 2021.
10. J. Tech, “Beamlink,” Retrieved May 16, 2022. [Online]. Available: https://www.jingtengtech.com/home/mr-meeting.html
11. A. Aristidou, A. Shamir, and Y. Chrysanthou, “Digital dance ethnography: Organizing large dance collections,” *Journal on Computing and Cultural Heritage (JOCCH)*, vol. 12, no. 4, pp. 1–27, 2019.
12. S. Ferguson, E. Schubert, and C. J. Stevens, “Dynamic dance warping: Using dynamic time warping to compare dance movement performed under different conditions,” in *Proceedings of the 2014 international workshop on movement and computing*, 2014, pp. 94–99.
13. L. Lik-Hang, T. Braud, P. Zhou, L. Wang, D. Xu, Z. Lin, A. Kumar, C. Bermejo, and P. Hui, “All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda.”
14. J. D. N. Dionisio, W. G. B. III, and R. Gilbert, “3D virtual worlds and the metaverse: Current status and future possibilities,” *ACM Computing Surveys (CSUR)*, vol. 45, no. 3, pp. 1–38, 2013.
15. W. LaDuke, “Traditional ecological knowledge and environmental futures,” *Colo. J. Int’l Envtl. L. & Pol’y*, vol. 5, p. 127, 1994.
16. M. Nadini, L. Alessandretti, F. Di Giacinto, M. Martino, L. M. Aiello, and A. Baronchelli, “Mapping the NFT revolution: market trends, trade networks and visual features,” *arXiv preprint arXiv:2106.00647*, 2021.
17. N. Lambert, “Beyond NFTs: A possible future for digital art,” *ITNOW*, vol. 63, no. 3, pp. 8–10, 2021.
18. W. Y. B. Lim, Z. Xiong, D. Niyato, X. Cao, C. Miao, S. Sun, and Q. Yang, “Realizing the metaverse with edge intelligence: A match made in heaven,” *arXiv preprint arXiv:2201.01634*, 2022.
19. M. Xu, D. Niyato, J. Kang, Z. Xiong, C. Miao, and D. I. Kim, “Wireless edge-empowered metaverse: A learning-based incentive mechanism for virtual reality,” *arXiv preprint arXiv:2111.03776*, 2021.
20. W. C. Ng, W. Y. B. Lim, J. S. Ng, Z. Xiong, D. Niyato, and C. Miao, “Unified resource allocation framework for the edge intelligence-enabled metaverse,” *arXiv preprint arXiv:2110.14325*, 2021.

21. H. Du, D. Niyato, J. Kang, D. I. Kim, and C. Miao, “Optimal targeted advertising strategy for secure wireless edge metaverse,” *CoRR*, vol. abs/2111.00511, 2021. [Online]. Available: https://arxiv.org/abs/2111.00511
22. Y. Jiang, J. Kang, D. Niyato, X. Ge, Z. Xiong, and C. Miao, “Reliable coded distributed computing for metaverse services: Coalition formation and incentive mechanism design,” *CoRR*, vol. abs/2111.10548, 2021. [Online]. Available: https://arxiv.org/abs/2111.10548
23. Y. Han, D. Niyato, C. Leung, C. Miao, and D. I. Kim, “A dynamic resource allocation framework for synchronizing metaverse with IoT service and data,” *arXiv preprint arXiv:2111.00431*, 2021.
24. J. Y. Lee, “A study on metaverse hype for sustainable growth,” *International journal of advanced smart convergence*, vol. 10, no. 3, pp. 72–80, 2021.
25. H. Duan, J. Li, S. Fan, Z. Lin, X. Wu, and W. Cai, “Metaverse for social good: A university campus prototype,” in *Proceedings of the 29th ACM International Conference on Multimedia*, 2021, pp. 153–161.
26. smita.verma, “A Comprehensive Guide To Building A Metaverse DApp Using Unity,” 2022. [Online]. Available: https://www.blockchain-council.org/metaverse/a-comprehensive-guide-to-building-a-metaverse-dapp-using-unity/
27. Q. Zhou, H. Huang, Z. Zheng, and J. Bian, “Solutions to scalability of blockchain: A survey,” *Ieee Access*, vol. 8, pp. 16 440–16 455, 2020.
28. wtflea, “Facebook Metaverse: Will it Support Blockchain?” 2021. [Online]. Available: http://www.itedge.cn/2021/11/22/facebook-metaverse-will-it-support-blockchain/
29. Solana, “Powerful for developers. Fast for everyone.” 2022. [Online]. Available: http://solana.io/
30. Avalanche, “Welcome to Multiverse,” 2022. [Online]. Available: http://avax.network
31. Linera, “Build on infrastructure with unprecedented scalability, url=https://linera.io/, year=2022.”
32. Sui, “Build without boundaries,” 2022. [Online]. Available: https://sui.io/
33. Aptos, “Committed to developing products and applications on the Aptos blockchain that redefine the web3 user experience.” 2022. [Online]. Available: https://aptoslabs.com/
34. H. Huang, X. Peng, J. Zhan, S. Zhang, Y. Lin, Z. Zheng, and S. Guo, “Brokerchain: A cross-shard blockchain protocol for account/balance-based state sharding,” in *Proc. of IEEE Conference on Computer Communications (INFOCOM)*, 2022.
35. S. Dick, “Artificial intelligence,” 2019.
36. S. R. Jammalamadaka, “Introduction to linear regression analysis,” 2003.
37. T. M. Oshiro, P. S. Perez, and J. A. Baranauskas, “How many trees in a random forest?” in *International workshop on machine learning and data mining in pattern recognition*. Springer, 2012, pp. 154–168.
38. C. C. Paige and M. A. Saunders, “Towards a generalized singular value decomposition,” *SIAM Journal on Numerical Analysis*, vol. 18, no. 3, pp. 398–405, 1981.
39. V. Vapnik, *The nature of statistical learning theory*. Springer Science & Business Media, 1999.
40. N. Ketkar, “Convolutional neural networks,” in *Deep Learning with Python*. Springer, 2017, pp. 63–78.
41. L. P. Kaelbling, M. L. Littman, and A. W. Moore, “Reinforcement learning: A survey,” *Journal of artificial intelligence research*, vol. 4, pp. 237–285, 1996.
42. J. Van Der Wal, “Stochastic dynamic programming,” Ph.D. dissertation, Methematisch Centrum Amsterdam, The Netherlands, 1980.
43. K. Arulkumaran, M. P. Deisenroth, M. Brundage, and A. A. Bharath, “Deep reinforcement learning: A brief survey,” *IEEE Signal Processing Magazine*, vol. 34, no. 6, pp. 26–38, 2017.
44. M. G. Kapteyn, J. V. Pretorius, and K. E. Willcox, “A probabilistic graphical model foundation for enabling predictive digital twins at scale,” *Nature Computational Science*, vol. 1, no. 5, pp. 337–347, 2021.
45. O. San, “The digital twin revolution,” *Nature Computational Science*, vol. 1, no. 5, pp. 307–308, 2021.

46. Q. Qi and F. Tao, "Digital twin and big data towards smart manufacturing and industry 4.0: 360 degree comparison," *IEEE Access*, vol. 6, pp. 3585–3593, 2018.
47. K. Malik and M. Farhan, "Merging virtual world with data sciences," *Int Rob Auto J*, vol. 2, no. 1, p. 00012, 2017.
48. Y. Ham and J. Kim, "Participatory sensing and digital twin city: updating virtual city models for enhanced risk-informed decision-making," *Journal of Management in Engineering*, vol. 36, no. 3, p. 04020005, 2020.
49. F. Xue, W. Lu, Z. Chen, and C. J. Webster, "From LiDAR point cloud towards digital twin city: Clustering city objects based on gestalt principles," *ISPRS Journal of Photogrammetry and Remote Sensing*, vol. 167, pp. 418–431, 2020.
50. K.-T. Lai, C.-C. Lin, C.-Y. Kang, M.-E. Liao, and M.-S. Chen, "Vivid: Virtual environment for visual deep learning," in *Proceedings of the 26th ACM international conference on Multimedia*, 2018, pp. 1356–1359.
51. D. Chen, L. J. Xie, B. Kim, L. Wang, C. S. Hong, L.-C. Wang, and Z. Han, "Federated learning based mobile edge computing for augmented reality applications," in *2020 International Conference on Computing, Networking and Communications (ICNC)*, 2020, pp. 767–773.
52. M. Mohammadi and A. Al-Fuqaha, "Enabling cognitive smart cities using big data and machine learning: Approaches and challenges," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 94–101, 2018.
53. R. V. Yampolskiy, B. Klare, and A. K. Jain, "Face recognition in the virtual world: Recognizing avatar faces," in *2012 11th International Conference on Machine Learning and Applications*, vol. 1, 2012, pp. 40–45.
54. M. Fabbri, F. Lanzi, S. Calderara, A. Palazzi, R. Vezzani, and R. Cucchiara, "Learning to detect and track visible and occluded body joints in a virtual world," in *Proceedings of the European conference on computer vision (ECCV)*, 2018, pp. 430–446.
55. H. Wang, Y. Gao, and X. Chen, "RL-DOT: A reinforcement learning NPC team for playing domination games," *IEEE Transactions on Computational intelligence and AI in Games*, vol. 2, no. 1, pp. 17–26, 2009.
56. C. Berner, G. Brockman, B. Chan, V. Cheung, P. Dębiak, C. Dennison, D. Farhi, Q. Fischer, S. Hashme, C. Hesse *et al.*, "Dota 2 with large scale deep reinforcement learning," *arXiv preprint arXiv:1912.06680*, 2019.
57. J.-F. Chen, W.-C. Lin, H.-S. Bai, C.-C. Yang, and H.-C. Chao, "Constructing an intelligent behavior avatar in a virtual world: a self-learning model based on reinforcement," in *IRI -2005 IEEE International Conference on Information Reuse and Integration, Conf, 2005.*, 2005, pp. 421–426.
58. J. Lee and K. H. Lee, "Precomputing avatar behavior from human motion data," *Graphical models*, vol. 68, no. 2, pp. 158–174, 2006.
59. I. Kastanis and M. Slater, "Reinforcement learning utilizes proxemics: An avatar learns to manipulate the position of people in immersive virtual reality," *ACM Transactions on Applied Perception (TAP)*, vol. 9, no. 1, pp. 1–15, 2012.
60. R. Rahmatizadeh, P. Abolghasemi, A. Behal, and L. Bölöni, "From virtual demonstration to real-world manipulation using LSTM and MDN," in *Thirty-Second AAAI Conference on Artificial Intelligence*, 2018.
61. R. Rouhollah, A. Pooya, B. Aman, and B. Ladislau, "Learning real manipulation tasks from virtual demonstrations using LSTM," *arXiv preprint arXiv:1603.03833*, 2016.
62. T. Wang, J. Li, Y. Deng, C. Wang, H. Snoussi, and F. Tao, "Digital twin for human-machine interaction with convolutional neural network," *International Journal of Computer Integrated Manufacturing*, pp. 1–10, 2021.
63. J. Pang, Y. Huang, Z. Xie, J. Li, and Z. Cai, "Collaborative city digital twin for the covid-19 pandemic: A federated learning solution," *Tsinghua Science and Technology*, vol. 26, no. 5, pp. 759–771, 2021.
64. S. Lee, G. Ha, H. Kim, and S. Kim, "A collaborative serious game for fire disaster evacuation drill in metaverse," *Journal of Platform Technology*, vol. 9, no. 3, pp. 70–77, 2021.
65. F. Tao and Q. Qi, "Make more digital twins," 2019.

66. T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, “Federated learning: Challenges, methods, and future directions,” *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 50–60, 2020.
67. N. Rieke, J. Hancox, W. Li, F. Milletari, H. R. Roth, S. Albarqouni, S. Bakas, M. N. Galtier, B. A. Landman, K. Maier-Hein *et al.*, “The future of digital health with federated learning,” *NPJ digital medicine*, vol. 3, no. 1, pp. 1–7, 2020.
68. Q. Yang, Y. Liu, Y. Cheng, Y. Kang, T. Chen, and H. Yu, “Federated learning,” *Synthesis Lectures on Artificial Intelligence and Machine Learning*, vol. 13, no. 3, pp. 1–207, 2019.
69. E. Castronova, “The price of bodies: A hedonic pricing model of avatar attributes in a synthetic world,” *Kyklos*, vol. 57, no. 2, pp. 173–196, 2004.
70. R. Schroeder, *The social life of avatars: Presence and interaction in shared virtual environments*. Springer Science & Business Media, 2012.
71. K. Merrick and M. L. Maher, “Motivated reinforcement learning for non-player characters in persistent computer game worlds,” in *Proceedings of the 2006 ACM SIGCHI international conference on Advances in computer entertainment technology*, 2006, pp. 3–es.
72. S. Razzaq, F. Maqbool, M. Khalid, I. Tariq, A. Zahoor, and M. Ilyas, “Zombies arena: fusion of reinforcement learning with augmented reality on NPC,” *Cluster Computing*, vol. 21, no. 1, pp. 655–666, 2018.
73. D. Guide, “Welcome to dota, you suck,” https://purgegamers.true.io/g/dota-2-guide/, Retrieved December 16, 2021.
74. Decentraland. (Retrieved December 16, 2021) Introduction. https://docs.decentraland.org/decentraland/introduction/.
75. Y. Ando, R. Thawonmas, and F. Rinaldo, “Level of interest in observed exhibits in metaverse museums,” *Proceedings of the innovations in information and communication science and technology IICST*, pp. 62–66, 2012.
76. J.-L. Lugrin and M. Cavazza, “Ai-based world behaviour for emergent narratives,” in *Proceedings of the 2006 ACM SIGCHI international conference on Advances in computer entertainment technology*, 2006, pp. 25–es.
77. M. Kreminski, B. Samuel, E. Melcer, and N. Wardrip-Fruin, “Evaluating AI-based games through retellings,” in *Proceedings of the AAAI Conference on Artificial Intelligence and Interactive Digital Entertainment*, vol. 15, no. 1, 2019, pp. 45–51.
78. A. Puder, S. Markwitz, F. Gudermann, and K. Geihs, “AI-based trading in open distributed environments,” in *Open Distributed Processing*. Springer, 1995, pp. 157–169.
79. X.-Y. Liu, H. Yang, J. Gao, and C. D. Wang, “FinRL: Deep reinforcement learning framework to automate trading in quantitative finance,” *arXiv preprint arXiv:2111.09395*, 2021.
80. X.-Y. Liu, J. Rui, J. Gao, L. Yang, H. Yang, Z. Wang, C. D. Wang, and J. Guo, “FinRL-meta: A universe of near-real market environments for data-driven deep reinforcement learning in quantitative finance,” *arXiv preprint arXiv:2112.06753*, 2021.
81. L.-H. Lee, Z. Lin, R. Hu, Z. Gong, A. Kumar, T. Li, S. Li, and P. Hui, “When creators meet the metaverse: A survey on computational arts,” *arXiv preprint arXiv:2111.13486*, 2021.
82. A. Timoshenko and J. R. Hauser, “Identifying customer needs from user-generated content,” *Marketing Science*, vol. 38, no. 1, pp. 1–20, 2019.
83. J. Kim, “The institutionalization of YouTube: From user-generated content to professionally generated content,” *Media, culture & society*, vol. 34, no. 1, pp. 53–67, 2012.
84. N. Köbis and L. D. Mossink, “Artificial intelligence versus Maya Angelou: Experimental evidence that people cannot differentiate AI-generated from human-written poetry,” *Computers in human behavior*, vol. 114, p. 106553, 2021.
85. Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, and X. Shen, “A survey on metaverse: Fundamentals, security, and privacy,” *IEEE Communications Surveys & Tutorials*, 2022.
86. K. Lyytinen, J. V. Nickerson, and J. L. King, “Metahuman systems= humans+ machines that learn,” *Journal of Information Technology*, vol. 36, no. 4, pp. 427–445, 2021.
87. U. Singer, A. Polyak, T. Hayes, X. Yin, J. An, S. Zhang, Q. Hu, H. Yang, O. Ashual, O. Gafni *et al.*, “Make-a-video: Text-to-video generation without text-video data,” *arXiv preprint arXiv:2209.14792*, 2022.

88. J. Ho, W. Chan, C. Saharia, J. Whang, R. Gao, A. A. Gritsenko, D. P. Kingma, B. Poole, M. Norouzi, D. J. Fleet, and T. Salimans, "Imagen video: High definition video generation with diffusion models," *ArXiv*, vol. abs/2210.02303, 2022.
89. Z. Feng, Z. Zhang, X. Yu, Y. Fang, L. Li, X. Chen, Y. Lu, J. Liu, W. Yin, S. Feng, Y. Sun, H. Tian, H. Wu, and H. Wang, "ERNIE-viLG 2.0: Improving text-to-image diffusion model with knowledge-enhanced mixture-of-denoising-experts," *ArXiv*, vol. abs/2210.15257, 2022.
90. Z. Dong, P. Wei, and L. Lin, "Dreamartist: Towards controllable one-shot text-to-image generation via contrastive prompt-tuning," *ArXiv*, vol. abs/2211.11337, 2022.
91. Y. Wu, Y. Mou, Z. Li, and K. Xu, "Investigating American and Chinese subjects' explicit and implicit perceptions of ai-generated artistic work," *Computers in Human Behavior*, vol. 104, p. 106186, 2020.
92. N. L. Latar, "The robot journalist in the age of social physics: The end of human journalism?" in *The new world of transitioned media*. Springer, 2015, pp. 65–80.
93. N. Ai, "Decentralized ai blockchain whitepaper," *Nebula AI Team, Montreal*, 2018.
94. T. N. Dinh and M. T. Thai, "AI and Blockchain: A disruptive integration," *Computer*, vol. 51, no. 9, pp. 48–53, 2018.
95. P. Mamoshina, L. Ojomoko, Y. Yanovich, A. Ostrovski, A. Botezatu, P. Prikhodko, E. Izumchenko, A. Aliper, K. Romantsov, A. Zhebrak *et al.*, "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," *Oncotarget*, vol. 9, no. 5, p. 5665, 2018.
96. J. Woods, "Blockchain: Rebalancing & amplifying the power of AI and machine learning (ML)," URL https://medium.com/cryptooracle/blockchain-rebalancing-amplifying-the-power-of-ai-andmachine-learning-ml-af95616e9ad9, *vol. online*, 2018.
97. M. Salimitari, M. Joneidi, and M. Chatterjee, "AI-enabled blockchain: An outlier-aware consensus protocol for blockchain-based IoT networks," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1–6.
98. H. Van der Valk, H. Haße, F. Möller, M. Arbter, J.-L. Henning, and B. Otto, "A taxonomy of digital twins." in *AMCIS*, 2020.
99. J. Stjepandić, M. Sommer, and S. Stobrawa, "Digital twin: conclusion and future perspectives," *DigiTwin: An Approach for Production Process Optimization in a Built Environment*, pp. 235–259, 2022.
100. J. Yu, A. Alhilal, P. Hui, and D. H. Tsang, "Bi-directional digital twin and edge computing in the metaverse," *arXiv preprint arXiv:2211.08700*, 2022.
101. Y. Han, D. Niyato, C. Leung, D. I. Kim, K. Zhu, S. Feng, S. X. Shen, and C. Miao, "A dynamic hierarchical framework for IoT-assisted digital twin synchronization in the metaverse," *IEEE Internet of Things Journal*, 2022.
102. M. Singh, E. Fuenmayor, E. P. Hinchy, Y. Qiao, N. Murray, and D. Devine, "Digital twin: Origin to future," *Applied System Innovation*, vol. 4, no. 2, p. 36, 2021.
103. J. Li, S. Guo, W. Liang, Q. Chen, Z. Xu, and W. Xu, "SFC-enabled reliable service provisioning in mobile edge computing via digital twins," in *2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*. IEEE, 2022, pp. 311–317.
104. J. Li, S. Guo, W. Liang, Q. Chen, Z. Xu, W. Xu, and A. Y. Zomaya, "Digital twin-assisted, SFC-enabled service provisioning in mobile edge computing," *IEEE Transactions on Mobile Computing*, 2022.
105. M. Grieves and J. Vickers, "Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems," *Transdisciplinary perspectives on complex systems: New findings and approaches*, pp. 85–113, 2017.
106. E. Glaessgen and D. Stargel, "The digital twin paradigm for future NASA and US air force vehicles," in *53rd AIAA/ASME/ASCE/AHS/ASC structures, structural dynamics and materials conference 20th AIAA/ASME/AHS adaptive structures conference 14th AIAA*, 2012, p. 1818.
107. T. Kaarlela, S. Pieskä, and T. Pitkäaho, "Digital twin and virtual reality for safety training," in *2020 11th IEEE international conference on cognitive infocommunications (CogInfoCom)*. IEEE, 2020, pp. 000 115–000 120.

108. Z. Lv, S. Xie, Y. Li, M. S. Hossain, and A. El Saddik, “Building the metaverse by digital twins at all scales, state, relation,” *Virtual Reality & Intelligent Hardware*, vol. 4, no. 6, pp. 459–470, 2022.
109. news.orlando.org, “Orlando to unveil world’s first digital twin of an entire region,” 2022. [Online]. Available: https://news.orlando.org/blog/orlando-to-unveil-worlds-first-digital-twin-of-an-entire-region/
110. smartcity.go.kr, “Seoul city builds the nation’s first urban problem solving simulation’digital twin s-map,” 2021. [Online]. Available: https://smartcity.go.kr/en/
111. theb1m.com, “Shanghai digital twin,” 2020. [Online]. Available: https://www.theb1m.com/video/how-china-cloned-shanghai
112. chinanews.com, “Shanghai digital twin,” 2022. [Online]. Available: https://www.chinanews.com.cn/cj/2022/09-05/9844546.shtml
113. nrf.gov.sg, “Virtual Singapore,” 2022. [Online]. Available: https://www.nrf.gov.sg/programmes/virtual-singapore
114. thenationalnews.com, “Dubai digital twin,” 2022. [Online]. Available: https://www.thenationalnews.com/uae/2022/03/30/dubais-digital-twin-to-broaden-horizons-in-brave-new-virtual-world/
115. L. Wang, T. Deng, Z.-J. M. Shen, H. Hu, and Y. Qi, “Digital twin-driven smart supply chain,” *Frontiers of Engineering Management*, vol. 9, no. 1, pp. 56–70, 2022.
116. K. Li, Y. Cui, W. Li, T. Lv, X. Yuan, S. Li, W. Ni, M. Simsek, and F. Dressler, “When internet of things meets metaverse: Convergence of physical and cyber worlds,” *arXiv preprint arXiv:2208.13501*, 2022.
117. Z. Lv, L. Qiao, Y. Li, Y. Yuan, and F.-Y. Wang, “Blocknet: Beyond reliable spatial digital twins to parallel metaverse,” *Patterns*, vol. 3, no. 5, p. 100468, 2022.
118. M. Aloqaily, O. Bouachir, F. Karray, I. Al Ridhawi, and A. El Saddik, “Integrating digital twin and advanced intelligent technologies to realize the metaverse,” *IEEE Consumer Electronics Magazine*, 2022.
119. D. Van Huynh, S. R. Khosravirad, A. Masaracchia, O. A. Dobre, and T. Q. Duong, “Edge intelligence-based ultra-reliable and low-latency communications for digital twin-enabled metaverse,” *IEEE Wireless Communications Letters*, 2022.
120. O. Hashash, C. Chaccour, W. Saad, K. Sakaguchi, and T. Yu, “Towards a decentralized metaverse: Synchronized orchestration of digital twins and sub-metaverses,” *arXiv preprint arXiv:2211.14686*, 2022.
121. S. B. Far and A. I. Rad, “Applying digital twins in metaverse: User interface, security and privacy challenges,” *Journal of Metaverse*, vol. 2, no. 1, pp. 8–16, 2022.
122. H. Zhang, N. Shlezinger, F. Guidi, D. Dardari, M. F. Imani, and Y. C. Eldar, “Near-field wireless power transfer for 6G internet of everything mobile networks: Opportunities and challenges,” *IEEE Communications Magazine*, vol. 60, no. 3, pp. 12–18, 2022.
123. K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y.-J. A. Zhang, “The roadmap to 6G: AI empowered wireless networks,” *IEEE communications magazine*, vol. 57, no. 8, pp. 84–90, 2019.
124. Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, “AI and 6G security: Opportunities and challenges,” in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. IEEE, 2021, pp. 616–621.
125. W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, “The road towards 6G: A comprehensive survey,” *IEEE Open Journal of the Communications Society*, vol. 2, pp. 334–366, 2021.
126. H. Yang, A. Alphones, Z. Xiong, D. Niyato, J. Zhao, and K. Wu, “Artificial-intelligence-enabled intelligent 6G networks,” *IEEE Network*, vol. 34, no. 6, pp. 272–280, 2020.
127. K. David, J. Elmirghani, H. Haas, and X.-H. You, “Defining 6G: Challenges and opportunities [from the guest editors],” *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, pp. 14–16, 2019.
128. J. Li, W. Liang, W. Xu, Z. Xu, X. Jia, W. Zhou, and J. Zhao, “Maximizing user service satisfaction for delay-sensitive IoT applications in edge computing,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 5, pp. 1199–1212, 2021.

129. J. Li, W. Liang, W. Xu, Z. Xu, Y. Li, and X. Jia, "Service home identification of multiple-source IoT applications in edge computing," *IEEE Transactions on Services Computing*, 2022.
130. J. Li, W. Liang, Z. Xu, X. Jia, and W. Zhou, "Service provisioning for multi-source IoT applications in mobile edge computing," *ACM Transactions on Sensor Networks (TOSN)*, vol. 18, no. 2, pp. 1–25, 2021.
131. M. Chen, W. Liang, and J. Li, "Energy-efficient data collection maximization for UAV-assisted wireless sensor networks," in *2021 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2021, pp. 1–7.
132. J. Li, W. Liang, W. Xu, Z. Xu, and J. Zhao, "Maximizing the quality of user experience of using services in edge computing for delay-sensitive IoT applications," in *Proceedings of the 23rd International ACM Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, 2020, pp. 113–121.
133. J. Li, W. Liang, Z. Xu, and W. Zhou, "Service provisioning for IoT applications with multiple sources in mobile edge computing," in *2020 IEEE 45th Conference on Local Computer Networks (LCN)*. IEEE, 2020, pp. 42–53.
134. Y. Li, W. Liang, J. Li, X. Cheng, D. Yu, A. Y. Zomaya, and S. Guo, "Energy-constrained D2D assisted federated learning in edge computing," in *Proceedings of the 25th International ACM Conference on Modeling Analysis and Simulation of Wireless and Mobile Systems*, 2022, pp. 33–37.
135. J. Li, W. Liang, W. Xu, Z. Xu, X. Jia, A. Y. Zomaya, and S. Guo, "Budget-aware user satisfaction maximization on service provisioning in mobile edge computing," *IEEE Transactions on Mobile Computing*, 2022.
136. Y. Li, W. Liang, and J. Li, "Profit driven service provisioning in edge computing via deep reinforcement learning," *IEEE Transactions on Network and Service Management*, 2022.
137. ——, "Profit maximization for service placement and request assignment in edge computing via deep reinforcement learning," in *Proceedings of the 24th International ACM Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, 2021, pp. 51–55.
138. J. Li, W. Liang, M. Huang, and X. Jia, "Providing reliability-aware virtualized network function services for mobile edge computing," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2019, pp. 732–741.
139. L. U. Khan, W. Saad, D. Niyato, Z. Han, and C. S. Hong, "Digital-twin-enabled 6G: Vision, architectural trends, and future directions," *IEEE Communications Magazine*, vol. 60, no. 1, pp. 74–80, 2022.
140. S. Boschert and R. Rosen, "Digital twin–the simulation aspect," *Mechatronic futures: Challenges and solutions for mechatronic systems and their designers*, pp. 59–74, 2016.
141. J. Li, J. Wang, C. Quan, Y. Li, and A. Y. Zomaya, "Digital twin-enabled service satisfaction enhancement in edge computing," in *IEEE INFOCOM 2023-IEEE Conference on Computer Communications*, 2023.
142. J. Li, W. Liang, M. Chen, and Z. Xu, "Mobility-aware dynamic service placement in D2D-assisted MEC environments," in *2021 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2021, pp. 1–6.
143. J. Li, W. Liang, and Y. Ma, "Robust service provisioning with service function chain requirements in mobile edge computing," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 2138–2153, 2021.
144. J. Li, W. Liang, M. Huang, and X. Jia, "Reliability-aware network service provisioning in mobile edge-cloud networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 31, no. 7, pp. 1545–1558, 2020.
145. Y. Ma, W. Liang, J. Li, X. Jia, and S. Guo, "Mobility-aware and delay-sensitive service provisioning in mobile edge-cloud networks," *IEEE Transactions on Mobile Computing*, vol. 21, no. 1, pp. 196–210, 2020.
146. S. Lin, W. Liang, and J. Li, "Reliability-aware service function chain provisioning in mobile edge-cloud networks," in *2020 29th International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 2020, pp. 1–9.

147. J. Li, W. Liang, Y. Li, Z. Xu, and X. Jia, “Delay-aware DNN inference throughput maximization in edge computing via jointly exploring partitioning and parallelism,” in *2021 IEEE 46th Conference on Local Computer Networks (LCN)*. IEEE, 2021, pp. 193–200.
148. J. Li, W. Liang, Y. Li, Z. Xu, X. Jia, and S. Guo, “Throughput maximization of delay-aware DNN inference in edge computing by exploring DNN model partitioning and inference parallelism,” *IEEE Transactions on Mobile Computing*, 2021.
149. F. Tang, X. Chen, T. K. Rodrigues, M. Zhao, and N. Kato, “Survey on digital twin edge networks (DITEN) toward 6G,” *IEEE Open Journal of the Communications Society*, vol. 3, pp. 1360–1381, 2022.
150. T. Liu, L. Tang, W. Wang, Q. Chen, and X. Zeng, “Digital-twin-assisted task offloading based on edge collaboration in the digital twin edge network,” *IEEE Internet of Things Journal*, vol. 9, no. 2, pp. 1427–1444, 2021.
151. F. Pires, A. Cachada, J. Barbosa, A. P. Moreira, and P. Leitão, “Digital twin in industry 4.0: Technologies, applications and challenges,” in *2019 IEEE 17th International Conference on Industrial Informatics (INDIN)*, vol. 1. IEEE, 2019, pp. 721–726.
152. S. Aheleroff, X. Xu, R. Y. Zhong, and Y. Lu, “Digital twin as a service (DTaaS) in industry 4.0: an architecture reference model,” *Advanced Engineering Informatics*, vol. 47, p. 101225, 2021.
153. G. Shao and M. Helu, “Framework for a digital twin in manufacturing: Scope and requirements,” *Manufacturing Letters*, vol. 24, pp. 105–107, 2020.
154. J. Vanschoren, “Meta-learning: A survey,” *arXiv preprint arXiv:1810.03548*, 2018.
155. L. Liu, S. Zhou, H. Huang, and Z. Zheng, “From technology to society: An overview of blockchain-based DAO,” *IEEE Open Journal of the Computer Society (OJ-CS)*, vol. 2, pp. 204–215, 2021.
156. A. infinity, “Play to earn,” https://axieinfinity.com/, Retrieved December 16, 2021.
157. A. ROY, “Metaverse data protection and privacy: The next big-tech dilemma?” https://www.xrtoday.com/virtual-reality/metaverse-data-protection-and-privacy-the-next-big-tech-dilemma/, Retrieved December 16, 2021.

Chapter 3
How to Address Storage Issues for Metaverse? Blockchains and Distributed File Systems

Huawei Huang, Jianru Lin, and Zibin Zheng

Abstract Constructing globally distributed file systems (DFS) has received great attention. Traditional peer-to-peer (P2P) distributed file systems have inevitable drawbacks such as instability and lacking auditing and incentive mechanisms. Thus, Inter-Planetary File Systems (IPFS) and Swarm, as the representative DFSs which integrate with blockchain technologies, are proposed and becoming a new generation of distributed file systems. Although the blockchain-based DFS successfully provides adequate incentives and security guarantees by exploiting the advantages of blockchain, a series of challenges, such as scalability and privacy issues, are also constraining the development of the new generation of DFSs. Mainly focusing on IPFS and Swarm, this chapter conducts an overview of the principle, layered structure, and cutting-edge studies of blockchain-based DSFs. Furthermore, we also identify their challenges, open issues, and future directions. We anticipate that this survey can shed new light on the subsequent studies related to blockchain-based distributed file systems.

Keywords Blockchain · Distributed file systems · Peer-to-peer · Swarm · Consensus algorithms · Scalability · Storage optimization

3.1 Introduction

There have been many attempts dedicated to constructing a distributed file system. The phenomenal popularity and study of peer-to-peer (P2P) services, such as Napster [1], Gnutella [2], Kazaa [3], and Morpheus [4], make implementing distributed file systems an exciting and promising research field. As one of the most successful P2P distributed file systems, BitTorrent [5] has supported over 100 million online users. It has a large-scale deployment where tens of millions of nodes

H. Huang · J. Lin · Z. Zheng (✉)
School of Software Engineering, Sun Yat-sen University, Zhuhai, Guangdong, China
e-mail: huanghw28@mail.sysu.edu.cn; zhzibin@mail.sysu.edu.cn

H. Huang et al. (eds.), *From Blockchain to Web3 & Metaverse*,
https://doi.org/10.1007/978-981-99-3648-9_3

join and churn every day. In a distributed file system, storage resources and system clients are dispersed in the network. Each user is both a creator and a consumer of data stored in the system. Thus, the challenge is to provide considerable incentives in an efficient, secure, and practical manner.

By far, the biggest distributed file system is HyperText Transfer Protocol (HTTP), which is a web server used to upload data. Then, other peers can access particular data anywhere all over the world. To ensure data accessibility in web servers, a maintenance cost needs to pay. Such maintaining cost increases along with the growth of data popularity. Moreover, another problem is that there are very few ways to share the burden of information dissemination with the clients directly. This is because HTTP lacks an upgrading design and thus fails to take advantage of the advanced file distribution techniques proposed in the past few years. Meanwhile, the P2P technique had been gathering at a great pace and soon dominated the majority of data packets on the Internet.

Such P2P file systems, like BitTorrent [5], optimize resources brilliantly by giving different pieces of popular data to clients and enabling them to swap the missing parts with each other. In this way, the bandwidth consumption of hosts can be balanced, and the overall cost of operational expenditure (OPEX) can be also degraded.

Although BitTorrent has a lot of advantages aforementioned, the following inevitable drawbacks cannot be ignored:

1. Downloading is unstable, which limits BitTorrent to be widely used on specific occasions.
2. Unable to verify file publishers, and it is hard to guarantee the credibility of the content downloaded.
3. There is no incentive mechanism such that the *seed* nodes are not rewarded for sharing their bandwidth and storage resources.

Anticipating to replace HTTP, Zeronet [6] adopted BitTorrent as the file distribution mechanism for Web content. However, simply sharing bandwidth, storage, and computing resources cannot provide the brilliant experience as HTTP users expect.

Recently, blockchain has become a buzzword in both industry and academia, and the combination of blockchain and distributed file systems is becoming a promising solution, where blockchain is expected to provide incentives and security for the stored files in systems. Currently, the popular blockchain-based distributed file systems include IPFS [7], Swarm [8], Storj [9], and PPIO [10]. Within those file systems, IPFS is a peer-to-peer distributed file system for storing and accessing files, websites, applications, and data; Swarm is a distributed storage platform and content distribution service based on Ethereum; Storj is another peer-to-peer decentralized cloud storage platform that allows users to share data without relying on a third-party data provider; and PPIO is a decentralized programmable storage network that permits users to store and retrieve any data from anywhere on the web. With respect to the combination with blockchains, IPFS, Swarm, and Storj file systems adopt Filecoin [11], Ethereum [12], and Metadisk [13] as their incentive mechanisms, respectively. PPIO exploits up to four proof algorithms, which are explained in Sect. 3.3, for its incentive layer.

Considering that the technologies of all distributed file systems are similar to IPFS and Swarm, we review the recent cutting-edge studies of blockchain-based DFSs mainly focusing on IPFS and Swarm.

The contribution of this chapter includes the following aspects:

- This chapter first introduces the layered structure of blockchain-based DFSs. We then make a comprehensive taxonomy of the cutting-edge studies on the *scalability* and *privacy* perspectives.
- We also clarified the challenges, open issues, and future directions of the blockchain-based DFSs.
- Our review in this chapter can help subsequent researchers well understand both the current development and the future trends of the blockchain-based DFS.

The rest of this chapter is organized as follows. In Sect. 3.2, we explain necessary preliminaries and basic concepts. Section 3.3 shows the layered structure of distributed file systems. Section 3.4 summarizes the cutting-edge studies. Section 3.5 discusses open issues, challenges, and future directions. Finally, Sect. 3.6 concludes this chapter.

3.2 Preliminaries

Since the blockchain-based distributed file systems emphasized in this chapter have a close correlation with the basic data structure of blockchains, we first introduce the preliminaries of Merkle tree and Merkle DAG. Then, we have an overview of BitTorrent, which can help us understand the rationale of distributed file systems such as IPFS and Swarm.

3.2.1 Merkle Tree and Merkle DAG

Merkle tree [14] is a binary tree built based on a cryptographic hash function. Each leaf in a Merkle tree has a hash value which is computed by one or multiple imported values. Each parent node derives its hash value from the children's value which is recursively dependent on all values in its sub-tree. Figure 3.1 illustrates an example of a Merkle tree, each leaf (H1–H4) obtains its value though computing imported value (D1–D4), and parents (H5–H6) derive values from their children (H1–H4), and finally the root of this Merkle tree (H7) is obtained which is relevant with every value in the tree.

In the blockchain area, the Merkle tree is usually used for integrity validations (e.g., the block validation in Bitcoin [15]) and quick validations (e.g., the light peers in Ethereum [12]). Since a tiny change in a Merkle tree can drastically change the root of the tree, we can do integrity validation by simply storing the root. To validate if a node is in a Merkle tree, only a few hashes of nodes are needed, instead of the

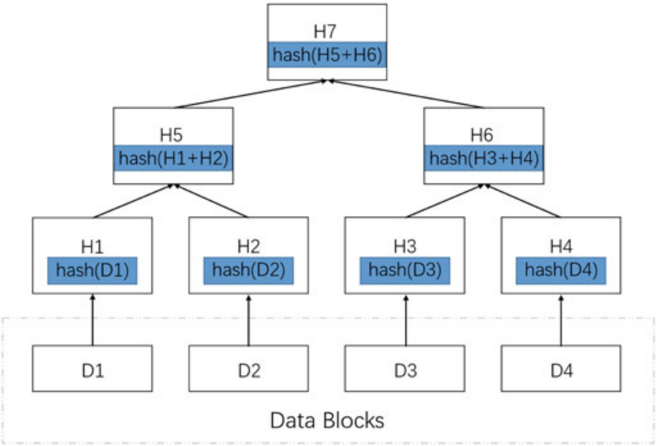


Fig. 3.1 An illustration of a Merkle tree

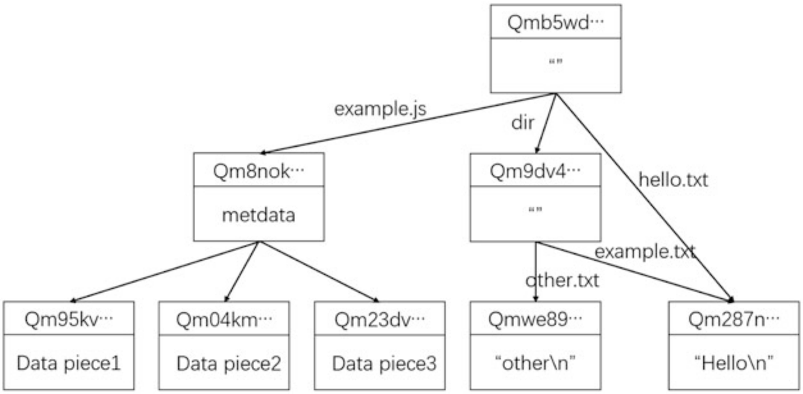


Fig. 3.2 Merkle DAG in IPFS

entire tree. For example in Fig. 3.1, H4 and H5 are needed to validate if H3 is in the tree. Using H3, H4, and H5, a root (H8) can be computed. By comparing H7 and H8, we can confirm that H3 is in the tree if the two roots are the same or H3 is not in the tree if the two roots are different.

Similar to the concept of Merkle tree, Merkle DAG (directed acyclic graph) [7] is used in IPFS as a data object model. An object in IPFS is a structure containing two attributes: *data* and *links*. Each link structure includes three attributes: name, hash and size. Using this object structure, IPFS can compose objects and build a directed acyclic graph. In IPFS, Merkle DAG organizes the structure of a file or even a file directory which is shown in Fig. 3.2. In Fig. 3.2, there are two files (example.js and hello.txt) and one file path (dir) in the root path of this file directory, example.js is divided into three different data pieces, and file path dir has two files: other.txt and

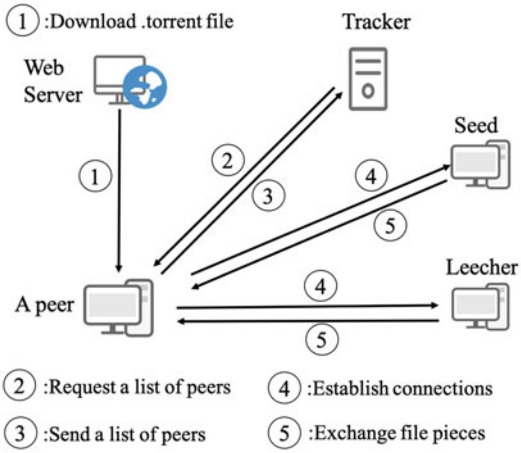


Fig. 3.3 Mechanism of file-sharing in BitTorrent, which can help us well understand the blockchain-based distributed file system IPFS

example.txt (here file contents of example.txt in dir and hello.txt in root path are exactly the same; therefore they are linked in one object); each object derives its value through computing its children's value or the content of data.

3.2.2 Overview of BitTorrent

As mentioned earlier, BitTorrent (BT) is one of the most popular distributed file systems. Basically, the process of file sharing in BitTorrent is illustrated in Fig. 3.3 and can be described with the following five steps:

- Peer A interacts with a Web server and downloads a *.torrent* file.
- Peer A interacts with the tracker which peer A finds in the **.torrent* file and requests a list of peers that are in the Torrent network.
- Tracker sends a list of a specified number of peers that are in the Torrent network.
- Peer A selects randomly a part of candidate peers from the list as its neighbors and establishes connections with each of them.
- Then peers A can exchange file pieces with its neighbors using the swarming technique.

In BitTorrent, an overlay network called Torrent is established when each file is being distributed. Torrent is composed of peers in a network which can be classified into two types: seed and leecher. A seed is a client which has a complete copy of a file, while a leecher is a client which is downloading a file. Besides seed and leecher, Web servers and trackers are also required. If a peer wants to join a Torrent network, it can obtain a *.torrent* file from a web server. This file contains information about a file including its name, length, hash digest, and the URL of the tracker. A tracker is a special peer storing the meta information of peers who are active in a Torrent network. A peer can interact with a tracker and obtain the list of IP/Port pairs of other peers in a Torrent and then select randomly about 20–40 peers from the list as its neighbors. In BitTorrent, a file exchanging technique called swarming is adopted to separate a file into fixed-size pieces each of which is usually 256 KB in size [5]. When a piece is fully downloaded, a peer compares its SHA1 hash value with the value in the *.torrent* file. If matches, the peer announces the availability of this complete piece to its neighbors for further file exchanging and downloading.

3.3 The Layered Structure of Blockchain-Based Distributed File Systems

In this section, we present the typical layered structure of blockchain-based distributed file systems by particularly emphasizing on IPFS and Swarm. The structure is shown in Table 3.1 in detail. Generally, we classify seven layers behind the popular distributed file systems, i.e., the identities layer, data layer, data-swap layer, network layer, routing layer, consensus layer, and incentive layer. Each layer is a critical module for distributed file systems. We summarize their functions and related references in Table 3.1.

Table 3.1 Layered structure of distributed file systems such as IPFS and Swarm

Layer	Function	Examples and references
Identity layer	Identity layer assigns unique id for each node	Keccak hash [16]
Data layer	Data layer organizes file structure in distributed file system	Merkle DAG [7]
Data-swap layer	Data-swap layer formulates file sharing strategy between each node	BitSwap [5]
Network layer	Network layer enables nodes to discover other nodes, establish connections, and exchange files with each other in a secure environment	libP2P [17], Devp2p [18]
Routing layer	Routing layer enables each file piece to be located and accessible by nodes in the network	Distributed sloppy hash table (DSHT) [19], distributed preimage archive (DPA) [20]
Consensus layer	Consensus layer ensures ledger recording transactions in each node are basically correct and encourages users to maintain the consistency of the network	"Expected Consensus" [21], proof-of-work [12]
Incentive layer	Incentive layer establishes reward and punishment mechanism of the distributed file system, encourages nodes in the network to be active and honest in the transaction	Filecoin [11], SWAP, SWEAR, and SWINDLE [8]

3.3.1 Identity Layer

To archive the content distribution between nodes in a P2P file system, each node has to be identified by a unique identifier, which needs to ensure collision-free. It means that two different data objects can never map to the same identifier. In IPFS, the encrypted hash (in *multi-hash* format) of a public key, i.e., *NodeId*, is used to identify each node. The format of multi-hash is ⟨hash function code⟩⟨hash digest length⟩⟨hash digest bytes⟩. Nodes periodically check public keys and *NodeId* when connecting with each other. In Swarm systems, the node hash address is generated by Keccak 256bit SHA3 [16] using the public key of an Ethereum account.

3.3.2 Routing Layer

Generally, the functionalities of the routing layer of a distributed file system include (1) maintaining peer-connection topology such that specific peers and data objects can be located, (2) responding to the queries from both local and remote peers, and (3) communicating with distributed hash tables.

IPFS adopts distributed sloppy hash table (DSHT) [19], which is implemented based on S/Kademlia [22] and Coral [23]. Such the DSHT located in a peer can help find (1) the network addresses of other peers and (2) the group of peers who can serve specific data objects. The conventional distributed hash table (DHT) stores small values. For larger values, DSHT stores references, i.e., the *NodeIds* of peers who can serve a block. It should be noticed that IPFS is highly modular, and DSHT is just a temporal protocol that can be displaced in the future.

Swarm implements its routing layer using distributed preimage archive (DPA) technique [20]. In such DPA, a source object is divided into equal-sized chunks which are then synced to different nodes. When receiving these content-addressed chunks, other nodes could sync them to their neighbors that are in the same address space.

3.3.3 Network Layer

Under the framework of IPFS, an advanced generic P2P solution, named libP2P [17], is exploited as the network layer. libP2P is developed based on BitTorrent DHT implementation. Based on libP2P, IPFS can use any network protocol to transfer data. If the underlying network is not stable, IPFS can alter to choose UTP [24] or SCTP [25]. IPFS achieves this free shifting mainly by using *multiaddr* formatted technique [7], which combines addresses and corresponding protocols.

Swarm relies on the Ethereum P2P network, which is comprised of three different protocols: (1) RLPx (recursive length prefix) [26] for node discovery and secure data transmission, (2) DevP2P [18] for node session establishment and message exchange, and (3) Ethereum subprotocol [27]. DevP2P [18] is inspired by libP2P and has security properties that are beneficial to Swarm. When discovering through RLPx, Swarm nodes establish TCP connections and send “HELLO” messages including *NodeId*, listening port, and other attributes based on DevP2P. Sessions start to transmit data packets. Due to the ecosystem of Ethereum, Swarm has a large number of long-term nodes, which support the robustness and stability of Swarm systems.

3.3.4 Data Layer

There are four levels of the data model in IPFS:

- Block: an arbitrary-sized piece of data.
- List: a collection of blocks or other lists.
- Tree: a collection of blocks, lists, or other trees.
- Commit: a snapshot in the version history of a tree.

Such a data model is similar to that of Git [28]. Based on this data model, IPFS systems employ Merkle DAG to store data. Merkle DAG identifies data and links in each data object with *multi-hash* technique [7], which protects stored data from tampering and makes file path to be retrieved easily because the data object is converted into the string-formatted path (with a format like/ipfs/object-hash/object-name). To divide a file into independent blocks, IPFS exploits many algorithms such as rsync rolling-checksum algorithm [29] and Rabin Fingerprints [30].

Swarm also defines a set of data structures:

- Chunk: a fixed-size (maximum 4 KB [7]) piece of data.
- File: a complete set of chunks.
- Manifest: a mapping between paths and files, which handles file collection.

Chunker, which is a Swarm’s component for splitting and recovering files, is able to process live stream data. After being split, chunks are collected to calculate the Swarm hashes, in which a hash algorithm is used to obtain the root hash of the Merkle tree. The root hash is then used to identify a specific file and avoid tampering. During this procedure, the hash of each chunk is also calculated and is treated as a reference to this chunk.

3.3.5 Incentive Layer

3.3.5.1 Incentive Layer of IPFS

As shown in Fig. 3.4, Filecoin [11] is a blockchain-based digital payment system, which supports digital storage and data retrieval for IPFS users. It is adopted as

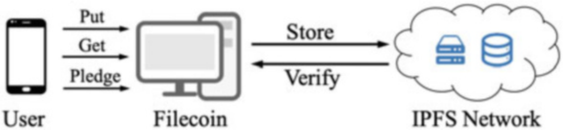


Fig. 3.4 Mechanism and position of Filecoin [11], which is adopted by IPFS and exploits blockchain as its fundamental component

an incentive layer for IPFS. There are two markets in Filecoin's ecosystem, i.e., a storage market and a retrieval market. The data of the storage market is stored on the Filecoin blockchain, and the data of the retrieval market is recorded off-chain.

These two markets provide data storage and data retrieval services via a network composed of *storage clients*, *storage miners*, *retrieval clients*, and *retrieval miners*. Those participants are explained as follows:

- *Storage Clients* are those who need file storage services. They are on the demand side of the storage market.
- *Storage Miners* are the nodes that provide storage to a Filecoin system using its free disk space. They are on the supply side of the storage market. The transactions that occurred on the storage market contribute new blocks to the Filecoin blockchain.
- *Retrieval Clients* are those who desire to retrieve a specific resource from the network. They are the demand side of the retrieval market.
- *Retrieval Miners* are those who provide network resources, such as bandwidth, helping retrieval clients search for the retrieval information. They are on the supply side of the retrieval market.

To store data in Filecoin, a storage client first submits a bid order to storage market. If a storage miner intends to take a bid order, it has to send a request order to storage market. When storage market is receiving a bid order and a request order, storage clients and storage miners start to exchange blocks and submit a signed deal order to storage market. After that, the storage miner must prove the data stored in its dedicated uniquely physical storage by repeatedly generating proofs of replication, which is then verified by IPFS.

To retrieve data from Filecoin, similarly, a retrieval client first submits a bid order to retrieval market. When retrieval market is receiving a request order from a retrieval client, the retrieval miners begin to transport data and submit a signed deal order to retrieval market to confirm whether a retrieve deal is succeeded or not.

3.3.5.2 Incentive Layer of Swarm

In Swarm, the incentive scheme consists of two important parts: (1) bandwidth incentives and (2) storage incentives. This is because bandwidth and storage are the two most important resources in a distributed file system.

Bandwidth Incentives In the context of Swarm, the service of delivering chunks is chargeable, and nodes can trade services for services or services for tokens. In order to motivate nodes to provide stable services in a credible context, Swarm proposes the Swarm Accounting Protocol (SWAP) [8]. Firstly, nodes negotiate chunk prices when communicating in the handshake protocol. Different prices mean varying bandwidth costs. After the chunk price is set, a checkbook contract is used to secure the payment. A checkbook contract is a kind of smart contract and has an ether (Ethereum token) balance. Another secure payment called *channel contract* is later proposed by Swarm and can be seen in [8]. Both modes of payment support secure off-chain transactions and delayed updates. All of the transactions are stored in the state of the Ethereum blockchain which cannot be tampered with. Finally, nodes establish network connections and exchange data.

Storage Incentives Swarm encourages nodes to preserve the data that has been uploaded to the network. Normally, long-term data preservation is not realistic. Unpopular chunks do not bring enough profits and may be cleaned up to make room for new chunks. In order to guarantee the long-term availability of data, the owner of each chunk needs to compensate for the storage of nodes. To manage storage deals, Swarm adapts a set of incentive schemes, *SWAP*, *SWEAR*, and *SWINDLE*, which are described as follows:

- **SWAP [8]:** Nodes establish connections with their registered peers which are the target nodes they want to compensate to and sign contracts with. Then they can swap information including syncing, receipting, price negotiation, and payments.
- **SWEAR [8]:** Registered peers are responsible for their promises of long-term storage, and they must register via the SWEAR (Secure Ways of Ensuring Archival or Swarm Enforcement And Registration) [8] contract on Ethereum by uploading their deposit. Peers are stood to be punished and lose deposit in an on-chain litigation process if they violate the rules.
- **SWINDLE [8]:** Nodes provide signed receipts for stored chunks. When dispute about whether the rules are violated has occurred, nodes that lost the chunk can submit a *challenge* to the SWINDLE (Secured With Insurance Deposit Litigation and Escrow) [8] contract by uploading the receipt of the lost chunk. Nodes can also propose the refutation of a *challenge* by uploading the chunk or proof of custody. Swindle contract decides which one is guilty by checking the hash of the chunk.

When chunks are being forwarded, a chain of contracts is created based on the incentive schemes aforementioned, which elegantly solve the disputes between nodes.

3.3.6 Data-Swap Layer

IPFS adopts BitSwap [5] as its data-swap layer. BitSwap is based on BitTorrent protocol. In detail, BitSwap nodes provide the blocks they are holding to each other directly, aiming to spread the blocks within their group. The debt of a node raises when it receives target blocks and decreases when it contributes blocks that the other nodes desire. Thus, BitSwap encourages nodes to cache and contribute blocks positively.

To prevent the nodes that never share, each BitSwap node checks the debt of the other peers before they exchange blocks. BitSwap nodes also keep ledgers that record the transferring history and exchange ledgers with each other when establishing connections. This exchange policy protects BitSwap ledger from tampering and isolates the malicious nodes that lose the ledger intentionally.

In Swarm, nodes store chunks for selling to get profits when they receive a data-retrieve request. If nodes do not have the target chunk claimed in the retrieve request, they pass the retrieve request to the nearest neighbor node. During managing storage transactions, *receipts* play an important role. When Swarm nodes interact with any contracts, receipts are generated and stored in Swarm. In this way, the source of a chunk is accessible, and a commitment in case of litigations can be traced.

3.3.7 Consensus Layer

A consensus mechanism is critical for every blockchain system. In a large distributed network, multiple peers form a network cluster normally through asynchronous communications. The network could be congested, resulting in that error messages propagating all over the system. Thus, peers could be failed if they cannot communicate with others with a consensus network view [31]. Therefore, it is necessary to define a resilient consensus protocol that can work in unreliable asynchronous networks for distributed file systems. The aim of such consensus protocol is to ensure that each peer reaches a secure, reliable, and consistent state without a centralized synchronizer.

In the following, we review several typical consensus protocols proposed by recent representative studies.

3.3.7.1 "Expected Consensus" Algorithm of Filecoin

Different from Ethereum which only has one main chain, Filecoin [11] contains not only a single main chain but also a *storage market* as well. Users in Filecoin interact with the storage market. These interactions of users are stored in the main-chain ledger. Three proofs that play an important role in the consensus process of Filecoin are summarized as follows:

- **Transaction Proof:** After the miner and user have reached a deal, the main chain locks the token of the user and the deposit of the miner. The main chain also records the information about the transaction including the hard disk sector of a miner, details of the deposit, transaction fee and storage deadline, etc.

- **Proof-of-Replication (PoRep):** A file is divided into pieces, and each piece is accepted by a storage miner. At this time, a storage miner may pretend to store a piece (this type of behavior is called a generation attack [32]). Furthermore, a miner may obtain a piece from another peer instead of itself (this type of behavior is called an outsourcing attack [32]). Another case is that a miner may create multiple fake peers and pretend to store several replications of a file piece (this type of behavior is called a Sybil attack [32]). To prevent these network attacks, Filecoin requires each miner to submit proof of replication to the main chain. Such the proof-of-replication ensures that each miner stores file pieces truly and independently.
- **Proof-of-Spacetime (PoSt):** To prove that miners keep storing a file piece in the effective time of the transaction, each miner has to submit proof of spacetime to the main chain regularly. In the current design of Filecoin, the proof is committed by providing spacetime every 20,000 blocks (roughly consuming 6 days to mine on average) [21] to prove that the file piece is not missing. The storage market has to validate the proofs uploaded by miners and decides whether to punish miners every 100 blocks (50 minutes to mine on average) [21].

The consensus algorithm of Filecoin is called *expected consensus* [21], in which a ticket is computed in each round of the consensus process. By comparing the ticket value and the effective storage of each peer, a peer or several peers can be the leaders of this round. A leader can select transactions to pack in the new blocks generated. When a block is packed, it will be sent to other peers for synchronization. Transactions in a block are executed by Ethereum virtual machine (EVM) [33], and the state of each account will be updated.

3.3.7.2 Consensus of Ethereum

There are four stages of Ethereum: Frontier, Homestead, Metropolis, and Serenity. In the first three stages, proof-of-work (PoW) [34] is adopted as the consensus mechanism of Ethereum, while in the fourth stage, the proof-of-stake (PoS) [35] will be adopted.

In PoW, each miner packs transactions from the transaction pool and constructs a new block in sequential order. Then miners adjust the nonce value constantly which is imported to PoW function [34] with the block header. A target indicator is also computed according to the difficulty of the blockchain. By comparing the result of this function with the target indicator, the miner decides whether it wins in the consensus process. When a miner confirms that it has won, it starts to broadcast its new block to other peers. Upon receiving a block from other peers, a miner stops computing to validate the nonce value of the newly received block. Each transaction of the new block is executed by EVM. After the processing of all transactions included in this new block, the state of this peer will be updated [33]. Currently, the average time of consensus in Ethereum is around 15 seconds, which ensures the consistency of all peers [36].

3.3.7.3 Consensus Algorithms of Other File Systems

Storj's Proofs of Retrievability Designed as a decentralized cloud object storage, Storj [9] proposed *Proof of Storage* in its first-version white paper. Interestingly, we found that in version 2.0 of Storj's white paper [37], the consensus algorithm has been changed to *proofs of retrievability* [38]. Proofs of retrievability aims at ensuring a certain piece of file exists on a host. It offers a high availability of files under an ideal proof, in which messages are with minimum size and pre-processing is minimal. According to the new white paper [37], poof of retrievability is still under ongoing research and implementation. We then analyze the reason behind the change of Storj's consensus algorithms. It probably because of that the current reputation systems, including proof of storage, fail to solve the *cheating client attacks* [37]. In such cheating attacks, it is hard to independently verify whether a privately verifiable audit under a reputation system was issued or not as claimed. Thus, the proof of storage lacks publicly verifiable practices.

PPIO's 4 Proof Schemes PPIO [10] exploits difference proof algorithms, i.e., PoRep, PoSt, proof of download (PoD), and light proof of capacity (LPoC), in which *PoD* and *LPoC* are two brand new proof mechanisms created by PPIO. *PoD* particularly supports the media streaming-related service. *LPoC* is designed to cold start storage miners. However, because LPoC technically occupies hard disk resources with no real values, the PPIO team has decided to abandon the implementation of LPoC.

3.3.8 Summary of the Layered Structure

As the efficient decentralized storage layer of the next-generation Internet, both IPFS and Swarm use similar technologies. They provide low-latency data retrieval, fault-tolerant guarantees, and decentralized/distributed storage solutions.

In the identities layer, multi-hash technique [7] is used by IPFS which can store the hash function and hash digest. Swarm uses the account address of Ethereum directly. In the network layer, Swarm adapts to the secure and stable network of Ethereum. IPFS uses libP2P which is a more generic solution. The incentive layer of Swarm relies on smart contracts of Ethereum, which support automated auditing and delayed payment. This saves transaction costs of Swarm and remains secure. Filecoin relies on proofs and consensus of blockchain which is an overuse of blockchain. The PoW consensus of Swarm stands the test of time, while the *expected consensus* of IPFS remains waiting for the test of real world.

Swarm inherits directly the technology design of Ethereum. For example, the identities layer, network layer, and consensus layer of Swarm are the same as Ethereum, as Swarm benefits from Ethereum with its large ecosystem, secure and living network, and reliable funding sources. IPFS is highly modular and can replace the existing component with state-of-the-art technology. In conclusion, the technology of Swarm is more stable, while the technology of IPFS is more advanced.

3.4 Cutting-Edge Studies of Blockchain-Based Distributed File Systems

In this section, we discuss recent cutting-edge studies of blockchain-integrated distributed file systems, mainly emphasizing IPFS and Swarm.

3.4.1 Scalability

With the number of transactions increasing in blockchain networks, each peer has to validate and store a growing size of transactions periodically. This incurs a huge burden of both storage and performance to each peer. In addition, the limited size of each block and the latency of consensus-achieving must be taken into account, because these factors induce delayed transactions. Meanwhile, as the cluster size and data replications grow in the network, the performance of IPFS and Swarm degrades severely.

In this part, we review several studies paying attention to the scalability issues of distributed file systems, mainly focusing on IPFS and Swarm. These works can be classified into two categories: (1) scalability evaluation and (2) storage optimization. For convenient identification, we summarize these studies on Table 3.2.

3.4.1.1 Scalability Evaluation

Although the performance of IPFS is under doubt by academia, we only found a few research studies that evaluate or discuss the scalability of IPFS. The representative papers are reviewed as follows. Wennergren et al. [39] discuss and analyze the scalability performance of IPFS. They conducted simulations with varying cluster sizes and replication factors. The simulation results show that the average download time of data stored in IPFS increases as cluster size and replication factor grows. In consequence, the response time among peers in an IPFS network grows, and the downloading speed reduces as well. The authors mentioned that the limited bandwidth of each instance of IPFS could be one of the critical reasons for the low scalability of IPFS.

Recently, Shen et al. [40] conducted systematic evaluations of the IPFS storage system by deploying real geographically distributed instances on Amazon EC2 cloud. The authors emphasize the data I/O operations from a client's perspective. The extensive measurement results show that the access patterns of clients can

Table 3.2 Scalability studies of distributed file systems

Category	Reference	File system	Methodology
Scalability evaluation	Wennergren et al. [39]	IPFS	Analyzed scalability performance via varying cluster sizes and replication factors
	Shen et al. [40]	IPFS	Evaluated storage system of IPFS on Amazon EC2 cloud, by emphasizing on the data I/O operations in a client's point of view
	BlockIPFS [41]	IPFS	Nyaletey et al. proposed a solution by integrating blockchain and IPFS, which can trace the access events of each file on IPFS. They evaluated the scalability of BlockIPFS by varying the number of system nodes
Storage optimization	Chen et al. [42]	IPFS	Proposed a new storage model based on zigzag code [43], for the block storage scheme adopted by IPFS
	Norvill et al. [44]	IPFS	Proposed an off-chain approach that moves contract-generation codes to IPFS database, aiming to improve the storage performance of distributed file system
	Design of Ethereum [45]	Swarm	Advocated that a chain of contracts in Swarm should be configured in off-chain storage
	White paper [9]	Storj	Storj encrypts data using sharding technique and enables data availability based on Reed-Solomon erasure coding [46]
	Lightning network [47], Plasma [48]	Off-chain file systems	Allows blockchain clients conducting transactions in the off-chain manner, aiming to offload the storage pressure of main chain

severely affect the I/O performance of IPFS. Further quantitative analysis indicates that downloading and resolving operations could be bottleneck factors while clients are reading objects from remote nodes.

To address the traceability problem of a distributed file system, Nyaletey et al. [41] proposed a solution combining the blockchain and IPFS which named BlockIPFS, which can trace and audit the access events of each file on IPFS. The authors conducted a group of experiments to evaluate the scalability of the proposed BlockIPFS by varying the number of nodes. Then, they measured the latency consumed by uploading, downloading, and reading transactions of each file stored in the system. The measurement results show that the increasing number of nodes does not cause a drastic growth in transaction times. Unfortunately, the scale of their experiments is too small since the number of nodes in the BlockIPFS system is ranging from 3 to 27. Thus, this group of experiments makes the scalability of their system unknown under a very large-scale deployment.

3.4.1.2 Storage Optimization

Erasure Codes To guarantee high data availability, some distributed file systems, e.g., Sia [49] and Storj [9], adopt the erasure codes for their storage strategy. In a typical (N, K) erasure code [50], an original file is usually divided into a number K (>1) of blocks. Each block is then encoded to a larger number N $(\geq K)$ of coded blocks. Out of those N encoded blocks, any K of them can reconstruct the original file. Thus, exploiting erasure codes can improve the storage resilience of distributed file systems. For example, to improve the user experience of a P2P file system, Chen et al. [42] proposed a new storage model based on zigzag [43] and blockchain techniques. The new storage model aims at improving the block storage strategy adopted by IPFS.

Storing Data Off-Chain On the other hand, we also found other optimized solutions related to the storage of transactions and smart contracts. For instance, to improve the storage performance of distributed file systems, Norvill et al. [44] proposed a solution that moves the contract-generation code to an off-chain by treating IPFS as a storage database. In their proposal, Ethereum loads complex contract codes by sending a simple hash value to IPFS peers. By this way, system clients only have to send hash values rather than the full codes when performing fast synchronizations. Thus, the bulk of network traffic can be reduced. In the design of Swarm [45], a chain of contracts is configured to maintain the basic operations. These contracts increase the data size of the blockchain such that Swarm is hard to be operated as a full blockchain ledger. Thus, according to reference [44], we know that the developers of Ethereum have been working on Swarm toward off-chain storage. Some other off-chain solutions such as Lightning Network [47] and Plasma [48] allow participants to execute transactions in an off-chain manner, such that a large portion of on-chain transactions and smart contracts can be offloaded from the main chain. Thus, integrating the off-chain techniques will bring new solutions to the storage policy of future distributed file systems.

3.4.2 Privacy

In Swarm and IPFS, data uploaded to the distributed file systems by users is divided into several pieces, which are then stored in different peers. Although the data uploaded can be encrypted, the data content stored in the network is accessible by every peer. Besides, according to the design of IPFS and Swarm, transactions that record the developments of a peer can be easily collected. User information can be revealed through the graph analysis of transactions. For example, according to Fanti and Viswanath [51], a client can be identified through the peers it directly connects to. Thus, transactions stored in the blockchain behind distributed file systems are publicly visible.

To address these issues, a number of efforts have been devoted to the privacy-preserving of distributed file systems. Through an extensive literature review, we have found many privacy-preserving solutions, mechanisms, and applications. Some representative works are classified into two main categories: (1) access control and (2) peer anonymity. We also compare several attributes of these studies in Table 3.3.

3.4.2.1 Access Control

In distributed file systems such as IPFS and Swarm, although users are not permitted freely to share data within a specific group of peers, this is necessary when taking privacy issues into account. To provide access control when sharing files, Steichen et al. [52] proposed a modified version of IPFS named *acl-IPFS* based on Ethereum. An acl-IPFS peer is constructed by an IPFS peer and an Ethereum account. The uploading, downloading, and transferring of data in IPFS networks are achieved through the interaction with smart contracts residing in Ethereum. Smart contracts dynamically maintain the access control lists of each file in acl-IPFS. Users can grant or revoke permission for a file through smart contracts, too. Aiming to enhance the privacy preservation of IoT data, Muhammad et al. [53] proposed a *modular consortium* architecture by combining the techniques of IoT and blockchains. The proposed architecture can provide decentralized management for IoT data by exploiting the advantages of blockchain and IPFS. Nizamuddin et al. [54] studied the authenticity of online digital and multimedia content. To provide originality proof, the authors proposed an authenticity solution based on IPFS and smart contracts. Based on IPFS, Ethereum, and attribute-based encryption (ABE) technologies, Wang et al. [55] investigated the data storage and sharing mechanism for distributed storage framework, in which no trusted private-key-generator is required. To achieve fine-grained access control, a data owner can distribute secret keys to other users and encrypt his data under a certain access policy. Then, toward

Table 3.3 Privacy studies of distributed file systems

Category	Reference	Technology foundation	Privacy level	Functionality
Access control	acl-IPFS [52]	Smart contract, Ethereum, IPFS	Strong	Provided an access control list for the files shared in the proposed acl-IPFS system
	Ali et al. [53]	Consortium blockchain, sidechain, IPFS	Strong	Proposed a *modular consortium* architecture for privacy preserving toward IoT data
	Nizamuddin [54]	IPFS, Ethereum smart contract	Strong	Proposed a solution to the authenticity of original online published digital works
	Wang et al. [55]	IIPFS, Ethereum and attribute-based encryption (ABE)	Unclear	Proposed a smart contract-based access control mechanism for decentralized storage systems
	Naz et al. [56]	IPFS, smart contract, RSA signatures	Strong	Proposed an IPFS-based secure data sharing framework to deliver digital assets
	Nyaletey et al. [41]	IPFS, Hyperledger Fabric	Strong	Proposed a solution BlockIPFS to trace the access events and provide audit access to files stored on IPFS
	Huang et al. [31]	Ethereum, local databases	Strong	Proposed an Ethereum-based access control and trustworthiness protection for multiple-domain participants

Peer anonymity	Zerocoin [57]	Bitcoin laundry system, zero-knowledge proof	Limited	Offered limited anonymity to the Bitcoin account addresses based on zero-knowledge proof
	E-voting system [58]	Bitcoin laundry system, Zerocoin	Limited	Provided an electronic-voting system based on Zerocoin, aiming to solve the privacy issues in original Bitcoin
	Zerocash [59]	Zero-knowledge argument, decentralized anonymous payment scheme	Strong	Provided a strong anonymous transactions by covering up the origins, destinations, and the total amount of a payment
	Mixcoin [60]	Accountable mixes, an independent cryptographic accountability layer	Strong	Proposed an anonymous payment protocol that can be deployed immediately with no changes to Bitcoin
	ReportCoin [61]	IPFS, blockchain	Strong	Proposed a blockchain-based reporting system for the management of smart city

transparency and quality of data, Naz et al. [56] proposed a secure digital-asset sharing framework based on integrated technology by combining IPFS, blockchain, and encryption mechanisms. Next, Huang et al. [31] proposed an Ethereum-based network-view sharing platform, which can bring global trustworthiness for multiple domains such as different IoT domain networks. In particular, the domain view of each partner is stored in their local databases, while the Ethereum-based system provides access control and trustworthiness protection over all participants.

3.4.2.2 Peer Anonymity

The privacy preservation of blockchain peers attracts particular attention in recent years. For example, considering that the original Bitcoin system has significant limitations on the privacy of Bitcoin peers, Miers et al. [57] proposed *Zerocoin*, which enables limited anonymity to the Bitcoin account addresses based on zero-knowledge proof. However, the proposed Zerocoin cannot guarantee full anonymity because at least the number of minted and spent coins and the denomination of transactions are visible to all users of this system. Using *Zerocoin*, Takabatake et al. [58] then proposed a new Bitcoin laundry middleware for Bitcoin. In this middleware, authors mentioned that the origin of transactions can be hidden and miners are able to validate transactions without signatures. However, the destination of a transaction and the amount of payment are still exposed to users. Thus, the proposed e-voting system has limited anonymity. Moreover, the execution speed of this voting system is also an obstacle that is hard to address. To address this problem, *Zerocash* [59] is claimed to fulfill a strong anonymity for payments, because it hides the transaction amount and the values of user-held coins, by invoking the zero-knowledge succinct non-interactive arguments of knowledge (*ZK-SNARKs*) [62]. *Mixcoin* [60] provided a combined service that transfers funds from multiple source addresses to multiple destination addresses. Thus, the relationship between the two accounts is hard to be revealed. Zou et al. [61] studied an incentive anonymous reporting mechanism based on blockchain and IPFS. The accounts and transactions stored in ReportCoin are open, transparent, and tamper-resistant. Thus, the anonymity of reporting sources can be protected with a high guarantee. The proposed ReportCoin was only evaluated through simulations, which make this work less convincing. The practicality of the proposed incentive mechanism requires more convincing proofs by real implementations.

3.5 Open Issues, Challenges, and Future Directions

In this section, we discuss open issues, challenges, and future directions of distributed file systems with respect to four perspectives: *scalability*, *privacy*, *applications*, and *big data*.

3.5.1 Scalability Issues

3.5.1.1 Scalability Performance

We have reviewed some representative studies [39] related to the scalability performance measurement of DFSs in the previous section. These existing works have shown us some insights into DFSs. For example, Wennergren et al. [39] mentioned that the limited bandwidth of each instance of IPFS could be one of the critical reasons for the low scalability of IPFS. The quantitative analysis [40] of systematic evaluations of the IPFS storage systems indicates that downloading and resolving operations could be bottlenecks while IPFS clients are reading objects from remote nodes. Nyaletey et al. [41] evaluated the scalability of the proposed BlockIPFS by varying the number of nodes. However, the scale of their experiments is too small, making the scalability performance of their system unclear under a very large-scale deployment.

Through the studies [39, 40, 44], we see that the current distributed file systems, such as IPFS and Storj, are still in their immature stages. For example, IPFS still faces some notable shortcomings, including the bottlenecks of resolving and downloading, and the high latency of I/O operations. Thus, to achieve large-scale commercial applications, IPFS must solve a number of challenges such as storage optimization, geo-distributed deployment of nodes, file request performance, etc.

From the storage-optimization perspective, although the conventional erasure coding zigzag codes [43] can be used to improve the storage efficiency for the proposed IPFS-based systems, some open issues should not be ignored. For example, reconstructing original files could bring a high consumption of both disk I/O and bandwidth to some associated peer nodes.

Another critical problem that IPFS needs to address is how to update the contents already stored on its system. This is because all data stored in the IPFS network is a series of hash addresses. Once a change occurs on a file stored in IPFS, the hash address changes, too. Therefore, an efficient update mechanism should be developed for IPFS.

Finally, to improve the scalability performance of blockchain-based DFSs, we believe that developing new solutions that can improve the efficiency of DFS's structure layers can be a promising direction. We wish to see the related studies will be proposed soon.

3.5.1.2 Performance Measurement Methodology

The performance measurement of IPFS and Swarm considering quality of service (QoS) metrics still needs to be further conducted widely and deeply in the future. Especially when integrating them into business models, users desire to know which one (either IPFS or Swarm) matches their requirements best. Fortunately, Zheng et al. [63] proposed a real-time performance monitoring framework for blockchain systems. This work has evaluated four famous blockchain systems, i.e., Ethereum [12], Parity [64], Cryptape Inter-enterprise Trust Automation (CITA) [65], and Hyperledger Fabric [66], with respect to the QoS metrics of *transactions per second*, *average response delay*, *transactions per CPU*, *transactions per memory second*, *transactions per disk I/O*, and *transactions per network data*. Such comprehensive performance evaluation results give us insightful viewpoints on the four well-known blockchain systems. Their experimental logs and technique report [67] can be found from http://xblock.pro. In addition, Curran et al. [68] mentioned that they plan to analyze the performance of IPFS, while a website is under an unexpected surge of visitors. However, we cannot find the subsequent technique report of their measurements.

3.5.1.3 System Measurement Standards

Based on the existing studies aforementioned, a new system measuring standards need to be proposed for IPFS and Swarm. Generally, system testing can be separated into two phases [69]: a standardization phase and a testing phase. In the former phase, a series of metrics have been designed to show the performance of systems in terms of transactions per second, contract execution time, and consensus-cost time. In the latter phase, systems are tested in different situations. For example, failures including network shutdown and high memory occupation could be injected. Then, the designed metrics could show the performance under different failures, which can help identify different types of failures. Furthermore, the transaction amount that are received by a blockchain system in one second could be adjusted in a testing environment. Thus, the system performance under different transaction rates could be measured.

Through the further review described above, we see that the system measurement of distributed file systems is still in its immature stage. Thus, we look forward to seeing exciting new studies on this topic.

3.5.2 Privacy/Security Issues

Some current versions of DFS, such as IPFS, do not tolerate Byzantine attacks. For instance, every peer can access every file stored on IPFS as long as it joins the system. This situation makes privacy and security issues weaknesses for IPFS systems. Therefore, importing some privacy-protection means such smart contract-based access control mechanisms [31] and encryption technologies [55] over the data stored on blockchain-based DFSs could be feasible solutions.

In addition, researchers are also considering whether will Reed-Solomon erasure coding [46] be implemented for IPFS. Note that Reed-Solomon coding is very popular in the datacenters as they provide great disk savings against data replication. IPFS has not yet addressed such a data replication problem. On the other hand, adopting such erasure coding can also enhance the privacy and security level of DFSs. This is because each data chunk is encoded under an erasure coding; even if a peer gets a chunk, it doesn't know what the content is. Furthermore, if a malicious attacker outside a DFS intends to eavesdrop on the DFS peers, the attacker must have all encoded pieces of data chunks associated with the desired file. This would be very difficult if the malicious attacker is blocked by an access-control mechanism.

In summary, we anticipate new solutions regarding data privacy/security policies of IPFS are going to be implemented in the near future.

3.5.3 Application Issues

IPFS is providing business solutions to enterprises. A growing number of applications based on IPFS have been developed. According to the original design, IPFS is used for storing data. For example, Jia et al. [70] developed a decentralized music-sharing platform called *Opus* employing both IPFS and Ethereum. Opus provides encrypted storage using IPFS. The keys of these encrypted data are traded using smart contracts. Opus is also able to prevent the monopoly of streaming platforms, track the digital ownership of artists, and compensate artists with reasonable monetary prices. Not only playing as a game-changer in the music domain, but IPFS has also been adopted in other areas. For instance, Tenorio-Forn et al. [71] proposed a decentralized publication system for open-access science based on IPFS. Their proposed distributed systems can record reviewers' reputations and handle transparent governance processes.

Recently, the IPSE team [72] proposed a new revolutionary search engine, which is implemented on top of IPFS and blockchain. Such IPSE focuses on user privacy and search efficiency because it allows users to search network files on IPFS and access the file without relying on a centralized entity such as Google or Baidu. More importantly, IPSE also enables users to take full control of their own network data by exploiting encryption technologies and smart contracts. Thus, IPSE is a good example that integrates a distributed file system with blockchain technologies.

It can be seen that most of these applications leverage the decentralized characteristics of IPFS. With the integration of Filecoin, smart contracts are imported into IPFS. This new feature brings great potential to IPFS. Thus, smart contracts make application development based on IPFS or Swarm a promising direction.

3.5.4 Big Data Issues

IPFS and Swarm can be also well combined with big data applications. We discuss the big data issues considering the following two aspects: *big data storage* and *big data analytics*.

On one hand, regarding big data storage, IPFS and Swarm can store data with their decentralized and secure characteristics. For example, Confais et al. [73] proposed an object store for fog and edge computing using IPFS and scale-out network-attached storage systems (NAS) [74]. The proposed system alleviated the issues of high latency of cloud computing architecture and thus is suitable for the Internet of Things (IoT). According to Jovović et al. [75], in the era of the fifth-generation communications network (5G), more IoT equipment requires larger and more secure storage. To fill this gap, blockchain-based distributed file systems such as Swarm and IPFS can play an important role as the secure storage layer.

On the other hand, with respect to big data analytics, the transactions on blockchains and the logs in file systems can be used for data analytics. For example, the analytics of transactions collected from blockchain systems can be used to extract the trading patterns of users. The data analytics of a peer's credit is also useful when deciding whether to sign deals with a peer. As a representative works of data analytics, Chen et al. [76–78] analyzed smart contracts collected from Bitcoin and Ethereum and then successfully detected a large number of market manipulations and *Ponzi Schemes* [79] using data mining and machine learning methods. Their studies can be viewed as a pioneer in combining big data analytics with blockchain. The technique reports, dataset, and even codes [80] can be downloaded from http://xblock.pro. Using similar approaches, transactions and data in the network can be analyzed such that malicious nodes in distributed file systems, e.g., IPFS and Swarm, can be detected.

3.6 Conclusion

The new generations of blockchain-based distributed file systems, such as IPFS and Swarm, have shown their great potential with their key characteristics: novel solutions of incentive, low-latency data retrieval, automated auditing, censorship-resistant, etc. This chapter first presents the rationale, layered structure, and an overview of blockchain-based distributed file systems, particularly focusing on IPFS and Swarm systems. Then, we introduce the cutting edge of the two systems and reveal a series of challenges that constrain their development. Open issues and future directions are finally discussed. We believe that blockchain-based distributed file systems will become very promising solutions for next-generation websites and data-sharing platforms. We anticipate that this article can trigger blooming investigations on blockchain-based distributed file systems in the near future.

References

1. M. Giesler and M. Pohlmann, “The anthropology of file sharing: Consuming Napster as a gift,” *ACR North American Advances*, 2003.
2. M. Ripeanu, “Peer-to-peer architecture case study: Gnutella network,” in *Proceedings first international conference on peer-to-peer computing*. IEEE, 2001, pp. 99–100.
3. N. S. Good and A. Krekelberg, “Usability and privacy: a study of Kazaa P2P file-sharing,” in *Proc. of the SIGCHI conference on Human factors in computing systems*. ACM, 2003, pp. 137–144.
4. H.-W. Tseng, Q. Zhao, Y. Zhou, M. Gahagan, and S. Swanson, “Morpheus: creating application objects efficiently for heterogeneous computing,” in *2016 ACM/IEEE 43rd Annual International Symposium on Computer Architecture (ISCA)*. IEEE, 2016, pp. 53–65.
5. J. Pouwelse, P. Garbacki, D. Epema, and H. Sips, “The bittorrent p2p file-sharing system: Measurements and analysis,” in *International Workshop on Peer-to-Peer Systems*. Springer, 2005, pp. 205–216.
6. J. E. Cater and J. Soria, “The evolution of round zero-net-mass-flux jets,” *Journal of Fluid Mechanics*, vol. 472, pp. 167–200, 2002.
7. J. Benet, “IPFS-content addressed, versioned, p2p file system,” *arXiv preprint arXiv:1407.3561*, 2014.
8. V. Trón, A. Fischer, and Nagy, “State channels on swap networks: claims and obligations on and off the blockchain (tentative title),” 2016.
9. S. Wilkinson, T. Boshevski, J. Brandoff, and V. Buterin, “Storj a peer-to-peer cloud storage network,” 2014.
10. “PPIO: a decentralized programmable storage and delivery network,” https://www.pp.io/docs/.
11. J. Benet and N. Greco, “Filecoin: A decentralized storage network,” *Protoc. Labs*, 2018.
12. G. Wood *et al.*, “Ethereum: A secure decentralised generalised transaction ledger,” *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.
13. S. Wilkinson, J. Lowry, and T. Boshevski, “Metadisk: a blockchain-based decentralized file storage application,” *Storj Labs Inc., Technical Report, hal*, pp. 1–11, 2014.
14. M. Szydlo, “Merkle tree traversal in log space and time,” in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2004, pp. 541–554.
15. S. Nakamoto *et al.*, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
16. G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche, “Keccak,” 2013.
17. “LibP2P,” https://github.com/libp2p.
18. “Devp2p,” https://github.com/ethereum/devp2p.
19. M. J. Freedman, E. Freudenthal, and D. M. Eres, “Democratizing content publication with coral,” in *Conference on Symposium on Networked Systems Design & Implementation*, 2004.
20. “Distributed preimage archive of swarm,” https://swarm-guide.readthedocs.io/en/latest/architecture.html#distributed-preimage-archive.
21. “Expected consensus,” http://www.ipfs.cn/news/info-100327.html.
22. I. Baumgart and S. Mies, “S/kademlia: A practicable approach towards secure key-based routing,” in *International Conference on Parallel & Distributed Systems*, 2007.
23. M. J. Freedman and D. Maziéres, “Sloppy hashing and self-organizing clusters,” 2003.
24. S. Shalunov, G. Hazel, J. Iyengar, and M. Kuehlewind, “Low extra delay background transport,” Internet-draft, Internet Engineering Task Force, Tech. Rep., 2010.
25. R. Stewart, Q. Xie, and M. C. Allman, “Stream control transmission protocol (SCTP): A reference,” *Publisher: Addison-Wesley*, 2001.
26. A. Chockalingam and G. Bao, “Performance of TCP/RLP protocol stack on correlated fading DS-CDMA wireless links,” *IEEE Transactions on Vehicular Technology*, vol. 49, no. 1, pp. 28–33, 1998.
27. S. Kim, “Measuring ethereum’s peer-to-peer network,” 2017.
28. “The Homepage of GIT,” https://git-scm.com/.
29. A. Tridgell, P. Mackerras *et al.*, “The rsync algorithm,” 1996.

30. A. Z. Broder, “Some applications of Rabin’s fingerprinting method,” in *Sequences II*. Springer, 1993, pp. 143–152.
31. H. Huang, S. Zhou, J. Lin, K. Zhang, and S. Guo, “Bridge the Trustworthiness Gap amongst Multiple Domains: A Practical Blockchain-based Approach,” in *Proc. of 11th IEEE International Conference on Communications (ICC’20)*, June 2020, pp. 1–6.
32. “Attacks of IPFS,” http://www.ipfs.cn/news/info-100379.html.
33. Y. Hirai, “Defining the ethereum virtual machine for interactive theorem provers,” in *International Conference on Financial Cryptography and Data Security*. Springer, 2017, pp. 520–535.
34. A. Gervais, G. O. Karame, V. Glykantzis, H. Ritzdorf, and S. Capkun, “On the security and performance of proof of work blockchains,” in *ACM SIGSAC Conference on Computer & Communications Security*, 2016.
35. I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, “Proof of activity:extending bitcoin’s proof of work via proof of stake [extended abstract]y,” *ACM Sigmetrics Performance Evaluation Review*, vol. 42, no. 3, pp. 34–37, 2014.
36. “Design rationale of ethereum,” https://github.com/ethereum/wiki/wiki/Design-Rationale.
37. S. Wilkinson, T. Boshevski, J. Brandoff, J. Prestwich, G. Hall, P. Gerbes, P. Hutchins, C. Pollard, and V. Buterin, “Storj a peer-to-peer cloud storage network (version 2.0),” Dec. 2016.
38. H. Shacham and B. Waters, “Compact proofs of Retrievability,” *Journal of cryptology*, vol. 26, no. 3, pp. 442–483, 2013.
39. O. Wennergren, M. Vidhall, and J. Sörensen, “Transparency analysis of distributed file systems: With a focus on interplanetary file system,” 2018.
40. J. Shen, Y. Li, Y. Zhou, and X. Wang, “Understanding i/o performance of IPFS storage: a client’s perspective,” in *Proc. of the International Symposium on Quality of Service (IWQoS’19)*, 2019, pp. 1–10.
41. E. Nyaletey, R. M. Parizi, Q. Zhang, and K.-K. R. Choo, “BlockIPFS-blockchain-enabled interplanetary file system for forensic and trusted data traceability,” in *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 18–25.
42. Y. Chen, H. Li, K. Li, and J. Zhang, “An improved P2P file system scheme based on IPFS and blockchain,” in *Proc. of IEEE International Conference on Big Data (Big Data)*, 2017, pp. 2652–2657.
43. I. Tamo, Z. Wang, and J. Bruck, “Zigzag codes: MDS array codes with optimal rebuilding,” *IEEE Transactions on Information Theory*, vol. 59, no. 3, pp. 1597–1616, 2012.
44. R. Norvill, B. B. F. Pontiveros, R. State, and A. Cullen, “IPFS for reduction of chain size in Ethereum,” in *Proc. of IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, pp. 1121–1128.
45. “IPFS & SWARM,” https://github.com/ethersphere/swarm/wiki/IPFS-&-SWARM.
46. J. S. Plank, “A tutorial on Reed–Solomon coding for fault-tolerance in RAID-like systems,” *Software: Practice and Experience*, vol. 27, no. 9, pp. 995–1012, 1997.
47. J. Poon and T. Dryja, “The bitcoin lightning network: Scalable off-chain instant payments,” 2016.
48. J. Poon and V. Buterin, “Plasma: Scalable Autonomous Smart Contracts,” *White Paper*, pp. 1–47, 2017.
49. D. Vorick and L. Champine, “Sia: Simple decentralized storage,” *Nebulous Inc*, 2014.
50. H. Huang, S. Guo, W. Liang, K. Wang, and Y. Okabe, “Coflow-like Online Data Acquisition from Low-Earth-Orbit Datacenters,” *IEEE Transactions on Mobile Computing (TMC)*, 2019, DOI: https://doi.org/10.1109/TMC.2019.2936202.
51. G. Fanti and P. Viswanath, “Deanonymization in the bitcoin P2P network,” in *Advances in Neural Information Processing Systems*, 2017, pp. 1364–1373.
52. M. Steichen, B. Fiz, R. Norvill, W. Shbair, and R. State, “Blockchain-based, decentralized access control for IPFS,” in *Proc. of IEEE International Conference on iThings, GreenCom, CPSCom and SmartData*, 2018, pp. 1499–1506.

53. M. S. Ali, K. Dolui, and F. Antonelli, “IoT data privacy via blockchains and IPFS,” in *Proc. of the Seventh International Conference on the Internet of Things*. ACM, 2017, p. 14.
54. N. Nizamuddin, H. R. Hasan, and K. Salah, “IPFS-blockchain-based authenticity of online publications,” in *International Conference on Blockchain*. Springer, 2018, pp. 199–212.
55. S. Wang, Y. Zhang, and Y. Zhang, “A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems,” *IEEE ACCESS*, vol. 6, pp. 38 437–38 450, 2018.
56. M. Naz, F. A. Al-zahrani, R. Khalid, N. Javaid, A. M. Qamar, M. K. Afzal, and M. Shafiq, “A secure data sharing platform using blockchain and interplanetary file system,” *Sustainability*, vol. 11, no. 24, p. 7054, 2019.
57. I. Miers, C. Garman, M. Green, and A. D. Rubin, “Zerocoin: Anonymous distributed e-cash from bitcoin,” in *Proc. of IEEE Symposium on Security and Privacy*, 2013, pp. 397–411.
58. Y. Takabatake, D. Kotani, and Y. Okabe, “An anonymous distributed electronic voting system using zerocoin,” *IEICE Technique Report*, 2016.
59. E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, “Zerocash: Decentralized anonymous payments from bitcoin,” in *Proc. of IEEE Symposium on Security and Privacy*, 2014, pp. 459–474.
60. J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, “Mixcoin: Anonymity for bitcoin with accountable mixes,” in *International Conference on Financial Cryptography and Data Security*. Springer, 2014, pp. 486–504.
61. S. Zou, J. Xi, S. Wang, Y. Lu, and G. Xu, “Reportcoin: A novel blockchain-based incentive anonymous reporting system,” *IEEE Access*, vol. 7, pp. 65 544–65 559, 2019.
62. H. Lipmaa, “Prover-efficient commit-and-prove zero-knowledge SNARKs,” in *Proc. of International Conference on Cryptology in Africa*. Springer, 2016, pp. 185–206.
63. P. Zheng, Z. Zheng, X. Luo, X. Chen, and X. Liu, “A detailed and real-time performance monitoring framework for blockchain systems,” in *Proc. of IEEE/ACM 40th International Conference on Software Engineering: Software Engineering in Practice Track (ICSE-SEIP)*, 2018, pp. 134–143.
64. “Parity documentation,” https://paritytech.github.io/wiki.
65. “Cita technical whitepaper,” https://github.com/cryptape/cita.
66. “Hyperledger fabric website,” https://hyperledger-fabric.readthedocs.io/en/release-1.4/write_first_app.html.
67. X. Team, “Performance Monitoring,” Website, Feb. 2020, http://xblock.pro/performance/.
68. T. Curran and B. de Graaff, “Analysing the performance of IPFS during flash crowds,” 2016.
69. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” in *Proc. of IEEE International Congress on Big Data (BigData Congress)*, 2017, pp. 557–564.
70. B. Jia, C. Xu, R. Gotla, S. Peeters, R. Abouelnasr, and M. Mach, “Opus-decentralized music distribution using interplanetary file systems (IPFS) on the ethereum blockchain v0. 8.3,” 2016.
71. A. Tenorio-Fornés, V. Jacynycz, D. Llop-Vila, A. Sánchez-Ruiz, and S. Hassan, “Towards a decentralized process for scientific publication and peer review using blockchain and IPFS,” in *Proc. of the 52nd Hawaii International Conference on System Sciences*, 2019.
72. I. Team”, “IPSE: A search engine based on IPFS,” https://ipfssearch.io/IPSE-whitepaper-en.pdf.
73. B. Confais, A. Lebre, and B. Parrein, “An object store for Fog infrastructures based on IPFS and a scale-out NAS,” in *RESCOM 2017*, 2017, p. 2.
74. G. A. Gibson, “Network attached storage architecture,” *Comm ACM*, vol. 43, no. 11, pp. 37–45, 2000.
75. I. Jovović, S. Husnjak, I. Forenbacher, and S. Maček, “5G, blockchain and IPFS: A general survey with possible innovative applications in industry 4.0,” in *3rd EAI International Conference on Management of Manufacturing Systems-MMS 2018*, 2018.

76. W. Chen, Z. Zheng, J. Cui, E. Ngai, P. Zheng, and Y. Zhou, "Detecting Ponzi schemes on ethereum: Towards healthier blockchain technology," in *Proc. of the 2018 World Wide Web Conference on World Wide Web*. International World Wide Web Conferences Steering Committee, 2018, pp. 1409–1418.
77. W. Chen, J. Wu, Z. Zheng, C. Chen, and Y. Zhou, "Market manipulation of bitcoin: Evidence from mining the Mt. Gox transaction network," in *IEEE Conference on Computer Communications*. IEEE, 2019, pp. 964–972.
78. W. Chen, Z. Zheng, E. C.-H. Ngai, P. Zheng, and Y. Zhou, "Exploiting blockchain data to detect smart Ponzi schemes on ethereum," *IEEE Access*, vol. 7, pp. 37 575–37 586, 2019.
79. "Ponzi scheme," https://en.wikipedia.org/wiki/Ponzi_scheme.
80. X. Team, "Fraud Detection," Website, Feb. 2020, http://xblock.pro/fraud-detection/.

Chapter 4
How to Organize Web3 Participants? Decentralized Autonomous Organizations

Huawei Huang, Lu Liu, Sicong Zhou, and Zibin Zheng

Abstract This chapter introduces how to organize Web3 participants, which include Web3 educators, investors, developers, and other users who are interested in Web3. Decentralized autonomous organizations (DAOs) are believed to play a significant role in our future Web3-featured society governed in a decentralized way. In this chapter, we first explain the definitions and preliminaries of DAO. Then, we conduct a literature review of the existing studies of DAO published in the recent few years. Through the literature review, we find out that a comprehensive overview of the state-of-the-art studies of DAO is still missing. To fill this gap, we perform such an investigation by identifying and classifying the most valuable proposals and perspectives closely related to the combination of DAO and blockchain technologies. We anticipate that this chapter can help researchers, engineers, and educators acknowledge the cutting-edge development of DAO.

Keywords Decentralization · Decentralized autonomous organizations · Bitcoin · Distributed ledger technology · Security threats · Governance

4.1 Introduction

Blockchain-based technologies have been deeply adopted by multiple applications that are closely related to every corner of our daily life, such as cryptocurrencies, tokenomics, business applications, Internet-of-Things (IoT) applications, etc. Decentralized autonomous organization (DAO), as one of the blockchain applications shown in Fig. 4.1, is growing rapidly and drawing great attention from both academia and governments around the world. Although DAO has brought a lot of opportunities to blockchain technologies, we are surprised to find out that an overview of DAO from the perspective of blockchains is still missing. Based on

H. Huang · L. Liu · S. Zhou · Z. Zheng (✉)
School of Software Engineering, Sun Yat-sen University, Zhuhai, Guangdong, China
e-mail: huanghw28@mail.sysu.edu.cn; liulu57@mail3.sysu.edu.cn; chowsch2@mail2.sysu.edu.cn; zhzibin@mail.sysu.edu.cn

H. Huang et al. (eds.), *From Blockchain to Web3 & Metaverse*,
https://doi.org/10.1007/978-981-99-3648-9_4

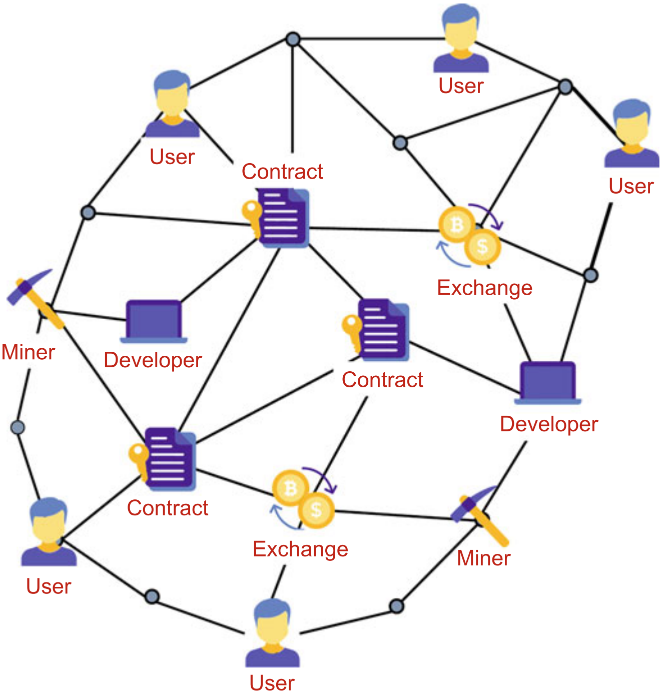


Fig. 4.1 The structure of a DAO

the background mentioned above, we perform a comprehensive classification on the latest studies combining the blockchain and DAO.

The taxonomy in this chapter mainly includes three categories. In the first category, we discuss the common problems and the related studies of blockchain and DAO, including various attacks and security issues of blockchains, and the counter-trend issues. In the second category, we focus on the issues related to DAO governance and the existing development of a more in-depth discussion. In the third category, we evaluate the latest development of DAO in various fields, such as e-government, economy, etc., and predict the future development directions of the relevant fields.

Although a small number of researchers are worried about the future of DAO and blockchain due to the *hard fork* caused by *The DAO* hacking incident [1], most of them still have high expectations on this technology. We also believe that with the inspiring pace of the development of DAO and blockchain, DAO projects will become mature and DAO will show substantial advantages.

Through this overview, we find the most important finding in this direction is that future efforts can be devoted to improving DAO from a better balance of decentralization, security, and scalability. We look forward to a new integration of both the social and organizational structure of DAO in the context of blockchain

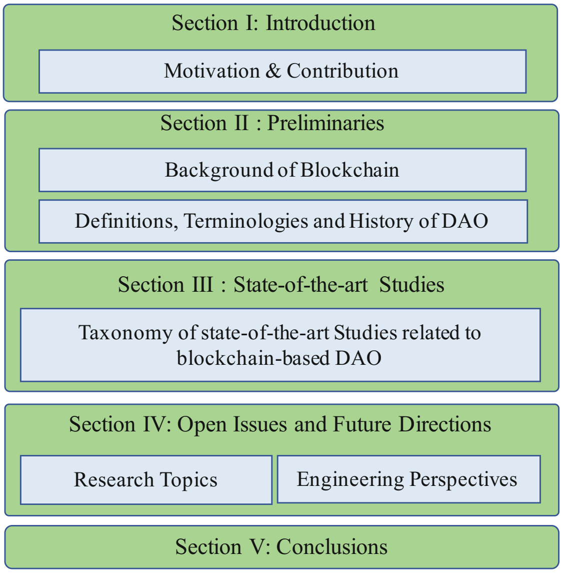

Section I: Introduction
Motivation & Contribution
Section II : Preliminaries
Background of Blockchain
Definitions, Terminologies and History of DAO
Section III : State-of-the-art Studies
Taxonomy of state-of-the-art Studies related to blockchain-based DAO
Section IV: Open Issues and Future Directions
Research Topics
Engineering Perspectives
Section V: Conclusions

Fig. 4.2 The roadmap of this chapter

technologies. To help have a clear clue of this chapter, Fig. 4.2 shows the organization of this chapter.

4.2 Preliminaries

4.2.1 Decentralization

In the general case of centralization, the use of a database is basically based on the trust of a third-party organization. For example, as a third party, people all trust the banking system, which can correctly manage the database and record our transactions. The bank keeps accounts for every transaction, and only the bank has the authority to keep users' accounts. However, the shortcoming of such a centralized organization is obvious. No one can make sure whether the centralized organization that manages the database is entirely trustworthy. For example, during the global economic crisis in 2008, the US government could issue money indefinitely, because it is the central institution of monetary management.

On the contrary, decentralization means that the database does not depend on a specific organization or administrator but is distributed among all peers. Blockchain (Fig. 4.3) is essentially a decentralized database. Each full node has a complete copy of the blockchain ledger. If the database is modified, the information saved by all nodes will be noticed. Thus, the information in the blockchain database will be open and transparent. Decentralization solves the trust problem through redundant data validation.

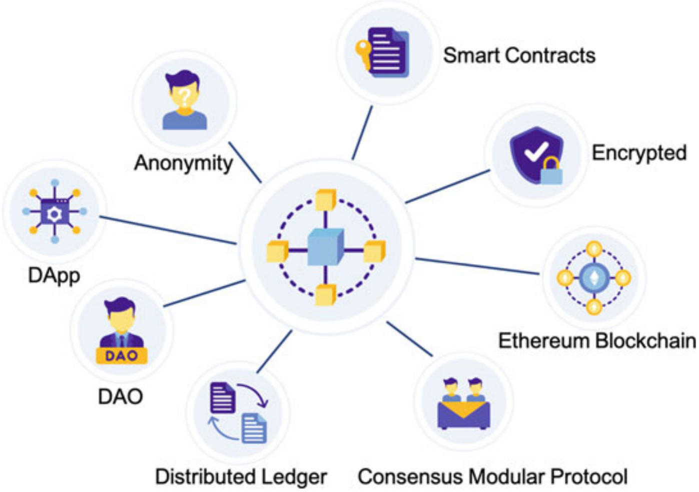


Fig. 4.3 Blockchain-related fields

4.2.2 *Bitcoin Blockchain*

Originally proposed by Satoshi Nakamoto [2], Bitcoin is the first application of the blockchain. In Bitcoin, the blockchain serves as a distributed database that stores all transactions originating from one account to another. The advantages of blockchain bring many pros to the Bitcoin ecosystem. For example, everyone has the right to validate accounts, the currency cannot be over-issued, and the entire ledger is completely open and transparent. When processing a transaction, Bitcoin adopts the techniques of digital signatures to identify the ownership of a coin. Each Bitcoin account address has private and public keys. The private key is private and is used to exercise the Bitcoin ownership of the Bitcoin account, while the public key is known to all nodes to verify the transaction and the balance of a Bitcoin account. When the transfer information of a transaction is published, a digital signature must be embedded by encrypting the digital summary of the transfer message together with the private key of the sender. Thus, other nodes can use the public key of the sender's account to decrypt and verify the legality of the transaction. After such verification, each blockchain node has acknowledged this transaction.

4.2.3 *Definition and Background of DAO*

DAO was originally introduced by the white paper [3], in which DAO is defined as an organization built on smart contracts that can execute autonomously. Unlike conventional centralized entities, it doesn't include central control or management.

As shown in Fig. 4.1, DAO achieves the decentralized organization by encoding a set of rules in smart contracts, where how DAO performs is predefined. Although this completely decentralized way makes investors typically don't know and trust each other, blockchain is a good tool to help achieve the goal of DAO. However, DAOs are not necessarily to be built on top of an existing blockchain such as Ethereum [4]. During the getting-start guidelines, Casino [2] was published as an introduction to DAO. It presents the concepts, characteristics, frameworks, applications, future trends of DAO, etc. The readers will gain a systematic overview of DAO that spans multiple domains.

4.2.4 Project the DAO

In the development of DAO, the first DAO project is proposed with historic and dramatic meaning. A particular historical moment of DAO is the creation of the first DAO and how it was eventually hacked. *The DAO* project was started on April 30, 2016. By the end of the entire funding period, more than 11,000 enthusiastic members had participated and raised 150 million dollars, making the *The DAO* the largest crowdfunding project in history. It was an overnight success, but the idea of *The DAO* vulnerability had been circulating in the developer community. Finally, on June 18, a hacker began using a "recursive call vulnerability" in the software to steal Ether coins from the token pool of *The DAO*. He took the advantage of a well-noticed but poorly implemented feature of DAO designed to prevent the majority from tyrannizing over dissenting DAO token holders. But this "split" feature was implemented to make *The DAO* vulnerable to catastrophic re-entrance errors. As a result, the attacker was able to steal about 3.6 million ETH, which are worth about $50 million at the time of the attack, bringing the price of the coin from more than 20 dollars to less than 13 dollars. Losses reached 70 million dollars. *The DAO*'s problems have had a notorious impact on both the Ethereum network and its cryptocurrency. The situation for *The DAO* investors is particularly precarious. Eventually, over 90% of Ethereum's hash rates indicated the support for a hard fork. *The DAO* fund was returned to investors as if the organization never existed. *The DAO* hack sparked a debate about hard forks and the decentralization spirit of blockchains. This hack event also led to the birth of Ethereum Classic [1].

4.2.5 To Launch a DAO Project

Although the first DAO project failed, it did not completely prevent the initiation and development of other DAO projects. The operation of launching a DAO project includes the following steps [5], which are also illustrated in Fig. 4.4:

1. Developing and deploying smart contracts according to predefined rules.
2. Handling the token issues (through ICO) at the initial financing stage.

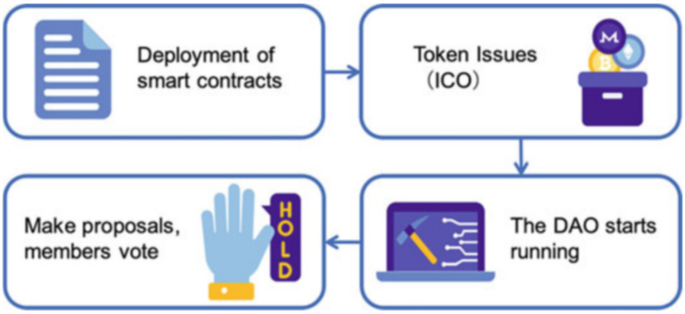


Fig. 4.4 The four-step launch of a DAO project

3. At the end of the financing phase, a DAO starts running.
4. Proposals are made and members can vote on them.

4.2.6 Existing Popular DAOs

The representative existing implementations of DAO are reviewed as follows.

4.2.6.1 Aragon

Aragon [6] is a platform that enables any participant to collaborate with others without any third-party organizers. On Aragon, people can create a decentralized digital jurisdiction for their company, community, and organization. The Aragon users are also allowed to create diverse communities. For example, a financial DAO can be generated to incentivize internal usage of Coinbase Apps, a council DAO is launched to expand the utilization of wealth management, or a pocket DAO is established to eliminate blockchain infrastructure monopolies.

4.2.6.2 Colony

Colony [7] is designed as an infrastructure that enables organizations to collaborate with each other via the decentralized software implemented on top of Ethereum. It treats every participant impartially. Unlike other DAOs, Colony advocates eliminating the requirement of voting from members. Instead, it focuses on mechanisms that enforce people to get their job done.

4.2.6.3 DAOstack

DAOstack [8] is an open-source, modular DAO project, which leverages the technology and adoption of decentralized governance, enabling people to create the DApps (decentralized apps), DAOs, and DAO tools.

Although several DAOs have been implemented, we should notice that DAOs are still in their immature stage, a large number of new DAOs will be developed in the future, and many insights into DAOs will be perceived then.

4.3 Taxonomy of State-of-the-Art Studies

In this part, we perform a thorough taxonomy of the existing up-to-date studies of blockchain-related DAO. Through the classification of the existing literature related to DAO, we find that in addition to the introduction of DAO systems, existing studies mainly focus on security issues, applications in various fields, and DAO governance issues. Therefore, we divide it into the categories presented in each subsection.

Among those categories, on the analysis of the questions about DAOs related issues, we divide them into two classes. On one hand, a DAO project is based on the blockchain; thus the problems existing in blockchain are also the existing problems of DAO. On the other hand, DAO induces some new problems in governance. Such relevant studies are reviewed in governance problems and solutions. Finally, in the last category, DAO and related areas, we pay attention to the current development of DAO in the context of various fields.

4.3.1 Existing Problems and Solutions of Blockchains

The hacking incident of the first *The DAO* project triggered the introspection of DAO projects [9]. The first-generation blockchain technology, blockchain 1.0, was mainly invented for cryptocurrency purposes. Then, the second generation of blockchain 2.0, represented by Ethereum, is an open platform that enables a new decentralized computing paradigm. The DAO is exactly based on Ethereum. While there are no obvious security vulnerabilities in pure cryptocurrency systems such as Bitcoin [10], the second-generation blockchain applications and semantics inevitably introduce security vulnerabilities [11, 12].

Besides, from the perspective of social development, we observe some common problems that need to be solved together for both blockchains and the DAO. For example, the typical problems include:

- the interpretation of fork culture by DAO hacker event;
- whether there are problems in the application development of distributed ledger technology (DLT);
- and whether the main trend of blockchain technology is reasonable.

Table 4.1 Existing DAO as blockchain problems and solutions

References	Recognition	Methodology
Li [13]	Security threats and enhancement solutions in blockchain	A systematic study on the security threats to blockchain and the corresponding real attacks and suggests some future directions to stir research efforts into this area
Zhou [15]	Scalability of blockchains	Existing blockchain scalability solutions are classified according to the blockchain hierarchy
Manski [14]	Countervailing trend	Blockchain applications could exacerbate inequality
LSE Team [16]	DLT	The potential of DLT is great but need to be assessed the feasibility

Inspired by those questions, the blockchain system hacker attacks [1], security issues [13], and blockchain counter-trend issues [14] have drawn a lot of attention (Table 4.1).

4.3.1.1 Security Threats and Enhancement Solutions in Blockchain

Blockchain technology has shown a promising application prospect since its birth. Blockchain has been used in many fields, ranging from the original cryptocurrency to various applications based on smart contracts [17, 18]. Along with the booming development of blockchains, the security and privacy of blockchains should not be ignored. On the basis of existing studies on blockchain security and privacy issues, Li et al. [13] systematically studied the security threats of blockchains through the analysis of popular blockchain systems. Their major contribution includes (a) analyzing the causes and possible consequences of each risk or vulnerability, (b) investigating the corresponding actual attack, and (c) analyzing the exploited vulnerability.

From the generation perspective of blockchains, we summarize the common risks of blockchain 1.0 as follows: (a) 51% vulnerability, (b) private key security, (c) criminal activity, (d) double spending, and (d) transaction privacy leakage. While for blockchain 2.0, the common risks include (a) criminal smart contracts, (b) vulnerabilities in smart contracts, (c) under-optimized smart contracts, and (d) underprice operations.

Furthermore, the popular attacks toward the blockchain include selfish mining attacks, DAO attacks (which is also the focus of this chapter), BGP hijacking attacks, eclipse attacks, liveness attacks, and balance attacks. Considering those attacks, Li et al. [13] summarized the security-enhancement solutions of the blockchain system as follows: (a) SmartPool, (b) quantitative framework, (c) Oyente, (d) Hawk, and (e) Town Crier. Those solutions have made a good prediction for the future direction of the blockchain.

4.3.1.2 Scalability of Blockchains

Similar to CAP theory in the field of traditional distributed systems, the three important attributes of blockchain systems, including decentralization, security, and scalability, cannot be fulfilled altogether. For example, Bitcoin faces performance problems with low-throughput and high transaction latency. Other cryptocurrencies also face these flaws, leading researchers to pay more attention to the scalability of blockchains. To have a clear clue about the blockchain scalability solutions, Zhou et al. [15] attempted to overview the related state-of-the-art studies by categorizing them according to their blockchain hierarchy. The hierarchical structure mainly consists of two layers. The first-layer solution is executed on the chain, focusing on the blockchain consensus, networks, and data structures. Such as increasing the block size of the Bitcoin blockchain, optimizing the storage scheme, as well as adopting sharding technology. Various improved consistency algorithms, where transaction throughput can be increased and transaction latency is decreased, are also reviewed. The second-layer solutions seek opportunities to extend the blockchain through the off-chain channels and side-chain and cross-chain protocols. Basically, these solutions have both advantages and limitations as they strive to achieve decentralization, security, and scalability at the same time. The insightful classification and analysis of current solutions can inspire further research.

4.3.1.3 Countervailing Trend

To our surprise, blockchain technology also somewhat shows a counter-trend problem. Blockchains, like other technologies, have shown a tendency to pursue different future trajectories, depending on their implementation details. For example, blockchain technology can help build a technology community in which advanced exchanges, communications, and decision-making technologies are used to aggregate, allocate, and manage capital at multiple levels. However, a series of anti-subsidy trends indicate a deepening of inequality and democratic decline. Because technology is stratified, a large number of employees are reduced to a less disposable population, regulation is reduced, and corporate personnel is technologized. While the mainstream trends in blockchain technology are greatly believed as distribution, decentralization, and democratization, the most powerful blockchain applications are likely to exacerbate inequality.

4.3.1.4 The Future of the DLT

In fact, blockchain is essentially an application of distributed ledger technology. LSE Team [16] describes the problem to be solved before DLT is used. The potential of DLT is too great to ignore. Its commitment to decentralization, data security, and privacy can help improve and make public services more affordable by reducing the role of the government as an intermediary. The decentralized and transparent properties of the DLT lead to greater collaboration and integration with the private and social sectors by enhancing the government's own transparency, accountability, and inclusiveness. However, there is no general rule book that specifies where a DLT should be deployed. If governments desire to use DLT for governance, they need to assess the feasibility of DLT and implement DLT-based applications only when the benefits of speed, security, and privacy outweigh the social costs. Governments must govern in the context when the implemented DLT applications are transparent to the underlying algorithms and ensure that the applications truly represent public value. All these visions will have to wait for the DLT technologies to evolve further.

4.3.2 Governance Problems and Solutions

DAO, as an application of blockchain in governance, raises new issues (Table 4.2) about governance that are not found in conventional blockchain. Through professional knowledge and experiments [19], there is still existing differences between code-based governance and blockchain-based governance. To use DAOs in certain areas, DuPont [20] argues that DAO may simply be a risky investment that masquerades as a new way of doing things. Furthermore, once governance is applied in the area of blockchains, legal problems are inevitable. In particular, the characteristics of blockchain governance have led to tensions between strict "on-chain" governance systems and possible "off-chain" governance applications [21]. Before *The DAO* attack, some lawyers expressed concerns about DAO programs, saying that DAOs have touched on legal issues related to security in several countries [22].

4.3.2.1 Fork and Culture for DAO

Interpreting fork culture based on *The DAO* hacker event, Tarasiewicz et al. [19] argue that a strong emphasis must be placed on interaction and communication between institutions and informal coding communities to further research and develop new blends of social and organizational structures.

4.3.2.2 Problems with DAOs Used in Corporate Governance

Agency theory is the dominant theory of governance conflicts among shareholders, company managers, and creditors, in which one party entrusts the work to the other party. The core agency conflict caused by the separation of ownership and control cannot be fully resolved under the existing theoretical and legal framework. Attempts to monitor agents are inevitably costly, and transaction costs are high.

Kaal et al. [23] point out that blockchain provides an unprecedented solution to the agency problem in corporate governance. DAO technology could help improve the agency relationship, but also proposed the potential of blockchain technology

Table 4.2 Governance problems and solutions

Categories	References	Recognition	Methodology
Fork	Tarasiewicz [19]	Fork and culture	The author interprets fork culture based on The DAO hacker event
Governance in company	Kaal [23]	Corporate governance	Problems with DAOs used in corporate governance
	Lafarre [24]	DAO in AGM	Problems with DAOs used in corporate governance (especially AGM)
Economy	Beck [25]	Blockchain economy	DAO could lead to blockchain economy
	Massacci [26]	Security and economics vulnerabilities	The failure of a security property, e.g., anonymity, can destroy a DAOs because economic attacks can be tailgated to security attacks
Law	Blemus [22]	Blockchain laws	This paper describes blockchain regulations discussed in the USA, EU, and major economic countries
	Reijers [21]	DAO in legal philosophy	This paper seeks to situate the blockchain discussion within the field of legal philosophy, examining how legal theory can apply in the context of blockchain governance
	Shakow [27]	DAO tax issues	This chapter explains how a decentralized autonomous organization operates and interacts with the US tax system

as an emerging technology of governance design, in which many ideal models and theoretical evaluations were limited by the real world. First of all, the blockchain is a fundamental technology, and its transformative impact will take decades rather than years to establish and reform system. In the corporate governance environment, the application of blockchain technology may develop in the existing centralized structure or decentralized environment. The former requires consensus on how and when to implement such technologies for governance use cases. For the latter, only when a true decentralized common blockchain emerges, with scalability and full security, can the proxy relationships be truly removed to overhaul them.

With the complexity of the agency relationship, human behavior in the agency relationship needs a backstop, namely, the continuous support of the human code. Without decentralized human support for code, the immutability of the blockchain and its cryptography security systems may not create true transactional guarantees and trust between principals and agents to maintain the integrity of their contractual relationships.

The blockchain-based corporate governance solution in DAO requires an incremental blockchain governance protocol. Thus, the socially optimal hard fork rule may not be applicable.

4.3.2.3 Problems with DAOs Used in AGM

The classic annual general meeting (AGM) has three functions for shareholders: information, forum, and decision-making. AGM also has important theoretical significance in the collective supervision of shareholders. However, AGM is often regarded as a dull and obligatory annual ceremony, and all three functions are actually eroded. For example, (almost) all information is often disclosed well before the AGM. In addition to expensive shareholder voting decisions, the decision-making function of the AGM also has static annual characteristics. Besides, the annual general meeting also has procedural defects. Especially when shareholders vote remotely, there is great uncertainty about whether the information between shareholders and the company (including shareholder voting records) is correctly communicated.

Lafarre et al. [24] therefore strongly call for the use of blockchain technology to modernize the AGM. Blockchain technology can significantly reduce the cost of shareholder voting and corporate organization. And it also can improve the speed of decision-making and promote the rapid and efficient participation of shareholders.

In calls for using blockchain technology to realize the modernization of the annual general meeting, however, at the same time, Lafarre et al. [24] also pointed out that it is important to realize the annual general meeting of shareholders based on blockchain will bring important legal issues. For example, whether it should abolish the physical classic AGM of shareholders, or let it coexist with the blockchain-based AGM? If it is desirable to organize a decentralized AGM only on the blockchain, how many forum functions are included in this technology? Record dates and notice periods must be reconsidered and the role of intermediaries in (cross-border) chains as well. More importantly, are shareholders and companies ready to participate in non-entity meetings? Recent evidence shows that even most institutional investors do not favor full virtualization.

4.3.2.4 Blockchain Economy's Rethink

Following the development of blockchain, the blockchain economy is on the rise and also needs new governance methods.

Blockchain and the smart contract supported by blockchain may give birth to a new economic system, which Beck et al. [25] call blockchain economy. The blockchain economy goes beyond the digital economy because agreed transactions are executed autonomously, by following rules defined in smart contracts, without the need for agency intervention or third-party approval. They can embed digital assets or tokens into digital representations of physical assets to enforce autonomous contract performance. The blockchain ensures that contracts are honored without being broken. It is in the new form of organization as DAO that the blockchain economy will manifest itself.

Beck et al. [25] explored a DAO case, Swarm City to explore the decision right, responsibility, and incentive mechanism related to governance. Decision rights involve controlling certain assets, which associate with accountability and incentives that motivate agents to take action. The authors used a novel IT governance framework to show that the emergence of the blockchain economy requires a rethink of governance. Compared with the digital economy, the location of decision-making power in the blockchain economy will be more decentralized. The accountability system in principle will be more and more established technically rather than institutionally, and the consistency of incentives will become more and more important.

Therefore, from the three governance dimensions, the authors proposed the governance research agenda in the blockchain economy in each dimension respectively. For example, in the aspect of decision rights, the research agenda includes (a) how to make decisions in the blockchain economy, (b) how to allocate decision management rights and decision control rights, (c) how to resolve decision-making differences in the blockchain economy, and (d) what is the role of ownership in the blockchain economy.

The work [25] has identified an important approach to governance research in the blockchain economy and provided a rich foundation for further theoretical work.

4.3.2.5 Security and Economy Vulnerabilities

Traditionally, security and economics functionalities in IT financial services and protocols (FinTech) have been separate goals. Only security vulnerabilities in security-critical systems that could be exploited by terrorists, criminals, or malicious government actors turned into security problems.

Massacci et al. [26] believe that security and economics are crucial issues for DAOs. *The DAO*'s hack is essentially a combination of a security vulnerability (recursive calls constantly extract coins from *The DAO*) and an economic attack (the user is only authorized to withdraw money the first time). In DAO futures exchange, on one hand, a failure of integrity could be dramatic for the agreement. On the other hand, if anonymity fails, futures exchange DAO may face economic attacks combining anonymity failure and price discrimination.

Failure of security attributes, such as anonymity, can destroy DAOs because economic attacks can be considered security attacks. The danger is not the vulnerabilities themselves, but the combination of an attack on software and an attack on the economy. Economic vulnerabilities, presumably, cannot be repaired, since the economic damage they may cause is unlikely to be reversed by pure technology such as forks. Thus for DAOs, economic vulnerabilities (security and economic vulnerabilities) are indeed the new "beast" to be ignored.

4.3.2.6 Infancy of Blockchain Laws

Blockchain has become a major topic for public policymakers around the world. As this disruptive and decentralized technology has become a key business issue for start-ups and market participants, central banks and financial regulators, particularly in the USA and EU, have shifted from initially intense hostility to a more cautious and market-friendly stance.

Blemus et al. [22] collected and compared regulatory trends in various applications or issues within the area of the USA, the European Union, and other key countries. These were supported by blockchain technologies, including Bitcoin/virtual currency/cryptocurrencies, smart contracts, decentralized autonomous organizations, initial coin offerings (ICO), and others. It mainly includes three supervision projects: (a) supervision of virtual currency, (b) supervision of ICO (and cryptocurrency), and (c) legal validity of blockchain technology and intelligent contract.

The conclusion shows that distributed ledger technology regulation is in its infancy. As of 2017, when the work [22] was published, uncertainty remains about the legal and economic qualifications of virtual currencies, tokens, ICOs, smart contracts, and distributed ledger technologies. Predictably, over time, the need for extensive research into blockchain technology will become less controversial.

4.3.2.7 Discussion of DAO in Legal Philosophy

Recently, the blockchain developer community has begun to turn its attention to governance issues. The governance of blockchain-based systems typically consists of various rules and procedures that can be implemented “on-chain” and “off-chain.” On-chain governance refers to the rules and decision processes that are directly encoded into the underlying infrastructure of blockchain-based systems. Off-chain governance includes all other rules and decision-making processes that may affect the operation and future development of blockchain-based systems. The characteristics of blockchain governance raise the issue of possible tensions between a strict “on-chain” governance system and possible “off-chain” governance applications.

Through investigations, Reijers et al. [21] believe that chain governance and Kelsen’s positivist concept of legal order [28] have a striking similarity. Blockchain-based systems become vulnerable when private interest groups use off-chain mechanisms to usurp governance systems on the chain. *The DAO* attack shows that while “code rules” can be formally followed in a specific chained order, in exceptional states, sovereignty is asserted through a chained mechanism.

As reflected in Kelsen’s argument, the combination of private interests is a weakness of positivist legal systems, and it can be assumed that this is an inherent weakness of governance on the chain of existing blockchain-based systems. Given these characteristics, future research could consider possible steps the blockchain community could take to address abnormal states in a manner consistent with their respective ideologies.

4.3.2.8 DAO Tax Issues

After *The DAO* hack, the Ethereum community voted to create a “hard fork” for the Ethereum chain, creating two Ethereum chains in the future. To add insult to injury, Securities and Exchange Commission (SEC) used this DAO to explain for the first time its view that some blockchain-related issuance would be considered securities subject to SEC regulation. The possibility of using smart contracts to allow entities to operate entirely autonomously on blockchain platforms seems attractive. It is not hard to see that these structures of DAO raise significant tax issues. However, little thought has been given to how such an entity would qualify for the tax system. Thus, Shakow et al. [27] explain how a decentralized autonomous organization operates and interacts with the US tax system by describing how a DAO works and raises the tax issues.

As a result, there is no evidence that DAOs have considered being subject to various requirements under the tax code. For those who want to comply, the easy solution is to use a site like Overstock.com. If they don’t, they may be penalized by the IRS. However, without international cooperation and innovation, it is difficult for tax administrators to find out who should tax a “DAO” income.

4.3.3 DAO Technologies and the Related Areas

It is nearly undeniable that DAO still has a certain trend across diverse sectors such as supply chain, business, healthcare, IoT, privacy, and data management [25, 29–31]. The emerging DAO is on the rise. The work of Beck et al. [25] and other papers have been discussed in the fields of blockchain economy, crowdfunding, accounting, and even electric cars and charging station billing systems. Especially, more than one study [25, 29] has found that in addition to e-government, the blockchain in the financial industry is also very promising (Table 4.3).

4.3.3.1 Corporate Governance on Ethereum’s Blockchain

Traditionally, principals have controlled the oversight tasks of their agents, which now can be delegated to decentralized computer networks, with the following advantages:

- Blockchain technology provides a formal guarantee for principals and agents involved in solving agency problems in corporate governance.

Table 4.3 DAO and related areas

Categories	References	Recognition	Methodology
Governance in company	Leonhard [32]	DAO corporation	A virtual DAO corporation with a corporate structure similar to the structure of a modern corporation
	Lumineau [33]	DAO corporation	DAO governance works differently than traditional contractual and relational governance
eGov DAO	Diallo [34]	DAO in e-government system	They provide a concrete use case to demonstrate the usage of DAO e-government and evaluate its effectiveness
	Jun [35]	DAO replacing existing social apparatuses and bureaucracy	Blockchain creating "absolute law" makes it possible to implement social technology that can replace existing social apparatuses including bureaucracy
Economy	Akgiray [36]	DAO tokens and money	The question of whether DAO tokens are money or not can be raised
	Zichichi [29]	Crowdfunding and DAO, LikeStarter	LikeStarter is structured as a DAO that fosters crowdfunding and recognizes the active role of donors, enabling them to support artists or projects while making profits
Accounting	Dai [30]	Blockchain in accounting profession	Blockchain has the potential to transform current auditing practices, resulting in a more precise and timely automatic assurance system
	Karajovic [37]	Blockchain in accounting profession	An analysis of the implications of blockchain technology in the accounting profession and its broader industry. Criticisms will be raised to address concerns regarding blockchain's widespread use
	Jeong [31]	Billing system	This paper proposes the blockchain-based billing system. The EV and the charging station store the billing information in the blockchain and prevent the modification
Voting	Zhang [38]	DAO in voting	This paper proposes a local voting mechanism based on blockchain

- Blockchain technology can facilitate the elimination of agents as intermediaries in corporate governance through code, peer-to-peer connectivity, groups, and collaboration.
- DAO token holders are not affected by the existing corporate hierarchy and its restrictive effect. DAO token holder focuses on adding value, which benefits all components.
- The "work value focus of workflow" in the DAO structure has the potential to reform the agency relationship.

DAO technology greatly contributes to improving the efficiency of agency relationships and reducing agency costs by an order of magnitude.

The purpose of Leonhard et al. [32] is to develop a virtual corporation with a corporate structure similar to the structure of a modern corporation. It offers a corporate governance structure where shareholders appoint the members of a board of directors, which then funds a Chief Executive Officer, who can then in turn pay salaries and acquire property on the corporation's behalf.

4.3.3.2 Blockchain Governance: A New Way of Organizing Collaborations?

Today, many companies are investing resources to develop and implement blockchain-based programs.

In traditional contract governance, the effectiveness of contract management cooperation depends on the quality of the national legal system to a large extent.

Conversely, DAO governance does not directly depend on the enforceability of external legal systems. Enforcement in a blockchain is achieved through prescribed code and algorithms, such as smart contracts. Even more, in governance, direct connections between collaborators are not required in a blockchain.

Thus, blockchain may be considered the first form of governance that truly leverages digital technology's computational- and data-based capabilities, well beyond traditional forms of social governance.

DAO, like other governance mechanisms, does not govern all types of transactions equally well.

Lumineau et al. [33] believe that DAO governance can reduce searching, monitoring, and enforcement costs but tends, but often means relatively high design costs.

4.3.3.3 eGov-DAO: A Better Government Using Blockchain-Based Decentralized Autonomous Organization

The e-government system has greatly improved the efficiency and transparency of the government's daily operations. However, most existing e-government services are provided centrally and rely heavily on individual control. Highly centralized IT infrastructures are more vulnerable to external attacks. Moreover, internal malicious users can easily compromise data integrity. In addition, relying on individuals to monitor some workflows makes the system error-prone and leaves room for corruption. In fact, both government and business services have been hacked multiple times, from ransomware to denial-of-service attacks. To address these challenges, Diallo et al. [34] report that blockchain technologies and decentralized autonomous organizations can improve e-government systems. The authors describe the high-level architecture of the government DAO and give the detailed design of a DAO e-government system. This is the first system to allow real-time monitoring and analysis of e-government services. The system retained all audit records, thereby limiting litigation between parties, increasing the speed of contract allocation and enforcement, and providing transparency, accountability, immutability, and better management of the national resources of the service. The evaluation of this system indicates that the government DAO system faces two main threats: data integrity and rule integrity. Besides, it can be found that modern government work does not require much delay. We can get conclusions that by implementing transparent and secure e-government systems at the lowest cost, eGov DAO's solution can help governments save unlimited resources, manage government businesses more effectively, and reduce the risk of providing contracts to companies that lack the capacity to deliver.

4.3.3.4 Blockchain Government: A Next Form of Infrastructure for the Twenty-First Century

Today, there are hundreds of blockchain projects around the world to transform government systems. There are signs that blockchain is a technology directly related to social organization. However, according to Jun et al. [35], there may be an epistemological rejection of the idea of blockchain-based automated systems replacing familiar public domains such as bureaucracy. Society must accept that such a shift is inevitable, and open discussion is needed to reduce the fear and side effects of introducing revolutionary new technologies. By applying Lawrence Lassig's "code is law" proposition, the authors of [35] suggested that five principles should be followed when replacing bureaucracy with a blockchain system: (a) introducing blockchain regulations; (b) transparent disclosure of data and source code; (c) implement independent executive management; (d) establish a governance system based on direct democracy; and (e) make distributed autonomous government. Jun et al. proposed a blockchain feature, which creates inviolable "absolute laws" and makes it possible to implement social technologies that can replace existing social institutions, including bureaucracy.

4.3.3.5 The Potential for Blockchain Technologies in Corporate Governance

Traditional platforms are rapidly becoming obsolete, and the trend is toward open platforms for financial services. Tech companies are starting to offer simple but disruptive financial services. In response, big financial firms are partnering with tech companies to maintain their market power.

Akgiray et al. [36] discuss the latest applications of blockchain technology in financial services and outlined regulatory responses. Economists consider money to have three basic functions: a medium of exchange, a unit of account, and a store of value. It is easy to imagine a variety of DAO tokens in the financial world, because transactions are expressed in real currencies or digital currencies (Alipay, Apple Pay, etc.) and real fiat money.

Therefore, Akgiray et al. [36] argue, if the tokens on the DAO can fulfill the three functions of money, then the question of whether it is money or not can be raised.

4.3.3.6 LikeStarter: A Smart Contract-Based Social DAO for Crowdfunding

Social media platforms are recognized as important media for the global transmission and dissemination of information. The combination of social interaction and crowdfunding represents a powerful symbiotic relationship. On the other hand, blockchain technology has revolutionized the way we think about the Internet. So Zichichi et al. [29] introduced LikeStarter, a social network where users can raise money for other users through simple "like" on the Ethereum blockchain. LikeStarter is built on the Ethereum blockchain, structured as a DAO that promotes crowdfunding without any central agency intervention and uses smart contracts to control and manage money. Zichichi et al. [29] have used a case study to show that LikeStarter successfully makes it easy for people to get funding and reach as many people as possible.

4.3.3.7 Toward Blockchain-Based Accounting and Assurance

Since 2009, blockchain has become a potentially transformative information technology that promises to be as revolutionary as the Internet. Accounting and insurance could be one of the industries where blockchain could bring huge benefits and fundamentally change the current model. However, the potential benefits and challenges that blockchain could bring to accounting and assurance remain to be explored.

For this reason, Dai et al. [30] proposed an accounting and assurance method (an accounting ecosystem that supports blockchain, real-time, verifiable, and transparent) based on the reference of multiple disciplines and ideas of the accounting industry. This method will provide real-time, verifiable information disclosure and step-by-step automation. As a result, blockchain can be used as a tool to verify any information related to auditing. However, it is worth pondering how to adapt the existing blockchain mechanism to the field of accounting and auditing. The insights of Dai et al. [30] will help integrate blockchain into the existing business processes and facilitate the transformation of the current audit model to the next generation.

4.3.3.8 Thinking Outside the Block: Projected Phases of Blockchain Integration in the Accounting Industry

The rapid growth of blockchain has sparked curiosity across the industry, leading to talks about setting up a blockchain consortium in accounting. Accountancy firms such as PwC, Deloitte, EY, and KPMG have pledged to integrate blockchain into their financial services. Innovative products such as Vulcan (for managing digital assets), Rubix (for improving supply change management), editable blockchain, and blockchain as a service are among there. Karajovic et al. [37] conducted an in-depth and detailed analysis of the application of blockchain technology in the accounting profession. As block linking becomes more mainstream, the technique can be used to simplify many redundant and vulnerable accounting practices. While the initial cost of developing and integrating blockchain infrastructure can be high, this can be offset by the cost savings it brings to the enterprise in terms of long-term, improved efficiency. Karajovic et al.'s philosophical analysis of the technology's application illustrates many questions about the uncertain relationship between accounting and blockchain. While the technology has the potential to reshape entire capital markets, the social and political barriers to blockchain proliferation need to be looked at critically. But one thing is certain: accounting is just one block in the chain that is being dramatically redefined by this disruptive technology.

4.3.3.9 Blockchain-Based Billing System for Electric Vehicle and Charging Station

DAO can also be used in the charging system. The charging results measured in the charging electric vehicles may differ from the amount claimed in the charging station. This is because electric vehicles and charging station measure the charge amount with their own measurement equipment. If the electric vehicles or charging station provide fault information, the billing may be invalid. In addition, billing information can be manipulated. To prevent these problems, Jeong et al. [31] proposed a blockchain-based billing system. After mutual authentication, electric cars and charging stations both store billing information in the blockchain. A DAO is a system where all nodes have the same ledger; thus the ledger data cannot tamper. Jeong et al. have shown that the system prevents users from modifying their records after electric vehicles have been charged.

4.3.3.10 A Privacy-Preserving Voting Protocol on Blockchains

Voting is a universal phenomenon and to some extent is part of various societies. As the technology matures and more voting is expected in the future, there is an urgent need for a local voting mechanism built directly on the blockchain network to decentralize and dis-intermediate the network. Zhang et al. [38] argue that the need for this voting mechanism is not limited to public blockchain networks, but also applies to syndicate-licensed blockchain networks.

In this regard, the authors categorized and summarized existing voting systems and proposed a local voting mechanism based on blockchain to facilitate the decision-making of nodes in the blockchain network. The core idea is (a) distribution voting, (b) distributed tally, and (c) cryptography-based verification. The implementation of the Hyperledger structure shows that the protocol is feasible for small- and medium-sized voting issues. The agreement protects the privacy of voters and allows for the detection and correction of cheating without any credible parties.

4.4 Open Issues

According to Diallo et al. [34], we can see that although The DAO project was abolished, the future of Ethereum is bright. In the future, research on DAO can start from the following aspects. To help gain a quick clue, we propose several questions here.

Based on the system design of the blockchain itself, the first question is how to optimize and handle the performance trilemma, i.e., decentralization, security, and scalability, in a balanced way in the context of DAO. Second, a better blockchain system and the evaluation tool of blockchain security-enhancement solutions are anticipated for DAO. Furthermore, the feasibility of those blockchain systems and evaluation tools needs to be assessed, because governance is possible only if the benefits of efficiency, security, and privacy of DAO exceed the social costs. Thus, another question is how to reduce the social costs such that the feasibility of DAO can be improved.

From the operation perspective of DAO, we have the following concerns:

- Only depending on the social-optimal hard-fork rule is not applicable. The corporate governance solution based on DAO needs to propose new protocols for blockchain governance.
- Leveraging DAO, it is necessary to create the trust of real transactions, thus maintaining the integrity of its contractual relationship.
- While “code rules” can be formally followed on a particular chain. In exceptional states, sovereignty is asserted through an off-chain mechanism. This requires the study of possible actions, which are taken by the blockchain community to address anomalies in ways that are consistent with their respective ideologies.

- Legal issues related to DAOs need to be taken into account, such as how an entity should comply with the tax system.
- Researchers need to explore the ultimate impact of DAO on human beings. The most powerful blockchain applications are likely to exacerbate inequality. Both researchers and engineers shall think about how to avoid and solve this issue.

All of the mentioned concerns require a strong emphasis on interaction and communication between institutions and informal coding communities; thus it can help further research and develop new integration of social and organizational structures.

Currently, people are still maintaining high expectations of DAO. Governments around the world are betting that it will change the way they govern [39]. For example, Dubai [40] has stored all government documents in the blockchains by 2020. Other governments are studying its potential applicability in central banking, electronic voting, identity management, and registry management. Blockchain transforms government operations to inspire new service delivery models for governments [41].

DAO is believed to have many advantages over existing solutions for the future Web3 ecosystem. With incredible development pace of Ethereum [42] and its Layer2 ecosystem, the platform that can support a large scale of decentralized applications is becoming mature [43]. In the infancy stage of DAO, smart contracts are bound to cause vulnerabilities like *The DAO* attack, which will lead to better code-checking mechanisms and secure coding practices for DAOs to avoid such pitfalls. In the future, not only may it be possible to establish full-fledged DAOs in multiple fields, but it is also very likely to establish a unified single currency platform leveraging the technologies of DAO.

4.5 Conclusion

DAO is viewed as a very promising paradigm for decentralized organizations, especially in the era of Web3. This chapter reviews the most recent research activities on both academic and engineering perspectives, which basically include the governance issues and typical DAO technologies. We hope that this chapter can help researchers and engineers identify the significance of blockchain-based DAO.

References

1. V. Dhillon, D. Metcalf, and M. Hooper, “The DAO hacked,” in *Blockchain Enabled Applications*. Springer, 2017, pp. 67–78.
2. F. Casino, T. K. Dasaklis, and C. Patsakis, “A systematic literature review of blockchain-based applications: current status, classification and open issues,” *Telematics and Informatics*, vol. 36, pp. 55–81, 2019.

3. V. Buterin *et al.*, “Ethereum white paper: a next generation smart contract & decentralized application platform,” *First version*, vol. 53, 2014.
4. G. Wood *et al.*, “Ethereum: A secure decentralised generalised transaction ledger,” *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.
5. P. Nobels, “Building the Lisk DAO project,” https://lisk.io/blog/apps/building-lisk-dao-project.
6. “Aragon,” Accessed on 2020. [Online]. Available: https://aragon.org/
7. “Colony,” 2020. [Online]. Available: https://colony.io/
8. “DAOstack,” 2020. [Online]. Available: https://daostack.io/
9. F. Santos and V. Kostakis, “The DAO: a million dollar lesson in blockchain governance,” *School of Business and Governance, Ragnar Nurkse Department of Innovation and Governance*, 2018.
10. H. Chen, M. Pendleton, L. Njilla, and S. Xu, “A survey on ethereum systems security: Vulnerabilities, attacks, and defenses,” *ACM Computing Surveys (CSUR)*, vol. 53, no. 3, pp. 1–43, 2020.
11. U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, “A brief survey of cryptocurrency systems,” in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, 2016, pp. 745–752.
12. M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, “A survey on security and privacy issues of bitcoin,” *IEEE Communications Surveys Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.
13. X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems,” *Future Generation Computer Systems*, 2017.
14. S. Manski, “Building the blockchain world: Technological commonwealth or just more of the same?” *Strategic Change*, vol. 26, no. 5, pp. 511–522, 2017.
15. Q. Zhou, H. Huang, Z. Zheng, and J. Bian, “Solutions to scalability of blockchain: A survey,” *IEEE Access*, vol. 8, pp. 16 440–16 455, 2020.
16. L. M. of Public Administration Capstone Team. [Online]. Available: https://www.centreforpublicimpact.org/building-on-blockchain/
17. Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, “An overview on smart contracts: Challenges, advances and platforms,” *Future Generation Computer Systems*, vol. 105, pp. 475–491, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X19316280
18. H. Huang, W. Kong, S. Zhou, Z. Zheng, and S. Guo, “A survey of state-of-the-art on blockchains: Theories, modelings, and tools,” *ACM Comput. Surv.*, vol. 54, no. 2, Mar. 2021. [Online]. Available: https://doi.org/10.1145/3441692
19. M. Tarasiewicz, “Forking as cultural practice: Institutional governance after the DAO.”
20. Q. DuPont, “Experiments in algorithmic governance: A history and ethnography of “the DAO,” a failed decentralized autonomous organization,” in *Bitcoin and Beyond (Open Access)*. Routledge, 2017, pp. 157–177.
21. W. Reijers, I. Wuisman, M. Mannan, P. De Filippi, C. Wray, V. Rae-Looi, A. C. Vélez, and L. Orgad, “Now the code runs itself: On-chain and off-chain governance of blockchain technologies,” *Topoi*, pp. 1–11, 2018.
22. S. Blemus, “Law and blockchain: A legal perspective on current regulatory trends worldwide,” *Revue Trimestrielle de Droit Financier (Corporate Finance and Capital Markets Law Review) RTDF*, no. 4-2017, 2017.
23. W. A. Kaal, “Blockchain solutions for agency problems in corporate governance,” *ECONOMIC INFORMATION TO FACILITATE DECISION MAKING, EDITED BOOK, EDITOR-KASHI R. BALACHANDRAN, WORLD SCIENTIFIC PUBLISHERS (2019)*, 2019.
24. A. Lafarre and C. Van der Elst, “Blockchain technology for corporate governance and shareholder activism,” *European Corporate Governance Institute (ECGI)-Law Working Paper*, no. 390, 2018.
25. R. Beck, C. Müller-Bloch, and J. L. King, “Governance in the blockchain economy: A framework and research agenda,” *Journal of the Association for Information Systems*, vol. 19, no. 10, p. 1, 2018.

26. F. Massacci, C. N. Ngo, J. Nie, D. Venturi, and J. Williams, “The seconomics (security-economics) vulnerabilities of decentralized autonomous organizations,” in *Cambridge International Workshop on Security Protocols*. Springer, 2017, pp. 171–179.
27. D. J. Shakow, “The tao of the DAO: Taxing an entity that lives on a blockchain,” *Tax Notes*, vol. 160, pp. 18–23, 2018.
28. M. P. Golding, “Kelsen and the concept of “legal system” 1,” *Archiv für Rechts-und Sozialphilosophie*, vol. 47, pp. 355–386, 1961.
29. M. Zichichi, M. Contu, S. Ferretti, and G. D’Angelo, “Likestarter: a smart-contract based social DAO for crowdfunding,” in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2019, pp. 313–318.
30. J. Dai and M. A. Vasarhelyi, “Toward blockchain-based accounting and assurance,” *Journal of Information Systems*, vol. 31, no. 3, pp. 5–21, 2017.
31. S. Jeong, N.-N. Dao, Y. Lee, C. Lee, and S. Cho, “Blockchain based billing system for electric vehicle and charging station,” in *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*. IEEE, 2018, pp. 308–310.
32. R. Leonhard, “Corporate governance on ethereum’s blockchain,” *Available at SSRN 2977522*, 2017.
33. F. Lumineau, W. Wang, and O. Schilke, “Blockchain governance–a new way of organizing collaborations?” *Organization Science*, 2020.
34. N. Diallo, W. Shi, L. Xu, Z. Gao, L. Chen, Y. Lu, N. Shah, L. Carranco, T.-C. Le, A. B. Surez *et al.*, “eGov-DAO: A better government using blockchain based decentralized autonomous organization,” in *2018 International Conference on eDemocracy & eGovernment (ICEDEG)*. IEEE, 2018, pp. 166–171.
35. M. Jun, “Blockchain government-a next form of infrastructure for the twenty-first century,” *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 4, no. 1, p. 7, 2018.
36. V. Akgiray, “The potential for blockchain technology in corporate governance,” 2019.
37. M. Karajovic, H. M. Kim, and M. Laskowski, “Thinking outside the block: Projected phases of blockchain integration in the accounting industry,” *Australian Accounting Review*, vol. 29, no. 2, pp. 319–330, 2019.
38. W. Zhang, Y. Yuan, Y. Hu, S. Huang, S. Cao, A. Chopra, and S. Huang, “A privacy-preserving voting protocol on blockchain,” in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. IEEE, 2018, pp. 401–408.
39. A. Alketbi, Q. Nasir, and M. A. Talib, “Blockchain for government services—use cases, security benefits and challenges,” in *2018 15th Learning and Technology Conference (L T)*, 2018, pp. 112–119.
40. C. Whiteoak, “Smart Dubai close to rolling out 20 blockchain-based services,” https://www.thenational.ae/business/smart-dubai-close-to-rolling-out-20-blockchain-based-services-1.695280.
41. A. Alketbi, Q. Nasir, and M. A. Talib, “Novel blockchain reference model for government services: Dubai government case study,” *International Journal of System Assurance Engineering and Management*, pp. 1–22, 2020.
42. D. Vujičić, D. Jagodić, and S. Ranđić, “Blockchain technology, bitcoin, and ethereum: A brief overview,” in *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*, 2018, pp. 1–6.
43. K. Jones, “Blockchain in or as governance? evolutions in experimentation, social impacts, and prefigurative practice in the blockchain and DAO space,” *Information Polity*, no. Preprint, pp. 1–18, 2019.

Chapter 5
How Economic Systems Enable Metaverse: Value Circulation in Metaverse via Web3

Huawei Huang, Qinnan Zhang, Taotao Li, Qinglin Yang, Xiaofei Luo, Zhaokang Yin, Junhao Wu, Jianming Zhu, Jiajing Wu, and Zibin Zheng

Abstract Economic systems play pivotal roles in the metaverse. However, we have not yet found an overview that systematically introduces economic systems for the metaverse. Therefore, we review the state-of-the-art solutions, architectures, and systems related to economic systems. When investigating those state-of-the-art studies, we keep two questions in our mind: (1) what is the framework of economic systems in the context of the metaverse? (2) What activities would economic systems engage in the metaverse? This chapter aims to disclose insights into the economic systems that work for both the current and the future metaverse. To have a clear overview of the economic system framework, we mainly discuss the connections among three fundamental elements in the metaverse, i.e., digital creation, digital assets, and the digital trading market. After that, we elaborate on each fundamental technology of the economic system for metaverse. Those technologies include incentive mechanisms, monetary systems, digital wallets, decentralized finance (DeFi), and cross-platform interoperability for the metaverse. For each technology, we mainly discuss three topics: (a) the rationale of this topic, (b) why the metaverse needs this technology, and (c) how this technology will evolve in metaverse. Through this chapter, we wish readers can better understand what economic systems the metaverse needs and the insights behind the economic activities in metaverse.

Keywords Metaverse · Economic systems · Blockchain · Value circulation · Non-fungible tokens · Incentive mechanisms · Decentralized exchange · Monetary systems

H. Huang · T. Li · Q. Yang · X. Luo · Z. Yin · J. Wu · J. Wu · Z. Zheng (✉)
School of Software Engineering, Sun Yat-sen University, Zhuhai, Guangdong, China
e-mail: huanghw28@mail.sysu.edu.cn; litt93@mail.sysu.edu.cn; yangqlin6@mail.sysu.edu.cn; wujiajing@mail.sysu.edu.cn; zhzibin@mail.sysu.edu.cn

Q. Zhang · J. Zhu
School of Information, Central University of Finance and Economics, Beijing, China
e-mail: zhangqnp@163.com; zjm@cufe.edu.cn

H. Huang et al. (eds.), *From Blockchain to Web3 & Metaverse*,
https://doi.org/10.1007/978-981-99-3648-9_5

5.1 Introduction

Metaverse has seized enormous attention from both academia and industries. Existing technologies that are enabling metaverse can be briefly classified into two categories, i.e., (a) *how to build the metaverse* and (b) *how to enter into and how experience the metaverse*. For the former category, technologies include digital twins, games, three-dimensional (3D) rendering, artificial intelligence (AI) algorithms, etc. As for the latter one, the related technologies involve interactivity technologies such as virtual reality (VR), augmented reality (AR), mixed reality (MR), human-computer interfaces, etc.

In addition to those two categories, metaverse also requires support from the bottom-layer infrastructures [1], including networking and computing, dedicated operating systems, and blockchains. First, networking and computational resources enable high-bandwidth and low-latency immersive experiences for metaverse users. Second, operating systems provide the system-level execution environment for the applications (apps) of metaverse. Third, blockchains can handle the high-volume transactions submitted by metaverse users when they are using metaverse apps.

The metaverse is not a virtual world that is independent of the real world; it is the extension of the physical world. Both worlds merge together to create an integrated ecosystem [2]. In this chapter, we concentrate on blockchain-based economic systems in the context of the metaverse. As shown in Fig. 5.1, we present our overview of the economic systems that are promising to enable any possible economic activities and issues in both the current and future metaverse.

Since Bitcoin [3], blockchains have been exploited to implement economic systems for various sectors, including decentralized finance (DeFi), cryptocurren-

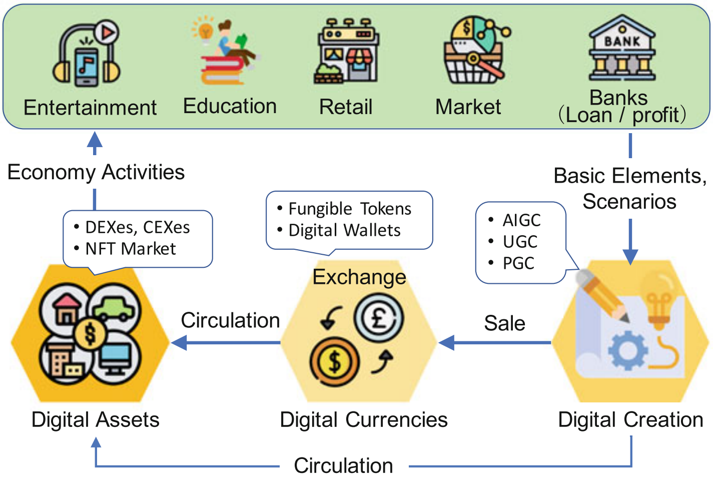


Fig. 5.1 Framework of economic systems for the metaverse

cies, non-fungible tokens (NFT), the trading platforms of digital assets, exchanges, etc. In the future, the metaverse will be a virtual living habitat for humans; all users create a complete supply chain to produce and consume digital content collaboratively. In order to protect the ownership of digital products, the owners need to control and track their circulation process. Blockchain, as the feasible decentralized infrastructure of Web 3.0, enables users to trade digital assets with the property of transparency and traceability. What's more, smart contracts enable programmability and automated execution of transactions. By minting digital products into NFT, all stakeholders can control the ownership of digital products and share the economic value of the metaverse. Encouraged by sharing economics, a large number of digital products are generated by users in a decentralized approach. The associated economic activities imply that the blockchain will play a crucial role in the economic systems of the future metaverse.

Although the economic systems existing in the current physical world have been deeply developed, we are wondering the question what economic systems should look like in both the current and the future metaverse. The reason why we are curious about this question is that we think the economic systems are the foundation of metaverse. Almost every activity that occurs in metaverse is related to the economy. In the virtual world of metaverse, the economic systems need to handle economic activities that are severely different from those in the real world [4]. It indicates that the real-world economic systems will not be applicable to the virtual-world economic environment in metaverse. However, we have not yet found a survey article that systematically discusses such a topic. To fill this gap, we are motivated to conduct this overview of economic systems and wish to contribute some viewpoints, thoughts, and insights to the communities of the metaverse.

The organization of this chapter is described as follows. Section 5.2 depicts the preliminaries of economic systems in the metaverse. Section 5.4 explores the role of monetary systems for the metaverse. Section 5.3 talks about the incentive mechanisms for the metaverse. Section 5.5 discusses the typical economic activities such as DeFi in the metaverse. Section 5.6 shows the insights of the cross-metaverse interoperability for the metaverse. Section 5.7 discusses the challenges of open issues of economic systems in the metaverse. Finally, Sect. 5.8 concludes this chapter.

5.2 Preliminaries of Economic Systems in Metaverse

5.2.1 Virtual-Real Interactions for Metaverse

We first show an overview using Fig. 5.2, in which the virtual-reality interactions are demonstrated between the real-world objects and those in the metaverse. In the real-world layer, the objects include users, smart devices such as AR/VR/MR that help users enter into the metaverse, service providers, etc. In the metaverse layer,

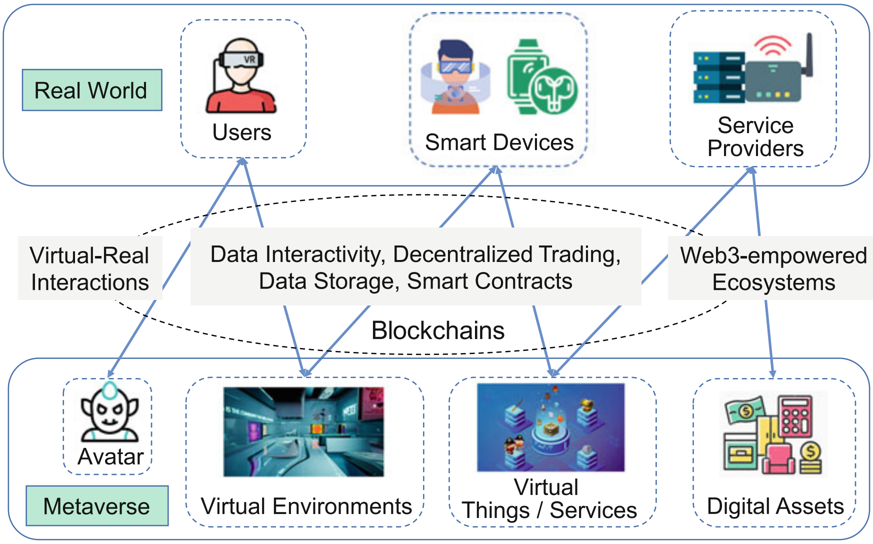

Real World
Users
Smart Devices
Service Providers
Virtual-Real Interactions
Data Interactivity, Decentralized Trading, Data Storage, Smart Contracts
Web3-empowered Ecosystems
Blockchains
Avatar
Metaverse
Virtual Environments
Virtual Things / Services
Digital Assets

Fig. 5.2 Virtual-real interactions between the physical world and metaverse

related objects include virtual things, virtual services, virtual environments, digital assets, etc. We then summarize all essential interactivity between those two layers as follows.

- Users and their avatars need blockchain-based services to have virtual-reality interactions.
- Users and their smart devices require data storage services, data interactivity applications, and trading systems, to interact with the virtual objects, virtual services, and virtual environments in the metaverse.
- Users manage their digital assets through the smart contract-enabled Web3 ecosystem.

5.2.2 *Technology Companies Investing in Metaverse*

Metaverse provides an interconnected virtual community that is changing social media and video game platforms. People interact in metaverse by using VR headphones, AR glasses, and the associated applications. Users can try on clothes, hang out in the virtual community, or even work in their virtual offices [5].

Some of the top technology companies are involved in the metaverse. Meta (previously Facebook) plans on developing an engaging and immersive social-interaction experience in the metaverse. Meta has launched a meeting software called Horizon Workrooms with the use of Oculus VR headsets. Nvidia designs and manufactures hardware for creating and supporting Web3 applications. Nvidia's Omniverse helps Web3 developers create projects in their metaverse [6].

Video game companies are also playing a leading role. Epic Games raised $1 billion for the long-term construction of the metaverse. The game platform Roblox [7] describes its blueprint for the metaverse, in which people can learn, work, play, create, and socialize together in millions of 3D experiences [8].

5.2.3 Digital Assets in the Metaverse

Van Niekerk [9] clearly defines the digital asset as "any item of text or medium that has been formatted into a binary source that includes the right to use it." From this perspective, the concept of *the digital asset* was born not due to the driving power of Internet technologies but due to the power of the *digital citizenry* concept coming to life [10].

Digital assets are the engine to drive the continued development of the economic system of the metaverse. The aim of this subsection is to introduce typical digital assets and the way how to create them in the metaverse.

5.2.3.1 Non-fungible Tokens (NFT)

NFT is a typical category of digital assets based on blockchains. NFTs ensure the uniqueness of digital assets by permanently storing historical encrypted transactions on the associated blockchain [11].

As a blockchain-based digital token as a proof of ownership and authenticity for crypto assets, NFT offers a futuristic possibility for art trading [12]. For instance, Minecraft [13] has a complicated economic system that allows players to accumulate online Axie Infinity [14], which is an NFT-driven game built on Ethereum. NFT can tokenize multiple types of digital assets like art, music, collectibles, video, and in-game items to guarantee uniqueness and authentication [15]. NFT plays an important role in determining authentic rights for metaverse assets [16]. Specifically, users can store their digital assets as NFT on blockchains and trade digital assets through smart contracts.

NFTs have strong cultural and interactive attributes. If a user purchases an NFT, he/she will be the only owner in the world to hold and prove that asset. Such a purchase behavior has strong social significance, by which consumers can demonstrate their unique purchasing ability, taste, and even social status in the digital field. Therefore, the recognition of the value and ownership of NFT on the basis of the technical blockchain requires a rich social activity and the consensus of a certain number of participants. NFT has everything to do with digital collections that realize the asset of virtual productions so that digital assets have tradeable entities.

The cost of minting an NFT includes the gas fee, account fee, and service fee. The gas fee is used to pay for dealing with the transaction on blockchains. Account fee means a small fee that a platform charges users to place their products on its platform. In basic finance, service fee denotes the fee that auctioneers, salespeople, and others are paid a commission for their services. A flat commission is charged to the seller.

5.2.4 Trading and Market of Digital Assets in Metaverse

The digital market includes all exchange activities of products and services that rely on Internet-based digital technologies. This market is composed of digitizing traditional products and services, such as e-commerce and online marketplaces that simply move offline transactions directly online. At the microlevel of the economic system for the metaverse, clients are the foundation of economic activities, working as both producers and consumers of user-generated content [17].

Meanwhile, as depicted in Figs. 5.3 and 5.4, the exchange is an intermediary bridging production and consumption. Compared with Fig. 5.3, we can find that the metaverse economy is powered by blockchain and cryptocurrency technologies. As shown in Fig. 5.4, this new fashion of economy differs from the traditional financial system. The decentralized metaverse economy provides financial products to users without involving intermediaries such as banks, brokerages, or insurance companies.

For trading digital assets, Hasan et al. [18] emphasize that proof of delivery (PoD) of the digital content is an immense need since these assets are subject to payment. To support the requirement of immutable and tamper-proof logs, accountability, and traceability, the authors propose a decentralized PoD by leveraging major features of blockchain and Ethereum smart contracts. Blockchains before Ethereum, such as Bitcoin, only support token transferring. Until the emergence of Ethereum, smart contracts begin to support Turing-complete programming. Complicated businesses could be executed in a virtual machine through smart contract codes. Ethereum

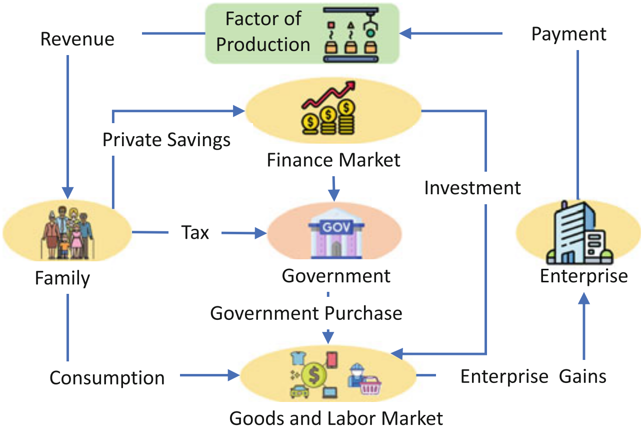


Fig. 5.3 Macroeconomic circulation in physical world

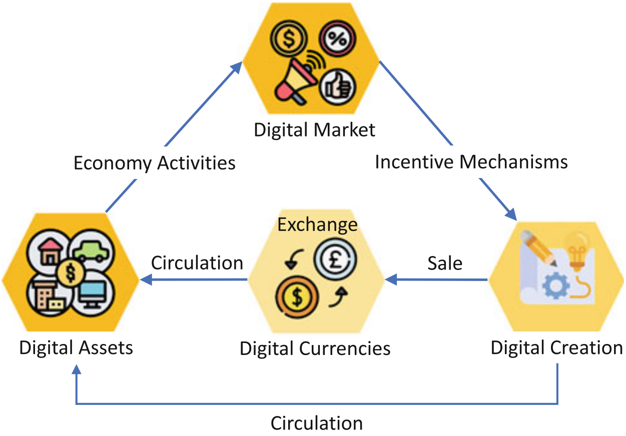


Fig. 5.4 Currency circulation in metaverse

realizes the upgrade of blockchain applications from cryptocurrency to crypto business.

Based on smart contracts and crypto tokens, decentralized finance (DeFi) offers a new approach to innovate economic models in the metaverse. Empowered by such advanced blockchain technologies, DeFi can boost the decentralized market and business in the metaverse. Existing successful solutions, such as Uniswap [19], a decentralized exchange (DEX) implemented on Ethereum, automatically provide users with liquidity for their metaverse tokens. We review a representative study related to the DeFi market and business here. More discussion can be found in Sect. 5.5. In [20], the authors analyze the behavior of arbitrage bots in the context of the cryptocurrency market. They find that arbitrage robots could observe the transactions in the transaction pool and perform arbitrage without risks. They also present a cooperative strategy to maximize the profit of arbitrage robots and point out that miners could act as arbitrage robots under certain circumstances. However, the miner extractable value (MEV) could incentivize the emergence of forking attacks. The authors propose a cooperative bidding strategy for them to strive for more profit. They also find that the current amount of MEV in a month is more than 25× the cost of a 51% attack on Ethereum.

5.3 Incentive Mechanisms for Metaverse

5.3.1 The Role of Incentive Mechanisms in Metaverse

The economic system established by metaverse users has become a promising topic for driving innovations toward the metaverse. Users, as essential stakeholders,

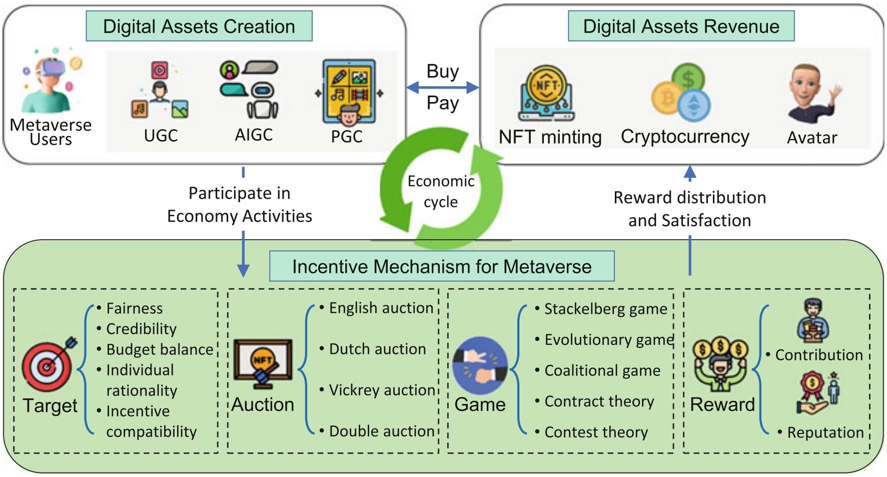


Fig. 5.5 Incentive mechanisms for metaverse

contribute resources and data to create a virtual world, where users own a large number of digital assets. In this regard, incentive mechanisms need to be designed to subsidize the contribution of users and encourage all stakeholders to benefit from the metaverse economic system. The economic cycle of digital assets is supported by incentive mechanisms as shown in Fig. 5.5. Metaverse users can generate a great number of digital content (i.e., UGC, AIGC, PGC) independently or with AI assistance. Users participate in economic activities (e.g., creation, exchange, and investment) to get some revenue. The incentive mechanism is responsible for the reward allocation fairly to support the metaverse economic system.

Without a series of reasonable incentive mechanisms, it is obvious that users are unwilling to contribute computation and data resources to participate in metaverse service computation tasks under the risk of privacy disclosure.

5.3.2 Design Target of Incentive Mechanisms

The design target of incentive mechanisms is to motivate more high-quality contributions through various forms of extrinsic rewards to meet the personal needs of contributors. Therefore, in order to make the incentive mechanism work continuously and effectively, the following properties should be considered.

- *Fairness*: Fairness may dramatically affect the optimal results of incentive mechanism [21]. The fairness of reward distribution determines the sustainability of the incentive mechanism. Han et al. [22] design a fairness-aware incentive based on the interest of data owners, which provides three fairness criteria, namely, contribution, regret distribution, and expectation. Existing works focus on the fairness of incentive mechanisms to prevent free-rider behavior, which refers to participants trying to earn income, but no contribution [23–27].

- *Credibility*: The credibility of the optimal strategy directly affects the execution effect of the incentive mechanism. Martín-Herrán et al. [28] characterize the credibility of incentive equilibrium strategies with linear-state games. BESIFL [29] is a blockchain-empowered decentralized federated learning paradigm. Blockchain is adopted to achieve malicious node detection and incentive management. Some existing truthful incentive mechanisms are designed to motivate users to devote resources to collaborative computation and offloading [30–33].
- *Budget Balance*: The incentive mechanism satisfies budget balance if and only if the payment of buyers is non-negative and the whole system does not need investments from another third party [34]. In other words, the summation of the money transfer between all parties is zero [35]. An auction satisfies the budget balance if and only if the payment collected from all buyers is at least as large as the payment to the sellers [36].
- *Individual Rationality (IR)*: The incentive mechanism satisfies IR if and only if the revenues of all participants are non-negative [37]. In the metaverse, rational resource pricing can improve the quality of the immersive experience of users, where users purchase bandwidth resources to reduce the communication latency of services, and metaverse service providers decide the price of the resource to achieve individual rationality.
- *Incentive Compatibility (IC)*: The incentive mechanism that satisfies IC is expressed as γ-truthfulness [38]. The reward information submitted by the platform is based on the evaluation of contributors' task value, while the contribution information submitted by contributors is calculated by their resource consumption. Bayesian incentive compatibility, efficiency, and budget balance of the standard Arrow-d'Aspremont-Gerard-Varet (AGV) mechanism [39] have been reviewed. Moreover, Ma et al. [40] propose an enhanced AGV mechanism to achieve IC, IR, and budget balance.

Most of the existing incentive mechanisms toward the metaverse ecosystem are designed based on economic theories, including auction mechanisms, game theory-based strategy optimization, reward systems, and reputation mechanisms. The existing representative incentive solutions are reviewed in the following subsections.

5.3.3 Auction Mechanisms

Auction has been regarded as a promising solution [41] to design incentive mechanisms. In the metaverse, auction mechanisms can assist buyers in bidding on the valuation of digital content to achieve an efficient circulation of digital assets. However, the heterogeneity of digital assets and the potential risk of privacy disclosure may lead to an unsustainable auction market and some issues, such as the winner's curse [42] and unfair bids [43]. There are some existing researches

Table 5.1 Auction mechanisms and representative examples

Auction name	Description	Examples
English auction	The classical public sale method, bidding starts from the lowest price	Jiao et al. [44], Zhang et al.[45]
Dutch auction	Reversing to the English auction, bidding starts from the highest price	Fan et al. [46], Xu et al. [47]
Vickrey auction	Also known as the sealed second-price auction, the final price is the second-highest bid	EPViSA [48], Zhang et al. [49], Luong et al. [50]
Double auction	Multiple buyers and sellers offer bids, and the final price is decided by matching the bids in a certain order	Ng et al. [51], Kim et al. [52], Wang et al. [53], Liew et al. [54]

that focus on designing more efficient auction mechanisms to motivate users to participate in metaverse economic activities. The existing auction mechanism can be classified into the following categories as described in Table 5.1

In metaverse services, the seamless, immersive, and interactive user experience need to rely on real-time data synchronization between multiple physical entities. Jiao et al. [44] propose a classical auction-based resource allocation mechanism for the edge computing service provider to maximize social welfare while achieving credibility, computational efficiency, and individual rationality. Fan et al. [46] develop a resource trading platform based on a hybrid blockchain, in which a reverse auction mechanism is executed automatically by a blockchain-based smart contract. In order to further improve the virtual driving experience, it’s essential to design an effective allocation mechanism for synchronizing real-time data from autonomous vehicles to roadside units (RSUs). To this end, EPViSA [48] is an enhanced second-score auction-based data synchronization scheme where the physical and virtual entities can synchronize data and resource in the vehicle-metaverse service market. The trading rule of the second-score auction belongs to a two-dimensional analog of the Vickrey auction. When utilizing digital twins to construct a virtual, there remains limited research on how to allocate station resources. Zhang et al. [49] solve the problem of the optimal resource allocation in the wireless channel. Payment rule based on the Vickrey Clarke Groves (VCG) auction is adopted to decide the payment rule of resources to maximize social welfare. Moreover, existing researches show that the double auction in resource allocation can achieve preferable economic properties. Ng et al. [51] adopt the double auction to assist in the resource allocation of the edge servers and determine the prices of resources to complete the coded distributed computing tasks.

Deep learning has proven effective in optimizing the auction mechanism. Luong et al. [50] optimize the auction for edge resource allocation by a multilayer neural network, which confirms the advantage that deriving high revenue auction using deep learning. Xu et al. [47] propose a double dutch auction-based incentive mechanism for VR service of the metaverse, in which deep reinforcement learning (DRL) is adopted to determine optimal pricing strategies and allocation rules of

VR services. Kim et al. [52] formulate the rule of data resource trading between IoT service providers and edge devices by McAfee double auction, in which a Q-learning algorithm is leveraged to evaluate the power level of edge devices. Liew et al. [54] adopt deep learning and double auction to address the energy allocation for IoT devices, in which the revenue of semantic service providers can be maximized. Through the combination of auction and learning algorithms, the interaction of system agents can be modeled and optimal to achieve the balance of the metaverse market.

Some researchers have paid attention to the privacy-disclosure problem in the auction mechanism. For instance, Zhang et al. [45] propose a privacy-preserving auction mechanism for data aggregation in mobile crowdsensing tasks, where the platform as auctioneer recruits workers to complete sensing tasks. Wang et al. [53] proposed a privacy-preserving and truthful double-auction mechanism named PS-TAHES based on additive homomorphic encryption [55], aiming to prevent personal privacy-information leakage in the auction. In general, research on auction mechanisms in the metaverse is still in its infancy and has not paid sufficient attention to privacy-preserving concerns.

5.3.4 Game Theory-Based Strategies

Game theory has been widely adopted in the existing incentive mechanisms. In the economic system of the metaverse, game theory can model the interaction among rational agents participating in the metaverse economic activities and achieve utility and social welfare maximization by individual strategy optimization. Game theory can model interactive decision-making, where each player's strategy depends on the actions of all other players. A comparison of different game theory-based strategy optimization methods is presented as follows.

Stackelberg games can construct a strategic model among leaders and followers, in which the leader move first, and then followers take action sequentially. In the vehicular metaverse, Jiang et al. [56] construct a game-theoretic hierarchical architecture, in which the Stackelberg game is considered to motivate more reliable workers to participate in the intensive rendering computation. Liu et al. [57] formulate a three-stage Stackelberg game to motivate users to pay sufficient transaction fees, which mitigates the issue of insufficient blockchain revenue. Huang et al. [58] model a Stackelberg game to price the resource service dynamically, in which metaverse service providers are leaders, and users are followers. The distributed and centralized approach is adopted to derive the Stackelberg equilibrium according to individual privacy requirements. Sun et al. [59] construct a two-stage Stackelberg game to motivate users to participate in aerial-assisted Internet of Vehicles (IoV), which promotes the development of dynamic digital twins. Jiang et al. [60] adopt the coalition game and Stackelberg game to assist in choosing reliable workers to participate in the coded distributed computing tasks in the metaverse. Daniel et al. [61] adopt a two-stage Stackelberg game to analyze a Nash equilibrium with negative externalities and unfair prices for blockchain data storage.

Evolutionary game is a typical dynamic game theory, which can model the dynamic decision process of evolution of individuals with biological characteristics in the metaverse. In the infrastructure layer of edge intelligence-empowered metaverse, Lim et al. [16] leverage evolutionary game to motivate the convergence of edge intelligence to support the metaverse engine. Specifically, the evolutionary game is used to model how the rewards from virtual service providers affect the contribution of sensing service providers during the service of the metaverse. The simulation shows that the synchronization frequency for virtual devices varies with the rewards.

Coalitional game refers to the players participating in the game in the form of alliances and cooperation, which aim to identify the best coalitions and a fair reward distribution among all participants [62]. In economics, public goods refer to a commodity or service that is made available to many customers, which is both nonexcludable and nonrivalrous. For public goods, like digital assets, the free-rider behaviors seriously hinder the enthusiasm of participants and fairness collaboration. Luo et al. [63] design an efficient incentive mechanism to motivate edge devices to execute collaborative fog computing tasks and achieve mutually beneficial resource cooperation based on the coalitional game theory. Considering the free-riding behaviors in collaboration, Pu et al. [64] adopt the coalitional game to formulate a time-average energy consumption-minimizing task under incentive constraints to motivate more contribution in collaboration.

Contract theory is another common method for modeling the interaction among players in the metaverse. Jiang et al. [65] propose an age of information-based *contract model* to motivate data sensing among industrial IoT devices for industrial metaverses, in which the age of information is introduced as the data freshness metric. Du et al. [66] provide an optimal contract design framework to model the interaction between the service providers and the network infrastructure providers in the metaverse, in which a novel metric named Meta-Immersion is proposed to measure the subjective feelings of metaverse users. In the collaborative communication of end-edge-cloud, a blockchain-based incentive mechanism named InFEDge [67] is designed to trade off the training overhead and model performance in the hierarchical federated learning (HFL) based on contract theory. Taking the incomplete information into account, the authors obtain the optimal solution by formulating a contract game. The blockchain is leveraged to achieve reliable economic incentives and prevent disturbance from unreliable nodes. For vehicular edge computing, Liu et al. [68] propose a smart contract-based incentive algorithm to encourage edge devices to contribute computation resources and evaluate the performance of federated learning.

Contest theory is a special type of game where contestants exert costly effort to obtain some expected rewards with some probability, which is a very common phenomenon in the metaverse. To further improve metaverse service quality, Wang et al. [69] introduce *contest theory* to create an incentive mechanism that motivates users to upload data more frequently. The authors design a semantic communication framework for sensing information from the physical world to the metaverse.

For the resource allocation of the metaverse, game theory can be well applied in the design of incentive mechanisms. Reasonable resource allocation supports seamless real-time immersive experience, especially during the data synchronization between physical entities and virtual worlds [70]. Han et al. [71] adopt a dynamic evolutionary game to motivate different device owners to update resource allocation strategies, in which revenue maximization can be achieved by trading off the resource supplies and demands. Lin et al. [72] design an effective congestion control incentive scheme for digital twin edge networks (DTENs), in which the long-term control decisions are decomposed into a series of online related decisions using Lyapunov optimization theory. In [73], the authors propose a resilient incentive mechanism to trade off the storage requirements and mining revenues in the blockchain. Shen et al. [74] propose a fair node resource allocation strategy to promote user cooperation and maintain reliable content storage collectively. Lin et al. [75] proposed a knowledge pricing strategy based on a noncooperative game for the blockchain-based knowledge market, so that knowledge generated by edge nodes can be traded in the edge AI-enabled Internet of Things. Hou et al. [76] formulate an incentive-driven resource allocation scheme to stimulate collaborative computing between edge servers and IIoT devices, in which an NP-hard problem is derived to optimize task assignment strategies and achieve utility maximization.

5.3.5 Fair and Credible Reward Systems

In a metaverse's economic system, the reward is one of the important ways to achieve incentive goals. Digital assets (i.e., cryptocurrencies, NFTs, and other tokens) are the main medium of rewards. These assets can be donated to the developers for the metaverse as an incentive mechanism [77]. Thomason et al. [78] propose tokenized incentives mechanism to motivate developers to participate in collaboration under microeconomic systems, aiming to make individual contributions consistent with the collaboration goals. For instance, GameFi [79] refers to play-to-earn blockchain games that offer a potential economic incentive mechanism to players, where avatars controlled by players can earn cryptocurrency and NFT as the reward for accomplishing game tasks. In Sandbox [80], users can seamlessly access the virtual world, in which users vote for governance decisions via the decentralized autonomous organization (DAO) to earn token revenues.

Reputation value is the main metric to evaluate the reliability of workers, and it can be used as the bases for the fair distribution of rewards. Jiang et al. [56] formulate a reputation evaluation metric based on the subjective logic model to select reliable employees in distributed computing. The reputation value is stored in the blockchain database to ensure reliable management. In order to expand the methods of employee selection, Zhao et al. [81] proposed a privacy-preserving incentive mechanism to encourage more IoT devices to participate in model training tasks and reduce malicious parameter updates. CoopEdge [82] is proposed to solve the credible incentive mechanism of edge nodes based on blockchain, in which reputation management motivates selfish edge nodes to perform distributed edge computing collaboratively. In this problem, the historical performance of edge nodes in performing offloading tasks to evaluate the reputation, which can be recorded in the blockchain. The reputation value is calculated by a novel consensus mechanism named Proof of Edge Reputation (PoER), which allows miners to record reputation value on the blockchain by consensus validation.

In addition, contribution is also viewed as one of the bases for reward allocation. Metachain [83] is a decentralized metaverse framework based on blockchains, in which an incentive mechanism based on the Stackelberg game is constructed to attract more contributions during participating in the autonomous metaverse activities. Sun et al. [59] propose a distributed incentive mechanism based on the alternating direction method to encourage more vehicles to contribute more resources to the physical-virtual synchronization in the metaverse. Their proposed mechanism can maximize the overall energy efficiency of vehicular in dynamic IoV scenarios.

5.4 Monetary Systems for Metaverse

5.4.1 Basics of Cryptocurrency in Metaverse

Cryptocurrencies are the best-performed blockchain applications in the past few years. The term *crypto* refers to encryption algorithms and techniques used to protect the native tokens of a specific blockchain system. The popular encryption methods exploited in blockchains include elliptical curve encryption, hashing functions, and public-private key signature technologies.

Although the cryptocurrency market attracts enormous criticisms, people still see the value of cryptocurrencies in the ecosystem of blockchains, because cryptocurrency is a medium of value exchange in the digital world. Thus, cryptocurrencies can bring liquidity to the economic market of digital assets.

Metaverse monetary systems require decentralized exchanges (DEXes) to enable the transactions of both UGC/AIGC and NFT. Currently, major economic activities in metaverse mainly involve the auction of virtual assets such as land, scarce items, and precious real estate, the development and leasing of land, rewards for accomplishing game tasks, and profits from investing in cryptocurrencies. Those activities can be supported by cryptocurrency-valued transactions. Furthermore, cryptocurrencies can be used in various other scenarios in the metaverse such as advertising, e-commerce, event organizing, social networks, etc.

5.4.2 Digital Wallets for Metaverse

Since users are the foundation of the metaverse ecosystem, a natural question is how to enable users to interact with the economic systems in metaverse. The related activities include the management of their digital assets and the participation in DeFi activities in metaverse. In this part, we discuss two related questions, i.e.,

- What are digital wallets in the real world?
- How do users interact with metaverse using their digital wallets?

5.4.2.1 Digital Wallets in Real World

A digital wallet is software that allows users to interact with blockchains. It provides users services such as storing private keys of users' crypto assets, conducting transactions, and invoking smart contracts. In Ethereum, digital wallets [84] are applications that help users connect with their Ethereum accounts. One can read his/her account balance, launch transactions, and connect to dApps using their wallets. MetaMask [85] is the most well-known crypto wallet, which can be used to link any crypto's trading platform of the user's choice. Users can deposit their local fiat currency and then convert it for cryptocurrencies through exchanges such as Coinbase and Binance.

According to the way of using private keys, digital wallets can be classified into *software wallets* and *hardware wallets*. Software wallets are further classified into *hot wallets* and *cold wallets* [86]. A hot wallet is connected to the Internet. Users can use digital assets directly through their web/mobile wallets. A cold wallet is offline to ensure that the private key is never exposed to the Internet. Thus, a cold wallet can effectively prevent hackers from stealing users' private keys to crypto assets.

5.4.2.2 How to Interact with Metaverse Using Digital Wallets

In blockchains, both token transfers between accounts, and interactions between users and smart contracts are driven by transactions. Users' wallets store their public addresses and the corresponding private keys. A user can initiate a transaction signed by his/her private key through the wallet, thus realizing interactions with blockchains.

All digital wallets have the function of balance querying, token receiving, and transferring metaverse tokens. In addition, some famous wallets also provide unique functions for business convenience. For instance, both *Trust Wallet* and *MetaMask* provide access to various NFT marketplaces and game assets.

Argent [87] is a smart-contract wallet controlled by codes instead of a user's private key. Any function of Argent can be realized through smart contracts. For instance, Argent provides *Guandians mechanism* to recover a wallet if a user's private key is lost. Moreover, Argent can set transfer limits, approve transfers to known addresses, and lock accounts to prevent crypto assets from getting spent. These functions can lower the threshold for users when they use cryptocurrencies.

Following the development of Ethereum, these mainstream wallets also support transactions on Ethereum's *Layer2* network. Layer2 solutions offer low fees and fast transactions without compromising security. Users can withdraw their crypto assets to a *Layer1* blockchain at any time. Argent has exploited zkSync [88] to support its Layer2 wallet.

5.5 Economic Activities for Metaverse Users

Decentralized finance (shortened as DeFi) is a paradigm of financial service technologies based on distributed ledgers built on top of blockchains. DeFi directly provide transaction services to customers without any intermediaries like centralized banks and governments. All DeFi transactions will be recorded in blockchains and become immutable.

In future metaverse, when users own their digital assets, they would very possibly participate in various economic activities such DeFi protocols, aiming to earn extra profit. Given that DeFi boosted the historical second-wave blockchain applications about 5 years ago, we are curious about the following three questions:

(i) What popular DeFi Protocols are there in real world?
(ii) What are the differences between the real-world DeFi and that in metaverse?
(iii) How do users take part in DeFi protocols in metaverse?

In the following, we first review popular DeFi protocols and then discuss how to participate into DeFi activities in metaverse.

5.5.1 Most Popular Real-World DeFi Protocols

Table 5.2, presents the 15 most popular categories of DeFi protocols provided by DefiLlama [89]. Those DeFi categories are ranked according to their total value locked (TVL), which is one of the key indicators to help us understand the value of a smart-contract DeFi protocol. In the following, we take the first three categories as examples to show the representative products for each.

5.5.1.1 DEXes

Uniswap [105] is essentially a smart contract-enabled decentralized exchange (DEX), which offers the trading protocol for cryptocurrencies and automatic liquidity. Using the native governance token *UNI*, Uniswap performs as an automated market maker (AMM), which conducts peer-to-peer market making based on an

Table 5.2 Popular DeFi protocols [89]

Name	Recognition
DEXes [90]	Protocols where users can swap and trade cryptocurrencies
Lending [91]	Protocols that allow users to borrow and lend assets
CDP [92]	Protocols that mint its own stablecoin using collateralized lending
Liquid Staking [93]	Protocols that allow users to stake assets in exchange for a reward
Bridge [94]	Protocols that bridge tokens from one network to another.
Yield [95]	Protocols that pay you a reward for your staking/LP on their platform
Services [96]	Protocols that provide a service to the user
Derivatives [97]	Protocols for betting with leverage
Yield Aggregator [98]	Protocols that aggregated yield from diverse protocols
Algo-Stables [99]	Protocols that provide algorithmic coins to stablecoins
Cross Chain [100]	Protocols that add interoperability between different blockchains
Synthetics [101]	Protocol that created a tokenized derivative that mimics the value of another asset
Launchpad [102]	Protocols that launch new projects and coins
Reserve Currency [103]	OHM forks: Protocols that use a reserve of valuable assets acquired through bonding and staking to issue and back its native token
Insurance [104]	Protocols that are designed to provide monetary protections

automated trading algorithm, and enables the swapping of multiple ERC-20 tokens on the Ethereum blockchain.

Curve [106] is another well-known DEX, mainly using stablecoins and its native governance token called *CRV*. As a liquidity aggregator, Curve pegs users' crypto assets with a specific token such as Bitcoin and stablecoins. Curve is widely exploited for the swap of stablecoins because it guarantees a low slippage rate and a low swap fee of 0.04%. In addition to providing liquidity, Curve's users can earn transaction fees and benefit from the interactions with other DeFi protocols like Compound, Synthetix, RenBTC, etc.

Saddle [107] implements an AMM on the Ethereum blockchain, optimized for trading pegged value crypto assets with minimal slippage. It efficiently supports DeFi trading between stablecoins and its pegged crypto assets such as wETH and wBTC.

5.5.1.2 Lending

Compound [108] is a lending protocol that supplies crypto assets as collateral in order to borrow the base asset. Compound accounts can earn interest by lending the base asset to the protocol. Meanwhile, its accounts can also acquire governance token called *COMP*, using which accounts can help make critical governance decisions of the protocol network.

Aave [109] is one of the most popular and cutting-edge lending protocols. It realizes a decentralized noncustodial liquidity protocol, in which users can participate as depositors or borrowers. As a depositor, a user can earn passive income by supplying liquidity to the market. While acting as a borrower, a user can get the borrowed assets either by the permanent excess mortgage or low-collateralized flash credit. The native token of Aave is named *AAVE*, which enables users to participate in the governance of its protocol.

5.5.1.3 Collateralized Debt Position (CDP)

MakerDAO [110] is a CDP protocol built on the Ethereum blockchain, dedicated to bringing stability to the cryptocurrency economy. It consists of the stablecoin *DAI*, the maker collateral vault, Oracle, and a voting mechanism. Using its native governance token *MKR*, the token holders can decide the key parameters of the MakerDAO protocol such as the swap rate of stablecoins and the ratio of collateral.

5.5.2 DeFi in Real World vs. DeFi for Metaverse

We now discuss the second question, i.e., what differences are there between the real-world DeFi and that in the metaverse? Observing that a lot of popular DeFi protocols have been developed and applied in the real-world crypto market, we are also curious about what DeFi activities and products in the metaverse will look like.

The future metaverse will definitely require DeFi protocols in the virtual world. Even today, we see that metaverse cryptocurrencies have already been exploited to enable the economic system in some metaverse games such as Roblox [7] and the Second Life [111]. For instance, the Second Life enables its players to shop in the built-in marketplace. Players can purchase millions of virtual fashions, home decor, and other items. The Second Life can even allow game players to generate users' own digital creations and monetize them to earn profits in a virtual economy powered by Tilia [112]. Here, Tilia is an all-in-one payment platform dedicated to the metaverse economy. With Tilia, game players, NFT providers, and the publishers of the virtual world can launch their payments, initiate virtual crypto tokens, and earn real assets in both the real world and the metaverse.

Metaverse enables people to shop, game, buy, and trade currencies and other objects. In the metaverse, cryptocurrencies serve as money in a virtual digital world. There exist several terms like "metaverse coins," "metaverse tokens," and "metaverse crypto." Every metaverse project has to handle transactions within a particular digital environment through its native tokens.

Recently, it is reported that the financial sector of Meta [113], i.e., Meta Financial Technologies, is exploring a new crypto token, internally named *MarkCoin*, to develop their economic system in Meta's virtual business. Numerous other metaverse projects have already been launched, and their individual tokens are available in the crypto market such as MANA [114], SAND [80], and HIGH [115]. MANA is the native token of Decentraland [114]. In this metaverse-style game, users can buy and sell virtual land, estates, avatar wearable gadgets, and even names in the Decentraland marketplace. All the transactions while stocking these digital goods are supported by the Ethereum blockchain. The Sandbox [80] was founded in 2012 by Pixowl as a mobile gaming platform. In 2021, it was upgraded to a play-to-earn blockchain version and becomes one of the fastest-growing crypto-driven metaverse games. In this new-version game, players can build their virtual worlds using the NFTs backed by Ethereum. For instance, using its native token SAND, people can buy a piece of land from The Sandbox metaverse to host their virtual events. HIGH is another metaverse project named "Highstreet" [115], which is an interesting project with VR-supported metaverse applications. A user can shop for things inside its virtual universe using the currency HIGH.

Via reviewing several real metaverse projects and their corresponding token systems, we see that the DeFi activities in the metaverse keep growing. In the next subsection, we investigate the third question, i.e., how do users take part in DeFi activities in the metaverse?

We answer this question following two threads, i.e., how to participate into DeFi activities as customers and how to engage in DeFi in metaverse as developers. The first thread is straightforward. As customers of DeFi protocols in the metaverse, the target is to earn *profit*. Thus, the users who own metaverse crypto assets can take part in various DeFi lending protocols aforementioned. However, please note that we are not encouraging anyone to invest any DeFi product. Any economic activity has the risk of failure. Please do your own research before taking actions.

5.5.3 *How to Enable DeFi in Metaverse as Developers?*

We take Polygon [116] as an example to present our thoughts.

5.5.3.1 What Is Polygon

Polygon [116] is claimed as a decentralized platform that is committed to bringing the world to Ethereum. Using it, developers can create low-fee dApps without compromising the security of the blockchain. Polygon aims to become a solution aggregator in the Layer2 blockchain of Ethereum and offer a modular, universal, and flexible framework to scale out the service level of Ethereum.

5.5.3.2 History of Polygon

Polygon has experienced several stages.

- *Early stage (2017–2019).* In 2017, Matic Network was born, which is the previous version of Polygon. At the beginning, Matic was positioned as a single Layer2 solution, which adopted the Plasma framework [117] as the solution.
- *Development stage (2017–2019).* As the project evolved, Matic Network expanded its scope from a single Layer2 solution to a "network of networks," eventually changing its name to "Polygon" in February 2021.
- *Current stage (2021–present).* Currently, Polygon has only one mature product named as *Polygon PoS* [118]. The Polygon team plans to focus more on *rollup* [119] solutions in the future.

5.5.3.3 Polygon PoS

Polygon PoS [118] is an extension solution of Ethereum that achieves fast transaction speed and low-cost fees by leveraging sidechains for transaction processing. It also uses Plasma [117] as a secure bridging framework and PoS validators to guarantee the security of the on-chain assets.

5.5.3.4 What We Can Learn from Polygon

In the future metaverse, there will be a universal standard that defines the rules of executing DeFi protocols. The question is that if moving the existing popular DeFi protocols to the metaverse scenarios, people are wondering can they work in the context of metaverse. We can imagine that metaverse needs a high-throughput and low-cost transaction hub like Polygon. Let us call this hub the *universal hub*, which aims to enable metaverse users to perform frequent interactions with the bottom-layer blockchains of multiple metaverse platforms.

Given that users' frequent cross-platform interactions of metaverse demand low-latency and high-throughput transactions across multiple metaverse platforms, the next question is what exactly Polygon inspires us to conduct DeFi in the metaverse. Firstly, Polygon has addressed the heterogeneity of the diverse blockchains in its bottom layer. Secondly, Polygon enables excellent ability of cross-platform transactions. In addition, the Polygon-like universal hub should support developers to implement customized solutions in Layer2 of the bottom blockchain while considering multiple metrics.

5.6 Cross-Chain Ecosystem for Metaverse

In this section, we first analyze why metaverse needs cross-chain solutions. Based on the existing cross-chain solutions and their pros and cons, combined with the characteristics of the metaverse economic system, we present our cross-chain solutions that are suitable for the metaverse. Through the observation of existing metaverse projects, we found that the behaviors and transaction rules across multiple metaverse platforms cannot be found yet. Therefore, following the cross-chain logic, we finally present a deductive analysis of interoperability across multiple metaverses.

5.6.1 Cross-Chain Technologies

Since the debut of Bitcoin, various blockchains and their applications are been proposed. According to the survey of CoinMarketCap [120], 9154 cryptocurrencies have been used in the real world, where more than 8000 independent blockchain systems are involved. Therefore, it is envisioned that [121, 122] the ecosystem will develop a multichain future where various blockchain protocols coexist. In the multichain ecosystem, users can experience the services of various blockchain systems by joining a blockchain system. Decentralized applications designed by developers are not limited to a single closed system. Instead, dApps intend to create enormous value in a more broad multiple-blockchain ecosystem. A newly deployed blockchain naturally chooses to cooperate with other existing mainstream blockchains and gain their support. The key to supporting multichain ecological integration is *cross-chain technologies*, which enable two or more independent blockchains to interoperate with on-chain objects (assets or other associated data).

Most blockchain ecosystems do not support cross-chain technologies. Gavin Wood, the co-founder of Ethereum, launched a heterogeneous multi-chain blockchain network named *Polkadot* to achieve interoperability across blockchains [123]. Particularly, the Polkadot network consists of multiple *parachains* and a *Relay Chain*. Parachains are used to process transactions in parallel. The Relay Chain is the main chain of the system, providing security guarantees for the Polkadot. Polkadot defines a set of message format standards to provide interoperability for parachains. In order to interact with external blockchains such as Bitcoin and Ethereum, Polkadot uses various *blockchain bridges* to allow external blockchains to share arbitrary data such as crypto assets and NFT.

5.6.2 Metaverse Needs Cross-Chain Solutions

The metaverse is a virtual space that maps from and is independent of the real world. It is not a single closed universe, but a constantly expanding digital universe composed of boundless virtual worlds and digital content. Blockchain technology can provide underlying infrastructure support for the metaverse. That is to say, the identity and economic system in the metaverse operate based on the blockchain infrastructure, which is independent of a specific operator so that the data is owned by the user and not monopolized by an operator. In particular, blockchain technologies guarantee the uniqueness, privacy, and security mechanisms of avatars in the metaverse. Furthermore, a decentralized economic system in the metaverse requires blockchains to ensure security and trust. In the metaverse, users may conduct a large number of transactions at any time, and those transactions must be verified in a decentralized way. In addition, digital assets must be capitalized with blockchains to identify their authority. The trading and circulation of those digital assets rely on the underlying blockchain technology.

The metaverse is essentially a digitized version of the real world. What it builds is a space where the real and virtual worlds are highly integrated and interactive. Meanwhile, the metaverse is also an open, fair, and distributed world. Every individual or organization can build a virtual space even another sub-metaverse in the metaverse. Moreover, the development of the metaverse is not decided by a single company or enterprise, but via multiparty collaboration. Therefore, cross-platform communications between or within the metaverse bring new challenges to user identity uniqueness, asset's transfer, and digital-content's circulation. All those mentioned facts imply that there is an urgent need to design cross-chain solutions for the metaverse.

5.6.3 Cross-Chain Protocols for Metaverse

Since blockchains are independent of each other, a cross-chain communication protocol that enables blockchains to communicate with each another is required. A typical cross-chain protocol is divided into four phases [124]: *pre-commit* phase, *verify* phase, *commit* phase, and *abort* phase. The *pre-commit* and *commit* phases are equivalent to locking and unlocking the states of the two blockchains, respectively. The *verify* phase is a key component of the cross-chain protocol because it allows one blockchain to perceive the state transition of the other. For instance, suppose that we have two blockchains, i.e., chains *X* and *Y*. In order to unlock assets on chain *Y*, consensus nodes of chain *Y* need to verify that the backed assets on chain *X* have been locked. The *abort* phase means that the *pre-commit* state reverts to the previous state if the *verify* or *commit* phase fails.

Table 5.3 Cross-chain protocols and their representative examples

Cross-chain protocols	Representative examples
Trusted cross-chain protocols	Notary [125], Tokrex [126], Corda [127], BTCB [128], HBTC [129], tBTC [130], ren [131], DeCus [132], Hop Exchange [133], Hyphen [134], Degate Bridge [135]
Trustless cross-chain protocols	Hash Time-lock [136], WBTC [137], cBridge [138], Lightning Network [139], SEPoW [140], Zcash XCAT [141], Interledger [142], BTCRelay [143]
Hybrid protocols	Xclaim [144], zkBridge [145], Plasma [117], Polkadot [123], Cosmos [146], Decentralized gateway [147]

According to the current design principles, cross-chain protocols can be classified into three categories: (i) trusted cross-chain protocols, (ii) *trustless cross-chain protocols*, and (iii) *hybrid protocols*, as described in Table 5.3.

The representative example of *trusted cross-chain protocol* is Notary [125]. In the *pre-commit* phase of protocols, a user locks the assets of chain X to the notary's committee address, aiming to obtain the corresponding unlocked assets on chain Y. In the *verify* phase, the notary waits for the assets on chain X that are to be confirmed. If these assets are confirmed, the protocol enters the *commit* phase. The notary unlocks the corresponding assets on chain Y to the user's address on chain Y and then completes the cross-chain transfer. We found that in the procedure described above, users' assets are managed and controlled by a notary. In order to become a notary, existing cross-chain protocols have different methods, such as depositing assets, evaluating applicants' reputation value, and selecting consensus committees. We then review the pros and cons of Notary protocol. Firstly, the Notary protocol's pros include (i) efficiency, which can quickly realize the cross-chain transfer of assets, and (ii) practicality, which can be better compatible with existing blockchain systems. On the other hand, Notary's cons include insecurity and high fees. The cross-chain transfer of assets relies on an external trusted committee. If the committee is malicious, cross-chain assets are vulnerable. The assets deposited by the committee are with high diversity. To balance the committee members' income, a higher cross-chain service fee is charged.

The representative example of *trustless cross-chain protocol* is hash time-lock [136]. In this protocol, the *pre-commit* and *commit* phases are conducted simultaneously, aiming to lock assets into the counterparty's address. In the *verify* phase, a user performs the unlocking operation on chain Y by revealing the unlocked secret. On the other hand, the counterparty who has obtained the revealed secret performs the unlocking operation on chain X and completes the exchange of assets. In addition, sidechain protocols [143] can also realize the cross-chain transfer of assets without a trusted third party. The advantage of these protocols is high security and no need an intermediary. However, their disadvantage is that they rely on synchronization assumptions, which entail that cross-chain participants must be online at the same time.

The representative example of *hybrid protocol* is *Xclaim* [144]. In this protocol, both trusted and trustless models are exploited. To transfer assets from chain X to chain Y, chain Y can verify the validity of transactions that took place on chain X without a trusted third party. This is realized by relaying consensus information, such as block headers, on chain X to the relay contract resided on chain Y. In the opposite direction, the transfer of the assets is completed by a trusted notary.

5.6.4 Promising Cross-Chain Solutions for Metaverse

The metaverse is an open and comprehensive virtual world. Every individual and organization can create their own metaverse platforms. They can adopt different technical solutions and design different customized application scenarios. Based on these characteristics, we believe that the following cross-chain solutions are promising for the metaverse.

5.6.4.1 Supporting the Interoperability of Heterogeneous Models

Different metaverses may be built on top of underlying heterogeneous blockchains with different functionalities and crypto algorithms. If the cross-chain protocol does not properly adapt to these heterogeneous blockchain models, it might lead to failures of cross-chain transfer. For instance, there exists a cross-chain protocol [143] in which its implementation depends on smart contracts. However, this protocol is useless for blockchains without equipped with smart contracts. In addition, the hash time-lock protocol requires two interlinked blockchains to use the same hash function. That is to say, chain X uses a function $H(\cdot)$ such that $h = H(x)$. On the other hand, chain Y uses a hash function $H'(\cdot)$ such that $h \neq H'(x)$. Therefore, a design challenge in cross-chain protocols is how to achieve interoperability between heterogeneous blockchains.

5.6.4.2 Supporting Privacy Preserving

Privacy is a pivotal property of metaverse ecosystems, which also applies to cross-chain protocols. Ideally, the assets of cross-chain transfer and the identity of the transfers can be hidden from the public. Unfortunately, most cross-chain protocols lack the module for privacy preservation. For instance, in the hash time-lock protocol, two transactions that execute asset commits on two blockchains are publicly recorded in the blockchain. By observing these two transactions, all blockchain users know who made these cross-chain transfers and how many tokens were transferred. Therefore, the metaverse should provide a cross-chain protocol that supports identity anonymity and asset-blinding mechanisms.

5.6.4.3 Supporting Multiple-Object Interoperability

A cross-chain protocol dedicated to the metaverse should support the interoperability of any information across multiple metaverses, including at least digital assets, instructions of smart contracts, and user identities. Among those economic activities across metaverse platforms, a typical example is the *asset transfer* through underlying blockchains. In order to improve cross-chain performance, it is necessary to realize automatic cross-chain asset transfer through smart contracts. Thus, the instructions of smart contracts across blockchains need to be supported by such cross-chain protocol. In addition, to facilitate users to travel across metaverses, the verification of users' identities across blockchains should be also implemented.

5.6.5 How Will Cross-Chain Ecosystem Evolve in Metaverse

In the real world, people can engage in a wide variety of activities. For instance, during work hours, people work in their companies for payments. At night, people spend in entertainment venues to enjoy their life with the money earned from their work. Similarly, users of the metaverse also need to travel freely through applications across different metaverse platforms. As shown in Fig. 5.6, as a metaverse user, Alice plays games in Sandbox [80] and earns crypto assets called *SAND*. Subsequently, Alice wants to participate in activities in Axie Infinity [14]. To this end, Alice needs to purchase *Axies* using her *SAND*. From this real-world example, we observe that in order to accomplish Alice's cross-metaverse activities, two events are involved, i.e., (i) the identity verification of cross-metaverse and

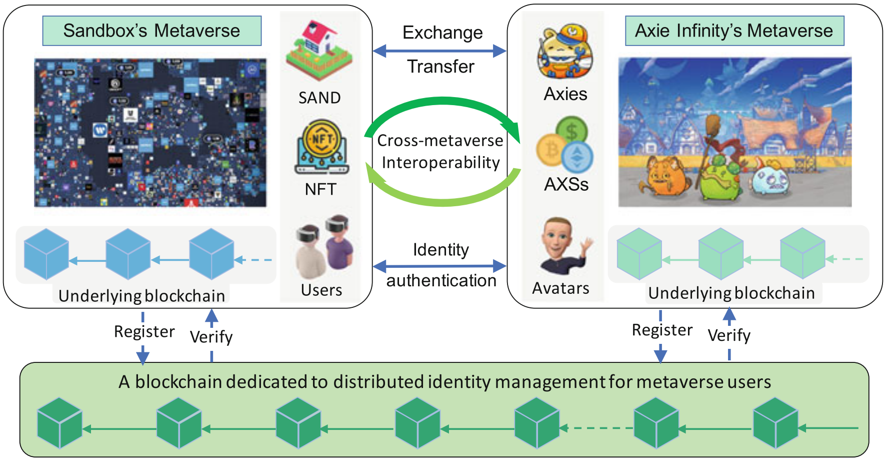


Fig. 5.6 Illustration of cross-metaverse interoperability, in which we take Sandbox's and Axie Infinity's metaverses as examples

(ii) the asset transfer across metaverse platforms. From a technical point of view, these two events sparked a cross-metaverse transaction. Since both Sandbox and Axie Infinity are built on top of blockchain technologies, the cross-chain protocol can handle the aforementioned cross-metaverse transactions. Thus, such cross-chain protocol can also support Alice's cross-metaverse activities. It can be foreseen that the cross-chain protocols will receive growing attention in the context of cross-metaverse applications.

5.7 Challenges and Open Issues

Although we have reviewed a lot of related studies, the economic systems dedicated to metaverse are still in its initial stage from the perspective of either industry or academia. In this section, we summarize challenges and open issues that still need to be addressed in the upcoming few years.

5.7.1 How to Interpret Authorship and Inventorship of AIGC

In the context of accelerated integration of the digital and physical worlds, AIGC is leading a profound change, reshaping the production and consumption modes of digital content. It will greatly enrich people's digital life and also is an indispensable force for the future development of digital civilization. However, an open issue is how to interpret the *authorship* of creations and the *inventorship* of inventions generated by AI algorithms [148]. We look forward to seeing new discussions and solutions proposed very soon.

5.7.2 Risk of Avatars in Metaverse

In the human-centric metaverse, the virtual world is composed of many avatars controlled by users. Avatars sense the physical world's state through interactive devices [149]. Users can enter and live in the virtual habitat through the digital avatars, which interact with other virtual entities [150] to communicate, collaborate, socialize, and work in the virtual world. The interactive activities of virtual and reality require large-scale distributed computing and communication infrastructure and rely on emerging multimedia technologies such as AR, VR, MR, and tactile Internet (TI). However, there are still some inherent risks following the current mode of digital avatars in metaverse. In this regard, we outlook some possible risks related to avatars as follows.

5.7.2.1 Fraud Risks

In an open metaverse ecosystem, avatars support the collaborative production-based economy. For instance, Roblox [7] allows any user to create games and avatars. However, in this multi-entity creative economy, each participant's credibility cannot be guaranteed [151]. Thus, it is a challenge to eliminate malicious frauds when creating and publishing digital entities.

5.7.2.2 Metaverse Crimes

The safety of avatars is being threatened by crimes in the metaverse. Such crimes seriously affect the stability of the virtual habitat. Yang et al. [152] propose a biometric identity authentication framework based on the chameleon signature to identify and track malicious players. In order to guarantee the consistency of the user and the associated avatar, the authors construct an identity model based on biometrics to achieve the verifiability of players' physical identity.

5.7.2.3 Financial Risks

In metaverse's trading market, the trading of virtual digital products among multiple entities has inherent financial risks (e.g., refusal to pay). For instance, because of a reentrancy flaw in smart contract codes [153], the metaverse project Paraluni based on Binance Smart Chain (BSC) lost over $1.7 million in 2022.

5.7.3 Outlook of Monetary Systems in Metaverse

In the future, multiple metaverses will definitely exist in our daily life. Although a metaverse is possibly built by a giant commercial group, the economic system in the metaverse must be operated based on decentralized token systems. This is because transactions in metaverse are conducted using cryptocurrencies without relying on any third-party intermediary. Due to safety and security reasons, transactions that occurred in the metaverse must be recorded in a blockchain. It can be foreseen that each metaverse very possibly will launch at least a native cryptocurrency, which becomes the virtual economy's legal cash. This paradigm also indicates that dedicated circulating protocols are needed to enable economic activities across metaverses.

Several representative real-world examples are reviewed here as references to design such metaverse's circulating protocols. Tian et al. [154] propose a distributed cryptocurrency exchange protocol, in which two types of consensus mechanisms (i.e., Proof of Work and Proof of Deposit) are used to select trustworthy users for constructing a validation committee. As an existing successful solution, Uniswap

[19] as a decentralized exchange built on Ethereum automatically provides services for the liquidity of cryptocurrencies.

Referring to those existing exchange protocols, we could imagine that virtual exchanges will appear in the future metaverse. People will directly trade digital assets including both fungible and non-fungible tokens and other digital assets via such new DEXes in the virtual world.

On the other hand, the risks related to virtual DEXes cannot be ignored. Even worse, virtual DEXes are possibly more vulnerable to hackers' attacks in the virtual world than those in physical world. In addition, it might be more difficult to detect some economic scams in the metaverse. For instance, phishing schemes [155] and Ponzi schemes [156] can be designed following completely new architectures in the metaverse. It causes difficulty for governance when those new types of scams are widely spread in the virtual world. Therefore, how to tackle those new threats toward the future healthier DEXes in the metaverse becomes a promising research direction.

5.7.4 How Cross-Chain Technologies Support Wallet Apps

The cross-chain wallet is an upgraded version of the conventional digital wallet. The cross-chain wallet is built for interoperable multichain-based economic applications. When powered with interoperability, a digital wallet becomes a cross-chain wallet that can connect to multiple-blockchain ecosystems [123]. Users can directly interact with a wide range of cross-chain Web3 applications with their unique wallet addresses, eliminating the hassle of maintaining multiple secret keys.

Cross-chain wallets comprise some unique capabilities that conventional wallets cannot provide. For instance, users can transfer their crypto assets and NFTs on different on-chain marketplaces. If someone's digital assets are distributed in different chains, he/she can know the total value of his/her assets through the cross-chain wallet. However, cross-chain wallets are still in the very initial development stage. New products and solutions are open to implementation in the upcoming years. Numerous technical challenges are needed to tackle, including privacy preservation of wallet users, security of users' assets, risks of hacking attacks, and of course the adaption to regulation and law issues in different areas.

5.7.5 Cross-Metaverse Interoperability

Multiple metaverse platforms are emerging with their unique blockchains, forming their own ecosystems. Different versions of metaverses may focus on either social networking, games with excellent graphical quality, or working scenarios with technical supports [157]. However, those metaverse platforms are mutually independent, and there is no information or value transfer among them. For instance, if Meta's and Nvidia's metaverse users intend to interact with each other, the authentication of users' identity is a huge challenge. Therefore, it is necessary for metaverse service providers to offer sufficient backend and interoperability support, aiming to bridge multiple metaverse platforms. As inspired by the solutions to bridge numerous blockchains, cross-chain technology is the key to achieving such cross-metaverse interoperability. We can foresee that the metaverse will develop a multichain future and will not be monopolized by Ethereum. Many coexisted metaverses will be supported by numerous interoperable blockchains [157].

At the current stage, almost the services provided by the blockchain-based metaverse are about the circulation of cryptocurrencies and NFT. In the upcoming stage, multiple-platform metaverse technologies will provide more immersive services for metaverse users, e.g., multiple-entity fully perceptive interactions, multiple-mode coordination, and super cities fusing both virtuality and reality in the metaverse. Those advanced services require stronger interoperability of smart contracts and applications across multiple metaverse ecosystems [157].

5.7.6 Economic Models of DAO in Metaverse

In the era of Web3, the ubiquitous metaverse can provide a decentralized immersive virtual habitat where users are able to construct a decentralized autonomous ecosystem to mitigate the critical issue of monopolists and dictators in the metaverse. In economic systems of the metaverse, users can create digital content based on the blockchain and participate in a decentralized autonomous organization (DAO), which could be widely used to organize massive users to create digital content collaboratively. In this regard, the economic value of digital assets needs to be shared among all stakeholders. This new paradigm, i.e., DAO, can drive the innovation of the metaverse ecosystem.

DAO has been believed as a promising organization for Web3 participants [158]. DAO has received real application scenarios from some metaverse games. For instance, MANA is a native token platform of Decentraland [114], enabling users to buy digital assets, like virtual land, avatars, and other game wearables. In this platform, owners of tokens can be encouraged to form a DAO to get the right to vote for the improvements of the platform. Although DAO provides the original spirit of a decentralized world, there is still a very long way to go before DAO can be widely adopted by the metaverse. This is because the economic model of DAO is facing the following several technical challenges.

- When metaverse users form a DAO, they have to design an economic model and issue cryptocurrencies, which can be devoted to the governance of communities. Designing a healthy economic model for a DAO is not easy, because the economic model decides the incentive mechanism of the organization.

- The most important feature of the economic model of a DAO is to provide high liquidity. However, the token systems of real-world DAOs are difficult to guarantee such high liquidity.
- Another technical challenge when designing the economic model of a DAO is how to ensure the profit can be delivered to core contributors of the community.

Anyway, the economic model of DAOs plays a crucial role for metaverse users in the future. This topic will attract growing research attention from both academia and industry.

5.8 Conclusion

Economic systems are the foundation of metaverse. In this chapter, we mainly introduce the preliminaries, basics of economic systems, the fundamental economic activities, challenges, and open issues of metaverse. We wish this chapter can inspire researchers, engineers, and educators to explore more paradigms, products, and dApps for a better future metaverse.

References

1. Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng, “Fusing blockchain and ai with metaverse: A survey,” *IEEE Open Journal of the Computer Society*, vol. 3, pp. 122–136, 2022.
2. A. Tlili, R. Huang, B. Shehata, D. Liu, J. Zhao, A. H. S. Metwally, H. Wang, M. Denden, A. Bozkurt, L.-H. Lee *et al.*, “Is metaverse in education a blessing or a curse: a combined content and bibliometric analysis,” *Smart Learning Environments*, vol. 9, no. 1, pp. 1–31, 2022.
3. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” BTC, Tech. Rep., 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
4. C. Chen, L. Zhang, Y. Li, T. Liao, S. Zhao, Z. Zheng, H. Huang, and J. Wu, “When digital economy meets web 3.0: Applications and challenges,” *IEEE Open Journal of the Computer Society*, 2022.
5. N. Garg, “What is Metaverse in Blockchain? And why does it Matter?” 2022. [Online]. Available: https://www.brsoftech.com/blog/metaverse-in-blockchain/
6. G. Weston, “Top Tech Firms Investing In Web 3.0,” 2022. [Online]. Available: https://101blockchains.com/top-tech-firms-investing-in-web-3-0/
7. Roblox, “Reimagining the way people come together.” 2022. [Online]. Available: https://corp.roblox.com/
8. “Facebook wants to lean into the metaverse. Here’s what it is and how it will work,” 2021. [Online]. Available: https://www.npr.org/2021/10/28/1050280500/what-metaverse-is-and-how-it-will-work
9. A. J. van Niekerk, “The strategic management of media assets: A methodological approach,” in *Allied Academies, New Orleans Congress*, 2006.
10. A. Toygar, C. Rohm Jr, and J. Zhu, “A new asset type: digital assets,” *Journal of International Technology and Information Management*, vol. 22, no. 4, p. 7, 2013.

11. M. Xu, W. C. Ng, W. Y. B. Lim, J. Kang, Z. Xiong, D. Niyato, Q. Yang, X. S. Shen, and C. Miao, "A full dive into realizing the edge-enabled metaverse: Visions, enabling technologies, and challenges," *IEEE Communications Surveys & Tutorials*, 2022.
12. M.-B. Lin, B. Wang, F. Y. Bocart, C. Hafner, and W. K. Härdle, "Dai digital art index: a robust price index for heterogeneous digital assets," DAI Digital, Tech. Rep., 2022.
13. D. J. Niemeyer and H. R. Gerber, "Maker culture and minecraft: Implications for the future of learning," *Educational Media International*, vol. 52, no. 3, pp. 216–226, 2015.
14. S. Mavis, "Axie infinity," 2022. [Online]. Available: https://axieinfinity.com/
15. Q. Wang, R. Li, Q. Wang, and S. Chen, "Non-fungible token (nft): Overview, evaluation, opportunities and challenges," *arXiv preprint arXiv:2105.07447*, 2021.
16. W. Y. B. Lim, Z. Xiong, D. Niyato, X. Cao, C. Miao, S. Sun, and Q. Yang, "Realizing the metaverse with edge intelligence: A match made in heaven," *arXiv preprint arXiv:2201.01634*, 2022.
17. Y. Chen and H. Cheng, "The economics of the metaverse: A comparison with the real economy," *Metaverse*, vol. 3, no. 1, p. 19, 2022.
18. H. R. Hasan and K. Salah, "Proof of delivery of digital assets using blockchain and smart contracts," *IEEE Access*, vol. 6, pp. 65 439–65 448, 2018.
19. G. Angeris, H.-T. Kao, R. Chiang, C. Noyes, and T. Chitra, "An analysis of uniswap markets," *arXiv preprint arXiv:1911.03380*, 2019.
20. P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels, "Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 910–927.
21. E. Fehr and K. M. Schmidt, "Fairness, incentives, and contractual choices," *European Economic Review*, vol. 44, no. 4-6, pp. 1057–1068, 2000.
22. H. Yu, Z. Liu, Y. Liu, T. Chen, M. Cong, X. Weng, D. Niyato, and Q. Yang, "A fairness-aware incentive scheme for federated learning," in *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 2020, pp. 393–399.
23. H. Gao, C. H. Liu, W. Wang, J. Zhao, Z. Song, X. Su, J. Crowcroft, and K. K. Leung, "A survey of incentive mechanisms for participatory sensing," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 918–943, 2015.
24. X. Zhu, J. An, M. Yang, L. Xiang, Q. Yang, and X. Gui, "A fair incentive mechanism for crowdsourcing in crowd sensing," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 1364–1372, 2016.
25. A. Sinha and A. Anastasopoulos, "Incentive mechanisms for fairness among strategic agents," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 2, pp. 288–301, 2017.
26. D. Li, L. Yang, J. Liu, and H. Liu, "Considering decoy effect and fairness preference: An incentive mechanism for crowdsensing," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8835–8852, 2019.
27. B. Zhu, W. Leon, L. Paul, and P. Gao, "Impact of crowdsourcee's vertical fairness concern on the crowdsourcing knowledge sharing behavior and its incentive mechanism," *Journal of Systems Science and Complexity*, vol. 34, no. 3, pp. 1102–1120, 2021.
28. G. Martín-Herrán and G. Zaccour, "Credibility of incentive equilibrium strategies in linear-state differential games," *Journal of Optimization Theory and Applications*, vol. 126, no. 2, pp. 367–389, 2005.
29. Y. Xu, Z. Lu, K. Gai, Q. Duan, J. Lin, J. Wu, and K.-K. R. Choo, "Besifl: Blockchain empowered secure and incentive federated learning paradigm in iot," *IEEE Internet of Things Journal*, 2021.
30. X. Zhang, G. Xue, R. Yu, D. Yang, and J. Tang, "Truthful incentive mechanisms for crowdsourcing," in *2015 IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 2015, pp. 2830–2838.
31. J. He, D. Zhang, Y. Zhou, and Y. Zhang, "A truthful online mechanism for collaborative computation offloading in mobile edge computing," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 7, pp. 4832–4841, 2019.

32. X. Wang, X. Chen, and W. Wu, "Towards truthful auction mechanisms for task assignment in mobile device clouds," in *Proc. of IEEE Conference on Computer Communications (INFOCOM)*, 2017, pp. 1–9.
33. M. Liwang, S. Dai, Z. Gao, Y. Tang, and H. Dai, "A truthful reverse-auction mechanism for computation offloading in cloud-enabled vehicular network," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4214–4227, 2018.
34. D. J. Ott and A. F. Ott, "Budget balance and equilibrium income," *The Journal of Finance*, vol. 20, no. 1, pp. 71–77, 1965.
35. M. Tang and V. W. Wong, "An incentive mechanism for cross-silo federated learning: A public goods perspective," in *IEEE INFOCOM 2021-IEEE Conference on Computer Communications*. IEEE, 2021, pp. 1–10.
36. D. Yang, X. Fang, and G. Xue, "Truthful incentive mechanisms for k-anonymity location privacy," in *2013 Proceedings IEEE INFOCOM*. IEEE, 2013, pp. 2994–3002.
37. D. K. Gode and S. Sunder, "Allocative efficiency of markets with zero-intelligence traders: Market as a partial substitute for individual rationality," *Journal of political economy*, vol. 101, no. 1, pp. 119–137, 1993.
38. R. B. Myerson, "Incentive compatibility and the bargaining problem," *Econometrica: journal of the Econometric Society*, pp. 61–73, 1979.
39. T. Wang, Y. Xu, C. Withanage, L. Lan, S. D. Ahipaşaoğlu, and C. A. Courcoubetis, "A fair and budget-balanced incentive mechanism for energy management in buildings," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3143–3153, 2016.
40. J. Ma, J. Deng, L. Song, and Z. Han, "Incentive mechanism for demand side management in smart grid using auction," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1379–1388, 2014.
41. A.-L. Jin, W. Song, P. Wang, D. Niyato, and P. Ju, "Auction mechanisms toward efficient resource sharing for cloudlets in mobile cloud computing," *IEEE Transactions on Services Computing*, vol. 9, no. 6, pp. 895–909, 2015.
42. R. H. Thaler, "Anomalies: The winner's curse," *Journal of economic perspectives*, vol. 2, no. 1, pp. 191–202, 1988.
43. M. Loosemore and B. Lim, "Inter-organizational unfairness in the construction industry," *Construction management and economics*, vol. 33, no. 4, pp. 310–326, 2015.
44. Y. Jiao, P. Wang, D. Niyato, and Z. Xiong, "Social welfare maximization auction in edge computing resource allocation for mobile blockchain," in *IEEE International Conference on Communications (ICC)*, 2018, pp. 1–6.
45. M. Zhang, L. Yang, S. He, M. Li, and J. Zhang, "Privacy-preserving data aggregation for mobile crowdsensing with externality: An auction approach," *IEEE/ACM Transactions on Networking*, vol. 29, no. 3, pp. 1046–1059, 2021.
46. S. Fan, H. Zhang, Y. Zeng, and W. Cai, "Hybrid blockchain-based resource trading system for federated learning in edge computing," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2252–2264, 2020.
47. M. Xu, D. Niyato, J. Kang, Z. Xiong, C. Miao, and D. I. Kim, "Wireless edge-empowered metaverse: A learning-based incentive mechanism for virtual reality," *arXiv preprint arXiv:2111.03776*, 2021.
48. M. Xu, D. Niyato, B. Wright, H. Zhang, J. Kang, Z. Xiong, S. Mao, and Z. Han, "Epvisa: Efficient auction design for real-time physical-virtual synchronization in the metaverse," *arXiv preprint arXiv:2211.06838*, 2022.
49. J. Zhang, M. Zong, and W. Li, "A truthful mechanism for multibase station resource allocation in metaverse digital twin framework," *Processes*, vol. 10, no. 12, p. 2601, 2022.
50. N. C. Luong, Z. Xiong, P. Wang, and D. Niyato, "Optimal auction for edge computing resource management in mobile blockchain networks: A deep learning approach," in *IEEE International Conference on Communications (ICC)*, 2018, pp. 1–6.
51. J. S. Ng, W. Y. B. Lim, Z. Xiong, D. Niyato, C. Leung, and C. Miao, "A double auction mechanism for resource allocation in coded vehicular edge computing," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 2, pp. 1832–1845, 2021.

52. S. Kim, "Auction, learning and bargaining based control scheme for edge assisted metaverse system," *Computer Networks*, p. 109462, 2022.
53. Q. Wang, J. Huang, Y. Chen, X. Tian, and Q. Zhang, "Privacy-preserving and truthful double auction for heterogeneous spectrum," *IEEE/ACM Transactions on Networking*, vol. 27, no. 2, pp. 848–861, 2019.
54. Z. Q. Liew, Y. Cheng, W. Y. B. Lim, D. Niyato, C. Miao, and S. Sun, "Economics of semantic communication system in wireless powered internet of things," in *ICASSP 2022-2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2022, pp. 8637–8641.
55. P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International conference on the theory and applications of cryptographic techniques*. Springer, 1999, pp. 223–238.
56. Y. Jiang, J. Kang, D. Niyato, X. Ge, Z. Xiong, C. Miao, and X. Shen, "Reliable distributed computing for metaverse: A hierarchical game-theoretic approach," *IEEE Transactions on Vehicular Technology*, 2022.
57. Y. Liu, Z. Fang, M. H. Cheung, W. Cai, and J. Huang, "An incentive mechanism for sustainable blockchain storage," *IEEE/ACM Transactions on Networking*, 2022.
58. X. Huang, W. Zhong, J. Nie, Q. Hu, Z. Xiong, J. Kang, and T. Q. Quek, "Joint user association and resource pricing for metaverse: Distributed and centralized approaches," *arXiv preprint arXiv:2208.06770*, 2022.
59. W. Sun, P. Wang, N. Xu, G. Wang, and Y. Zhang, "Dynamic digital twin and distributed incentives for resource allocation in aerial-assisted internet of vehicles," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 5839–5852, 2021.
60. Y. Jiang, J. Kang, D. Niyato, X. Ge, Z. Xiong, and C. Miao, "Reliable coded distributed computing for metaverse services: Coalition formation and incentive mechanism design," *arXiv preprint arXiv:2111.10548*, 2021.
61. E. Daniel and F. Tschorsch, "Ipfs and friends: A qualitative comparison of next generation peer-to-peer data networks," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 31–52, 2022.
62. F. Shams and M. Luise, "Basics of coalitional games with applications to communications and networking," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, no. 1, pp. 1–20, 2013.
63. S. Luo, X. Chen, Z. Zhou, X. Chen, and W. Wu, "Incentive-aware micro computing cluster formation for cooperative fog computing," *IEEE Transactions on Wireless Communications*, vol. 19, no. 4, pp. 2643–2657, 2020.
64. L. Pu, X. Chen, J. Xu, and X. Fu, "D2d fogging: An energy-efficient and incentive-aware task offloading framework via network-assisted d2d collaboration," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 12, pp. 3887–3901, 2016.
65. J. Kang, D. Ye, J. Nie, J. Xiao, X. Deng, S. Wang, Z. Xiong, R. Yu, and D. Niyato, "Blockchain-based federated learning for industrial metaverses: Incentive scheme with optimal aoi," in *2022 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2022, pp. 71–78.
66. H. Du, J. Liu, D. Niyato, J. Kang, Z. Xiong, J. Zhang, and D. I. Kim, "Attention-aware resource allocation and qoe analysis for metaverse xurllc services," *arXiv preprint arXiv:2208.05438*, 2022.
67. X. Wang, Y. Zhao, C. Qiu, Z. Liu, J. Nie, and V. C. Leung, "Infedge: A blockchain-based incentive mechanism in hierarchical federated learning for end-edge-cloud communications," *IEEE Journal on Selected Areas in Communications*, 2022.
68. H. Liu, S. Zhang, P. Zhang, X. Zhou, X. Shao, G. Pu, and Y. Zhang, "Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 6073–6084, 2021.
69. J. Wang, H. Du, Z. Tian, D. Niyato, J. Kang *et al.*, "Semantic-aware sensing information transmission for metaverse: A contest theoretic approach," *arXiv preprint arXiv:2211.12783*, 2022.

70. X. Shen, J. Gao, W. Wu, M. Li, C. Zhou, and W. Zhuang, "Holistic network virtualization and pervasive network intelligence for 6g," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 1–30, 2021.
71. Y. Han, D. Niyato, C. Leung, C. Miao, and D. I. Kim, "A dynamic resource allocation framework for synchronizing metaverse with iot service and data," in *ICC 2022-IEEE International Conference on Communications*. IEEE, 2022, pp. 1196–1201.
72. X. Lin, J. Wu, J. Li, W. Yang, and M. Guizani, "Stochastic digital-twin service demand with edge response: An incentive-based congestion control approach," *IEEE Transactions on Mobile Computing*, 2021.
73. Y. Liu, Z. Fang, M. H. Cheung, W. Cai, and J. Huang, "Economics of blockchain storage," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE, 2020, pp. 1–6.
74. B. Shen, J. Guo, and W. Tan, "An equity-based incentive mechanism for decentralized virtual world content storage," in *International Conference on e-Business Engineering*. Springer, 2019, pp. 19–32.
75. X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, "Making knowledge tradable in edge-ai enabled iot: A consortium blockchain-based efficient and incentive approach," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6367–6378, 2019.
76. W. Hou, H. Wen, N. Zhang, J. Wu, W. Lei, and R. Zhao, "Incentive-driven task allocation for collaborative edge computing in industrial internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 706–718, 2021.
77. T. Huynh-The, Q.-V. Pham, X.-Q. Pham, T. T. Nguyen, Z. Han, and D.-S. Kim, "Artificial intelligence for the metaverse: A survey," *Engineering Applications of Artificial Intelligence*, vol. 117, p. 105581, 2023.
78. J. Thomason, "Metaverse, token economies, and non-communicable diseases," *Global Health Journal*, vol. 6, no. 3, pp. 164–167, 2022.
79. GameFi, "Gaming Guilds: Easy to Earn & Free to Join," 2022. [Online]. Available: https://gamefi.org/
80. T. S. Game, "Join the Metaverse," 2022. [Online]. Available: https://www.sandbox.game/en/
81. Y. Zhao, J. Zhao, L. Jiang, R. Tan, D. Niyato, Z. Li, L. Lyu, and Y. Liu, "Privacy-preserving blockchain-based federated learning for iot devices," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1817–1829, 2020.
82. L. Yuan, Q. He, S. Tan, B. Li, J. Yu, F. Chen, H. Jin, and Y. Yang, "Coopedge: A decentralized blockchain-based platform for cooperative edge computing," in *Proceedings of the Web Conference 2021*, 2021, pp. 2245–2257.
83. C. T. Nguyen, D. T. Hoang, D. N. Nguyen, and E. Dutkiewicz, "Metachain: A novel blockchain-based framework for metaverse applications," in *2022 IEEE 95th Vehicular Technology Conference:(VTC2022-Spring)*. IEEE, 2022, pp. 1–5.
84. ETHEREUM, "The key to your digital future," 2022. [Online]. Available: https://ethereum.org/en/wallets/
85. MetaMask, "A crypto wallet & gateway to blockchain apps," 2022. [Online]. Available: https://metamask.io/
86. S. Suratkar, M. Shirole, and S. Bhirud, "Cryptocurrency wallet: A review," in *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*, 2020, pp. 1–7.
87. Argent, "The best of Ethereum. A fraction of the cost." 2022. [Online]. Available: https://www.argent.xyz/
88. Zksync, "The future-proof zkEVM," 2022. [Online]. Available: https://zksync.io/
89. DefiLlama, "Protocol Categories," 2022. [Online]. Available: https://defillama.com/categories
90. Dexes, "Total Value Locked ETH LSDs," 2022. [Online]. Available: https://defillama.com/protocols/Dexes
91. Lending, "Lending TVL Rankings," 2022. [Online]. Available: https://defillama.com/protocols/Lending

92. CDP, “CDP TVL Rankings,” 2022. [Online]. Available: https://defillama.com/protocols/CDP
93. Liquid Staking, “Liquid Staking TVL Rankings,” 2022. [Online]. Available: https://defillama.com/protocols/Liquid%20Staking
94. Bridge, “Bridge TVL Rankings,” 2022. [Online]. Available: https://defillama.com/protocols/Bridge
95. Yield, “Yield TVL Rankings,” 2022. [Online]. Available: https://defillama.com/protocols/Yield
96. Services, “Services TVL Rankings,” 2022. [Online]. Available: https://defillama.com/protocols/Services
97. Derivatives, “Derivatives TVL Rankings,” 2022. [Online]. Available: https://defillama.com/protocols/Derivatives
98. Yield Aggregator, “Yield Aggregator TVL Rankings,” 2022. [Online]. Available: https://defillama.com/protocols/Yield%20Aggregator
99. Defillama, “Algo-Stables TVL Rankings,” 2022. [Online]. Available: https://defillama.com/protocols/Algo-Stables
100. Cross Chain, “Cross Chain TVL Rankings,” 2022. [Online]. Available: https://defillama.com/protocols/Cross%20Chain
101. Synthetics, “Synthetics TVL Rankings,” 2022. [Online]. Available: https://defillama.com/protocols/Synthetics
102. Launchpad, “Launchpad TVL Rankings,” 2022. [Online]. Available: https://defillama.com/protocols/Launchpad
103. Defillama, “Reserve Currency TVL Rankings,” 2022. [Online]. Available: https://defillama.com/protocols/Reserve%20Currency
104. Insurance, “Insurance TVL Rankings,” 2022. [Online]. Available: https://defillama.com/protocols/Insurance
105. Uniswap, “Welcome to Uniswap Docs,” 2022. [Online]. Available: https://docs.uniswap.org/
106. imToken, “DeFi: What is Curve and how do I use it?” 2022. [Online]. Available: https://medium.com/imtoken/defi-what-is-curve-and-how-do-i-use-it-4da29b2743ca
107. S. Finance, “About Saddle,” 2022. [Online]. Available: https://docs.saddle.finance/
108. Compound, “Introduction,” 2022. [Online]. Available: https://docs.compound.finance/
109. Aave, “Aave Document Hub,” 2022. [Online]. Available: https://docs.aave.com/
110. MarkerDAO, “A better, smarter currency ,” 2022. [Online]. Available: makerdao.com
111. T. S. Life, “EXPLORE. DISCOVER. CREATE.” 2022. [Online]. Available: https://secondlife.com/
112. Tilia, “All-in-One Payment Platform for Digital Economies,” 2022. [Online]. Available: https://www.tilia.io/
113. wtflea, “Facebook Metaverse: Will it Support Blockchain?” 2021. [Online]. Available: http://www.itedge.cn/2021/11/22/facebook-metaverse-will-it-support-blockchain/
114. Decentraland, “Welcome to Decentraland,” 2022. [Online]. Available: https://decentraland.org/
115. H. Market, “Move-in to Your New Home All-Terrain Trailer,” 2022. [Online]. Available: https://www.highstreet.market/
116. Polygon, “Blockchains for mass adoption,” 2022. [Online]. Available: https://polygon.technology/
117. Ethereum, “PLASMA CHAINS,” 2022. [Online]. Available: https://ethereum.org/en/developers/docs/scaling/plasma/
118. Polygon, “Proven scalability on Ethereum,” 2022. [Online]. Available: https://polygon.technology/solutions/polygon-pos
119. Ethereum, “Optimistic Rollups,” 2022. [Online]. Available: https://ethereum.org/en/developers/docs/scaling/optimistic-rollups/
120. Coinmarketcap, “Today’s Cryptocurrency Prices by Market Cap,” 2022. [Online]. Available: https://coinmarketcap.com/

121. B. Intelligence, “Multi-chain future likely as Ethereum’s DeFi dominance declines Bloomberg Professional Services,” 2022. [Online]. Available: https://www.bloomberg.com/professional/blog/multi-chain-future-likely-as-ethereums-defi-dominance-declines/
122. A. AL-BALAGHI, “A multichain approach is the future of the blockchain industry,” 2022. [Online]. Available: https://cointelegraph.com/news/a-multichain-approach-is-the-future-of-the-blockchain-industry
123. A. Takyar, “CROSS-CHAIN WEB3 APPLICATIONS ON POLKADOT,” 2022. [Online]. Available: https://www.leewayhertz.com/cross-chain-web3-applications-on-polkadot/
124. A. Zamyatin, M. Al-Bassam, D. Zindros, E. Kokoris-Kogias, P. Moreno-Sanchez, A. Kiayias, and W. J. Knottenbelt, “Sok: Communication across distributed ledgers,” in *Financial Cryptography and Data Security*, vol. 12675, 2021, pp. 3–36.
125. Coinbase, “Jump start your crypto portfolio,” 2022. [Online]. Available: https://www.coinbase.com/
126. Mayer Christoph,Mai Jesse N, and Tom M, “Tokrex,” 2017. [Online]. Available: www.tokrex.org
127. Corda, “The future of digital finance is built on trust.” 2022. [Online]. Available: https://corda.net/
128. Binance, “How to Buy Bitcoin BEP2 (BTCB) Guide,” 2022. [Online]. Available: https://www.binance.com/en/how-to-buy/bitcoin-bep2
129. Huobi, “Official Launch Of Huobi BTC (HBTC) On Ethereum Network,” 2022. [Online]. Available: https://www.huobi.com/support/en-us/detail/900000196603/
130. Threshold, “The NEW tBTC dApp is here!” 2022. [Online]. Available: https://dashboard.threshold.network/tBTC/how-it-works
131. Ren, “ren,” 2022. [Online]. Available: https://renproject.io/
132. DeCus, “How does the system work?” 2022. [Online]. Available: https://docs.decus.io/mechanism
133. C. Whinfrey, “Hop: Send Tokens Across Rollups,” 2022. [Online]. Available: https://hop.exchange/whitepaper.pdf
134. Hyphen, “Hyphen - Instant Cross-Chain Transfers,” 2022. [Online]. Available: https://docs.biconomy.io/products/hyphen-instant-cross-chain-transfers
135. Degate, “Trade easy, Sleep easy,” 2022. [Online]. Available: https://www.degate.com/?lang=en-US
136. M. Herlihy, “Atomic cross-chain swaps,” in *Proceedings of the 2018 ACM symposium on principles of distributed computing*, 2018, pp. 245–254.
137. K. NETWORK, “Wrapped Tokens: A multi-institutional framework for tokenizing any asset,” 2022. [Online]. Available: https://wbtc.network/assets/wrapped-tokens-whitepaper.pdf
138. cBridg, “Welcome to cBridgee,” 2022. [Online]. Available: https://cbridge-docs.celer.network/#/
139. L. Network, “Lightning Network Scalable, Instant BitcoinBlockchain Transactions ,” 2022. [Online]. Available: https://lightning.network/
140. T. Li, M. Wang, Z. Deng, and D. Liu, “Sepow: Secure and efficient proof of work sidechains,” in *International Conference on Algorithms and Architectures for Parallel Processing*. Springer, 2021, pp. 376–396.
141. Z. XCAT, “Cross-chain Atomic Trades,” 2022. [Online]. Available: https://github.com/zcash/zcash/projects/4
142. Interledger, “A Protocol for Interledger Payments,” 2022. [Online]. Available: https://interledger.org/interledger.pdf
143. Btcrelay, “BTC Relay,” 2019. [Online]. Available: https://github.com/ethereum/btcrelay
144. A. Zamyatin, D. Harz, J. Lind, P. Panayiotou, A. Gervais, and W. Knottenbelt, “Xclaim: Trustless, interoperable, cryptocurrency-backed assets,” in *IEEE Symposium on Security and Privacy*. IEEE, 2019, pp. 193–210.
145. T. Xie, J. Zhang, Z. Cheng, F. Zhang, Y. Zhang, Y. Jia, D. Boneh, and D. Song, “zkbridge: Trustless cross-chain bridges made practical,” in *ACM Conference on Computer and Communications Security*, 2022, pp. 3003–3017.

146. Cosmos, "The Internet of Blockchains." 2022. [Online]. Available: https://cosmos.network/
147. B. C. Ghosh, T. Bhartia, S. K. Addya, and S. Chakraborty, "Leveraging public-private blockchain interoperability for closed consortium interfacing," in *IEEE Conference on Computer Communications*. IEEE, 2021, pp. 1–10.
148. R. M. Ballardini, "Ai-generated content: authorship and inventorship in the age of artificial intelligence," *Online Distribution of Content in the EU*, 2019.
149. L. Heller and L. Goodman, "What do avatars want now? posthuman embodiment and the technological sublime," in *2016 22nd International Conference on Virtual System & Multimedia (VSMM)*. IEEE, 2016, pp. 1–4.
150. A. Genay, A. Lécuyer, and M. Hachet, "Being an avatar "for real": a survey on virtual embodiment in augmented reality," *IEEE Transactions on Visualization and Computer Graphics*, vol. 28, no. 12, pp. 5071–5090, 2021.
151. S. Liao, J. Wu, A. K. Bashir, W. Yang, J. Li, and U. Tariq, "Digital twin consensus for blockchain-enabled intelligent transportation systems in smart cities," *IEEE Transactions on Intelligent Transportation Systems*, 2021.
152. K. Yang, Z. Zhang, Y. Tian, and J. Ma, "A secure authentication framework to guarantee the traceability of avatars in metaverse," *arXiv preprint arXiv:2209.08893*, 2022.
153. Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, and X. Shen, "A survey on metaverse: Fundamentals, security, and privacy," *IEEE Communications Surveys & Tutorials*, 2022.
154. H. Tian, K. Xue, X. Luo, S. Li, J. Xu, J. Liu, J. Zhao, and D. S. Wei, "Enabling cross-chain transactions: A decentralized cryptocurrency exchange protocol," *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 16, pp. 3928–3941, 2021.
155. J. Wu, Q. Yuan, D. Lin, W. You, W. Chen, C. Chen, and Z. Zheng, "Who are the phishers? Phishing scam detection on ethereum via network embedding," *IEEE Trans. Syst. Man, Cybern. Syst. (TSMC)*, vol. 52, no. 2, pp. 1156–1166, Feb. 2022.
156. W. Chen, Z. Zheng, J. Cui, E. Ngai, P. Zheng, and Y. Zhou, "Detecting Ponzi schemes on Ethereum: Towards healthier blockchain technology," in *Proc. of WWW*. ACM, Apr. 2018, pp. 1409–1418.
157. "Web3 Engine Leads the Cross-Chain Future of the Metaverse," 2022. [Online]. Available: https://medium.com/rangersprotocol/web3-engine-leads-the-cross-chain-future-of-the-metaverse-3b2ba8b02d5e#:~:text=Cross-chain%20is%20the%20key%20to%20the%20multi-chain%20future,to%20realize%20the%20cross-chain%20future%20of%20the%20Metaverse.
158. L. Liu, S. Zhou, H. Huang, and Z. Zheng, "From technology to society: An overview of blockchain-based DAO," *IEEE Open Journal of the Computer Society (OJ-CS)*, vol. 2, pp. 204–215, 2021.

Chapter 6
When Digital Economy Meets Web3: Applications and Challenges

Chuan Chen, Lei Zhang, Yihao Li, Tianchi Liao, Siran Zhao, Zibin Zheng, Huawei Huang, and Jiajiang Wu

Abstract Web3 has attracted a considerable amount of attention due to its unique decentralized characteristics. The digital economy is a driver of high-quality economic development and is currently in a rapid development stage. In digital economy scenarios, the centralized nature of the Internet and other characteristics usually bring about security issues such as infringement and privacy leakage. Therefore, it is necessary to investigate how to use Web3 technologies to solve the pain points encountered in the development of the digital economy. By fully exploring the critical technologies of digital economy and Web3, in this chapter we discuss the aspects of Web3 that should be integrated with the digital economy. Our aim is to find a better entry point to solve the problems in machine learning, finance, and data management, by examining the latest advances of Web3. We hope this chapter will inspire those who are involved in both academia and industry and finally help to build a favorable ecosystem for digital economy in the era of Web3.

Keywords Digital economy · Web3 · Distributed ledger · Cryptography · Privacy computing

C. Chen · L. Zhang · Y. Li · T. Liao · S. Zhao · Z. Zheng (✉)
School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou, Guangdong, China
e-mail: chenchuan@mail.sysu.edu.cn; zhanglei73@mail2.sysu.edu.cn; liyh328@mail2.sysu.edu.cn; liaotch@mail2.sysu.edu.cn; zhaosr3@mail2.sysu.edu.cn; zhzibin@mail.sysu.edu.cn

H. Huang · J. Wu
School of Software Engineering, Sun Yat-sen University, Zhuhai, Guangdong, China
e-mail: huanghw28@mail.sysu.edu.cn; wujiajing@mail.sysu.edu.cn

H. Huang et al. (eds.), *From Blockchain to Web3 & Metaverse*,
https://doi.org/10.1007/978-981-99-3648-9_6

6.1 Introduction

The digital economy grows rapidly in recent years and has been fueled by a fresh round of technical revolution and industrial change, and the digital economy is playing an increasingly significant role in the global economy. The digital economy is an essential driver of high-quality economic development. Tapscott, an American economist, originally put forth the idea of the digital economy in his book *The Digital Economy* in 1994 [1]. When the Internet was still in its infancy, the primary characteristic of the digital economy at the time was the utilization of information in the network for digital flow and transmission. Tapscott predicted that the Internet will fundamentally alter both the global economy and society. In 1998, the US Department of Commerce released a report on the new digital economy and adopted the term "digital economy" for the first time, and thus the concept of the digital economy has gradually been widely recognized by governments and scholars [2].

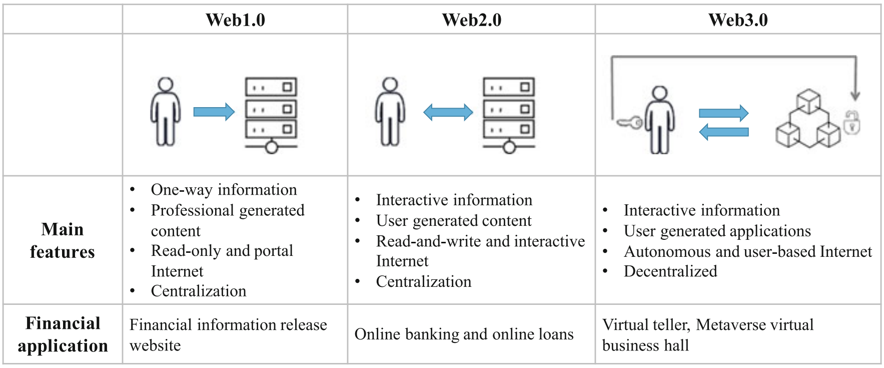
With the progress of the era, the digital economy is developing rapidly and its great potential has been recognized worldwide. The digital economy is increasingly influential in people's lives and has now become the most dynamic and innovative economic form. Nowadays, the digital economy has been acting in various fields, gaining prominence in optimizing the economic structure and promoting industrial innovation. Obviously, the digital economy is an essential part of global economic development [3], becoming a key role in restructuring global factor resources, reshaping the global economic structure, and changing the global competitive landscape.

Digital economy is a new form of economic operation that emerged in the late stage of industrial economy development, which utilizes information network as the major carrier and makes digital resources as production factors [4]. Through modern communication and Internet technologies, the digital economy makes effective usage of resources in various industries of society, thereby creating higher economic benefits than traditional industrial economy operations [5]. Although the development of technology has changed the operation and transaction methods of enterprises and accelerated the reliance of consumers on the Internet, the simple movement of services from "offline" to "online" has been insufficient to meet the demand for online services in the new century [6]. Therefore, many companies are investing significant time and financial resources in providing virtual reality. Thereby, in the process of digital economy development, a series of new information technologies such as cloud computing [7, 8], big data [9, 10], and artificial intelligence [11, 12] has gradually spawned. Thus, it provides technical support to further expand the scale of new industries and economies. A new economic era with the Internet as the main driving force for the economic and social development of each country has opened.

Today, the development of information technology has allowed the digital economy to drive a comprehensive overhaul of production methods, lifestyles, and governance. The popularity of the Internet has led to the massive rise of online economic industries such as social networking, digital art, virtual worlds, etc., while also making security issues such as copyright infringement and privacy breaches easier and more prevalent. At present, unified rules for measuring the value of data have not yet been formed, the digitization of industry has not yet been completed, and digital technology has not yet been industrialized. As we all know, each time a user interacts via the Internet, he or she sends data to the service provider who provides the server, which can easily lead to data security, privacy, and control issues [13, 14]. Therefore, a "decentralized" Internet based on blockchain distributed storage technology, i.e., Web3, has been developed in recent years.

Web3 is described as the potential next phase of the Internet, which is a "decentralized" Internet running on top of blockchain-related technologies. In Web3, data presents a distributed storage structure, so that there will be no central node for data management, which significantly reduces the service cost of managing data [15]. Therefore, the digital economy platform established based on Web3 technology is the new trend of the current development.

Since the creation of the World Wide Web in 1989 [16], the Internet has experienced the Web 1.0 era with TCP/IP and other open protocols as the underlying technologies. Web 1.0 is mainly characterized by the user's access to information provided and understood in a single direction. Users can usually only click on the links on the web page to browse the text, images, and other contents set by the developer. Soon, Web 1.0 was replaced by Web 2.0. Web 2.0 is characterized by user-created personalized recommendations for interaction, where users are not limited to browsing the Web but can also create their own content and upload it to the Web to share with others. The original purpose of Web 2.0 was to bring the Internet closer to democracy and to make users more interactive. Nowadays, the Internet has entered the Web3 era based on blockchain and artificial intelligence and marked by decentralization and intelligence [17]. The Web3-based Internet has shifted banking business from offline to online, and digital transformation of the Internet has formed an industry consensual. And the development of web technologies could be illustrated in Fig. 6.1.



	Web1.0	**Web2.0**	**Web3.0**
Main features	• One-way information • Professional generated content • Read-only and portal Internet • Centralization	• Interactive information • User generated content • Read-and-write and interactive Internet • Centralization	• Interactive information • User generated applications • Autonomous and user-based Internet • Decentralized
Financial application	Financial information release website	Online banking and online loans	Virtual teller, Metaverse virtual business hall

Fig. 6.1 The evolution of web technologies

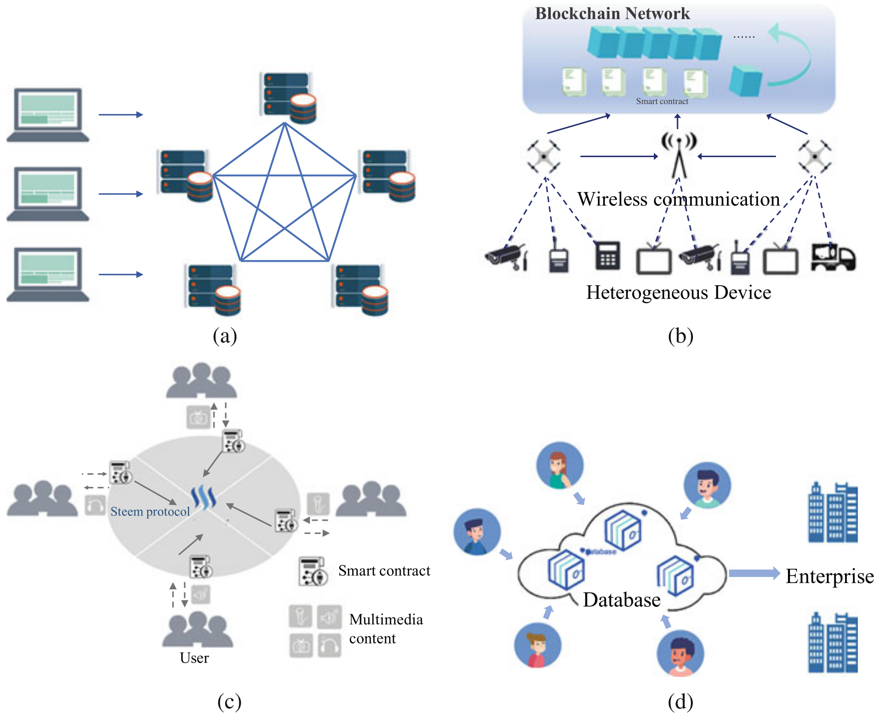


Fig. 6.2 Applications of digital economy in the era of Web3. (**a**) Decentralized storage. (**b**) UAV-assisted IIoT. (**c**) DAO. (**d**) Data transaction

In Web3, websites are allowed to have the ability to learn on autonomy themselves [18]. Moreover, blockchain distributed storage technology is adopted to realize a decentralized autonomous network. Users can accomplish content publishing, economic transactions, and other actions without going through a centralized platform. They employ DAO to manage their digital identities, assets, and data by themselves, through the extended reality (XR) technology hardware and blockchain distributed storage technology together which form the technical foundation of Web3 [19]. Therefore, Web3 can provide decentralized services for the digital economy, as well as unified consensus data valorization services, thus providing a favorable foundation for the development ecology of the digital economy. And some typical applications of combining digital economy with Web3 are illustrated in Fig. 6.2.

In summary, the contributions of this chapter are described as follows.

- We introduce the preliminaries of Web3 and review the state-of-the-art studies of Web3.
- We present four core components of the digital economy and then discuss how Web3 can be effectively integrated with the digital economy in each component.

- We envision typical challenges to shape the future digital economy in the next decades.

The organization of this chapter is as follows. Section 6.2 introduces the preliminary of blockchain, distributed storage, and privacy computing. Section 6.3 systematically introduces the related works on Web3 technologies. Some applications and challenges of combining digital economy with Web3 technology are introduced in Sects. 6.4 and 6.5 respectively. Finally, Sect. 6.6 concludes this chapter.

6.2 Preliminary

In this section, several fundamentals about Web3 will be introduced, such as blockchain, distributed storage, and privacy computing.

6.2.1 Blockchain

Blockchain is the main foundation of the decentralized system of Web3, and it returns digital sovereignty to users through the decentralized power of blockchain. The technology architecture of blockchain is given as Fig. 6.3. The key technology stack [20] will be introduced.

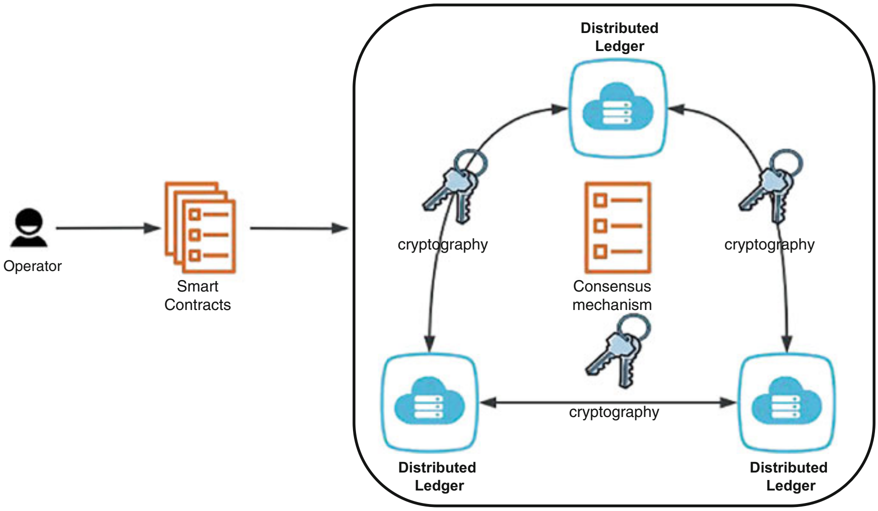


Fig. 6.3 Technology architecture of blockchain

6.2.1.1 Distributed Ledger

The distributed ledger is a database on a peer-to-peer network without a central administrator that maintains data consistency among multiple enterprises or institutions through a consensus mechanism. Each node/enterprise/institution has a complete and identical copy of the data. Any changes or additions made to the ledger are reflected and copied to all participants in a matter of seconds or minutes [21]. Distributed ledgers are inherently more difficult to be attacked because all of the distributed copies need to be changed simultaneously for an attack to be successful. As a result, cyberattacks are reduced using distributed ledgers. And financial fraud is also reduced by the use of distributed ledgers because distributed ledgers provide for an easy flow of information [22], which makes an audit trail easy to follow for accountants when they conduct reviews of financial statements. This helps remove the possibility of fraud occurring on the financial books of a company.

6.2.1.2 Cryptography

Since blockchain operates with a decentralized, peer-to-peer network, model and nodes don't have to trust one another [23]. Therefore, blockchain must ensure appropriate safeguards for transaction information on unsecured channels while maintaining transaction integrity [24]. And consequently, cryptography becomes an essential requirement for blockchain to safeguard user transaction information and privacy alongside ensuring data consistency [25]. Blockchain leverages the real-world concept of signatures by using cryptography techniques and encryption keys. Basically, cryptography is a technique for transmitting secure information between two or more participants [26]. The whole process works by the sender encrypting the message with a specific type of key and algorithm and then sending it to the receiver. The receiver uses decryption to get the original message. Encryption keys ensure that unauthorized recipients or readers cannot read messages, data values, or transactions. They ensure that only the intended recipient can read and process a specific message, data value, or transaction. In recent years, many new tools related to cryptographic applications in blockchain have emerged with different functionalities.

6.2.1.3 Consensus Mechanism

In order to maintain the consistency of the distributed ledger, the blockchain needs to reach a consensus on the block transaction history. How to make each node keep its respective data consistent through a rule is a crucial problem. The solution to this problem is to develop a consensus mechanism.

The consensus mechanism is actually a rule according to which each node confirms its own data. In the blockchain systems, the most commonly used consensus algorithms include PoW, PoS, DPoS, and PBFT [27]. The blockchain system uses this consensus algorithm to make the ledger data of each node in the network agreeable.

6.2.1.4 Smart Contracts

Smart contracts are decentralized, information-sharable program codes deployed on the blockchain that define the logic of applications on a decentralized network [28]. Typically, they function as a digital protocol that follows specific rules for enforcement. These rules are predefined by computer code and are replicated and enforced by all network nodes. Blockchain smart contracts support the creation of de-trusted protocols. This means that both parties to the contract make commitments through the blockchain without the need to know or trust each other [29]. In addition, the use of smart contracts eliminates the need for intermediaries, thereby significantly reducing operational costs. Smart contracts are autonomous and decentralized. Specifically, they usually automatically run the procedures defined in the smart contract when predefined conditions are met, without the intervention of any contract signatory. Besides, they not only give programmability to the underlying data of blockchain but also encapsulate the complex behavior of each node in the blockchain network, providing a convenient interface for establishing upper-layer applications based on blockchain technology [30], and therefore have a significant impact on blockchain. However, when smart contracts are exposed to untrusted systems and lack government oversight, they still have security issues.

6.2.2 Distributed Storage

Distributed storage is the core technology that must be perfected first for the Web3 ecosystem and is an important cornerstone for building the underlying infrastructure of the Web3 ecosystem [31]. Distributed storage is based on blockchain technology that uses open-source applications and algorithms to store sliced data in multiple independent network nodes. It advocates privacy protection, data backup redundancy, and value-oriented data by providing incentives for network nodes and content uploaders. Among the aforementioned features, the incentive model is an important aspect of distributed storage because it allows for long-term data preservation and security. Distributed storage technology in Web3 raises awareness of data security and user data ownership. The major distributed storage projects currently include BitTorrent, Filecoin, and Crust, in which some of these projects will be introduced in the following subsections.

6.2.2.1 BitTorrent

BitTorrent is a decentralized transfer scheme proposed by Bramcoon in 2003. It uses an efficient software distribution system and peer-to-peer technology to share large files (such as a movie or TV show) and enables each user to provide upload services. It did not require the content resource publisher to own the high-performance server to transfer the data, and the more users downloading the same file, the faster the download speed can be. In addition, the free model also attracts the use of the majority of Internet users. However, BitTorrent must use the torrent file containing all targeted content addresses to perform the download. The downloading content is strictly restricted within the scope of the torrent file. Furthermore, BitTorrent lacked incentives to motivate users to share unpaid files. So BitTorrent can be described as a prototype of the distributed storage model.

6.2.2.2 Filecoin

Filecoin is a content-addressable and peer-to-peer distributed protocol and defines how files are stored, retrieved, and transferred in a distributed system, and this enables permanent and decentralized preservation of files. Besides, Filecoin is also a peer-to-peer network for storing files, with built-in economic incentives to motivate the behavior of various players in the network's storage and retrieval market, ensuring the safe and secure storage of files. Filecoin is built on top of IPFS to create a distributed storage marketplace for long-term storage.

6.2.2.3 Crust

Crust is an incentive layer protocol that implements distributed storage and is adapted to multiple storage protocols including IPFS. Besides, Crust is also known as the "Filecoin" on the Polkadot network, an incentive layer protocol based on the Polkadot parallel chain construct. What makes Crust different from other distributed storage projects is its pioneering use of a hardware solution, trusted execution environment (TEE) technology, as the core solution to quantify and verify the actual workload of nodes within the local CPU hardware. Based on TEE, Crust proposed Meaningful Proof of Work (MPoW) to count the storage workload of nodes and report it to the chain. Crust also proposes a PoS consensus algorithm that defines the number of storage resources, called Guaranteed Proof of Stake (GPoS). The workload report is recorded and packaged into a block along with other transactions to calculate a Staking amount, and then based on this amount, PoS consensus is performed.

6.2.3 Privacy Computing

Web3 emphasizes the protection of users' personal data, and therefore, as a key technology to solve the data privacy problem, privacy computing is becoming the immediate need of Web3 existence. Privacy computing technology can analyze and calculate data under the premise of protecting data privacy and security, which provides a strong guarantee for efficient and safe circulation of data across industries and organizations. Currently, privacy computing technologies are classified as secure multi-party computing, federated learning, and trusted execution environment (TEE). In the following, we will introduce each of them.

6.2.3.1 Secure Multi-Party Computation

Secure multi-party computation (MPC) [32] was proposed by Andrew Chi-Chih Yao in 1982 through the Millionaire problem. It aims to solve the problem of collaborative layout for privacy protection among a group of participants who do not trust each other. Furthermore, it provides the data demanders with the ability of multi-party collaborative computing without disclosing the original data. MPC is mainly concerned with the problem of how to securely compute an agreed function without a trusted third party while requiring that each participant cannot get any input information from other participants except the computation result. It mainly involves zero-knowledge proof, homomorphic encryption, differential privacy, inadvertent transmission techniques, etc. However, the higher computational or communication complexity puts some limitations on the usability of MPC.

6.2.3.2 Federated Learning

Federated learning is a machine learning technique developed to solve the problem of data silos [33]. Its goal is to conduct efficient machine learning among multiple participants or multiple computing nodes while guaranteeing security and protecting privacy when exchanging data. Currently, federated learning is classified into three categories according to the different data distributions among participants: horizontal federated learning, vertical federated learning, and federated transfer learning. The workflow of federated learning is given in Fig. 6.4.

6.2.3.3 Trusted Execution Environment

The trusted execution environment is based on a hardware-secure CPU that implements memory-isolated secure computing, allowing privacy-preserving computations to be performed with guaranteed computational efficiency [34]. The basic idea is that all calculations of sensitive data are performed in an isolated memory

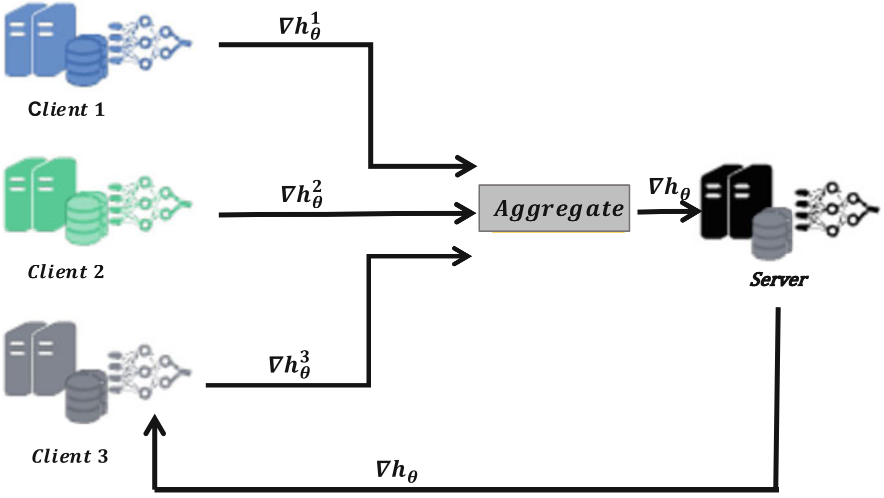


Fig. 6.4 The workflow of federated learning

that no other hardware parts can access except for authorized interfaces. In this way, private computation of sensitive data is achieved. The security comes from the isolated hardware device's ability to resist attacks while avoiding additional communication processes and significant computational overhead. However, the disadvantage is that its security relies heavily on the hardware implementation, making it vulnerable to attacks from different attack surfaces.

6.3 Related Work

Recently, Web3 has been widely researched, and more representative technologies will be introduced.

6.3.1 Fundamental Research

The crucial component of Web3 is the network structure and security is important nature of Web3. In order to enhance the security of the network to meet the requirements of Web3, there are several efforts to give their respective solutions.

Nowadays, web applications are built on centralized network protocols, and these protocols have disadvantages such as being vulnerable to attacks and prone to single points of failure. And therefore, Mainframe [35], a fully decentralized communications layer, is proposed to replace the original centralized network protocols. Based on this, many applications could be easily extended to decentralized scenarios, such as email service.

According to the definition of Web3, blockchain is a core component and could be regarded as a backbone where Web3 applications are built and where the data is stored. For privacy issues, the data should be encrypted and stored in a distributed manner with multiple copies. However, traditional solution proof-of-replication (PoRep) consumes a lot of resources. For reducing the consumption of resources, Kan et al. proposed a new PRE scheme [36], in which transferring the ciphertext into a new one is not required, therefore conserving computing resources.

Recently, blockchain technology has also been widely researched, and Huang et al. [37] reviewed the research related to blockchain and then gave several major research directions. In terms of smart contracts, Zheng et al. [38] reviewed the research related to smart contracts, and Kong et al. [39] proposed a novel method to characterize and detect gas-inefficient patterns. Considering smart contracts are vulnerable to attack, SmartDagger [40] is proposed to detect cross-contract vulnerability based on the bytecode of smart contract. To make blockchain technology healthier, Park [41] used parallel-fork symbolic execution to accelerate smart contract vulnerability detection. Considering the lack of regulation of blockchain, the Ponzi schemes on Ethereum [42] should be detected, and permissions [43] should be appropriately limited.

6.3.2 Benefits to Artificial Intelligence

Traditional artificial intelligence technologies are typically presented in a centralized form; however, this generally leads to inflexibility, poor scalability, etc.

Cao et al. presented a new concept named decentralized artificial [44], and the authors also give the main research areas where Web3 and artificial intelligence are combined, such as edge intelligence and decentralized communication.

With Web3, artificial intelligence could present a decentralized form, and data could be stored by different parties. However, relevant laws and regulations, such as GDPR, may constrain the transmission of data, which has a significant impact on AI technologies that require large amounts of data to support them. To make data available in privacy-protection scenarios and enjoy the benefits of decentralization, federated learning [45] is proposed. In the federated settings, models with local data characteristics replace the original data for transmission and aggregation, and after several rounds of training, a global model with all data features is obtained. For mobile edge computing, combining blockchain with deep reinforcement learning, the performance of computation offloading could be increased [46], and the bitcoin network could be used to enhance complex network analysis [47].

6.3.3 Benefits to Education

COVID-19 makes it impossible for many educational institutions to conduct face-to-face sessions, leading online education especially important. Jiang [48] believes Web3 could bring a new environment for online education and provide personalized technologies to enhance learning effectiveness.

To improve learning outcomes, an online 3D meeting application [49] based on virtual reality (VR) and Web3 is developed. A holographic-based approach is used to ensure intuitive learning and to bridge the remote monitoring gap.

For academic staff or students in higher education, subject information and resources are vital in teaching activities and scientific research. However, these resources are stored separately, and this also poses a challenge for information integration. Considering Web3 is also known as the semantic web where knowledge is connected, bringing the ideas of Web3 for information integration could be a good idea for information integration. Therefore, Han et al. [50] proposed to build a subject information integration system using the new technologies of Web3.

6.3.4 Benefits to Data Management

Recently, the generation of large amounts of data has increasingly tended to be decentralized, and this poses a great challenge to data management. Fortunately, Web3 technologies could be used for the management of large amounts of decentralized data.

IoT devices should be controlled by a third party, and they usually require for transmitting sensitive user data [51]. Therefore, Ayoade et al. [52] proposed a decentralized system of data management for IoT devices, where all data access privileges are stored in the blockchain and smart contracts are used to manage interactions between devices. To make the system safer, TEE is used to store the row data.

When using blockchain to construct data management systems, storage should receive more attention. Since the former data could not be deleted, the storage costs can increase significantly. InterPlanetary File System could be used to solve this problem [53]. When storing data in the blockchain, the hash value is uploaded, rather than the row data, and the hash value could be acquired by uploading data into IPFS. Considering the hash value is smaller than the data itself, storing the hash value decreases costs. And to enhance the security of data storage, MOOCsChain [54] is proposed to incorporate blockchain to enhance security.

6.3.5 Benefits to Business

Web3 could be applied to the financial domain and may change the way how companies use the collected information and sell their products. Almeida et al. [55] analyze how Web3 affects business and give nine kinds of potential business models.

Business models are explored from many aspects. Momtaz et al. [56] believe Web3 may give rise to new products and business models since the components of Web3 reduce transaction costs and the trust of interaction between social and economic has been formed for the decentralized consensus mechanisms.

Toyoda et al. [57] apply Web3 to behavioral economics and propose an incentive mechanism based on crypto-enabled services, and this mechanism is general and even can be applied for services that required making decisions under an uncertain environment. In order to prevent from Internet giants monopolizing the power to use user data, Web3 needs to establish a decentralized identifier (DID), and the DID could be used to link user data in the form of DID documents. Hence, user assets also need to be represented decentrally. Non-fungible token (NFT) [58] is proposed to represent physical assets in a decentralized form, which have become an important part of Web3. However, the development standards of NFT are missing, leading to a couple of underlying systems and failing to govern physical asset value mapping. Yang et al. proposed a general NFT architecture for Web3 [59], and they used a universal connector to connect the upper application environment and the underlying value mapping of the physical asset environment.

Based on Web3, an online shopping platform [60] is designed. The platform incorporates mainstream technology into artificial intelligence and visualizes the 3D presentation of products to ultimately enhance the shopping experience. These mainstream technologies include Web3D, augmented reality (AR), and so on.

6.4 Digital Economy in the Era of Web3

Web3 is considered as an emerging way of how to organize an Internet structure. Many Internet and industrial applications are now obeying the paradigm of server-client structure. Unlike most of the above applications, the new decentralized Web3 applications like cryptocurrency provide many systems with a new organizing method to satisfy the new meets of security, parallel, and other requirements in recent Internet environments.

In this section, first we will introduce the conception and the classification of digital economy and then describe all these categories by analyzing the existing technologies and applications, also by giving an intuitive case as an example in each subsection.

The detailed classification of digital economy and its conception could be divided into four parts as follows:

- Digital Industrialization: The industry includes all the products, hardware, and software around the information technology industry. This is the most important topic where most recent applications using Web3 appeared. In this part, some new technologies like cryptocurrency, decentralization social software, and metaverse software will be introduced.
- Industry Digitization: Industry digitization is committed to using advanced information and digital technology to accelerate innovation in traditional industries like agriculture to help achieve better efficiency and progress during the production process. The main point in this topic often focuses on designing an industrial internet to implement better cooperation during the production process.
- Digital Governance: Digital governance helps all kinds of cooperation agencies to reestablish their rule-based management system by combing with digital technology and also provides assistance to public service. Due to the traditional rule or contract having borne the latent risk of unforeseen and unordered humankind activity like rule-breaking, the introduction of digital technology aims to reduce the influence of these kinds of manners and creates a cooperation system mainly by agreements formulated previously and executed strictly by the machine.
- Data Valorization: Most research on data science attempt to augment the value of data, especially in ways like machine learning. Federated learning is a typical way of using a distributed way to carry out the process of machine learning and satisfy the demand for data security and other needs like calculation efficiency and privacy or so. The main topic of data valorization is finding out a method to collect and fully utilize the everyday data produced by each individual.

The main Web3 applications and their connections with digital economy are listed in Table 6.1. And the relation between digital economy and Web3 could be illustrated in Fig. 6.5. As this figure illustrates, Web3 could promote the development of the digital economy as an engine. Taking digital industrialization as an example, with the help of blockchain, digital technology could be presented as a decentralized form and therefore enhance the security of the digital economy environment.

Table 6.1 Web3 vs. digital economy

	Blockchain	Decentralization	Metaverse
Digital industrialization	DeFi, cryptocurrency, NFT	Decentralized storage technology	Metaverse software
Industry digitization	IIoT	M2M mechanism	AR
Digital governance	Smart city	DAO	–
Data valorization	Federated learning	Data storage	Metaverse with AI

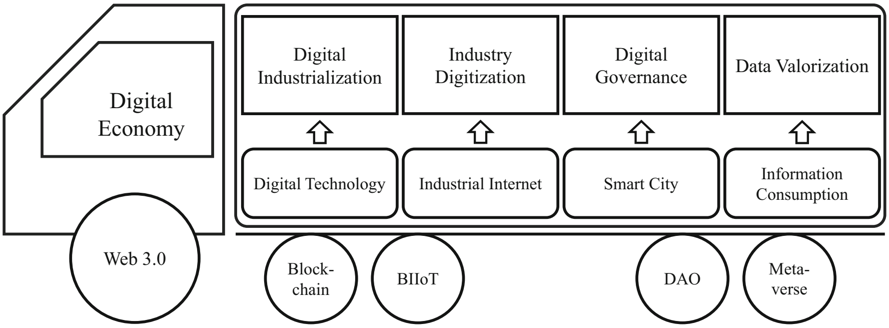


Fig. 6.5 The correlation between digital economy and Web3

6.4.1 Digital Industrialization

Web3 is an emerging way of network architecture organization. The applications based on it naturally impact the related industries of Internet and information technology. With the adoption of a novel design of the blockchain system, Nakamoto first designed a digital currency Bitcoin [61], which opened the prelude to the transformation of the digital economic system, also described as decentralized finance. The key feature of blockchain has brought this cryptocurrency a lot of benefits on persistency, anonymity, and auditability [62]. After that, various cryptocurrencies like Litecoin [63], Ethereum [64], and USDT have emerged one after another and put forward a new idea for the new situation of currency under Web3 to satisfy the new need for a digital currency. In addition to this, blockchain has become a solution for many other applications due to its features of decentralization, privacy, and security preserving. The Smart Red Belly Blockchain system [65] created an enhanced transaction management system for the decentralized applications to use. In this newly designed blockchain system, the author provides all the decentralized apps with faster transaction execution. In addition, the Hyperledger Fabric project [66] gives the developer a powerful tool to develop new applications based on blockchain. This project has given a very clear and direct definition of blockchain which can be seen as a cooperative ledger organized in a decentralized way. Based on this SDK, developers can use whatever programming language to implement a blockchain system on their own.

Another important application of blockchain in Web3 is a non-fungible token (NFT). NFT almost like its name creates a non-fungible mark on the chain to enable artists to create works that can be traded with their digital certificates. According to the definition of NFTs, NFTs represent the rights to unique digital assets and are presented in digital form, and NFTs could even be traded on the market using blockchain technology [67].

The metaverse is an aggregated vessel where lots of technologies can be used to build a virtual world. Therefore, a lot of research put their eye on how to apply Web3 technology into the metaverse [68].

Storage is another important content in the network infrastructure. Given that most of the current storage is collective, the Web3 tech gives a new consumption of constructing a decentralized storage system. We may be familiar with this form of storage like the P2P file sharing system BitTorrent protocol [69] early in 2003. This storage form without a central server may bring out many challenges, but it's a vital question for real decentralized applications, considering the data in these apps must be decentralized too. The technology route of decentralized storage is divided into two main parts according to whether it is based on blockchain or not. Like the IPFS protocol, we discussed the previous chapter and the application Filecoin [70] based on it. The article [71] analyzes the IPFS storage protocol function as a layer of Web3 storage. Also, there exist some storage systems relying on blockchain like Arweave [72] which is similar to Ethereum to store the data on the chain and use the token as a reward to motivate the miner storing files on the chain. Many decentralized applications now still rely on a centralized client for simplicity and usability, so storing the data decentrally will be a critical point to the coming of the real decentralized Web3.

6.4.2 Industry Digitization

The main infrastructure of industry digitization is industrial internet, and the design of industrial Internet aims to connect machines to networks and harvest the production data while also being able to control them remotely, which finally achieves the goal of combing software and machines together. The abstraction of software connects the physical world and can optimize the whole factory above the scale of a single machine. Some entity assets will be replaced by online software, and human labor can also be liberated by the productive forces of a highly connected Internet of machines.

To build an industrial Internet, it should be considered how to connect machines with the upper layer of the Internet. Internet of Things [73] has provided a good research base for the communication between physical objects with the networks. The emergence of blockchain naturally gives these distributed machines a good way to organize an industrial Internet of Things (IIoT) as the basis of industrial Internet [74, 75]. To implement a reliable IIoT, some key features like interoperability, heterogeneity, confidentiality, and safety vulnerabilities must be solved with a reliable plan. And some of these challenges that arise in IIoT can be overcome by using a current form of blockchain techniques that provides solutions with enhanced safety and dependability [76].

Some component has been used in the industrial Internet already and has shown a great influence in the blockchain-based IIoT. A novel communication model, named M2M [77, 78], uses the blockchain to connect the machine with the machine and integrate the factorized machine. Based on this system, some design a power management system, in which the power is transacted between the generator and the machine and can also automatically adjust the load state of the different grids of the machine. The unmanned aerial vehicle (UAV)-assisted M2M system [79] further enhanced the stability of the IIoT, which makes a more capable system of data computation and decision-making.

In addition to these specific models, the Web3-formed IIoT has already been used in various industries. For instance, the blockchain has already been used in the food supply chain as an effective way of monitoring the quality and safety of food by providing a more traceable and transparent chain of food production [80, 81]. The whole supply chain contains from production to transportation and meanwhile involves many subjects like enterprise, consumer, and logistics, which gives the traditional way of monitoring lots of issues that is hard to solve [82]. Smart farming is another important field in which the factors impacting agriculture are complicated and messy and bring many challenges. Fishing now uses many sensors which can provide many data like temperature, humidity, water level, etc. Blockchain can help integrate these decentralized data and helps farmers to monitor and control [83]. Other industries like manufacturing [84, 85], petrochemical industry [86, 87], and automotive manufacturing [88, 89] also use the blockchain as a plan to collect and analyze the production data.

Another possible form of the industrial internet is complemented by metaverse. Metaverse aims to communicate the 3D-formed virtual worlds with the real physical worlds [90]. With the help of AR and VR, many applications can be implemented in the world of metaverse like the healthcare [91], the social software [92], the entertainment [93], and the smart city construction [94].

6.4.3 Digital Governance

Decentralized autonomous organization (DAO) is an important method to achieve digital governance, enabling people to coordinate and govern themselves mediated by a set of self-executing rules deployed on blockchain. The governance form of DAO is decentralized [95]. The early-stage application of DAO like crowdfunding is a specific example with the problem that small-scale investors may suffer from financial mismanagement and outright fraud. The blockchain system Ethereum [96] may have the possibility to solve the issues above. Ethereum acts as an intermediary between the participants and the token, which represents the profit and the right of the participant in this DAO.

Recent community is committed to exploring the other usage of the blockchain and its token of DAO. The stem is a social media platform; it uses the "stem" token to reward the user who uploads the content of text, image, video, or live stream which receive "likes" from others. In this form of social media, the benefits are owned by the content generator instead of the platform, making the participants both users and owners [97]. Another application is Augur [98] based on Ethereum to create a market forecasting system.

6.4.4 Data Valorization

Data valorization analyzes the daily produced data and makes them benefit economically. And the progress of data valorization is often divided into four steps: data requirement and labeling, data analysis, data storage, and data transaction. Due to the limitation of the calculation capability and the storage, putting all these progress distributable often becomes a good way. Moreover, decentralizing all these progresses helps the acquisition of data from the number of users, the calculation using enough computing power, and the storage of data.

Federated learning [99, 100] studies the distribution machine learning program which includes data communication, privacy security, and making good use of the amount of data to train a reliable model. Obviously, the nature of the blockchain can provide the federated learning system with some key components and satisfy some vital requirements of federated learning [101]. Fed2Coin [102] model implements the federated learning system by using blockchain to help overcome the difficulty of the calculation of Shapley Value, the contribution of each user in the cooperation. Fed2Coin helps solve the profit distribution problem among all the participants during the data valorization. Besides, the model BAFFLE [103] aims to design an aggregator based on blockchain. Considering federated learning systems are vulnerable to attacks, BFLC [104] is proposed to defend against byzantine attacks and proved convergent [105].

6.5 Challenges and Open Issues

6.5.1 Web3 for Digital Industrialization

Digital industrialization is primarily to promote digital technology to form a large-scale industry. Currently, Web3 is based on the concept of decentralization and the application of blockchain and other digital technologies to create a new digital ecosystem that integrates multiple scenarios into one. Besides, Web3 is an Internet infrastructure owned and trusted by users and builders. Therefore, in the role of Web3, digital technology based on blockchain and other digital technologies promotes information technology services and consequently accelerates digital industrialization based on digital technologies.

In the era of big data, organizations tend to collect as much data as possible, which is prone to the problem of user privacy violation and threatens the data security of enterprises and individuals [106]. Undeniably, blockchain technology has many advantages in terms of privacy protection. However, the existing technology is still in the stage of development and improvement, while the characteristics of blockchain itself can no longer meet the user's demand for privacy protection. Anonymity is a critical feature of blockchain technology, but this feature brings conflict with privacy protection [107]. In addition to privacy issues, Web3 is a technology that is considered impractical and expensive. However, blockchain-based Web3 systems are extremely cost-inefficient compared to centralized systems such as Amazon Web Services, which can only process a few transactions per minute [108]. Since Web3 can truly achieve the "trustworthiness" of blockchain, it must achieve consensus across the network, which will inevitably affect the transaction throughput. Due to the inefficient PoW algorithm of the blockchain, it consumes a large amount of energy when we save data on the blockchain [109]. Thus, Web3 tends to be energy intensive and technically wasteful and handles only a limited amount of data.

6.5.2 Web3 for Industry Digitization

Industry digitization is mainly to use digital technology to support and promote the transformation and upgrading of traditional industries, while Web3 provides a new scene for this process and can accelerate the growth of information consumption, thus promoting industrial digitization. During the process of industry digitization, data is a key component. And therefore, efficient data management technology in Web3 should be paid more attention to make data work better.

In the context of Web3, the design of the industrial Internet is now facing the issues like communication among heterogeneous devices under the circumstance of calculation resource constraints. The example of the previous UAV-assisted IIoT is a way to fix this by using a different strategy of deployment of the base station, especially when the devices of the industry are often located fragmentedly where the communication condition is poor. Research on edge computing [110] may help resolve the heterogeneity. Another imagination of the industrial internet is the digital twin [111] using the metaverse technology which is now still under exploitation. The problem of practicalizing the metaverse lies in the cyber world's scalability and the computer graphic's bottleneck [90].

6.5.3 Web3 for Digital Governance

Lawrence Lessig argues in *CODE* [112] that the network order will be regulated by laws, codes, markets, and codes at the same time. With the network operator as the main target of regulation, the thought behind it is to require the operator to have the ability to be responsible for the data in the server, which is the traditional regulatory thought in the era of network centrality. Currently, digital governance is regulating blockchain information service providers as well as the filing system, without really considering the challenges that decentralization brings to regulation, let alone the challenges that DAO operations bring to regulation.

Decentralization is the essential feature of blockchain technology, and the existing traditional regulatory model is the exact opposite of this feature, which will inevitably bring great difficulties to digital governance. First, for the purpose of promoting the development of technology, timely and effective regulation of the technology itself is difficult. Besides, the cost of regulation is excessive. Blockchain technology was born among a group of anarchists called "cyberpunks," and the "decentralization" has led to the fact that the privacy on the chain is no longer centrally and uniformly managed but held by the users of each node. In this process, the scope of regulation is not clear, and the subject of regulation cannot be identified, so it is difficult to counter the "dishonesty" of the technology itself under the cloak of the "trustworthiness" of Web3. For instance, one of the earliest and most successful applications of blockchain is Bitcoin, which was in a sense created with evil intentions. Admittedly, Bitcoin is widely used in the "dark web" as a way to launder money and illicit transactions [113], as well as a tool to fund terrorists and insurgents. Therefore, while maintaining the advantages of the blockchain, integration into real-world regulatory systems is a necessary path to the widespread adoption of Web3.

6.5.4 Web3 for Data Valorization

Considering the decentralized feature of Web3, the five core progresses of data valorization, data collection and labeling, data analysis, data storage, and data trading have the potential for decentralization, thus breaking through the limitations of computation and storage. However, in the process of decentralization, many problems may arise.

When building a blockchain-based federated learning system for data analysis, the client's model is uploaded to the blockchain's distributed ledger in the form of a transaction. However, considering the storage as well as consensus efficiency issues, a limit is generally imposed on the size of a single transaction, while in practice, the client-side model may adopt a very large model, resulting in exceeding the blockchain's constraint on transaction size [114]. Although reducing the size of the model as much as possible can alleviate this problem to a certain extent [115], it not only cannot solve the problem fundamentally but also may have the side effect of decreasing the effectiveness of the model and the accuracy of data analysis. Therefore, more efficient consensus algorithms need to be researched. As the model training process proceeds, more and more models will be saved to the blockchain. When model aggregation is performed on the blockchain, the query time will increase when there are more models on the blockchain, because all client models uploaded in this round need to be queried.

6.6 Conclusion

Web3 technologies are expected to play an important role in the digital economy. For instance, blockchain technology could be used to enable decentralized data storage while combining with federated learning to solve possible privacy problems in the process of data analysis and can guarantee the transparency and fairness of the data-trading environment. Combined with the relevant technologies of Web3, the pain point problems in the digital economy will be solved, and the latest applications can be developed rapidly.

By investigating the most relevant work of Web3 in artificial intelligence, education, data management, finance, and Web3-based technologies, we summarize technologies that can be applied to the four core components of the digital economy and provide Web3-based solutions to the problems existing in the development of digital economy. Furthermore, we also analyze the critical challenges and unresolved issues that may arise in deeply integrating Web3 with the digital economy and point out the direction for future research and applications in this area for a good development ecology of the digital economy.

References

1. J. P. Bowman, “The digital economy: promise and peril in the age of networked intelligence,” 1996.
2. D. J. Kim, D. L. Ferrin, and H. R. Rao, “A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents,” *Decision support systems*, vol. 44, no. 2, pp. 544–564, 2008.
3. K. Li, D. J. Kim, K. R. Lang, R. J. Kauffman, and M. Naldi, “How should we understand the digital economy in asia? critical assessment and research agenda,” *Electronic commerce research and applications*, vol. 44, p. 101004, 2020.
4. U. A. Pozdnyakova, I. V. Mukhomorova, V. V. Golikov, S. P. Sazonov, and G. G. Pleshakov, “Internet of things as a new factor of production in the conditions of digital economy,” in *Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT*. Springer, 2019, pp. 1145–1151.
5. H. Kagermann, “Change through digitization–value creation in the age of industry 4.0,” in *Management of permanent change*. Springer, 2015, pp. 23–45.
6. S.-Y. Choi and A. B. Whinston, “The future of the digital economy,” *Handbook on electronic commerce*, pp. 25–52, 2000.
7. V. M. Dincă, A. M. Dima, and Z. Rozsa, “Determinants of cloud computing adoption by romanian smes in the digital economy,” *Journal of Business Economics and Management*, vol. 20, no. 4, pp. 798–820, 2019.
8. A. Strømmen-Bakhtiar, “Digital economy, business models, and cloud computing,” in *Global virtual enterprises in cloud computing environments*. IGI Global, 2019, pp. 19–44.
9. K. H. Tan, G. Ji, C. P. Lim, and M.-L. Tseng, “Using big data to make better decisions in the digital economy,” pp. 4998–5000, 2017.
10. S. V. Novikov, “Data science and big data technologies role in the digital economy,” *TEM Journal*, vol. 9, no. 2, p. 756, 2020.
11. M. Chui, “Artificial intelligence the next digital frontier,” *McKinsey and Company Global Institute*, vol. 47, no. 3.6, pp. 6–8, 2017.

12. A. Bahtizin, V. Bortalevich, E. Loginov, and A. I. Soldatov, "Using artificial intelligence to optimize intermodal networking of organizational agents within the digital economy," in *Journal of Physics: Conference Series*, vol. 1327, no. 1. IOP Publishing, 2019, p. 012042.
13. A. Acquisti, C. Taylor, and L. Wagman, "The economics of privacy," *Journal of economic Literature*, vol. 54, no. 2, pp. 442–92, 2016.
14. W. Kerber, "Digital markets, data, and privacy: competition law, consumer law and data protection," *Journal of Intellectual Property Law & Practice*, vol. 11, no. 11, pp. 856–866, 2016.
15. H. Cui-hong, "Research on web3. 0 application in the resources integration portal," in *2012 Second International Conference on Business Computing and Global Informatization*. IEEE, 2012, pp. 728–730.
16. J. M. Gillies, J. Gillies, R. Cailliau *et al.*, *How the Web was born: The story of the World Wide Web*. Oxford University Press, USA, 2000.
17. M. Hussein, "Transition to web 3.0: E-learning 3.0 opportunities and challenges," in *Proc. EELU Int. Conf. E-Learn.*, 2014, pp. 1–15.
18. J. M. Silva, A. S. M. Mahfujur Rahman, and A. El Saddik, "Web 3.0: a vision for bridging the gap between real and virtual," in *Proceedings of the 1st ACM international workshop on Communicability design and evaluation in cultural and ecological multimedia system*, 2008, pp. 9–14.
19. T. R. Gadekallu, T. Huynh-The, W. Wang, G. Yenduri, P. Ranaweera, Q. Pham, D. B. da Costa, and M. Liyanage, "Blockchain for the metaverse: A review," *CoRR*, vol. abs/2203.09738, 2022. [Online]. Available: https://doi.org/10.48550/arXiv.2203.09738
20. X. Zheng, Y. Zhu, and X. Si, "A survey on challenges and progresses in blockchain technologies: A performance and security perspective," *Applied Sciences*, vol. 9, no. 22, p. 4731, 2019.
21. M. Rauchs, A. Glidden, B. Gordon, G. C. Pieters, M. Recanatini, F. Rostand, K. Vagneur, and B. Z. Zhang, "Distributed ledger technology systems: A conceptual framework," available at SSRN 3230013, 2018.
22. H. Hyvärinen, M. Risius, and G. Friis, "A blockchain-based approach towards overcoming financial fraud in public sector services," *Business & Information Systems Engineering*, vol. 59, no. 6, pp. 441–456, 2017.
23. H. Treiblmaier and C. Sillaber, "The impact of blockchain on e-commerce: a framework for salient research topics," *Electronic Commerce Research and Applications*, vol. 48, p. 101054, 2021.
24. A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE symposium on security and privacy (SP)*. IEEE, 2016, pp. 839–858.
25. G. R. Carrara, L. M. Burle, D. S. Medeiros, C. V. N. de Albuquerque, and D. M. Mattos, "Consistency, availability, and partition tolerance in blockchain: a survey on the consensus mechanism over peer-to-peer networking," *Annals of Telecommunications*, vol. 75, no. 3, pp. 163–174, 2020.
26. J. Katz and Y. Lindell, *Introduction to modern cryptography*. CRC press, 2020.
27. C. Zhang, C. Wu, and X. Wang, "Overview of blockchain consensus mechanism," in *Proceedings of the 2020 2nd International Conference on Big Data Engineering*, 2020, pp. 7–12.
28. S. Rouhani and R. Deters, "Security, performance, and applications of smart contracts: A systematic survey," *IEEE Access*, vol. 7, pp. 50 759–50 779, 2019.
29. J. Lyu, Z. L. Jiang, X. Wang, Z. Nong, M. H. Au, and J. Fang, "A secure decentralized trustless e-voting system based on smart contract," in *IEEE International Conference On Trust, Security And Privacy In Computing And Communications*. IEEE, 2019, pp. 570–577.
30. P. L. Seijas, S. J. Thompson, and D. McAdams, "Scripting smart contracts for distributed ledger technology," *IACR Cryptol. ePrint Arch.*, p. 1156, 2016. [Online]. Available: http://eprint.iacr.org/2016/1156

31. A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "A survey on network codes for distributed storage," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 476–489, 2011.
32. D. Evans, V. Kolesnikov, M. Rosulek *et al.*, "A pragmatic introduction to secure multi-party computation," *Foundations and Trends® in Privacy and Security*, vol. 2, no. 2-3, pp. 70–246, 2018.
33. Q. Li, Z. Wen, Z. Wu, S. Hu, N. Wang, X. Liu, and B. He, "A survey on federated learning systems: Vision, hype and reality for data privacy and protection," *CoRR*, vol. abs/1907.09693, 2019. [Online]. Available: http://arxiv.org/abs/1907.09693
34. M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: what it is, and what it is not," in *IEEE Trustcom/BigDataSE/ISPA*, vol. 1. IEEE, 2015, pp. 57–64.
35. A. Clarke, A. Craig, B. Hagen, C. Youngblood, C. Jaquier, D. Perillo, L. Tavazzani, M. Larson, M. Hagen, M. Mošić *et al.*, "Mainframe: the web3 communications layer," 2018, accessed September 21, 2018. https://mainframe.docsend.com/view/j39qpui.
36. J. Kan, J. Zhang, D. Liu, and X. Huang, "Proxy re-encryption scheme for decentralized storage networks," *Applied Sciences*, vol. 12, no. 9, p. 4260, 2022.
37. H. Huang, W. Kong, S. Zhou, Z. Zheng, and S. Guo, "A survey of state-of-the-art on blockchains: Theories, modelings, and tools," *ACM Computing Surveys*, vol. 54, no. 2, pp. 1–42, 2021.
38. Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," *Future Generation Computer Systems*, vol. 105, pp. 475–491, 2020.
39. Q.-P. Kong, Z.-Y. Wang, Y. Huang, X.-P. Chen, X.-C. Zhou, Z.-B. Zheng, and G. Huang, "Characterizing and detecting gas-inefficient patterns in smart contracts," *Journal of Computer Science and Technology*, vol. 37, no. 1, pp. 67–82, 2022.
40. Z. Liao, Z. Zheng, X. Chen, and Y. Nan, "Smartdagger: a bytecode-based static analysis approach for detecting cross-contract vulnerability," in *Proceedings of the 31st ACM SIGSOFT International Symposium on Software Testing and Analysis*, 2022, pp. 752–764.
41. P. Zheng, Z. Zheng, and X. Luo, "Park: accelerating smart contract vulnerability detection via parallel-fork symbolic execution," in *Proceedings of the 31st ACM SIGSOFT International Symposium on Software Testing and Analysis*, 2022, pp. 740–751.
42. W. Chen, Z. Zheng, J. Cui, E. Ngai, P. Zheng, and Y. Zhou, "Detecting ponzi schemes on ethereum: Towards healthier blockchain technology," in *Proceedings of the 2018 world wide web conference*, 2018, pp. 1409–1418.
43. P. Zheng, Q. Xu, X. Luo, Z. Zheng, W. Zheng, X. Chen, Z. Zhou, Y. Yan, and H. Zhang, "Aeolus: Distributed execution of permissioned blockchain transactions via state sharding," *IEEE Transactions on Industrial Informatics*, 2022.
44. L. Cao, "Decentralized ai: Edge intelligence and smart blockchain, metaverse, web3, and desci," *IEEE Intelligent Systems*, vol. 37, no. 3, pp. 6–19, 2022.
45. Q. Yang, Y. Liu, Y. Cheng, Y. Kang, T. Chen, and H. Yu, "Federated learning," *Synthesis Lectures on Artificial Intelligence and Machine Learning*, vol. 13, no. 3, pp. 1–207, 2019.
46. X. Qiu, L. Liu, W. Chen, Z. Hong, and Z. Zheng, "Online deep reinforcement learning for computation offloading in blockchain-empowered mobile edge computing," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 8, pp. 8050–8062, 2019.
47. B. Tao, H.-N. Dai, J. Wu, I. W.-H. Ho, Z. Zheng, and C. F. Cheang, "Complex network analysis of the bitcoin transaction network," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 3, pp. 1009–1013, 2021.
48. D. Jiang *et al.*, "What will web 3.0 bring to education?" *World Journal on Educational Technology: Current Issues*, vol. 6, no. 2, pp. 126–131, 2014.
49. Y. P. Gupta, A. Chawla, T. Pal, M. P. Reddy, and 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*. IEEE, 2022, pp. 1–5.

50. H. Xiaoting and N. Li, “Subject information integration of higher education institutions in the context of web3. 0,” in *International Conference on Industrial Mechatronics and Automation*, vol. 2. IEEE, 2010, pp. 170–173.
51. E. Fernandes, J. Jung, and A. Prakash, “Security analysis of emerging smart home applications,” in *2016 IEEE symposium on security and privacy (SP)*. IEEE, 2016, pp. 636–654.
52. G. Ayoade, V. Karande, L. Khan, and K. Hamlen, “Decentralized iot data management using blockchain and trusted execution environment,” in *2018 IEEE International Conference on Information Reuse and Integration*. IEEE, 2018, pp. 15–22.
53. P. Poornima Devi, S. A. Bragadeesh, and A. Umamakeswari, “Secure data management using ipfs and ethereum,” in *Proceedings of International Conference on Computational Intelligence, Data Science and Cloud Computing*. Springer, 2021, pp. 565–578.
54. D. Li, D. Han, Z. Zheng, T.-H. Weng, H. Li, H. Liu, A. Castiglione, and K.-C. Li, “Moocschain: A blockchain-based secure storage and sharing scheme for moocs learning,” *Computer Standards & Interfaces*, vol. 81, p. 103597, 2022.
55. F. Almeida, J. D. Santos, and J. A. Monteiro, “e-commerce business models in the context of web3.0 paradigm,” *CoRR*, vol. abs/1401.6102, 2014. [Online]. Available: http://arxiv.org/abs/1401.6102
56. P. P. Momtaz, “Some very simple economics of web3 and the metaverse,” 2022, available at SSRN.
57. K. Toyoda, X. Tran, M. S. Nguyen, and H. T. Dinh, “Web3 meets behavioral economics: An example of profitable crypto lottery mechanism design,” *CoRR*, vol. abs/2206.03664, 2022. [Online]. Available: https://doi.org/10.48550/arXiv.2206.03664
58. Q. Wang, R. Li, Q. Wang, and S. Chen, “Non-fungible token (NFT): overview, evaluation, opportunities and challenges,” *CoRR*, vol. abs/2105.07447, 2021. [Online]. Available: https://arxiv.org/abs/2105.07447
59. L. Yang, X. Dong, Y. Zhang, Q. Qu, and Y. Shen, “Generic-nft: A generic non-fungible token architecture for flexible value transfer in web3,” 2022, techRxiv. Preprint. https://doi.org/10.36227/techrxiv.20486610.v2.
60. T. Xiao, Z. Hu, and L. He, “The design of online shopping platform support system based on web3. 0,” in *International Conference on Economics, Finance and Statistics (ICEFS 2017)*. Atlantis Press, 2017, pp. 230–235.
61. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” *Decentralized Business Review*, p. 21260, 2008.
62. E. G. Weyl, P. Ohlhaver, and V. Buterin, “Decentralized society: Finding web3’s soul,” available at SSRN 4105763, 2022.
63. M. Haferkorn and J. M. Quintana Diaz, “Seasonality and interconnectivity within cryptocurrencies-an analysis on the basis of bitcoin, litecoin and namecoin,” in *International Workshop on Enterprise Applications and Services in the Finance Industry*. Springer, 2014, pp. 106–120.
64. H. Chen, M. Pendleton, L. Njilla, and S. Xu, “A survey on ethereum systems security: Vulnerabilities, attacks, and defenses,” *ACM Computing Surveys*, vol. 53, no. 3, pp. 1–43, 2020.
65. D. Tennakoon and V. Gramoli, “Smart red belly blockchain: Enhanced transaction management for decentralized applications,” *CoRR*, vol. abs/2207.05971, 2022. [Online]. Available: https://doi.org/10.48550/arXiv.2207.05971
66. C. Cachin *et al.*, “Architecture of the hyperledger blockchain fabric,” in *Workshop on distributed cryptocurrencies and consensus ledgers*, vol. 310, no. 4. Chicago, IL, 2016, pp. 1–4.
67. K. B. Wilson, A. Karg, and H. Ghaderi, “Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity,” *Business Horizons*, 2021.
68. Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng, “Fusing blockchain and ai with metaverse: A survey,” *IEEE Open Journal of the Computer Society*, vol. 3, pp. 122–136, 2022.

69. D. Erman, D. Ilie, and A. Popescu, "Bittorrent session characteristics and models," *Traffic and Performance Engineering for Heterogeneous Networks*, vol. 61, no. 84, p. 61, 2022.
70. D. P. Bauer, "Filecoin," in *Getting Started with Ethereum*. Springer, 2022, pp. 97–101.
71. D. Trautwein, A. Raman, G. Tyson, I. Castro, W. Scott, M. Schubotz, B. Gipp, and Y. Psaras, "Design and evaluation of ipfs: a storage layer for the decentralized web," in *Proceedings of the ACM SIGCOMM 2022 Conference*, 2022, pp. 739–752.
72. S. Williams, V. Diordiiev, L. Berman, and I. Uemlianin, "Arweave: A protocol for economically sustainable information permanence," *Arweave Yellow Paper*, www.arweave.org/yellow-paper.pdf, 2019.
73. K. Rose, S. Eldridge, and L. Chapin, "The internet of things: An overview, 2015," 2015.
74. F. Ahmad, Z. Ahmad, C. A. Kerrache, F. Kurugollu, A. Adnane, and E. Barka, "Blockchain in internet-of-things: Architecture, applications and research directions," in *2019 International conference on computer and information sciences*. IEEE, 2019, pp. 1–6.
75. W. Chen, Z. Zhang, Z. Hong, C. Chen, J. Wu, S. Maharjan, Z. Zheng, and Y. Zhang, "Cooperative and distributed computation offloading for blockchain-empowered industrial internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8433–8446, 2019.
76. R. L. Kumar, F. Khan, S. Kadry, and S. Rho, "A survey on blockchain for industrial internet of things," *Alexandria Engineering Journal*, vol. 61, no. 8, pp. 6001–6022, 2022.
77. X. Wu, B. Duan, Y. Yan, and Y. Zhong, "M2m blockchain: The case of demand side management of smart grid," in *IEEE International Conference on Parallel and Distributed Systems*. IEEE, 2017, pp. 810–813.
78. Z. Meng, Z. Wu, C. Muvianto, and J. Gray, "A data-oriented m2m messaging mechanism for industrial iot applications," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 236–246, 2016.
79. M. Li, F. R. Yu, P. Si, R. Yang, Z. Wang, and Y. Zhang, "Uav-assisted data transmission in blockchain-enabled m2m communications with mobile edge computing," *IEEE Network*, vol. 34, no. 6, pp. 242–249, 2020.
80. D. Tse, B. Zhang, Y. Yang, C. Cheng, and H. Mu, "Blockchain application in food supply information security," in *IEEE International Conference on Industrial Engineering and Engineering Management*, 2017, pp. 1357–1361.
81. M. Peña, J. Llivisaca, and L. Siguenza-Guzman, "Blockchain and its potential applications in food supply chain management in ecuador," in *The international conference on advances in emerging trends and technologies*. Springer, 2019, pp. 101–112.
82. Q. Lin, H. Wang, X. Pei, and J. Wang, "Food safety traceability system based on blockchain and epcis," *IEEE access*, vol. 7, pp. 20 698–20 707, 2019.
83. L. Hang, I. Ullah, and D.-H. Kim, "A secure fish farm platform based on blockchain for agriculture data integrity," *Computers and Electronics in Agriculture*, vol. 170, p. 105251, 2020.
84. S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," *International journal of research in engineering and technology*, vol. 5, no. 9, pp. 1–10, 2016.
85. J. Leng, G. Ruan, P. Jiang, K. Xu, Q. Liu, X. Zhou, and C. Liu, "Blockchain-empowered sustainable manufacturing and product lifecycle management in industry 4.0: A survey," *Renewable and sustainable energy reviews*, vol. 132, p. 110112, 2020.
86. H. Lu, K. Huang, M. Azimi, and L. Guo, "Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks," *Ieee Access*, vol. 7, pp. 41 426–41 444, 2019.
87. R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, and M. Omar, "Blockchain in oil and gas industry: Applications, challenges, and future trends," *Technology in Society*, vol. 68, p. 101941, 2022.
88. R. Guhathakurta, "Blockchain in automotive domain," *The Age of Blockchain: A Collection of Articles; IndraStra Global: New York, NY, USA*, p. 17, 2018.
89. P. K. Sharma, N. Kumar, and J. H. Park, "Blockchain-based distributed framework for automotive industry in a smart city," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4197–4205, 2018.

90. K. Li, Y. Cui, W. Li, T. Lv, X. Yuan, S. Li, W. Ni, M. Simsek, and F. Dressler, "When internet of things meets metaverse: Convergence of physical and cyber worlds," *CoRR*, vol. abs/2208.13501, 2022. [Online]. Available: https://doi.org/10.48550/arXiv.2208.13501
91. T. F. Tan, Y. Li, J. S. Lim, D. V. Gunasekeran, Z. L. Teo, W. Y. Ng, and D. S. Ting, "Metaverse and virtual health care in ophthalmology: Opportunities and challenges," *The Asia-Pacific Journal of Ophthalmology*, vol. 11, no. 3, pp. 237–246, 2022.
92. L. Jiaxin and G. Gongjing, "Socializing in the metaverse: The innovation and challenge of interpersonal communication," in *2022 8th International Conference on Humanities and Social Science Research*. Atlantis Press, 2022, pp. 2128–2131.
93. B. Kye, N. Han, E. Kim, Y. Park, and S. Jo, "Educational applications of metaverse: possibilities and limitations," *Journal of Educational Evaluation for Health Professions*, vol. 18, 2021.
94. S.-C. Yoo, D. Piscarac, and S. Kang, "Digital outdoor advertising tecoration for the metaverse smart city," *International Journal of Advanced Culture Technology*, vol. 10, no. 1, pp. 196–203, 2022.
95. S. Hassan and P. De Filippi, "Decentralized autonomous organization," *Internet Policy Review*, vol. 10, no. 2, pp. 1–10, 2021.
96. G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.
97. M. Chang, Q. Min, and Z. Li, "Understanding members' active participation in a DAO: an empirical study on steemit," in *23rd Pacific Asia Conference on Information Systems, PACIS 2019, X'ian, China, July 8-12, 2019*, K. K. Wei, W. W. Huang, J. K. Lee, D. Xu, J. J. Jiang, and H. Kim, Eds., 2019, p. 197. [Online]. Available: https://aisel.aisnet.org/pacis2019/197
98. J. Peterson and J. Krug, "Augur: a decentralized, open-source platform for prediction markets," *CoRR*, vol. abs/1501.01042, 2015. [Online]. Available: http://arxiv.org/abs/1501.01042
99. C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, "A survey on federated learning," *Knowledge-Based Systems*, vol. 216, p. 106775, 2021.
100. H. Huang, R. Li, J. Liu, S. Zhou, K. Lin, and Z. Zheng, "Contextfl: Context-aware federated learning by estimating the training and reporting phases of mobile clients," *Proc. of IEEE ICDCS. IEEE*, pp. 1–11, 2022.
101. D. Li, D. Han, T.-H. Weng, Z. Zheng, H. Li, H. Liu, A. Castiglione, and K.-C. Li, "Blockchain for federated learning toward secure distributed machine learning systems: a systemic survey," *Soft Computing*, vol. 26, no. 9, pp. 4423–4440, 2022.
102. Y. Liu, Z. Ai, S. Sun, S. Zhang, Z. Liu, and H. Yu, "Fedcoin: A peer-to-peer payment system for federated learning," in *Federated Learning*. Springer, 2020, pp. 125–138.
103. P. Ramanan and K. Nakayama, "Baffle: Blockchain based aggregator free federated learning," in *IEEE International Conference on Blockchain*. IEEE, 2020, pp. 72–81.
104. Y. Li, C. Chen, N. Liu, H. Huang, Z. Zheng, and Q. Yan, "A blockchain-based decentralized federated learning framework with committee consensus," *IEEE Network*, vol. 35, no. 1, pp. 234–241, 2020.
105. C. Che, X. Li, C. Chen, X. He, and Z. Zheng, "A decentralized federated learning framework via committee mechanism with convergence guarantee," *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 12, pp. 4783–4800, 2022.
106. P. Jain, M. Gyanchandani, and N. Khare, "Big data privacy: a technological perspective and review," *Journal of Big Data*, vol. 3, no. 1, pp. 1–25, 2016.
107. F. Gille and C. Brall, "Limits of data anonymity: lack of public awareness risks trust in health system activities," *Life Sciences, Society and Policy*, vol. 17, no. 1, pp. 1–8, 2021.
108. Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry," *Financial innovation*, vol. 2, no. 1, pp. 1–12, 2016.
109. C. Xu, K. Wang, P. Li, S. Guo, J. Luo, B. Ye, and M. Guo, "Making big data open in edges: A resource-efficient blockchain-based approach," *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 4, pp. 870–882, 2018.

110. K. Cao, Y. Liu, G. Meng, and Q. Sun, "An overview on edge computing research," *IEEE access*, vol. 8, pp. 85 714–85 728, 2020.
111. F. Tao, H. Zhang, A. Liu, and A. Y. Nee, "Digital twin in industry: State-of-the-art," *IEEE Transactions on industrial informatics*, vol. 15, no. 4, pp. 2405–2415, 2018.
112. L. Lessig, "Code is law," *Harvard magazine*, vol. 1, p. 2000, 2000.
113. Y. Li, W. Susilo, G. Yang, Y. Yu, X. Du, D. Liu, and N. Guizani, "Toward privacy and regulation in blockchain-based cryptocurrencies," *IEEE Network*, vol. 33, no. 5, pp. 111–117, 2019.
114. S. M. Shah and V. K. Lau, "Model compression for communication efficient federated learning," *IEEE Transactions on Neural Networks and Learning Systems*, 2021, https://doi.org/10.1109/TNNLS.2021.3131614.
115. L. Cui, X. Su, Z. Ming, Z. Chen, S. Yang, Y. Zhou, and W. Xiao, "Creat: Blockchain-assisted compression algorithm of federated learning for content caching in edge computing," *IEEE Internet of Things Journal*, 2020.

Chapter 7
What Financial Crimes Are Hidden in Metaverse? Taxonomy and Countermeasures

Jiajing Wu, Kaixin Lin, Dan Lin, Ziye Zheng, Huawei Huang, and Zibin Zheng

Abstract The concept of metaverse has sparked widespread attention from the public to major industries. With the rapid development of blockchain and Web3 technologies, the decentralized metaverse ecosystem has attracted a large influx of users and capital. Due to the absence of industry standards and regulatory rules, the Web3-empowered metaverse ecosystem has witnessed a variety of financial crimes, such as scams, code exploits, wash trading, money laundering, and illegal services and shops. To this end, in this chapter, we first summarize and classify the financial security threats on the Web3-empowered metaverse. Then, from the perspective of academic research and government policy, we summarize the current anticrime measurements and technologies in the metaverse.

Keywords Metaverse · Financial crimes · Code exploit · Scams · Wash trading · Money laundering · Anticrimes

7.1 Introduction

Financial crimes are often defined as crimes against property and involve the unlawful transfer of money or other types of property belonging to another person. In the process of committing financial crimes, offenders usually use illegally acquired property for personal use and benefit. According to the International Monetary Fund, financial crime is "any non-violent crime that generally results in

J. Wu (✉) · H. Huang
School of Software Engineering, Sun Yat-sen University, Zhuhai, Guangdong, China
e-mail: wujiajing@mail.sysu.edu.cn; huanghw28@mail.sysu.edu.cn

K. Lin · D. Lin · Z. Zheng
Computer Science and Engineering, Sun Yat-sen University, Guangzhou, Guangdong, China
e-mail: zhzibin@mail.sysu.edu.cn

Z. Zheng
School of Software Engineering, South China Normal University, Foshan, China

H. Huang et al. (eds.), *From Blockchain to Web3 & Metaverse*,
https://doi.org/10.1007/978-981-99-3648-9_7

a financial loss" [1]. In the UK, the Financial Services and Markets Act defines financial crime as "any offense involving fraud or dishonesty; misconduct in, or misuse of information relating to, a financial market; or handling the proceeds of crime" [2]. Typical financial crimes include scams, wash trading, money laundering, etc. These crimes not only bring losses to investors and users but also pose a certain degree of threat and challenge to the current economic ecosystem.

Along with the recent development of Web3, financial crimes have been given a more diverse and complex meaning in the metaverse ecosystem. Based on the employment of blockchain in metaverse, many fraudsters have found new opportunities for illicit profits, including money laundering, identity theft, and scams [3]. Due to the decentralized and anonymous nature of the metaverse, financial crimes on the metaverse are usually more covertly disguised, making crime detection and financial regulation on the metaverse more difficult.

Therefore, while the advent of the metaverse era has injected new momentum into the financial system and created trade opportunities for social commerce, the lack of effective regulation on blockchain or Web3 may make the metaverse a hotbed of criminal activities, promoting the occurrence of financial crimes such as scams, code exploits, wash trading, money laundering, and illegal services and shops. To this end, an investigation into metaverse financial crimes is particularly urgent and critical. In this section, we provide an overview and taxonomy of financial crimes that have emerged since the development of the metaverse.

7.2 Financial Crimes in Metaverse

7.2.1 Scams

The concept of scam has been around for a long time, with the so-called Golden Age of the Great Scam having been documented in the relevant academic literature in the late nineteenth and early twentieth centuries [4, 5]. Subsequently, Market Business News (MBN) defined scams as dishonest or fraudulent schemes. Such a scheme attempts to obtain money or something of value from people and is a confidence trick perpetrated by a dishonest group, individual, or company. The person or organization committing the scam is often referred to as a scammer, trickster, or swindler [6]. Whereas scams used to occur frequently in offline social interactions, with the growth of the Internet in the past decades, scams have successfully infiltrated online networks. While scams used to occur frequently in offline social interactions, in recent years, with the growth of the Internet, scams have successfully infiltrated online networks. More specifically, in the cryptocurrency market, scammers use the pseudonymous characteristics of cryptocurrencies to perpetrate untraceable crypto-asset scams and attempt to defraud investors for ill-gotten gains [7]. Scams on metaverse can be categorized into the following types [7–9]: (i) Ponzi schemes (Fig. 7.1a); (ii) rug pulls (Fig. 7.1b); (iii) phishing attacks

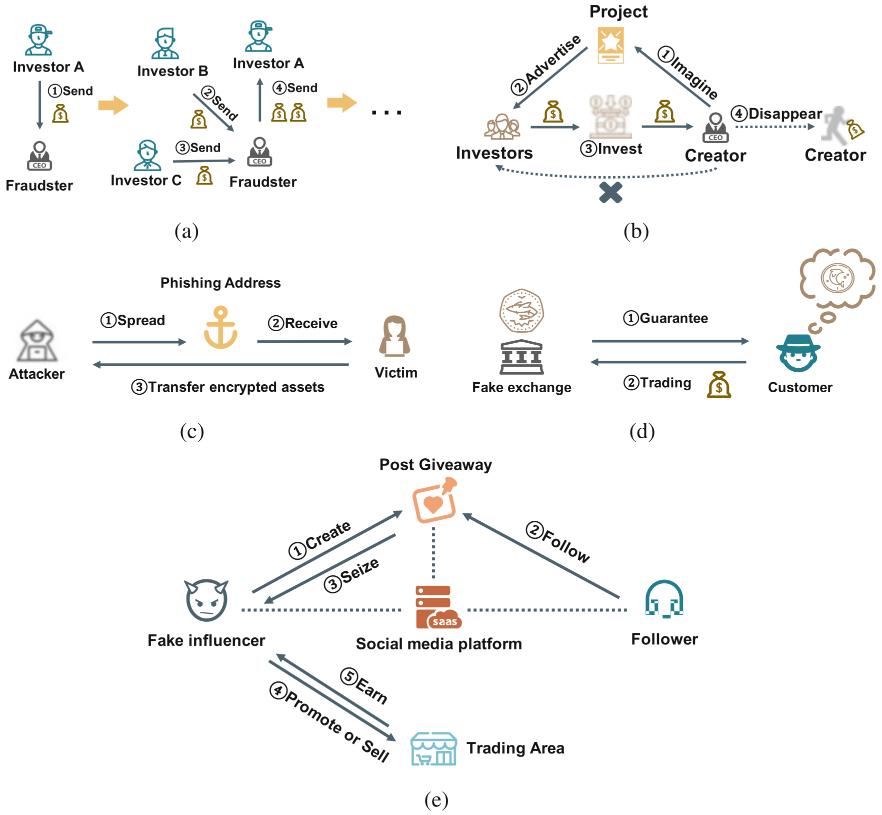


Fig. 7.1 Various types of scams in the context of metaverse. (**a**) Ponzi schemes. (**b**) Rug pulls. (**c**) Phishing attacks. (**d**) Fake exchanges. (**e**) Giveaway scams

(Fig. 7.1c); (iv) fake exchanges (Fig. 7.1d); and (v) giveaway scams (Fig. 7.1e). The basic workflows of various types of scams in the metaverse are shown in Fig. 7.1.

Based on the discussion in Sect. 7.3, the metaverse needs to rely on the existence of crypto markets to operate. This fact has led, on the one hand, to an increasing amount of retail and institutional capital entering the crypto space, bringing a wealth of crypto assets to the metaverse; on the other hand, investors in the emerging economic ecosystem of the metaverse usually have limited education in keeping their money safe and identifying illegal activities, etc. [8]. As a result, a steady stream of scams has also emerged in the metaverse. Furthermore, the diversity of crypto assets in the metaverse has allowed for an expansion of the types of scams. Derivative scams such as fake metaverses, fake land expansions, technical support scams, and 3D social engineering have emerged (these derivative scams will be discussed in detail in the Emerging Crimes in the Metaverse section) [8]. With the development of the metaverse, scams have gradually become a major concern for the security of the decentralized financial system in the metaverse.

7.2.1.1 Ponzi Schemes

Back in December 2017, the staff at Sky Mavis, a Vietnamese studio, conceived the idea of combining cryptocurrency with online gaming and set out to create an Ethereum-based online game called Axie Infinity [10]. This game allows players to own virtual assets and rewards those who are able to reach advanced skill levels. However, due to the introduction of the play-to-earn (P2E) concept in the game [11], many players from low-income South Asian countries began to use the game as their main source of income [12, 13]. This phenomenon has attracted wide attention, and opponents have begun to question this Ponzi-like mechanism of making money from games.

7.2.1.2 Rug Pulls

In early 2022, the creators of the "Big Daddy Ape Club" project, associated with the NFT private collection, presented a private collection of 2222 apes to investors. It then received an investment amount of 9136 SOL, or about $1.3 million, before disappearing from the public eye. This was called the largest "rug pulls" in the history of the Solana blockchain [14]. Notably, it had been verified by the decentralized identity verification company Civic before that. However, this fraudulent act of raising funds and breaking promises still took place.

7.2.1.3 Phishing Attacks

In the same year, Sandbox Game, a community-driven platform that provides a service for user creators to create and monetize voxel assets and gaming experiences on the blockchain, received the onslaught of fraudulent websites claiming to be releasing land for sale in the second quarter [15]. These fraudulent sites have designed and disguised their pages to launch phishing attacks on users of the Sandbox Game.

7.2.1.4 Fake Exchanges

Fake exchanges are also a type of scam that may pose a threat to the security of the metaverse. In December 2017, the Bitcoin community and South Korean authorities exposed a fake exchange called BitKRX [16]. BitKRX lured innocent users by posing as a legitimate exchange and disguising itself as an offshoot of the large and reputable trading platform KRX to scam users out of the amount of money they were holding.

7.2.1.5 Giveaway Scams

Recently, some cases of giveaway scams related to metaverse assets have gradually emerged. In March 2022, when the Yuga Labs team announced the launch of MetaRPG and the native crypto asset ApeCoin, a number of fraudulent actors on social media platforms tried to trick users into clicking on malicious links or sending funds for fraudulent giveaways. In the process, these fraudulent actors managed to raise approximately $900,000 [8].

Researchers have begun to explore the crypto scams involved in the metaverse. Bartoletti et al. [7] review the scientific literature on cryptocurrency scams. A systematic classification of scams was performed based on a new taxonomy, and a unified dataset consisting of thousands of cryptocurrency scams was created by collecting data from different public sources. Smaili et al. [17] provide strategies to deter, detect, and prevent scams by considering both individual (user) and organizational levels. Currently, research on metaverse frauds is still in a relatively preliminary stage, while in-depth methods and applications need to be further explored.

7.2.2 Code Exploit

Since the success of Bitcoin, the applications of blockchain technology are gradually emerging in many fields and services, such as financial markets, Internet of Things, supply chains, healthcare, and storage. Since these systems usually store rich information, blockchain has also become a high-value target for cybercriminals or hackers [18]. Such attacks on the blockchain are usually manifested in various ways of “hacking” into the blockchain system. For instance, some blockchain attacks focus on the poor protection of private keys by blockchain account owners or cryptocurrency exchanges to steal cryptocurrencies or the personal assets of others. Other cyber attackers exploit vulnerabilities in blockchain protocols or their smart contract implementations to compromise blockchain systems [19, 20]. Attacks in this manner are often referred to as code exploit attacks. On the one hand, protocol design vulnerabilities occur when blockchain architects fail to adequately consider the impact of features built into their technology. A typical example is the attack on the Verge cryptocurrency, whose attackers exploit approximately 10% of the hashes of the blockchain for a 51% attack [19]. This problem is not caused by any programming error, but by the design of the protocol itself. On the other hand, many hackers have exploited the vulnerabilities in smart contracts to steal crypto assets. For instance, in June 2016, the smart contract code vulnerability of the DAO was maliciously exploited by hackers to empty more than 2 million ($40 million) Ether coins [21].

Similar to DeFi, there exist a large number of smart contracts in the metaverse. Therefore, cybercriminals can likewise take advantage of poorly structured smart contracts or vulnerabilities in smart contracts to steal cryptocurrencies and NFTs in

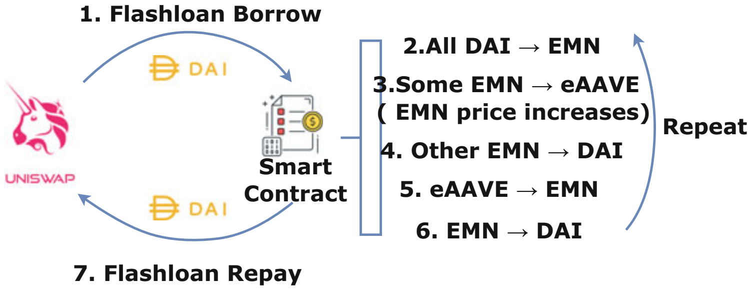


Fig. 7.2 A hacker attacks on Eminence (EMN) by flash loan

the metaverse. There are already examples of code being maliciously exploited in metaverse projects. In September 2020, a developer of Yearn Finance developed an NFT game called Eminence Finance, which has its own token called EMN. Without much understanding of this project, some investors discovered the token and minted $15 million worth of EMN in a few hours. They used a smart contract designed to allow players to exchange DAI (a stablecoin) for EMN to fund in-game purchases. However, a hacker discovered a way to deplete the funds in the contract using a flash loan, which caused the price of the token to drop dramatically. The whole process of the flash loan case on Eminence is shown in Fig. 7.2.

On August 21, 2021, some hackers managed to break into the NFT mint contract for the NFT Gods metaverse game protocol on the Binance Smart Chain. They bypassed the private key check through technical means and stole nearly 9 million LG tokens, the platform's native asset. They then sold these tokens for $1.45 million through a crypto asset exchange service which did not require KYC checks [8]. Additionally, while NFTs are blockchain-based, exchanges and marketplaces such as OpenSea and Rarible operate in a centralized manner, making them unable to take advantage of peer review systems that can identify and fix errors. As a result, they are vulnerable to code exploit attacks. In September 2021, 42 NFTs worth over $100,000 disappeared into thin air due to a vulnerability in the OpenSea token marketplace [22].

At this stage, research on code exploit attacks has mainly focused on the exploration of smart contract vulnerabilities in Ethereum. However, with the development of the metaverse, research on smart contract vulnerabilities in the metaverse is gradually emerging. Ndiaye et al. [23] summarized cryptocurrency crimes by assessing the cost of attacks and losses caused by smart contracts. Moreover, they provide an in-depth analysis of the root causes and consequences behind the attacks and the defense strategies that exist. Kshetri et al. [24] discussed malicious attacks and disruptions on cryptocurrencies and NFTs in the metaverse and provided an in-depth analysis of cyberattacks on crypto assets.

7.2.3 Wash Trading

Wash trading is a market manipulation behavior that has appeared in traditional financial scenarios [25] and is recognized as a financial crime in most countries. Generally speaking, it refers to the repeated trading of assets in order to provide misleading information to the market. For the purpose of commercial competition or commercial interests, wash trading is generally done by several users who collude with each other and appear to be trading, but in fact they do not change their position or assume any real market risks [26]. The US Commodity Futures Trading Commission defines wash trading as "trading or intending to trade that makes the trade appear to be completed without creating market risk or changing the trader's market position" [27]. Wash trading activities inevitably lead to an increase in (fake) trading volume and create a false sense of prosperity.

Wash trading in the metaverse economic system exists mainly in the native cryptocurrency, ERC20 token market, and NFT market.

In fact, many exchanges have been accused of inflating trading volumes through wash trading. In March 2019, Bitwise Asset Management reported to the US Securities and Exchange Commission that 95% of Bitcoin trading volume is fake. By faking volume, the exchanges with the highest trading volumes can receive listing fees from ICOs, reportedly in the millions of dollars [28]. In August 2020, Coinbit, the third-largest cryptocurrency exchange in South Korea, was charged by the police with allegedly faking more than 99% of its trading volume [29]. In the NFT market of the metaverse, wash trading is also quite rampant.

According to Elliptic [8], 95% of all activities on the decentralized NFT trading platform LooksRare are associated with wash trading. There are two main scenarios of NFT wash trading observed so far. One is the fictitious trading volume in order to get on the new NFT collection, which is similar to ICOs' conducting token washing in order to go public. One of the requirements for the centralized NFT trading platform OpenSea to validate an NFT collection is at least 100 ETH transaction volume, which may be difficult to meet for newly launched collections. This requirement appears to encourage fraudulent transactions, where fictitious transactions are executed between multiple accounts under the control of the attackers to artificially inflate transaction volumes. The other main scenario of NFT wash trading is to obtain other token rewards by wash trading through NFT transactions. Chainalysis [30] reported blatant double trading of three identical NFTs between two wallets, trading approximately 650,000 ETH and costing $114 million in transaction fees. They ended up with approximately $185.5 million worth of tokens from the NFT trading platform, bringing in nearly $71 million in profits. This type of wash trading is not without its victims. First, the metaverse project trading platform pay rewards for trading in the fake NFT trading activity, and the wash traders illegally take the rewards of the NFT trading. Second, NFT collectors throughout the metaverse marketplace may be misled by the wash trading into believing that there was active trading activity in native currency or the marketplace for wearables and land NFTs of this metaverse. Therefore, wash traders influence the valuation of metaverse assets and even manipulate the metaverse market.

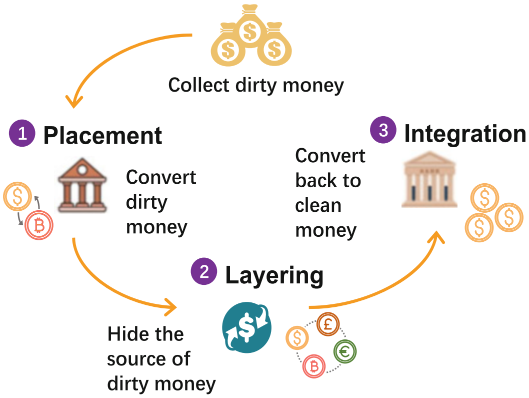
It is extremely challenging to detect and count wash trading. The current main methods of wash trading are based on transaction data. Some work constructs a transaction network by abstracting the transfer relationship between users and employs the network topology theory to analyze and detect the wash trading activities. For instance, Victor et al. [26] proposed a wash trading detection method for decentralized exchanges based on the identification of network loops and cycles. This method found various wash trading structures and manipulated volumes of IDEX and EtherDelta with a total value of $159 million. Serneels et al. [31] proposed three methods to flag suspicious NFT wash trading activities, namely, closed loop token trades, closed loop value trades, and high transaction volumes. Inspired by Victor et al. [26], [32] detected suspicious wash trading in NFT and counts the proportion of suspicious wash trading in the NFT set to the total transaction volume, as well as the proportion of wash trading in the mainstream NFT trading market. Existing work also proposes to design washing behavior indicators through empirical analysis. For instance, Chen et al. [29] designed several metrics to analyze wash trading on centralized exchanges based on off-chain transaction data and on-chain transaction data.

7.2.4 Money Laundering

Money laundering, which is a serious financial crime that fuels crimes such as drug trafficking and terrorism, has a negative impact on the global economy. The Association of Internationally Recognised Anti-Money Launderers (ACAMS) defines money laundering as acquiring the proceeds of crime and disguising their illicit origin in order to use those funds for legal or illegal activities [33]. Intuitively, money laundering is the process of making dirty money look clean. The process of money laundering can be subdivided into three specific steps, as illustrated in Fig. 7.3, namely, placement, layering, and integration [34]. First, illicit funds are surreptitiously channeled into the legitimate financial system. Then, complex financial transactions are used to hide the source of illicit funds, sometimes by wire transfer or by transferring money through numerous accounts to create confusion. Finally, the funds are integrated into the financial system through additional transactions until the “dirty money” looks “clean.” Due to the huge negative financial impacts of money laundering crimes on society, most financial organizations now have anti-money laundering (AML) policies in place to detect and prevent such activities [35].

In a metaverse ecosystem where crypto assets such as NFTs are widely used but legal regulation of metaverse transactions is still immature [36], the potential for money laundering is considered high. In particular, with the growing trend of total sales of land assets and wearables (also known as “skins,” which are clothing and accessories for avatars), in the metaverse, it is highly likely that criminals will use these new assets for illegal money laundering operations.

Fig. 7.3 Three typical steps of money laundering



In terms of metaverse land assets, the total sales of all crypto assets (including land assets in virtual platforms) in the blockchain-powered virtual reality platforms like Decentraland, Cryptovoxels, the Sandbox, and Somnium Space have exceeded $500 million in 2021 [8]. Of those, with millions of dollars of plots sold, the average land value in Decentraland reaches tens of thousands of dollars by 2021 [8], indicating a potential way for a large amount of illicit money to be transferred. In addition, unlike real-world purchases of property or land, purchasing metaverse land often requires only a crypto asset address and some funds without KYC checks, which also makes it extremely convenient for money laundering and other criminal activities.

In terms of wearable device assets, the wearable market is expected to reach $3 trillion by the end of 2023. Criminals can buy a wearable device in one metaverse and then move it to another, cashing out through secondary sales, thus making the money flow harder to track as it spans multiple blockchains. These data suggest that as metaverse financial assets continue to evolve, illegal actors are likely to use them as a conduit for laundering illicit assets that may come from real-world activities or other crypto-based crimes, and criminals can hide their origin [8] by exchanging them for metaverse-based assets (e.g., land in the metaverse, wearable devices, etc.). These data suggest that as metaverse financial assets continue to evolve, it is likely that illicit actors will use them as a primary conduit for laundering illicit assets that may come from real-world activities or other crypto-based crimes and that criminals can hide their origin by exchanging them for metaverse-based assets (e.g., land in a metaverse, wearables, etc.) [8].

With the booming growth of the metaverse and the expansion of crypto assets therein, it is urgent to conduct the investigation and prevention of money laundering crimes on the metaverse economic ecosystem. Recently, Qin et al. [37] discussed money laundering crimes in the crypto market and analyze the legal level measures proposed by countries or regions such as the EU, Japan, and the USA on the prevention of cryptocurrency money laundering crimes in the context of the metaverse. Moreover, Gu et.al et al. [38] and Kampers et al. [39] proposed algorithms to detect unusual transactions in cryptocurrencies in 2022.

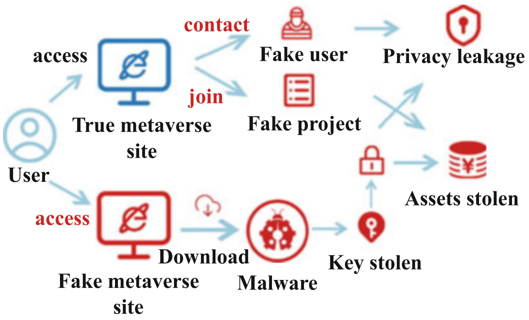


Fig. 7.4 Common fraud pitfalls in metaverse

7.2.5 *Emerging Crimes in Metaverse*

Financial crimes have existed for centuries, but in the metaverse, crimes have taken on a more multifaceted meaning, with multiple types of crime closely related to metaverse crypto assets. Figure 7.4 shows the trap that users may fall into. In this section, six emerging and noteworthy forms of crime, namely, illegal services and shops, fake metaverses, fake land expansions, technical support scams, 3D social engineering, and sanctions and terrorism funding, will be discussed in turn.

7.2.5.1 Illegal Services and Shops

Art galleries, topic-based museums, and project social spaces are popular applications in the metaverse which are closely related to their corresponding real-life scenes. Hybrid shops are a typical way to combine virtual and reality in metaverse business. These shops allow users to purchase items in a metaverse and then pick up the goods offline. During the Decentraland Fashion Week in March 2022, there are shops selling clothing and accessories that allow users to buy goods in a metaverse and have them delivered to a realistic address provided by the user. However, unscrupulous actors may use these shops to sell illegal services and goods, using the items in metaverse shops as a cover for illegal goods in the real world. However, instead of seeing metaverse shops as their main expansion opportunity at the moment [8], illicit actors seem to be focusing their attention on other dark web activities.

7.2.5.2 Fake Metaverses

Criminals sometimes defraud users of their account information and crypto assets by announcing the launch of a new metaverse project or by creating a fake NFT website that resembles a legitimate project. In the case of a fake metaverse, illicit actors may use social media and marketing to promote a metaverse that does not exist. When users try to connect through their MetaMask, they see their accounts wiped out. In the scenario of a fake NFT website, the user is taken to a fake website that appears to be the same as the legitimate website by means of a link and is directed to download the malware present on the website to the user's device. Through malware intrusion, the stored credentials of the user are stolen and used to access the cryptocurrency wallet of the user and transfer all of the crypto assets of the user. A case in point is the fake clone of the MetaversePRO website [40], a fair, community-managed Metaverse financial infrastructure platform, where the fake clone of the website was designed to be indistinguishable from the legitimate website by choosing a slightly different domain name and visually similar pages to make it difficult for users to tell the difference, and then a step-by-step guide to defraud users of their crypto assets.

7.2.5.3 Fake Land Expansions

In a metaverse where the supply of land assets is limited, illicit actors deceive users into buying by launching fake land expansions of new areas or creating fake versions of land assets of famous metaverse projects. This type of scam exists because land resources in the metaverse world are often limited. For instance, the metaverse project of Decentraland started with 90,601 land plots, a portion of which was reserved for community ownership [8]. As limited land resources are gradually sold, reserved land becomes more expensive and appealing as demand outstrips supply, so illegal actors use the scarcity of land and users' inability to recognize the authenticity of metaverse land to falsify and defraud users.

7.2.5.4 Technical Support Scams

Criminals attempt to induce new users to share their private keys or connect their MetaMask wallets to illegal and malicious websites by impersonating staff or technicians of the Metaverse project. In fact, this type of crime is widespread in many areas related to new technologies. Broadly speaking, this type of crime involves scammers using scare tactics to induce users to pay for unnecessary technical support services [41].

7.2.5.5 3D Social Engineering

Social engineering attacks are increasingly rampant in today's networks. Attackers aim to manipulate individuals and businesses to leak valuable and sensitive data [42], using malicious activities accomplished in interpersonal interactions to psychologically influence a person to leak confidential information or compromise security procedures [43]. This attack is manifested in the metaverse primarily in the form of a 3D avatar that the illicit actor may take to impersonate a colleague of the user to psychologically influence and actively share sensitive information and access through legitimate communication.

7.2.5.6 Sanctions and Terrorism Funding

Cybercriminals use crypto assets in the metaverse to assist bad actors to evade sanctions or fund terrorism. This type of crime intends to conduct illegal fundraising through metaverse-related assets. However, the amount of most crypto assets is currently relatively small compared to the total amount needed for terrorism activities, somewhat suggesting that the potential for fundraising in this manner is limited. Moreover, as the metaverse ecosystem evolves, this type of crime may become a serious issue of concern. In this regard, an account with a possible link to the Ryuk ransomware has raised suspicions [8]. Ryuk, a ransomware attributed to the hacker group WIZARD SPIDER [44], was recently discovered. Ryuk is typically used by hackers to target high-value targets, infect systems, and encrypt files in order to force the target to pay a ransom. This account holds NFTs associated with the metaverse and interacts with Ethereum and some ERC20 tokens, and it is estimated that this scammer may have netted a total of $150 million by the end of 2020. While Ryuk and other ransomware campaigns are not sanctioned, the fact that Ryuk and other ransomware campaigns are often operated by sanctioned entities and nation-states suggests that the account is likely committing illegal asset fundraising.

7.3 Anti-crimes in Metaverse

No matter how much emphasis is placed on the “decentralization” and “data freedom” of the Web3-enabled metaverse, regulation is always a key part of the metaverse architecture. In this section, we discuss the current research on the regulation of the metaverse and its basic components from the perspectives of academic research and related policies and measures.

7.3.1 Academic Research

With the rise of the metaverse and the widespread occurrence of related financial crimes, some efforts have been devoted to combating these crimes. The following is a brief overview of existing research on anti-crimes in metaverse from the perspectives of three academic disciplines.

7.3.1.1 Computer Science Field

In the past decade, a series of studies from computer science or software engineering fields focused on blockchain smart contract security, behavioral mining, and anomaly detection.

In terms of smart contract security, Atzei et al. [45] analyzed the security vulnerabilities of smart contracts on Ether, revealing the financial security issues they can cause. In 2022, Kushwaha et al. [46] conducted a systematic review of research on smart contract security issues up to 2022. In addition, security tools [47] and analytical frameworks [48] have been put forward to address security concerns in smart contracts.

In terms of behavioral mining and anomaly detection, according to an overview given in [49], existing work can be divided into four parts: entity identification, transaction pattern recognition, illegal activity detection, and transaction tracking. For instance, Victor et al. [50] proposed a clustering heuristic for entity identification based on the Ethernet account model, Huang et al. [51] modeled the Ethereum transaction records as a large-scale transaction network and proposed a GCN-based model to classify account in Ethereum, and Liu et al. [52] proposed a method called FA-GNN to deal with the heterophily issue for account classification in Ethereum. In [53], Wu et al. proposed temporal attribute heterogeneous modalities and implemented transactional pattern recognition using modal detection. In an environment where the anonymity of cryptocurrencies has led to their widespread use in financial crimes, Akcora et al. [54] propose a cryptocurrency-based ransomware detection framework that can be used to automatically detect ransomware. In addition, a series of data modeling and transaction tracking methods have been proposed [55–62].

Recently, some work started to analyze metaverse security. For instance, Kshetri et al. [24] discussed the impact of possible attacks and various types of frauds on NFT. However, anti-crime research on the metaverse is still at a more preliminary stage compared to related research in the blockchain and cryptocurrency.

Outside of academia, the industry has also paid much attention to security issues in blockchain, Web3, and the metaverse. Several cryptocurrency and Web3 service companies have released reports on security and anti-crime issues. For instance, CERTIK published HACK3D: The Web3 Security Quarterly Report [63], in the second quarter of 2022. This report states that the security of individual projects in Web3 is dependent on the security of the entire ecosystem; ELLIPTIC analyzed potential metaverse financial crime types and proposes corresponding measures to prevent them in a report entitled The Future of Financial Crime in the Metaverse [8] published in 2022; SlowMist analyzed some typical security incidents and published an advanced analysis method for the tracking of coin blender funds in its Blockchain Security and Anti-Money Laundering Analysis Report for the first half of 2022 [64]. Kaggle, the renowned data modeling and analytics competition platform, is also organizing an It's Time to Protect Web3 themed competition in 2022 in partnership with Forta, a community-based decentralized security platform, to identify phishing scam accounts and maintain the security of the Web3 ecosystem.

7.3.1.2 Financial Field

The virtual economic system is a crucial part of the metaverse and the financial community has long studied financial issues in the virtual economy. Smaili et al. [17] flagged the different kinds of fraud risks that can be posed by the metaverse. Wronka et al. [65] analyzed the impact of DeFi on efforts to combat financial crime. Back in 2018, the National Bureau of Economic Research released a study on the Bitcoin economic system [66]. The Financial Action Task Force on Money Laundering (FATF), one of the world's foremost international organizations combating money laundering, updated its guidance on virtual assets and virtual asset service providers [67] in 2021, further requiring countries to assess and mitigate the risks of their virtual asset financial activities. There are corresponding studies in academia, such as Barone et al. [68] comparing usury in traditional economic systems with cryptocurrency as a means of money laundering.

7.3.1.3 Legal Field

Metaverse ecosystem provides the fertile ground for financial crimes, we need norms to reduce the risks to which participants are exposed, and work has been done by researchers on this. Murray et al. [69] considered the legal problems that people need to face in a metaverse. Bokovnya et al. [70] discussed how realistic laws can be changed to combat cryptocurrency crime. Teichmann et al. [71] later proposed a more effective international regulatory standard using the Liechtenstein Blockchain Act [72] as a benchmark.

In addition to these three disciplines, there are many fields such as sociology, political science, international relations, etc. that are concerned with the changes that the metaverse may bring about, especially whether new financial crimes may evolve in such a "beautiful new world" as the metaverse. Since the day the financial markets were created, researchers and practitioners have been actively seeking strategies to combat financial crimes in various emerging areas in order to safeguard the smooth functioning of the system. Research into the financial aspects of the metaverse is still at an early stage and further exploration is needed in the future.

7.3.2 Regulatory Policies and Measures

As mentioned above, the new fertile soil of the metaverse has given birth to many new opportunities but is also coveted by many unscrupulous elements.

Many criminals have expanded their scams to the area of the metaverse. They take advantage of various loopholes in the still incomplete emerging technology to conduct attacks, causing many participating investors to lose their property. Such financial crimes have largely undermined investors' confidence in the future of the metaverse, which is obviously not conducive to its long-term development. Therefore, government organizations around the world have started to introduce policies to regulate various digital assets and related services.

7.3.2.1 United States

In the Anti-Money Laundering Act of 2020 [73] introduced in the United States, virtual assets and digital asset service providers have been included in the regulation of the Bank Secrecy Act. In March 2022, US President Biden signed a presidential order [74] to ensure the responsible development of digital assets, which encourages regulators to monitor the risks posed by digital assets and develop policies to address vulnerabilities and support technological advances to ensure the security of digital assets.

7.3.2.2 Canada

Canada has proposed stricter regulations for virtual currency trading. Cryptocurrency issuance service providers are considered as securities issuers, and virtual currency dealers must register as money service businesses.

7.3.2.3 European Union

Cryptocurrencies in the EU are regulated by the Fifth Money Laundering Directive (5AMLD) [75] introduced back in 2020. It refers to the classification of cryptocurrencies and cryptocurrency exchanges as obligated entities, which involves customer service due diligence and suspicious activity reporting obligations. In addition, it gives financial intelligence units the power to obtain the address identities of owners of virtual currencies. The 5AMLD also proposes that exchanges and wallet providers need to be registered with the relevant domestic authorities, although this is in some sense contrary to the anonymity of cryptocurrencies.

7.3.2.4 United Kingdom

The UK government supports the circulation of cryptocurrencies. They endorse stablecoin as a means of payment; meanwhile, they have also proposed an economic crime legislative review process for crypto assets. In November 2022, the UK financial regulator's joint statement [76] on sanctions and the crypto-asset industry called on crypto-asset firms to identify customers and monitor transactions, update risk assessments of customers and transactions, and conduct reports in a timely manner.

7.3.2.5 Australia

In Australia, crypto assets are regulated as financial products supervised by the Australian Securities and Investments Commission or as consumer products supervised by the Australian Competition and Consumer Commission. Crypto asset exchanges or crypto asset secondary service providers are required to register and be subject to AML/CFT regulation.

7.3.2.6 Singapore

In Singapore, crypto assets are considered “digital payment tokens,” and crypto asset service providers are considered “digital payment token services” and are both governed by the Payment Services Act.

Singapore recently passed the Financial Services and Markets Act 2022 [77], which brings crypto asset companies located in Singapore but providing services outside of Singapore under the regulatory umbrella. Additionally, the bill introduces significant new licensing requirements and grants the Monetary Authority of Singapore new powers.

7.3.2.7 Japan

Japan was one of the first countries in the world to introduce regulation of cryptocurrencies. Different types of tokens are governed by different regulatory provisions in Japan. Their regulatory status is documented in the Japanese Payment Services Law [78].

7.3.2.8 China

In China, the only cryptocurrency currently recognized as legal tender is the E-CNY, while trading in other cryptocurrencies is prohibited since September 2021. Overall, the regulation of digital assets is currently at an immature and experimental stage, with countries having different tools and measures.

7.3.2.9 ICO Regulations

In addition, Initial Coin Offering (ICO) scams have caused a lot of property losses, and countries have proposed related regulatory strategies for ICOs. The strictest countries are China and South Korea, both of which have explicitly banned ICO activities. In Russia, Thailand, and the Philippines, ICOs are not banned, but they are also regulated in a strict manner. Russia has set a cap on the number of funds raised for ICO projects (not to exceed 1 billion rubles), and the Philippines' ICO activities need to be approved by the Philippine Securities and Exchange Commission. Similarly, ICO projects in Thailand are regulated by the authorities such as the Thailand Securities and Exchange Commission, and ICO companies are obliged to provide the names of buyers and sellers and transaction information to the

Anti-Money Laundering Office. In addition, the Thai tax authority will charge 7% VAT and 15% capital gains tax on cryptocurrencies and ICOs. Take Singapore as an example; there is also a part of the country that has always maintained a positive attitude toward ICOs. The Monetary Authority of Singapore only regulates related activities if the ICO poses specific risks.

As for the NFT and Defi programs, there are very few regulatory strategies implemented. In summary, the regulation of crypto assets is still in a preliminary and immature stage, and the relevant agencies will intervene to improve security while inevitably reducing the anonymity and decentralization of transactions and curbing the free development of the industry to a certain extent. Therefore, how reconciling the contradiction between the two is still a proposition that all countries in the world need to think about.

7.4 Opportunities and Challenges

Nowadays, financial regulation and illegal behavior identification technologies related to the metaverse are mainly focused on the cryptocurrency level, and the research on regulation for Web3 is still in its initial stage. However, we can foresee that, in the near future, metaverse technologies will play a fundamental role in a broader field, and the financial regulation on the Web3-enabled metaverse will also show the diversity and uniqueness of technology. Therefore, exploring the possible regulatory opportunities and challenges of the metaverse helps us propose ideas and insights to ensure the healthy development of the metaverse. Since the Web3-enabled metaverse integrates various emerging technologies and systems built on it as its foundation, the regulatory opportunities and challenges for them may also be inherited by the metaverse. As mentioned earlier, the underlying technical foundation of the metaverse is blockchain technology. Thus, the data of the metaverse also has excellent natures of blockchain data, i.e., open and transparent, forgery-proof, tamper-proof, and traceable. Those natures provide unprecedented opportunities for researchers to understand and solve related problems by analyzing blockchain data. Therefore, this section focuses on several opportunities and challenges of financial regulation in metaverse from a data-driven perspective.

7.4.1 Opportunities

Next, we discuss the opportunities of data-driven financial governance in Web3-enabled metaverse at four levels, i.e., the bottom level is data sources, the second level is data acquisition, the third level is data query and indexing, and the top level is data analysis and application, as shown in Fig. 7.5.

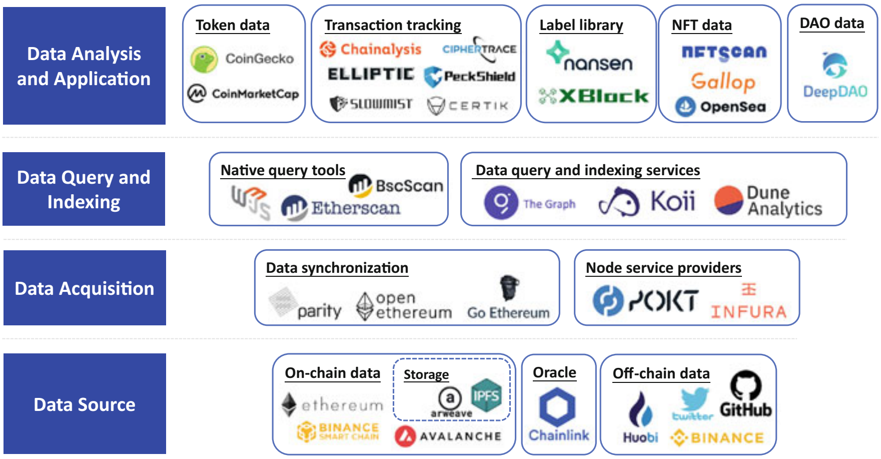
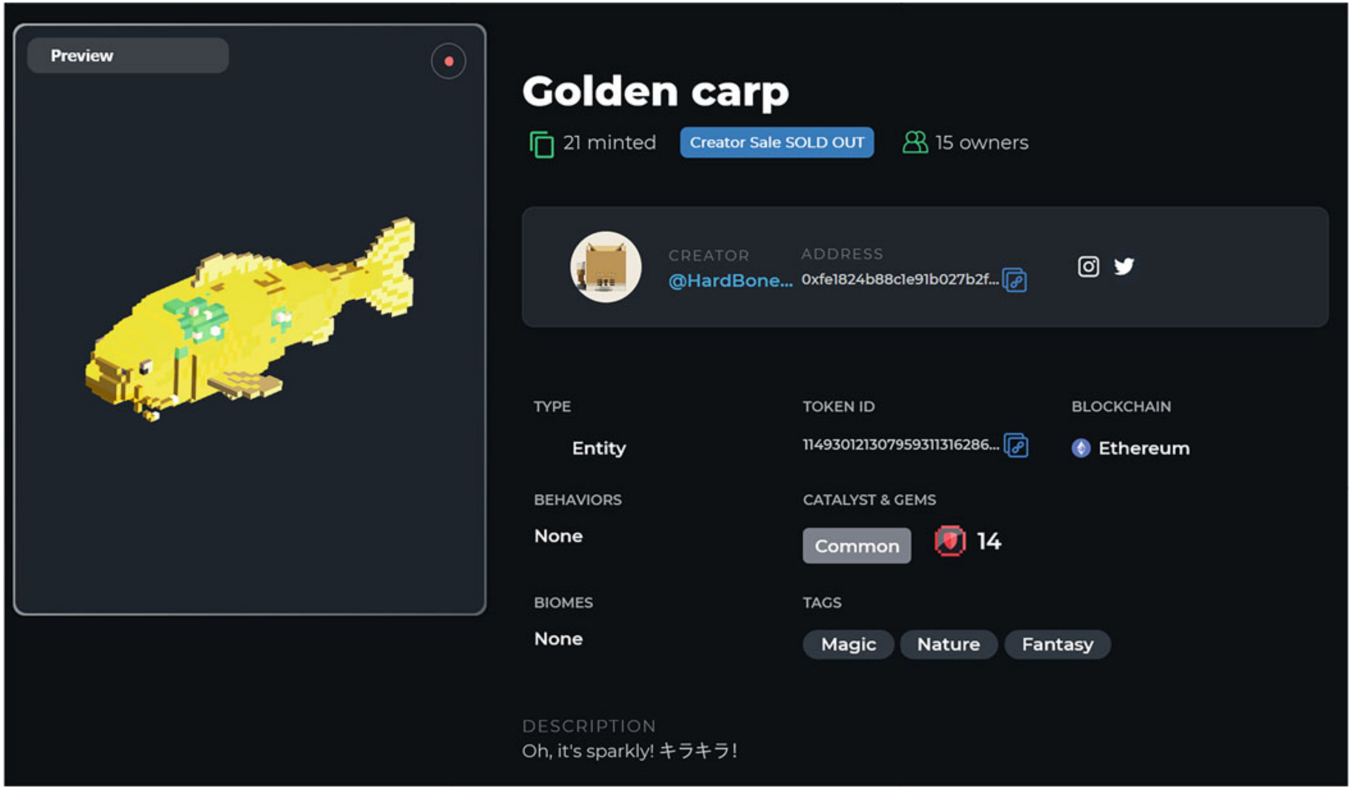


Fig. 7.5 Data track structure for Web3 and metaverse

7.4.1.1 Data Source

The data of blockchain and metaverse can be categorized into on-chain data and off-chain data. On-chain data mainly includes blocks, transfer transactions, wallet addresses, smart contract bytecodes, smart contract events, digital asset information, and other data. In addition, decentralized storage is also the main source of on-chain data, for example, NFT can be saved in the Interplanetary File System (IPFS) [79], a peer-to-peer hypermedia transfer protocol. The off-chain data, on the other hand, mainly includes data from centralized exchanges (e.g., Cryptocurrency Exchange), as well as some typical Web2 data, such as social media data, GitHub website data, etc. For on-chain data, we consider the metaverse project Sandbox (https://www.sandbox.game) as an example. The Sandbox is a virtual metaverse built on the Ethereum blockchain where players can create, own, and monetize their gaming experiences. In the Sandbox game, the ERC-20 protocol is used to execute transactions, including tokens for custom avatars, land purchases, and general game interactions; ERC-1155 and ERC-721 are used to store and trade digital assets (including LAND, player-created ASSET). The Sandbox's NFT or DT transaction data is stored on the Ethereum public chain, and the rest of the NFT attribute information, such as images, is stored on IPFS, which is publicly accessible. Figure 7.6 shows a digital asset on the Sandbox,[1] the asset's transaction and wallet address 0xa342f5d851e866e18ff98f351f2c6637f4478db5 associated with it. The rest of the information, including image, creator address, creator profile url, voxel

[1] https://www.sandbox.game/en/assets/golden-carp/9fbe8f95-af9a-4aa3-a1ec-48921375b01d/.



Golden carp

21 minted | Creator Sale SOLD OUT | 15 owners

CREATOR: @HardBone...

ADDRESS: 0xfe1824b88c1e91b027b2f...

TYPE: Entity

TOKEN ID: 114930121307959311316286...

BLOCKCHAIN: Ethereum

BEHAVIORS: None

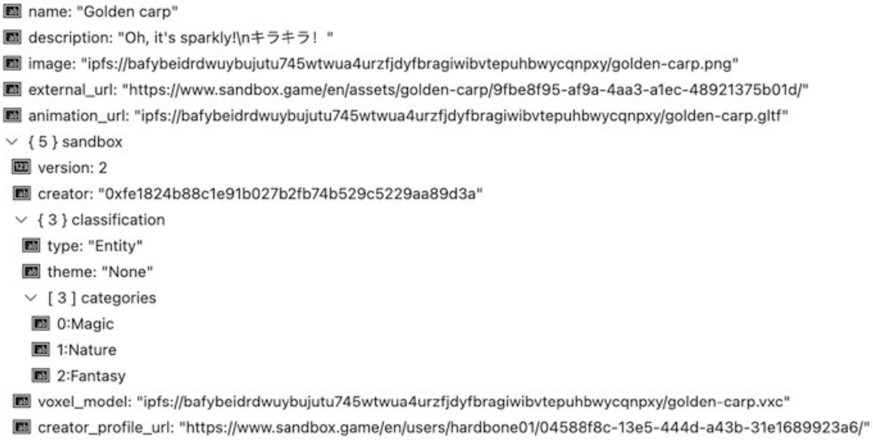
CATALYST & GEMS: Common 14

BIOMES: None

TAGS: Magic Nature Fantasy

DESCRIPTION: Oh, it's sparkly! キラキラ!

Fig. 7.6 A digital asset on the Sandbox



```
name: "Golden carp"
description: "Oh, it's sparkly!\nキラキラ！ "
image: "ipfs://bafybeidrdwuybujutu745wtwua4urzfjdyfbragiwibvtepuhbwycqnpxy/golden-carp.png"
external_url: "https://www.sandbox.game/en/assets/golden-carp/9fbe8f95-af9a-4aa3-a1ec-48921375b01d/"
animation_url: "ipfs://bafybeidrdwuybujutu745wtwua4urzfjdyfbragiwibvtepuhbwycqnpxy/golden-carp.gltf"
∨ { 5 } sandbox
  version: 2
  creator: "0xfe1824b88c1e91b027b2fb74b529c5229aa89d3a"
  ∨ { 3 } classification
    type: "Entity"
    theme: "None"
    ∨ [ 3 ] categories
      0:Magic
      1:Nature
      2:Fantasy
  voxel_model: "ipfs://bafybeidrdwuybujutu745wtwua4urzfjdyfbragiwibvtepuhbwycqnpxy/golden-carp.vxc"
  creator_profile_url: "https://www.sandbox.game/en/users/hardbone01/04588f8c-13e5-444d-a43b-31e1689923a6/"
```

Fig. 7.7 JSON file on IPFS of a digital asset named "Golden carp" on the Sandbox, a metaverse project

model, etc., can be obtained from IPFS on json,[2] as shown in Fig. 7.7. For the off-chain data, we take the metaverse project Decentraland (https://decentraland.org) as an example. Decentraland prepares resource information about technical components for community members or technicians, and it is open source on the GitHub site https://github.com/decentraland/. Moreover, the latest activities of the project can be found on its Twitter site (https://twitter.com/decentraland).

7.4.1.2 Data Acquisition

There are more diverse ways to obtain Web3-enabled metaverse data, but since off-chain data is often the data of centralized institutions (e.g., centralized trading platforms) or Web2 type data, the ways to obtain it vary greatly, so this paper mainly discusses the acquisition of on-chain data.

The underlying blockchain data of metaverse contains a large amount of heterogeneous data, and there are various methods to obtain metaverse on-chain data. Taking the Ethereum-based metaverse project as an example, the main ways to obtain Ethereum on-chain data include: (1) Downloading and directly parsing block files. This method is simple and fast to implement, but it cannot collect complete data. This is because internal transactions are not stored in the blockchain and therefore cannot be obtained by parsing blocks. (2) Deploying an Ethereum client, such as the Parity client's API allowing users to directly access internal transactions and external transactions in Ethereum. However, this method has limited access to

[2] https://ipfs.io/ipfs/bafybeicliqwmhkue4d5ddrvdwhxpu3r3skh4kyxephwutz7dcywwle74ge/1.json.

data, for example, contracts' bytecode data and token transfer data are not accessible [80]. In addition, these two methods require high time, money, and technical costs for users, and thus node service providers facilitating blockchain data acquisition have emerged. Node service providers can therefore also be considered as the infrastructure for data analysis and mining in the Web3-enabled metaverse. Some of the more well-known decentralized data service providers are Pocket Network (https://www.pokt.network/), whose core business is to provide decentralized data relay services (or RPC services) for developers on various public chains. Pocket Network's decentralized infrastructure is helping Klaytn (an open-source meta-universe public chain project[3]) realize its metaverse vision by driving Klaytn to new levels of decentralization, scalability, and cross-chain capabilities.

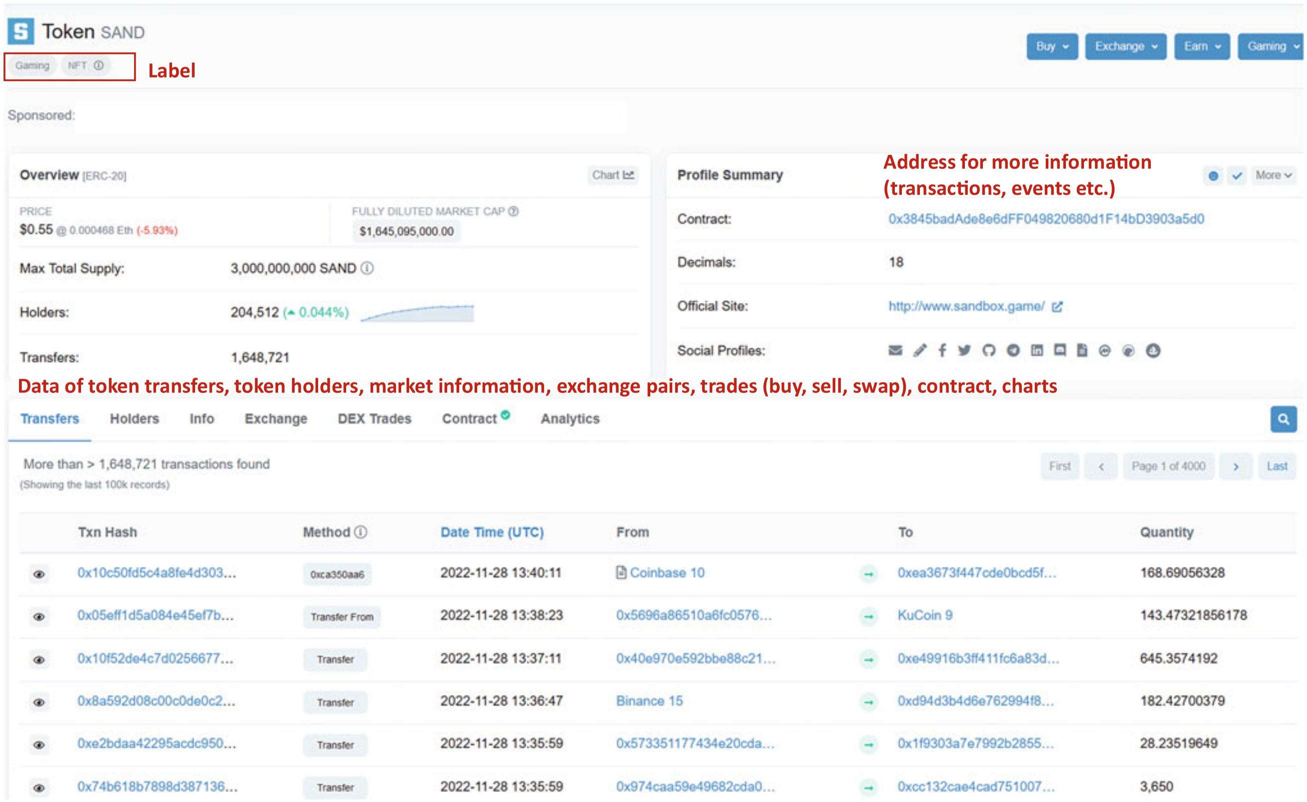
7.4.1.3 Data Query and Indexing

As mentioned earlier, almost all blockchain transactions in the metaverse are publicly available on the blockchain. However, it is usually a daunting work to query and index the raw transaction data, which is often large and diverse in data type. The earliest tools for querying and indexing metaverse data were the APIs of the underlying public chain and blockchain browsers, such as the Web3 API and the Ethereum browser provided by Etherscan. Web3 API uses a remote procedure call (RPC) to communicate with Etherscan nodes. For instance, we call web3.eth.getTransaction() to get data of a specified hash transaction. Etherscan, the Ethereum browser, allows users to search for information on the chain directly through the web page, including data on the chain, data on blocks, transaction data, smart contract data, address data, etc. As shown in Fig. 7.8, according to the address of Sandbox's SAND (traded and governed ERC20 tokens) 0 x3845badAde8e6dFF049820680d1F14bD3903a5d0, and its Token tracker,[4] we can see a wealth of valuable information. This kind of data provides a database for Web3-enabled metaverse data mining and abnormal behavior identification.

In addition to the blockchain browsers of the underlying public chains of the metaverse, there are also service providers that offer data query and indexing services. They make raw data more accessible and usable by parsing and structuring it on top of node service providers that interact directly with various public chains. In what follows, we give two representative examples: (1) Dune Analytics (https://dune.com/) is a comprehensive Web3 data platform that adds raw data to SQL tables and parses them based on APIs provided by node service providers to enable users to query, analyze, and visualize through dashboards in real-time in their well-built databases using SQL. To date, over 10,000 analysts have created approximately 100,000 queries on Dune's platform, ranging from metrics for OpenSea NFTs

[3] https://developer.klaytn.foundation/technology-overview/.

[4] https://cn.etherscan.com/token/0x3845badAde8e6dFF049820680d1F14bD3903a5d0.



Label

Overview [ERC-20]

PRICE
$0.55 @ 0.000468 Eth (-5.93%)

FULLY DILUTED MARKET CAP
$1,645,095,000.00

Max Total Supply: 3,000,000,000 SAND

Holders: 204,512 (▲ 0.044%)

Transfers: 1,648,721

Profile Summary

Address for more information (transactions, events etc.)

Contract: 0x3845badAde8e6dFF049820680d1F14bD3903a5d0

Decimals: 18

Official Site: http://www.sandbox.game/

Social Profiles:

Data of token transfers, token holders, market information, exchange pairs, trades (buy, sell, swap), contract, charts

More than > 1,648,721 transactions found
(Showing the last 100k records)

	Txn Hash	Method	Date Time (UTC)	From		To	Quantity
👁	0x10c50fd5c4a8fe4d303...	0xca350aa6	2022-11-28 13:40:11	Coinbase 10	→	0xea3673f447cde0bcd5f...	168.69056328
👁	0x05eff1d5a084e45ef7b...	Transfer From	2022-11-28 13:38:23	0x5696a86510a6fc0576...	→	KuCoin 9	143.47321856178
👁	0x10f52de4c7d0256677...	Transfer	2022-11-28 13:37:11	0x40e970e592bbe88c21...	→	0xe49916b3ff411fc6a83d...	645.3574192
👁	0x8a592d08c00c0de0c2...	Transfer	2022-11-28 13:36:47	Binance 15	→	0xd94d3b4d6e762994f8...	182.42700379
👁	0xe2bdaa42295acdc950...	Transfer	2022-11-28 13:35:59	0x573351177434e20cda...	→	0x1f9303a7e7992b2855...	28.23519649
👁	0x74b618b7898d387136...	Transfer	2022-11-28 13:35:59	0x974caa59e49682cda0...	→	0xcc132cae4cad751007...	3,650

Fig. 7.8 Metaverse project the Sandbox's SAND token on the Token Tracker page of Etherscan, the Ethereum browser

to custom balance sheets for DAOs.[5] A series of user-created metaverse-related dashboards can be seen on Dune Analysis, with one of the most popular items being Metaverse & Virtual Real Estate,[6] showing information such as today's hottest metaverse land deals, metaverse rankings, average prices, and other key information. There is also a user-created NFT Wash Trader dashboard on Dune[7] dedicated to exposing the activity of LooksRare Wash Traders, including wallets, trades, and NFT used, which provides NFT swipe detection technology research [81–84] and provides the technical foundation. (2) The Graph (https://thegraph.com) is a decentralized on-chain data indexing protocol for querying networks like Ether and IPFS. The Graph is a cloud service like API composed of decentralized indexing nodes. The Graph can be accessed directly through subgraphs to obtain information, quickly and resource-efficiently. For instance, Xia et al. [85] use The Graph protocol to obtain trading events associated with the decentralized exchange Uniswap (e.g., mint, swap, and burn events). Based on the data queried and parsed by The Graph, they deeply analyze the fraudulent tokens on Uniswap V2 and propose an effective and accurate method to detect fraudulent tokens, identifying over 10K fraudulent tokens and fraudulent liquidity pools, revealing the surprising fact that Uniswap is flooded with fraudulent tokens. This side-by-side demonstrates the necessity and feasibility of regulation in the decentralized financial ecosystem of the Web3 meta-universe.

7.4.1.4 Data Analysis and Applications

One layer up from the data query and indexing is the encapsulated, deliverable data products that can provide metaverse data value directly to users. The players in this layer can be broadly classified according to the type of data as token data analysis, on-chain transaction tracking, label library applications, NFT data analysis, DAO data analysis, etc.

- **Token data analysis.** One representative platform is CoinMarketCap (https://coinmarketcap.com, established in 2013, which is used to observe and track token prices, trading volume, market value, etc. For instance, CoinMarketCap gives a market cap ranking of metaverse tokens (including trading tokens or governance tokens)[8] and a "play-to-earn" ranking of metaverse projects[9] for players' reference. In the area of regulation, Chen et al. [86] conducted an empirical study on the analysis of cryptocurrency exchange swipes based on scores and rankings of exchanges provided by CoinMarketCap. Another

[5] https://blockworks.co/news/web3-data-firm-dune-analytics-hits-unicorn-status.

[6] https://dune.com/metaland/Metaverse-Land-Community.

[7] https://dune.com/cryptok/NFT-Wash-Trading.

[8] https://coinmarketcap.com/view/metaverse/.

[9] https://coinmarketcap.com/watchlist/6163287dad9db6359e33775b/.

data platform similar to CoinMarketCap is CoinGecko (https://www.coingecko.com/), which has been used by a number of researchers to conduct research on cryptocurrency and DeFi applications. For instance, DeFiRanger [87] refers to the market capacity and the price of tokens of five vulnerable DeFi apps provided by CoinGecko, to represent the market value of these DeFi apps, and proposes a price manipulation identification technique for DeFi apps. The rug pull research [88] also makes reference to the CoinGecko, CoinMarketCap, and Etherscan data analysis websites and unearths 674 token lists marked as nonmalicious to study and identify rug pull in DeFi applications. DefiLlama (https://defillama.com/) is a popular aggregator of DeFi statistics cited in academic papers [89] and official reports [90] on DeFi. DefiLlama also provides a list of hack incidents in the blockchain, DeFi, and cross-chain bridge space over the years,[10] including amount of loss, hacked public chains, attack categories, and other information. These classifications and statistics help researchers summarize and generalize the models of different types of attacks and design more accurate and efficient methods for DeFi attack detection and DeFi attack defense [91, 92].

- **On-chain transaction tracking.** The on-chain transaction tracking platform is a platform that has been around since the birth of Bitcoin. The representative platform is Chainalysis (https://www.chainalysis.com/), established in 2014 to help governments, cryptocurrency exchanges, international law enforcement agencies, banks, and other customers comply with compliance requirements, assess risk, and identify illegal activity through on-chain data monitoring and analysis. Research by companies such as Chainalysis has been an inspiration for the supervision of the entire ecosystem in metaverse. The Chainalysis Crime report [93], which summarizes the crimes committed in 2018, provides a more in-depth look at the economic losses caused by phishing scams and provides case examples to inspire a series of subsequent papers on phishing scam detection [94–100]. Recently, Chainalysis has revealed examples of NFT wash trading in its Web3 report [101], which also provides inspiration for subsequent papers on NFT wash trading detection. Other on-chain transaction tracking platforms like Chainalysis include Ciphertrace (https://ciphertrace.com), Elliptic (https://www.elliptic.co), PeckShield (https://peckshield.com/), and SlowMist.com/), SlowMist (https://www.slowmist.com), CertiK (https://www.certik.com), etc. For blockchain forensics and on-chain transaction tracking tools, Srivasthav et al. [102] conduct a review of platforms and propose a taxonomy to map the identified advanced forensic features to the investigated supporting forensic tools. Transactions are the smallest unit of economic activity in the Web3-enabled metaverse; thus, on-chain transaction tracking platforms can effectively support the forensic and analytical work of financial crimes.
- **Label library applications.** The representative platform in industry is Nansen (https://www.nansen.ai/), founded in 2020. Nansen provides a number of wallet

[10] https://defillama.com/hacks.

labels,[11] a way to tag and identify wallet addresses, classify wallets as "Fund," "Heavy DEX trader," "Legendary NFT collector," etc. Mapping on-chain data with a database of millions of labels, researchers can understand what is happening on the blockchain in the metaverse and the types of wallets executing transactions, and can see who is behind these transactions. The representative platform in the academic community is XBlock (http://xblock.pro/), which provides several datasets that allow for transaction data analysis and anomalous behavior detection [103–107], including token price datasets, phishing scams datasets, and Ponzi scam datasets. In addition to the datasets, the XBlock platform has launched XLabelCloud, an open-label database that provides an online Chrome web plugin to facilitate researchers' investigations in scenarios such as blockchain browsers [108, 109].

- **NFT data analysis.** Founded in 2021, the NFTscan platform (https://www.nftscan.com/) provides NFT collectors and investors and researchers with an API[12] to access NFT asset data and historical data held at any wallet address, as well as data analysis including top mint, gas tracker, NFT marketplace, trending collection, etc. NFTscan is designed to help users better track and evaluate the value of NFT assets to help make informed investment decisions. Such NFT data platforms have been used by researchers in academic studies, e.g., Cho et al. [110] utilized data from six profile picture (PFP) collection-type NFT collections provided by Gallop (https://www.higallop.com/), including transaction history, price, the associated wallet address, visual features, and attachment of the NFT. The article also describes some of the challenges associated with NFT transaction data and data preprocessing recommendations. The dataset is currently open source [111].
- **DAO data analysis.** As we know, in the process of on-chain decision-making of a DAO, members first vote on the proposal on the chain to decide whether to execute the proposal, and then the smart contract will automatically execute the proposal after the vote is passed. As the first DAO comprehensive data platform, DeepDAO (https://deepdao.io/), founded in 2020, analyzes, explores, and ranks DAO based on multiple dimensions. For instance, DeepDAO provides an overview of the DAO of Decentraland,[13] including information on project members' shares, proposals, voting coalitions, etc.[14] Based on the data analysis of DeepDAO, future researchers can explore the possible financial crimes in the metaverse DAO ecosystem, such as vote manipulation of DAOs, money laundering through DAOs, collusion or cronyism, and vote swiping of proposals.

[11] https://www.nansen.ai/guides/wallet-labels-emojis-what-do-they-mean.

[12] https://docs.nftscan.com/nftscan/APIOverview.

[13] https://dao.decentraland.org/en/.

[14] https://deepdao.io/organization/60c9b31c-4495-4028-aeac-eb7bb117fece/organization_data/members.

As mentioned above, the underlying layer of the metaverse economic system is the blockchain. Due to the openness, traceability, and immutability of the blockchain, the transaction data, contract data, DAO members, and other data of the metaverse that contains rich information can be accessed publicly and completely. Meanwhile, based on various levels of metaverse data, many platforms are exploring and developing tools for data source, acquisition, query, indexing, and analysis, which provides unprecedented opportunities for data-driven research on metaverse financial regulatory technologies. The value of analyzing and mining metaverse financial data is twofold. (1) Researchers can broadly explore the evolution of user behavior, transaction networks, wealth distribution, asset values, and organizational decisions in the metaverse economic system, as a reference for other financial activities. (2) In recent years, various types of financial crimes have started to appear in the metaverse. Metaverse financial data analysis can help identify illegal behaviors among them and provide effective regulatory solutions for building a healthier metaverse ecology, and the related technology can also be a reference for metaverse transaction regulation in political affairs and other scenarios. In conclusion, these publicly available, processed, and easy-to-use data sources and access, query, and analysis platforms can not only enhance the theoretical value and application of data mining, social network analysis, quantitative trading, and other techniques in the financial system but also help enhance the financial security and regulation of the meta-universe economic system.

7.4.2 Challenges and Open Issues

Although the publicly available data of metaverse provides opportunities for technical research to prevent financial crimes, the “decentralized” nature of Web3 also poses a great challenge to the governance of the metaverse. On the one hand, since the Web3 economic system integrates the latest technologies and systems such as blockchain, smart contracts, and digital assets as its foundation, the metaverse is very likely to inherit the regulatory challenges of these underlying technologies. On the other hand, the financial regulation of Web3 may face new challenges in the new scenarios of metaverse.

7.4.2.1 Challenges Introduced by Web3 Fundamentals

From a technical point of view, Web3 provides the technical basis for the current hotly debated metaverse. From the economic point of view, compared with Web2, the most significant feature of Web3 is that it is a distributed Internet infrastructure, user-centered, emphasizing the autonomy of users’ digital identity, personal data, and algorithms, and equal rights for users and builders. According to the technical basis of Web3, the challenges of metaverse regulation brought by Web3 have three main levels:

- **The underlying blockchain.** Different from traditional finance scenarios, blockchain is decentralized, borderless, and anonymous while not limiting the number of accounts each user can open. Similar to blockchain, users of metaverse can conduct a large number of frequent transactions between accounts under their control. These result in the difficulty of identifying the entities of the Web3 accounts, with a large number of anonymous transactions and uncertain behavior. While de-anonymization may be possible through transaction data mining techniques, this in turn may raise other issues, such as user privacy breaches. Countless records of user activities and traces of user interactions will be retained in the metaverse. As these data are stored on the public blockchain, the accumulation of records and traces over time may cause user privacy disclosure problem.
- **Smart contracts and digital assets.** Smart contracts enable all types of digital assets, including stablecoins, fungible tokens, NFTs, etc. Smart contracts enable various types of digital assets to be exchanged on a trading platform. At the same time, Turing-complete smart contracts can represent and execute more complex application logic and functionality, leading to more complex transaction patterns. Meanwhile, as mentioned in the previous section, there are already many regulatory policies and measures for blockchain cryptocurrencies (e.g., Bitcoin, Ether, etc.) at home and abroad. The future regulation of the Web3 at home and abroad also needs to dovetail with the norms and measures for cryptocurrencies.
- **DeFi and DAO.** The goal of DeFi is to create a decentralized, open-source, permissionless, and transparent economic system that operates behind a DAO [112] that operates strictly through programmed code/protocols. Although DeFi offers great opportunities for Web3 and the metaverse, DeFi and the DAOs behind it still need to be adequately regulated in order to ensure the trustworthiness of DeFi in the metaverse. However, users of current DeFi protocols or DApps are not mandated to meet anti-money laundering (AML) and know-your-customer (KYC) requirements. As described by Salami [112], if a Web3 project has achieved a high degree of decentralization, they need to be operated and managed entirely by the DAO of the programming code/protocols without any influence from a centralized authority such as software developers. Then, it will become very difficult to hold anyone accountable for crimes and errors in the operation of the DeFi protocol in Web3-enabled metaverse.

7.4.2.2 Open Issues Introduced by the Metaverse

The metaverse constructs a new social structure where the virtual and the real are highly intertwined. The users of the metaverse are also residents of the real world, thus also making traditional security risks and nontraditional security risks superimposed on each other, and the virtual economy of the metaverse and the real economy of the real world will inevitably interact with each other. In this part, we will discuss the open issues introduced by the metaverse to financial regulation in terms of the different paths into the metaverse.

- **Digital twin.** A digital twin is a digital mapping of the physical world, where the user enters the metaverse with their digital body. At this point, the definition of personal identity becomes problematic. In the real world, financial regulation regulates the actual person. It is then a challenge to regulate the interaction between this digital avatar and the real-world person in a metaverse regulatory regime.
- **Digital primordial.** The digital native is a virtual universe parallel to the physical world, where multiple avatars of the self in the metaverse can multitask, collaborate, and talk to each other. Therefore, a criminal in the real world can have multiple doppelgangers in the metaverse, and it will be difficult to correspond between the metaverse and the real-world "person" in fact. At the same time, the metaverse breaks through national geographical boundaries, which poses a major obstacle to effective financial regulation and enforcement in individual countries.
- **Virtual-real synthesis.** The real world interacts with the virtual world. A real-world criminal can take the assets he illegally obtained in the metaverse (e.g., stealing assets via DeFi exploits) and can exchange the stolen assets on the chain for real-world fiat currency through an exchange that does not require KYC. The laundered fiat currency, in turn, flows into the real-world financial system and may be used to finance real-world terrorism. Thus, the interconnection of the real world and virtual world in the metaverse makes the metaverse economic system will face more severe risks than the traditional financial industry, which puts higher demands on the risk awareness of the metaverse financial system.

7.4.3 A Vision for the Future Regulation in Metaverse

The Web3-enabled metaverse relies on decentralized autonomous organizations (DAOs). For the future governance and supervision of Web3, it may be possible to use the DAOs of metaverse to encode the operation and governance rules of metaverse in the form of smart contracts on the blockchain and establish reward and punishment measures with the help of tokens, NFTs, and other economic rights to finally realize the autonomous governance and autonomous supervision of Web3. However, the regulation and governance rules of DAOs may not cover all the risks and security issues in the metaverse. Therefore, the government should pay high attention to crimes against the metaverse, prevent them from happening, guide the development of a set of universally applicable industry standards for the metaverse, and implement blockchain-based industry autonomy. At the same time, the government should cultivate industry consensus and optimize the regulatory scheme in the governance process in order to avoid the various drawbacks caused by brutal developments followed by strong governance.

7.5 Conclusion

This chapter reviews various financial crimes in the Web3-empowered metaverse ecosystem, e.g., scams, code exploits, wash trading, money laundering, and illegal services and shops. We first summarize and classify the financial security threats on the Web3-empowered metaverse. Then, we perform an overview of the current anti-crime studies and technologies in the context of metaverse.

References

1. IMF. (2001) International Monetary Fund Annual Report 2001: Making the Global Economy Work for All. [Online]. Available: https://www.imf.org/en/Publications/AREB/Issues/2016/12/30/International-Monetary-Fund-Annual-Report-2001-Making-the-Global-Economy-Work-for-All-15216
2. FSMA. (2000) Financial Services and Markets Act 2000. [Online]. Available: https://www.legislation.gov.uk/ukpga/2000/8/contents
3. T. Kadar. (2022) The metaverse fraud question: What are the risks? [Online]. Available: https://seon.io/resources/metaverse-fraud/
4. A. Lindesmith, *The Big Con: The Story of the Confidence Man and the Confidence Game*. JSTOR, 1940.
5. J. R. Weil and W. T. Brannon, *The Con Game and "Yellow Kid" Weil*. ReadHowYouWant.com, 1948.
6. Market Business News. (2022) What is a scam? Definition and examples. [Online]. Available: https://marketbusinessnews.com/financial-glossary/scam/
7. M. Bartoletti, S. Lande, A. Loddo, L. Pompianu, and S. Serusi, "Cryptocurrency scams: Analysis and perspectives," *IEEE Access*, vol. 9, pp. 148 353–148 373, 2021.
8. Elliptic. (2022) The future of financial crime in the metaverse. [Online]. Available: https://www.elliptic.co/hubfs/Crime%20in%20the%20Metaverse%202022%20final.pdf
9. APWG. (2021) The APWG Ecrime Exchange (ECX). [Online]. Available: https://apwg.org/
10. S. Mavis. (2021) Official Axie Infinity whitepaper. [Online]. Available: https://whitepaper.axieinfinity.com/
11. O. Alam. (2022) Understanding the economies of blockchain games: An empirical analysis of Axie Infinity. [Online]. Available: https://pub.tik.ee.ethz.ch/students/2022-FS/BA-2022-08.pdf
12. J.Brustein. (2022) A billion-dollar crypto gaming startup promised riches and delivered disaster. [Online]. Available: https://www.bloomberg.com/news/features/2022-06-10/axie-infinity-axs-crypto-game-promised-nft-riches-gave-ruin
13. K. Servando and I. C. Sayson. (2021) This video game is turning the pandemic jobless into crypto traders. [Online]. Available: https://www.bloomberg.com/news/articles/2021-08-25/axie-infinity-how-game-is-turning-pandemic-jobless-into-crypto-nft-traders
14. Coincu. (2022) Big Daddy Ape Club $1.3M scam, although it had civic 'verification'. [Online]. Available: https://news.coincu.com/60266-big-daddy-ape-club-1-3m-scam/

15. Reddit. (2022) Sandbox beta email…is this a scam? : TheSandboxGaming. [Online]. Available: https://www.reddit.com/r/TheSandboxGaming/comments/ttqvg5/sandbox_beta_email_is_this_a_scam/
16. J. Young. (2017) South Korean government concerned with scams in Bitcoin market, fake exchanges. [Online]. Available: https://cointelegraph.com/news/south-korean-government-concerned-with-scams-in-bitcoin-market-fake-exchanges
17. N. Smaili and A. de Rancourt-Raymond, "Metaverse: Welcome to the new fraud marketplace," *Journal of Financial Crime*, 2022.
18. I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," *International Journal of Network Security*, vol. 19, no. 5, pp. 653–659, 2017.
19. S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Applied Sciences*, vol. 9, no. 9, p. 1788, 2019.
20. R. M. Parizi, Amritraj, and A. Dehghantanha, "Smart contract programming languages on blockchains: An empirical evaluation of usability and security," in *International Conference on Blockchain*, 2018, pp. 75–91.
21. Emin Gün Sirer. (2016) Thoughts on the DAO hack. [Online]. Available: https://hackingdistributed.com/2016/06/17/thoughts-on-the-dao-hack/
22. BTC Peers Reporter. (2021) $100,000 worth of NFTs disappear forever, thanks to OpenSea bug. [Online]. Available: https://btcpeers.com/100-000-worth-of-nfts-disappear-forever-thanks-to-opensea-bug/
23. M. Ndiaye and P. K. Konate, "Cryptocurrency crime: Behaviors of malicious smart contracts in blockchain," in *International Symposium on Networks, Computers and Communications*, 2021.
24. N. Kshetri, "Scams, frauds, and crimes in the nonfungible token market," *Computer*, vol. 55, no. 4, pp. 60–64, 2022.
25. Y. Cao, Y. Li, S. Coleman, A. Belatreche, and T. M. McGinnity, "Detecting wash trade in the financial market," in *IEEE Conference on Computational Intelligence for Financial Engineering & Economics*, 2014, pp. 85–91.
26. F. Victor and A. M. Weintraud, "Detecting and quantifying wash trading on decentralized cryptocurrency exchanges," in *Proceedings of the ACM Web Conference*, 2021, pp. 23–32.
27. C. F. T. Commission. (2022) CFTC Glossary. [Online]. Available: https://www.cftc.gov/LearnAndProtect/EducationCenter/CFTCGlossary/glossary_wxyz.htm#washtrading
28. B. A. Management. (2019) Bitwise Asset Management: Presentation to the U.S. securities and exchange commission. [Online]. Available: https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5164833-183434.pdf
29. J. Chen, D. Lin, and J. Wu, "Do cryptocurrency exchanges fake trading volumes? An empirical analysis of wash trading based on data mining," *Physica A: Statistical Mechanics and its Applications*, vol. 586, p. 126405, 2022.
30. Chainalysis. (2022) The Chainalysis 2021 NFT market report. [Online]. Available: https://go.chainalysis.com/nft-market-report.html
31. S. Serneels, "Detecting wash trading for nonfungible tokens," *Finance Research Letters*, Sept. 2022.
32. D. Das, P. Bose, N. Ruaro, C. Kruegel, and G. Vigna, "Understanding security issues in the NFT ecosystem," *arXiv preprint arXiv:2111.08893*, 2021.
33. ACAMS. (2012) Study guide for the CAMS. [Online]. Available: https://www.acams.org
34. FATF. (2021) What is money laundering. [Online]. Available: https://www.fatf-gafi.org/faq/moneylaundering/
35. FINRA. (2022) Anti-money laundering (AML). [Online]. Available: https://www.fatf-gafi.org/faq/moneylaundering/
36. E. Hartwich, P. Ollig, G. Fridgen, and A. Rieger, "Probably something: A multi-layer taxonomy of non-fungible tokens," *arXiv preprint arXiv:2209.05456*, 2022.
37. H. X. Qin, Y. Wang, and P. Hui, "Identity, crimes, and law enforcement in the metaverse," *arXiv preprint arXiv:2210.06134*, 2022.

38. Z. Gu, D. Lin, and J. Wu, "On-chain analysis-based detection of abnormal transaction amount on cryptocurrency exchanges," *Physica A: Statistical Mechanics and its Applications*, vol. 604, p. 127799, 2022.
39. O. Kampers, A. Qahtan, S. Mathur, and Y. Velegrakis, "Manipulation detection in cryptocurrency markets: An anomaly and change detection based approach," in *Proceedings of the ACM/SIGAPP Symposium on Applied Computing*, 2022, pp. 326–329.
40. Trendmicro. (2022) NFT scam: Fake MetaversePRO website. [Online]. Available: https://news.trendmicro.com/2022/02/24/nft-scam-fake-metaversepro-website/
41. Microsoft. (2022) Tech support scams. [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/support-scams?view=o365-worldwide
42. R. Kalniņš, J. Puriņš, and G. Alksnis, "Security evaluation of wireless network access points," *Applied Computer Systems*, vol. 21, no. 1, pp. 38–45, 2017.
43. N. N. Pokrovskaia and S. O. Snisarenko, "Social engineering and digital technologies for the security of the social capital' development," in *International Conference "Quality Management, Transport and Information Security, Information Technologies"*, 2017, pp. 16–18.
44. AVAST. (2022) What is Ryuk ransomware? [Online]. Available: https://www.avast.com
45. N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts (sok)," in *International Conference on Principles of Security and Trust*, 2017, pp. 164–186.
46. S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, "Systematic review of security vulnerabilities in Ethereum blockchain smart contract," *IEEE Access*, vol. 10, pp. 6605–6621, 2022.
47. P. Tsankov, A. Dan, D. Drachsler-Cohen, A. Gervais, F. Buenzli, and M. Vechev, "Securify: Practical security analysis of smart contracts," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 67–82.
48. L. Brent, A. Jurisevic, M. Kong, E. Liu, F. Gauthier, V. Gramoli, R. Holz, and B. Scholz, "Vandal: A scalable security analysis framework for smart contracts," *arXiv preprint arXiv:1809.03981*, 2018.
49. J. Wu, J. Liu, Y. Zhao, and Z. Zheng, "Analysis of cryptocurrency transactions from a network perspective: An overview," *Journal of Network and Computer Applications*, vol. 190, pp. 103–139, 2021.
50. F. Victor, "Address clustering heuristics for Ethereum," in *International Conference on Financial Cryptography and Data Security*, 2020, pp. 617–633.
51. T. Huang, D. Lin, and J. Wu, "Ethereum account classification based on graph convolutional network," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 5, pp. 2528–2532, 2022.
52. J. Liu, J. Zheng, J. Wu, and Z. Zheng, "Fa-gnn: Filter and augment graph neural networks for account classification in ethereum," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 4, pp. 2579–2588, 2022.
53. J. Wu, J. Liu, W. Chen, H. Huang, Z. Zheng, and Y. Zhang, "Detecting mixing services via mining bitcoin transaction network with hybrid motifs," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 4, pp. 2237–2249, 2021.
54. C. G. Akcora, Y. Li, Y. R. Gel, and M. Kantarcioglu, "Bitcoinheist: Topological data analysis for ransomware detection on the bitcoin blockchain," *arXiv preprint arXiv:1906.07852*, 2019.
55. S. Phetsouvanh, F. Oggier, and A. Datta, "Egret: Extortion graph exploration techniques in the bitcoin network," in *IEEE International Conference on Data Mining Workshops*, 2018, pp. 244–251.
56. H. Yousaf, G. Kappos, and S. Meiklejohn, "Tracing transactions across cryptocurrency ledgers," in *28th USENIX Security Symposium*, 2019, pp. 837–850.
57. D. Lin, J. Chen, J. Wu, and Z. Zheng, "Evolution of Ethereum transaction relationships: Toward understanding global driving factors from microscopic patterns," *IEEE Transactions on Computational Social Systems*, vol. 9, no. 2, pp. 559–570, 2022.
58. D. Lin, J. Wu, Q. Yuan, and Z. Zheng, "T-edge: Temporal weighted multidigraph embedding for ethereum transaction network analysis," *Frontiers in Physics*, vol. 8, p. 204, 2020.

59. ——, “Modeling and understanding ethereum transaction records via a complex network approach,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 11, pp. 2737–2741, 2020.
60. C. Jin, J. Jin, J. Zhou, J. Wu, and Q. Xuan, “Heterogeneous feature augmentation for ponzi detection in ethereum,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2022.
61. D. Lin, J. Wu, Q. Xuan, and K. T. Chi, “Ethereum transaction tracking: Inferring evolution of transaction networks via link prediction,” *Physica A: Statistical Mechanics and its Applications*, vol. 600, p. 127504, 2022.
62. J. Zhou, C. Hu, J. Chi, J. Wu, M. Shen, and Q. Xuan, “Behavior-aware account de-anonymization on ethereum interaction graph,” *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 3433–3448, 2022.
63. CERTIK. (2022) CERTIK’s HACK3D: The Web3 Security Quarterly Report. [Online]. Available: https://www.certik.com/resources/blog/7fuXtbfo4CXEXcwy5Pqijp-hack3d-the-web3-security-quarterly-report-q2-2022
64. SLOWMIST. (2022) 2022 Mid-Year Blockchain Security and Anti-Money Laundering Analysis Report. [Online]. Available: https://www.slowmist.com/report/first-half-of-the-2022-report(EN).pdf
65. C. Wronka, “Financial crime in the decentralized finance ecosystem: new challenges for compliance,” *Journal of Financial Crime*, 2021.
66. J. Abadi and M. Brunnermeier, “Blockchain economics,” National Bureau of Economic Research, Tech. Rep., 2018.
67. F. A. T. Force, “Guidance for a risk-based approach to virtual assets and virtual asset service providers,” *Paris, June*, 2019.
68. R. Barone and D. Masciandaro, “Cryptocurrency or usury? crime and alternative money laundering techniques,” *European Journal of Law and Economics*, vol. 47, no. 2, pp. 233–254, 2019.
69. M. D. Murray, “Ready lawyer one: Lawyering in the metaverse,” *SSRN Electronic Journal*, 2022.
70. A. Y. Bokovnya, A. A. Shutova, T. G. Zhukova, and L. V. Ryabova, “Legal measures for crimes in the field of cryptocurrency billing,” *Utopía y Praxis Latinoamericana*, vol. 25, no. 7, pp. 270–275, 2020.
71. F. M. J. Teichmann and M.-C. Falker, “Cryptocurrencies and financial crime: solutions from liechtenstein,” *Journal of Money Laundering Control*, 2020.
72. Liechtenstein. (2019) Liechtenstein: Parliament Adopts Blockchain Act. [Online]. Available: https://www.loc.gov/item/global-legal-monitor/2019-10-30/liechtenstein-parliament-adopts-blockchain-act/
73. AMLA. (2020) Anti-Money Laundering Act of 2020. [Online]. Available: https://complyadvantage.com/insights/a-guide-to-the-us-anti-money-laundering-act-amla/
74. Whitehouse. (2022) President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets. [Online]. Available: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/09/fact-sheet-president-biden-to-sign-executive-order-on-ensuring-responsible-innovation-in-digital-assets/
75. 5AML. (2020) 5th Anti-Money Laundering Directive (5AMLD). [Online]. Available: https://complyadvantage.com/insights/5mld-fifth-anti-money-laundering-directive/
76. UK. (2022) Joint statement from UK financial regulatory authorities on sanctions and the cryptoasset sector. [Online]. Available: https://www.fca.org.uk/news/statements/uk-financial-regulatory-authorities-sanctions-cryptoasset-sector
77. Singapore. (2022) Explanatory Brief for Financial Services and Markets Bill 2022. [Online]. Available: https://www.mas.gov.sg/news/speeches/2022/explanatory-brief-for-financial-services-and-markets-bill-2022
78. Japan. (2022) Explanatory Brief for Financial Services and Markets Bill 2022. [Online]. Available: https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/japan

79. J. Benet, "Ipfs-content addressed, versioned, p2p file system," *arXiv preprint arXiv:1407.3561*, 2014.
80. T. Chen, Z. Li, Y. Zhang, X. Luo, A. Chen, K. Yang, B. Hu, T. Zhu, S. Deng, T. Hu, J. Chen, and X. Zhang, "DataEther: Data exploration framework for Ethereum," in *International Conference on Distributed Computing Systems*, 2019, pp. 1369–1380.
81. V. von Wachter, J. R. Jensen, F. Regner, and O. Ross, "NFT Wash Trading: Quantifying suspicious behaviour in NFT markets," *arXiv preprint arXiv:2202.03866*, 2022.
82. S. Serneels, "Detecting wash trading for nonfungible tokens," *Finance Research Letters*, Sept. 2022, http://dx.doi.org/10.1016/j.frl.2022.103374.
83. D. Das, P. Bose, N. Ruaro, C. Kruegel, and G. Vigna, "Understanding security issues in the NFT ecosystem," *arXiv preprint arXiv:2111.08893*, 2021.
84. S. A. Tariq and I. Sifat, "Suspicious trading in nonfungible tokens (NFTs): Evidence from wash trading," *SSRN Electronic Journal*, 2022, http://dx.doi.org/10.2139/ssrn.4097642.
85. P. Xia, H. Wang, B. Gao, W. Su, Z. Yu, X. Luo, C. Zhang, X. Xiao, and G. Xu, "Trade or trick? Detecting and characterizing scam tokens on uniswap decentralized exchange," *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, vol. 5, no. 3, pp. 1–26, 2021.
86. J. Chen, D. Lin, and J. Wu, "Do cryptocurrency exchanges fake trading volumes? An empirical analysis of wash trading based on data mining," *Physica A: Statistical Mechanics and its Applications*, vol. 586, p. 126405, 2022.
87. S. Wu, D. Wang, J. He, Y. Zhou, L. Wu, X. Yuan, Q. He, and K. Ren, "DeFiRanger: Detecting price manipulation attacks on DeFi applications," *arXiv preprint arXiv:2104.15068*, 2021.
88. B. Mazorra, V. Adan, and V. Daza, "Do not rug on me: Leveraging machine learning techniques for automated scam detection," *Mathematics*, vol. 10, no. 6, p. 949, 2022.
89. B. K. Meister and H. C. Price, "Yields: The galapagos syndrome of cryptofinance," *arXiv preprint arXiv:2202.10265*, 2022.
90. P. T. Roukny, *Decentralized finance: information frictions and public policies: Approaching the regulation and supervision of decentralized finance*. Publications Office of the European Union, 2022, http://dx.doi.org/10.2874/444494.
91. S.-H. Wang, C.-C. Wu, Y.-C. Liang, L.-H. Hsieh, and H.-C. Hsiao, "ProMutator: Detecting vulnerable price oracles in DeFi by mutated transactions," in *IEEE European Symposium on Security and Privacy Workshops*, 2021, pp. 380–385.
92. K. Qin, L. Zhou, B. Livshits, and A. Gervais, "Attacking the DeFi ecosystem with flash loans for fun and profit," in *Financial Cryptography and Data Security*, 2021, pp. 3–32.
93. Chainalysis. (2019) Cryptocrime report: Decoding darknet markets, hacks, and scams. [Online]. Available: https://go.chainalysis.com/2019-Crypto-Crime-Report.html
94. J. Wu, Q. Yuan, D. Lin, W. You, W. Chen, C. Chen, and Z. Zheng, "Who are the phishers? Phishing scam detection on Ethereum via network embedding," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 2, pp. 1156–1166, 2022.
95. W. Chen, X. Guo, Z. Chen, Z. Zheng, and Y. Lu, "Phishing scam detection on Ethereum: Towards financial security for blockchain ecosystem," in *International Joint Conferences on Artificial Intelligence Organization*, 2020, pp. 4506–4512.
96. Z. Yuan, Q. Yuan, and J. Wu, "Phishing detection on Ethereum via learning representation of transaction subgraphs," in *Blockchain and Trustworthy Systems*, 2020, pp. 178–191.
97. J. Chen, H. Xiong, D. Zhang, Z. Liu, and J. Wu, "TEGDetector: A phishing detector that knows evolving transaction behaviors," *arXiv preprint arXiv:2111.15446*, 2021.
98. S. Li, G. Gou, C. Liu, C. Hou, Z. Li, and G. Xiong, "TTAGN: Temporal transaction aggregation graph network for Ethereum phishing scams detection," in *Proceedings of the ACM Web Conference*, 2022, pp. 661–669.
99. H. Wen, J. Fang, J. Wu, and Z. Zheng, "Hide and seek: An adversarial hiding approach against phishing detection on ethereum," *IEEE Transactions on Computational Social Systems*, 2022.
100. Y. Xia, J. Liu, and J. Wu, "Phishing detection on ethereum via attributed ego-graph embedding," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 5, pp. 2538–2542, 2022.

101. Chainalysis. The chainalysis state of web3 report. [Online]. Available: https://go.chainalysis.com/2022-web3-report.html
102. D. P. Srivasthav, L. P. Maddali, and R. Vigneswaran, "Study of blockchain forensics and analytics tools," in *Blockchain, Robotics and AI for networking security conference*, 2021, pp. 39–40.
103. P. Zheng, Z. Zheng, J. Wu, and H.-N. Dai, "XBlock-ETH: Extracting and exploring blockchain data from Ethereum," *IEEE Open Journal of the Computer Society*, vol. 1, pp. 95–106, 2020.
104. Z. Wu, J. Liu, J. Wu, and Z. Zheng, "Transaction tracking on blockchain trading systems using personalized PageRank," *arXiv preprint arXiv:2201.05757*, 2022.
105. D. Lin, J. Chen, J. Wu, and Z. Zheng, "Evolution of Ethereum transaction relationships: Toward understanding global driving factors from microscopic patterns," *IEEE Transactions on Computational Social Systems*, vol. 9, no. 2, pp. 559–570, 2022.
106. D. Lin, J. Wu, Q. Yuan, and Z. Zheng, "Modeling and understanding Ethereum transaction records via a complex network approach," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 11, pp. 2737–2741, 2020.
107. J. Wu, J. Liu, Y. Zhao, and Z. Zheng, "Analysis of cryptocurrency transactions from a network perspective: An overview," *Journal of Network and Computer Applications*, vol. 190, p. 103139, 2021.
108. W. Chen, Z. Zheng, J. Cui, E. Ngai, P. Zheng, and Y. Zhou, "Detecting ponzi schemes on ethereum: Towards healthier blockchain technology," in *Proceedings of the 2018 world wide web conference*, 2018, pp. 1409–1418.
109. C. Jin, J. Zhou, J. Jin, J. Wu, and Q. Xuan, "Time-aware metapath feature augmentation for ponzi detection in ethereum," *arXiv preprint arXiv:2210.16863*, 2022.
110. J. B. Cho, S. Serneels, and D. S. Matteson, "Non-fungible token transactions: Data and challenges," *arXiv preprint arXiv:2210.07393*, 2022.
111. S. Serneels, J. B. Cho, and D. S. Matteson. Data containing transaction history and visual traits of eight highly valued Non-fungible token (NFT) collections. [Online]. Available: https://ecommons.cornell.edu/handle/1813/111404
112. I. Salami, "Challenges and approaches to regulating decentralized finance," *AJIL Unbound*, 2021, https://doi.org/10.1017/aju.2021.66.

Chapter 8
What Is the Implication of Web3 and Metaverse?

Huawei Huang and Qinglin Yang

Abstract In this chapter, we summarize the implication of Web3 & metaverse. In the first section, we discuss how Web3 enables other fields. Specifically, we show our understanding of the correlations among the concepts of Web3, blockchain, DAO, NFT, and metaverse. In the next section, we then summarize how to participate in metaverse from the perspective of users and practitioners, including two topics: (i) the way to join metaverse ecology for ordinary users and (ii) the routine of participating in the development of metaverse for practitioners.

Keywords Web3 · Metaverse · Blockchain · DAO · NFT

8.1 How Web3 Enables Other Fields

As defined by Ethereum co-founder Gavin Wood, Web3 is a blockchain technology that enables innovative interactions between parties based on a *trustless* interaction system. In the author's view, Web3 can be described as a collection of Internet technologies used in the process of transforming traditional Web2 world applications into decentralized applications via blockchain technologies. This collection includes new technologies, new paradigms, and the birth of new organizational forms (i.e., DAOs), as well as new values and worldviews. Therefore, the author believes that Web3 will dominate the landscape of the next-generation Internet.

H. Huang (✉) · Q. Yang
School of Software Engineering, Sun Yat-sen University, Zhuhai, Guangdong, China
e-mail: huanghw28@mail.sysu.edu.cn

H. Huang et al. (eds.), *From Blockchain to Web3 & Metaverse*,
https://doi.org/10.1007/978-981-99-3648-9_8

8.1.1 The Correlations Among Web3, Blockchain, and Metaverse

What is the relationship among Web3, blockchain, and metaverse? This question is undoubtedly very representative, both in terms of the question itself and the social role of questioners. Apparently, this question involves three independent concepts: Web3, blockchain, and the metaverse. Their correlations can be summarized as the following three patterns:

- Web3 can exist without involving the metaverse.
- Blockchain can work independently without involving Web3 or the metaverse. For example, Bitcoin itself, as a blockchain system, has no direct correlation with the other two concepts.
- The metaverse can exist without using blockchain or involving Web3.

Of course, such three patterns do not mean that these three concepts are completely unrelated to each other. Let's discuss specific reasons.

Firstly, we believe that the narrative of the metaverse is the most grandiose. From the perspective of consumers, the user experience offered by the metaverse is the most direct. After all, people are vision-driven species. The visual effects presented to users in the metaverse are completely different from the experience obtained from the real world.

Secondly, from an industrial perspective, the impact of blockchain is the most far-reaching. This is because blockchain affects the underlying economic infrastructure of both Web3 and metaverse. This is because blockchains create new economic models for them. Therefore, we say that the impact of blockchain is the most far-reaching. However, consumers' perceptions of blockchain technology may not be so strong.

Finally, users can easily see the wide-ranging impact of Web3 products in the near future. The biggest value of Web3 is to address the contradictions between value creators and the platforms of Web2's businesses. In fact, the basic appeal of Web3 is to *decentralize* businesses, in which users have their individual authority. Such the appeal aims at tackling the contradiction between traditional oligarchic business models and *decentralized finance* models. Furthermore, from a technical perspective, plenty of Web3 solutions have been introduced in the market. Therefore, we believe that Web3 is the most promising future that ordinary users can expect.

As depicted in Fig. 8.1, we show our understanding of the relationship among blockchain, Web3, and the metaverse from four perspectives: development progress, industrial structure, ecology, and technical architecture.

- Firstly, no matter from which perspective, blockchain is undoubtedly the underlying infrastructure shared by the other two concepts. The following introduction of this chapter will elaborate on this. Therefore, we mainly explore the relationship between Web3 and the metaverse.

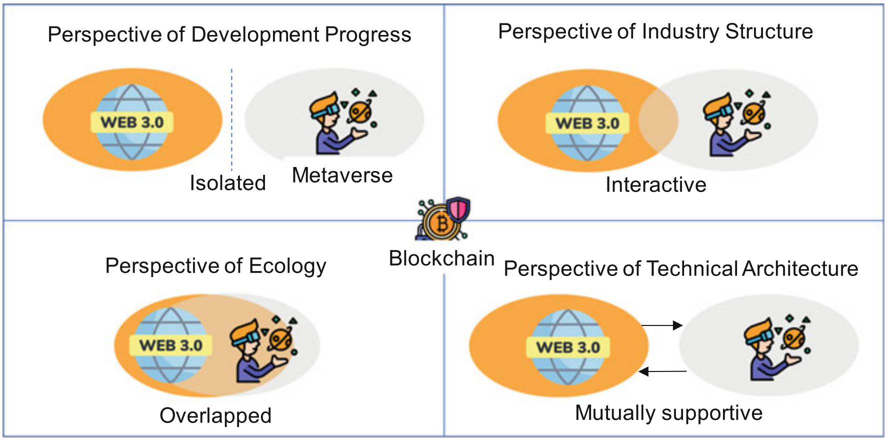


Fig. 8.1 The relationship among Web3, blockchain, and metaverse

- In terms of development, Web3 and metaverse developed along their own logic in the early stages, and there was no connection between them. Specifically, the term "Web3" was first proposed by Tim Berners Lee around 2000. Later, the concept of Web3.0 was proposed by Jeffrey Zeldman in a blog post criticizing Web2.0 in 2006. Subsequently, Gavin Wood proposed and explained the definition of Web3 related to blockchain in 2014. In contrast, as detailed in the previous sections of this book, the early development of the metaverse went through the gestation period of the concept in the 1990s, the shaping period after 2000, and the rapid development period since 2021. It can be seen that there is no obvious connection between the early development of Web3 and the metaverse.
- From the perspective of industrial structure, Web3 and metaverse have interacted with each other. This is because the builders of the metaverse realized that the metaverse needs an economic system that is not controlled by a dominant enterprise. Coincidentally, Web3 can build a decentralized economic system for the metaverse by exploiting blockchain technologies.
- Furthermore, optimistic concept theorists refer to Web3 and the metaverse as the "next-generation internet," and the two seem to overlap almost completely from the perspective of the ecosystem. This is a dialectical point of view worth considering.
- Finally, from the perspective of technical developers, they do not think that the two concepts overlap but rather show a mutually supportive relationship. For example, Web3 can provide the metaverse with decentralized economic systems such as DeFi protocols, decentralized organizational forms (e.g., DAO), a variety of NFTs, etc. metaverse can provide space and platforms for Web3 to exert its power.

8.1.2 The Correlations Among Web3, Blockchain, and DAO

Let's revisit the definition of Web3. Web3 refers to a decentralized online ecosystem established on top of blockchain technologies. Many believe that it represents the next stage of the Internet. A partner of a traditional investment institution believes that the current Web3 industry is very similar to the Internet in 2000.

Currently, some prototype products have emerged in Web3 industries. For example, Metamask, which is seen as a decentralized Alipay; Audius, which is seen as a decentralized music platform; and Opensea, which is the world's largest NFT trading platform. These decentralized applications have attracted millions of users worldwide, and these companies have gradually become the most influential companies globally.

If we summarize the relationship among Web3, blockchain, and DAO in short words, I think blockchain offers the technology framework for Web3; DAO defines the organizational toolbox; and Web3 is a culture.

Nowadays, Web3 and DAO have been applied to only a few representative industries such as the fields of DeFi and encrypted arts. However, this trend has quietly developed for a decade. The public's understanding of Web3 culture is still far from mature.

8.1.3 The Correlations Between NFT and Metaverse

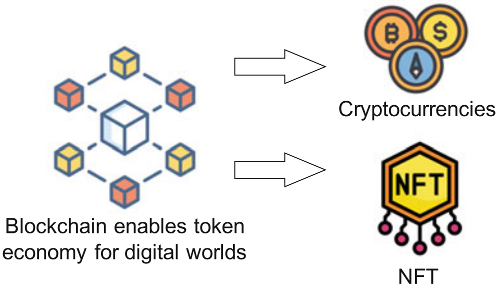
When people notice that blockchain technologies could provide new ways for the publication and circulation of digital arts, they began to recognize the value of NFTs. This is because when digital arts are minted into NFTs, they have the attributes of digital assets. In addition, continuous hype from the investment industry has accelerated the popularity of NFTs. Especially since 2021, the rise of the metaverse has directly promoted the popularity of NFTs.

Then, what are the correlations between NFTs and metaverse?

NFTs are closely related to both blockchain and metaverse. Blockchain technology provides a secure and transparent way to record and verify NFTs' ownership, which greatly enhances the value and credibility of NFTs. What's more, NFTs can be used to represent other assets, such as property assets in the physical world and virtual assets in the metaverse, as digital assets on blockchains. Therefore, NFTs have great potential to reshape digital assets when they are represented, traded, and owned in the digital world. For example, metaverse players can purchase virtual-land NFTs.

Let's disclose more insights into the correlations between NFT and metaverse.

Fig. 8.2 Blockchain technologies enable token economy, which relies on cryptocurrencies and NFTs



8.1.3.1 Blockchain Offers Infrastructures for NFT and Metaverse

Blockchain is the underlying infrastructure for NFTs and the metaverse. Blockchains can record all transactions and events generated by NFTs and the metaverse that require on-chain storage, providing the users of NFTs/metaverse with a transparent, trustworthy, and traceable public ledger. By exploiting the blockchain, people can mint NFTs, which can be used and traded in the metaverse as a form of encrypted assets.

Next, let's discuss the characteristics of the two major types of encrypted assets, i.e., cryptocurrencies and NFTs (as shown in Fig. 8.2), from the following two aspects.

Firstly, NFTs will exist in human society continuously alongside the metaverse. This is because NFT is a *paradigm* that will not disappear once appeared. Here, let's give an example to explain such a paradigm. Just like computers, it is a new paradigm, which is also a new way of computing, for people. When computers were invented, humans can enhance their capabilities when facing complex computing tasks and can never go back to the world before computer invention. Similarly, NFT is a new way of thinking for people in the field of encrypted arts, providing people with a new way of presenting encrypted assets.

Secondly, a specific blockchain usually issues a type of native cryptocurrency. Cryptocurrencies are different from NFTs because they are fungible tokens within the context of a blockchain system. The advent of Bitcoin represented the birth of cryptocurrency, followed by thousands of other cryptocurrencies. Although the technologies behind these various cryptocurrencies vary substantially, they are essentially tokens running on the blockchain. Crypto tokens are essential to our future society in the era of Web3. By exploiting token economics, cryptocurrencies can create incentive mechanisms that can activate the ecology of Web3 applications. For example, various cryptocurrencies have been used as governance tokens in DAOs, in which developers and other contributors are driven to make their contributions to the DAO community.

8.1.3.2 NFT and Metaverse Mutually Support Each Other

On the one hand, the integration of NFT and metaverse is a trend, and the combination of these two concepts creates an effect of $1 + 1 > 2$. The development of metaverse and NFT mutually inspire each other, and their players highly overlap. Both concepts are characterized by decentralization, heavily depending on social networks, and involving virtual-real integration. NFT is considered an important component of the economic system in metaverse. This is because NFT can provide support for key aspects such as identity identification and the authority of digital assets in metaverse. Meantime, metaverse ensures the market vitality and social attention of NFTs.

On the other hand, even without metaverse, NFT can exist independently in the cyberspace of the real world. Currently, many industries, including arts, games, and the Internet, have exploited NFTs. For example, traditional artists can release digital collections through NFT production platforms and sell them on NFT trading platforms. It can be seen that NFT has created a new business model, which can transform many traditional artworks into real digital assets. From this perspective, NFT can indeed be understood as a new business model. Although NFT trading is strictly regulated in China, the overseas NFT market has gained rapid development. A notable example is from the National Basketball Association (NBA) of the United States, which produces NFTs using the highlighted scoring moments of their basketball stars. Those NFTs are known as NBA TopShots.[1] NBA fans can purchase, collect, and trade them freely on legal trading platforms.

8.1.3.3 NFT and Metaverse Resonate in the Same Frequency

In 2021, Facebook changed its name to Meta, indicating the fact that many technology companies are deploying their commercial plans in emerging markets such as metaverse and NFT in order to seek market dominance at an early stage. Facing environmental deterioration, resource scarcity, wealth disparity, and social stratification, people hope that metaverse can promote the second evolution of social production relations and establish a true global village in the virtual world. Ordinary users also hope that NFT can provide new opportunities for them to share digital creativity dividends in the context of metaverse.

Although both NFT and metaverse bring new opportunities for the next generation of the Internet, the risks behind them cannot be ignored. NFT is still a virtual currency in nature and is directly related to the economic system of metaverse as an important component. Once NFT's business model loses control, it will directly impact the ecology of metaverse. Metaverse will have a great impact on the safety and stability of the NFT market. For example, leveraging the popularity of metaverse, a large number of "virtual land" has emerged in the NFT market, and

[1] NBA Top Shot, https://nbatopshot.com/.

the "virtual real estate market" once flourished. When the concept of metaverse fluctuates, the NFT real estate prices also show exponential growth or a cliff-like decline. This linkage phenomenon adds many uncontrollable factors to the development of the virtual economy in metaverse and may even cause serious social problems.

8.2 How to Participate in Metaverse as Users and Practitioners

8.2.1 The Way to Join Metaverse Ecology

As ordinary users, how can we participate in the ecology of the metaverse? The authors believe that we have the following three ways, i.e., (i) participating in experiencing, (ii) participating in an investment, and (iii) participating in creation.

First of all, experiencing refers to ordinary users who can establish their intuitive understanding of the metaverse through various virtual-reality devices and digital avatars.

The second aspect is investing. From the perspective of financial investment, users can purchase metaverse-related financial products while fully understanding market risks. Based on their personal interests and hobbies and in compliance with legal policies, users can purchase a wide range of digital collections, NFTs, and other virtual assets.

Finally, it's about participating in creation. In the future, within the metaverse, everyone can create and sell their digital works, thus generating value. Digital cultural products may have a vast market, and new professions may emerge, such as face sculptors for virtual characters, artists of virtual artwork, etc.

8.2.2 Participating in the Development of Metaverse

As industrial practitioners and developers in the metaverse, what should they pay attention to?

We believe that practitioners can focus on the infrastructure of the metaverse, i.e., the six key technologies represented by the acronym BIGANT: blockchain technology, game engines, independent chip design, 5G/6G networks, cloud computing and edge computing, AI-enabled technology, and the industrial Internet of Things (IIoT).

As developers of the metaverse, they can pay attention to the content-generation ecosystem, including both customer-oriented applications and business-oriented applications. Customer-oriented applications mainly involve applications in the domains of gaming and social networking, striving to create new leisure and entertainment modes in the metaverse. Business-oriented applications aim to provide support for the fields of scientific research, industrial manufacturing, healthcare, education, etc.

8.3 Conclusion

In this chapter, we discussed the implication of Web3 & metaverse. Firstly, we summarize how Web3 enables other fields. The correlations among Web3, blockchain, DAO, NFT, and metaverse have been elaborated. Finally, we also summarize how to participate in the ecology of the metaverse as ordinary users and industrial practitioners.