Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.038403

ARTICLE

Research on Metaverse Security and Forensics

Guangjun Liang[1,2,3], Jianfang Xin[4,*], Qun Wang[1,2], Xueli Ni[1,2,3], Xiangmin Guo[1,2,3] and Pu Chen[1]

[1]Department of Computer Information and Cyber Security, Jiangsu Police Institute, Nanjing, China

[2]Engineering Research Center of Electronic Data Forensics Analysis, Nanjing, China

[3]Key Laboratory of Digital Forensics, Department of Public Security of Jiangsu Province, Nanjing, China

[4]School of Intelligent Engineering, Nanjing Institute of Railway Technology, Nanjing, China

*Corresponding Author: Jianfang Xin. Email: xinjfang@163.com

Received: 11 December 2022 Accepted: 15 June 2023 Published: 31 October 2023

ABSTRACT

As a subversive concept, the metaverse has recently attracted widespread attention around the world and has set off a wave of enthusiasm in academic, industrial, and investment circles. However, while the metaverse brings unprecedented opportunities for transformation to human society, it also contains related risks. Metaverse is a digital living space with information infrastructure, interoperability system, content production system, and value settlement system as the underlying structure in which the inner core is to connect real residents through applications and identities. Through social incentives and governance rules, the metaverse reflects the digital migration of human society. This article will conduct an in-depth analysis of the metaverse from the perspective of electronic data forensics. First, from the perspective of Internet development, the background and development process of the metaverse is discussed. By systematically elaborating on the concept and connotation of the metaverse, this paper summarizes the different views of current practitioners, experts, and scholars on the metaverse. Secondly, from the perspective of metaverse security, the social risk and crime risks of the metaverse are discussed. Then the importance of metaverse forensics is raised. Third, from the perspective of blockchain, smart wearable devices, and virtual reality devices, the objects and characteristics of metaverse forensics have been studied in depth. Taking smart wearable devices as an example, this paper gives the relevant experimental process of smart bracelet forensics. Finally, many challenges faced by metaverse forensics are summarized by us which provide readers with some exploratory guidance.

KEYWORDS

Metaverse; forensics; blockchain; smart wear; virtual reality

1 Introduction

"Metaverse" comes from the science fiction novel "Snow Crash" written by Neil Stephenson in 1992, which is described in the book: "Put on headphones and eyepieces, find the connection terminal, and you can enter the computer simulation, A virtual space parallel to the real world." From the conception of the "matrix" setting in the real world in the film "The Matrix" at the end of the 20th century, to the "oasis" for people to escape and enjoy in "Ready Player One", in many science

fiction film and television works. In the book, I also imagined and predicted the metaverse world where the virtual and the real merged. Since entering the 21st century, with network technology (Fifth Generation Mobile Communication (5G), Internet of Things (IoT), etc.), data processing technology (cloud computing, fog computing, edge computing, etc.), virtual reality technology (Visual Identity (VI), Artificial Intelligence (AI), digital twin, etc.), privacy protection technology (blockchain, trusted computing, etc.), as well as breakthroughs in management and operation and maintenance technology, the metaverse has received unprecedented attention. The layout and investment of forces from all walks of life represented by technology companies in the metaverse have made mankind truly begin to feel the once-distant vision. The possibility of gradually moving towards reality. Although the concept of the metaverse has not yet been unified, driven by technology, the metaverse serves as the "wind vent" for the next generation of technological waves. The metaverse and its related industries have quickly attracted widespread attention from various countries, with local governments and technology giants joining in one after another, and are generally optimistic about its vast growth space. Science and technology have a huge, profound, and comprehensive impact on economic and social development, but the development of any technology always presents the basic characteristics of opportunities and challenges coexisting. Similarly, the metaverse will also bring opportunities and challenges at multiple levels and fields.

An earlier reference to the metaverse was written by Dionisio et al. in 2013 [1]. The author summarized the development of the metaverse and focused on the four aspects of reality, universality, interoperability, and scalability. In the literature [2], it was proposed that the most advanced technologies, such as Virtual Reality (VR), blockchain, etc., are used to construct a kind of parallel universe that can map the real world to a parallel universe. Virtual environments such as Augmented Reality (AR)/VR/Mixed Reality (MR) are good candidate solutions for opening communication channels between robots and virtual environments because of their prominent feature of visualizing content [3]. In addition, various industrial instances integrate virtual environments that enable human users to understand robot operations, such as task scenario analysis and safety analysis. Thus, human users build trust and confidence with robots, leading to a paradigm shift towards human-robot collaboration [4]. How to seamlessly interact between users and digital entities in AR is the key to connecting the real world with the metaverse [5]. Pierce et al. [6] presented a system solution where users can use both hands to select and transform gestures to process virtual content. Yang et al. [7] first proposed to apply blockchain technology to the development of the metaverse, and discussed the potential relationship between blockchain and metaverse in the hierarchical structure of the data layer, network layer, etc. by integrating artificial intelligence. Jeon et al. [8] analyzed the importance of blockchain and artificial intelligence to the metaverse, which mainly involves the processing of extensive data and the stability analysis of decentralized networks. In the metaverse, IoT devices communicate in the network. To solve the problem that transactions in the virtual world may be tampered with, Majeed et al. [9] proposed that applications and users will be able to share and access IoT data using blockchain technology. The characteristics of the virtual world make the transaction data in the virtual world not easy to be tampered with. Dorri et al. [10] gave a more explicit solution for IoT data security based on [9], the data communicated between users in the metaverse is stored in real-time, and blockchain technology allows stakeholders to track their IoT data record. It can effectively solve the data security problem in the metaverse. A blockchain-enabled metaverse can authorize personal data using private keys, does not allow third parties to obtain data from various sources, and data owners have the right to regulate when, where, and how third parties can access their information [11]. Artificial intelligence can provide personalized services for the metaverse, and intelligently interact with users and virtual characters through intelligent models such as supervised, unsupervised, semi-supervised, and Reinforcement

Learning (RL) [12]. Huynh et al. [13] explored the role of AI in the infrastructure and development of the metaverse. Park et al. [14] discussed the performance of the metaverse, e.g., hardware, software, and content components, and reviewed the user interaction and implementation of applications in the metaverse. Xu et al. [15] deeply explored the application of network communication, computing, and blockchain in the metaverse.

This paper conducts research on electronic data forensics in the metaverse. Firstly, it outlines the birth background, development process, concept, and connotation of the metaverse, trying to make readers understand metaverse as soon as possible. Then, from a sociological perspective, the security of the metaverse, the risk of crime, and the necessity of forensics are studied. Finally, the three aspects of metaverse forensics are discussed from the technical point of view, and the specific experimental process is given. The main contributions of this paper are as follows:

1) Summarize the background and development process of the metaverse, and give the concept and connotation of the metaverse;

2) Discussed the security issues of the metaverse, and pointed out the importance of metaverse forensics;

3) Taking smart wearable devices as an example, the relevant experimental process of smart bracelet forensics is given.

The next sections of this paper are arranged as follows. The second section is related work. The third section summarizes the birth and development of the metaverse. In the fourth section, the security issue of the metaverse is highlighted. The fifth section focuses on metaverse forensics. The sixth section is the experimental simulation verification. The challenge of metaverse forensics is discussed in the seventh section. The last is the summary outlook.

2 Related Work

In 1984, the Federal Bureau of Investigation (FBI) established the Computer Analysis Response Team (CART) to research potential computer evidence which is known as the beginning of electronic data forensics. Since the 21st century, with the acceleration of the global digitalization process, electronic data forensics has ushered in a new stage.

Montasari [16] studied the current status of electronic data forensics policing in the context of AI and big data. UK, US, and EU cybersecurity and data intelligence practices are highlighted. Fran et al. [17] reviewed the research progress in various fields of electronic data forensics, identified themes, and identified their main challenges. In addition, procedural issues of preparation, reporting, presentation, and ethical aspects of the discovery process are considered. Akbari et al. [18] reviewed the last decade of digital forensics work in the field of source video identification. In addition, certain challenges during forensics due to compression, stabilization, scaling, and cropping are also pointed out. Kim et al. [19] proposed a direct connection-based forensics model for wearable devices in IoT. The forensics model is based on the ecosystem of wearable devices, adopting wireless or interface methods, which can realize logical and physical forensics, respectively. Oh et al. [20] conducted research on the problem of data recovery in the process of forensics. Taking the metadata file in New Technology File System (NTFS) system as an example, the mechanism of its record storage is studied, and a recovery method for records without fixed value is proposed.

The rapid development of the metaverse will eventually be integrated into all aspects of our lives, and its security research still needs to be in-depth [21]. Khan et al. [22] summarized the methods and frameworks related to electronic digital forensics. In particular, the problem of screening for forgery

and tampering in the chain of custody of evidence is pointed out. In addition, some emerging forensics methods and tools are also highlighted. Yaacoub et al. [23] studied forensics and anti-forensics approaches in the IoT domain, including tools, techniques, types, and challenges. In particular, anti-anti-forensics is discussed as a new anti-forensics protection mechanism. Gragnaniello et al. [24] discussed the application of deep learning (DL) technology in the field of electronic data forensics. Further discuss the security and privacy protection issues faced by metaverse forensics. Li et al. [25] studied electronic data forensics technology in the field of digital twins. Considering the shared distributed ledger attribute of blockchain, a digital twin electronic data forensics method based on blockchain is proposed. Abiodun et al. [26] evaluated the impact of artificial intelligence on electronic data forensics and pointed out new issues faced in metaverse scenarios.

3 Birth and Development of the Metaverse

3.1 What Is the Next Generation Internet?

On September 27, 2021, the theme of "Internet of Everything, Smart Twins-Next Generation Internet Forum" was held in Wuzhen, Zhejiang, China. Zhou Hongren, the former executive deputy director of the National Informatization Expert Advisory Committee, said at the forum that from the Internet to the Internet of Things, the Internet of Things has two distinctive features. One is global interconnection, which may extend to the outer layer in the future, space or even other planets; the second is that people, machines, and things are fully connected, and each person and each object does not need to log in, it becomes the interface of the underlying network. Based on the existing Internet, Internet of Things, intelligent computing, new sensors, etc., the Internet of Things will be possible to reconstruct the topological structure of interconnection and become a new platform for the integration of global economic and social development. Table 1 compares Internet Now and Next Generation Internet.

Table 1: Internet now *vs.* next generation Internet

Today's Internet	Next generation Internet
No Internet access in deserts, oceans, etc.	Globally interoperable
Network interworking reaches 50 hops	Network interworking only requires satellite transfer
Rely on mobile phones, computers and other 2D devices to browse and consult	Using VR/AR equipment, 3D experie
Take the server as the center, and the platform monopolizes the core data	User centric, no server
Paper transactions with us dollar and local currency as the main currency	Based on blockchain and cryptocurrency as the main currency, the whole process of circulation can be traced

The development of the Internet can be roughly divided into three stages: from the computer Internet (Internet 1.0) in the 1980s and 1990s to the mobile Internet (Internet 2.0) in the late 20th and early 21st centuries, and then to the next full Internet or "metaverse" (Internet 3.0) is an inevitable trend in human history. The new generation of the Internet that appeared in the middle of the 21st century, whether it is called the full-real Internet, "virtual reality", or "metaverse", will eventually come as the Internet 3.0 era. In the era of Internet 1.0 and 2.0, the Internet was regarded as an object

alienated from human beings, belonging to an instrumental existence outside the body, but in the era of Internet 3.0, the Internet began to become a kind of subjective existence inside the body, which can through immersive VR devices, it can appear in a relatively isolated form from reality; it can also be presented in daily life in a form of integration with reality through integrated AR devices. Devices such as smartphones that are currently widely used in daily scenes are likely to be replaced by immersive devices such as VR and AR in the future. As shown in Fig. 1, Internet 3.0 will be fully integrated into our lives.

Figure 1: Internet 3.0 and our lives

3.2 Definition of Metaverse

The metaverse raises the interface (experience) of the user's interaction with the Internet from "two-dimensional" to "three-dimensional", which will play a role in promoting the technology and development of the Internet. Although it is said that the metaverse cannot be equated with Internet 3.0, from the current development point of view, the metaverse will be one of its most typical applications. In other words, the metaverse can give you the answer to what the next-generation Internet is.

There is currently no unified view on the definition of the metaverse. Chen and others from Peking University believe that the metaverse is a digital living space with a new social system. By using technological means to build a virtual world, it achieves mapping and interaction with the real world. Ning et al. from Beijing University of Science and Technology pointed out that the metaverse is essentially a generalized cyberspace. The metaverse encompasses physical space, social space, cyberspace, thinking space, and integrates various digital technologies to gather networks, hardware and software devices, as well as users in a virtual reality system. It is a virtual world that is both mapped to and independent of the real world. BBC Technology journalist Marc C. defines the metaverse as an immersive Internet. In the metaverse, every real person has a virtual avatar and uses virtual reality, 3D technology, and sensor technology to allow humans to control it.

Although the definitions of the metaverse in academia and business are not the same, their application prospects are still unanimously optimistic. Strictly speaking, the author believes that the metaverse is not a new concept, but a collection of several technologies, the evolution of which pushes people's lives into a new era. The six supporting technologies of the metaverse are shown in Fig. 2. Blockchain, intelligent wearable devices, and virtual reality devices occupy important positions in metaverse forensics. Blockchain is the underlying foundation of the core, while intelligent wearable and virtual reality devices are the flagship applications of the metaverse.

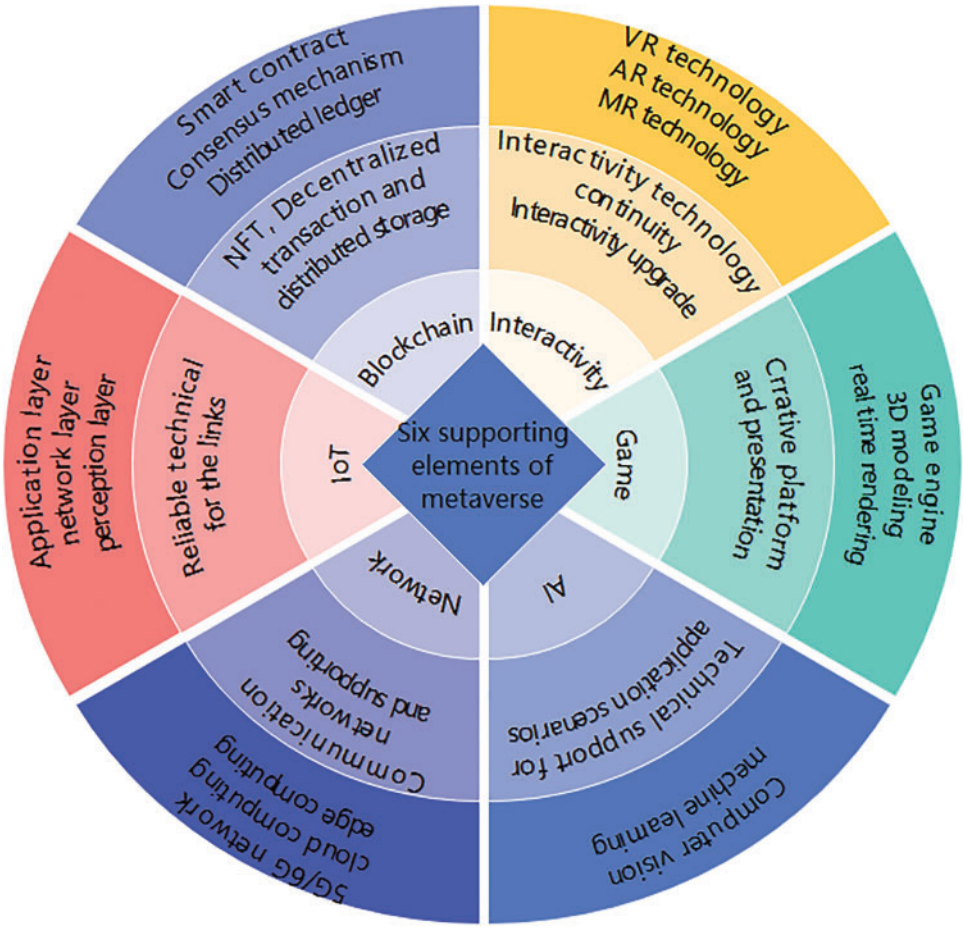

Figure 2: The six supporting technologies of the metaverse

3.3 Development History of Metaverse

As shown in Fig. 3, we discuss the three developmental stages of the metaverse in this subsection.

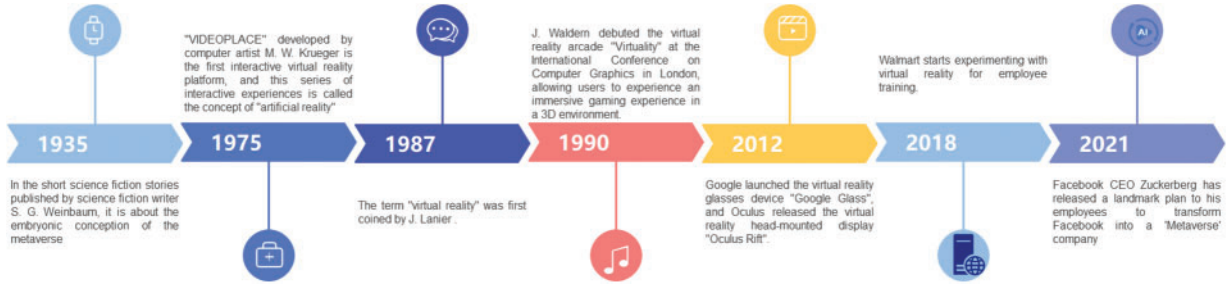

Figure 3: The three stages of development of the metaverse

1) The embryonic stage of the metaverse

In 1935, science fiction writer S. G. Weinbaum published a short science fiction story in which he described the peculiar experience of the protagonist Pygmalion entering another world after

wearing special goggles [27]. This is also the earliest description involving the sensory experience of virtual reality such as hearing, vision, and touch, and it is the bud of the conception of the metaverse. In 1961, Philco engineers Comeau and Brian developed a simple motion-tracking head-mounted display called "Headsight," which is now known as Head Mounted Displays (HMD) [28]. In 1968, computer graphics pioneer Sutherland first developed a head-mounted display connected to a virtual environment, dubbed the "Sword of Damocles" due to its similarity in shape [29]. Integrating interaction art and virtual reality experience, "VIDEOPLACE" developed by computer artist Krueger in 1975 is the first interactive virtual reality platform, this series of interactive experiences is what he calls the "Artificial Reality" (Artificial Reality) concept [30]. In 1985, the National Aeronautics and Space Administration (NASA) announced the research results based on virtual workstations. In 1986, Furness III developed a flight simulator called a super cockpit, enabling the pilot to see and see in real-time, the helmet's tracking system and sensors allow the pilot to control the aircraft using gestures, voice, and eye movements [31].

2) The rising stage of the metaverse

It was not until 1987 that Lanier first proposed the term "virtual reality". As the founder of Visual Programming Lab (VPL), he is dedicated to the development of virtual reality devices such as data gloves and videophone head-mounted displays, which is also the first company to sell virtual goggles and gloves. The concept of virtual reality is clarified and recognized by all walks of life [32]. In 1990, Waldern first demonstrated the virtual reality arcade "Virtuality" at the International Computer Graphics Conference in London, allowing users to obtain an immersive gaming experience in a 3D environment. In 1991, the gaming video giant Sega announced the completion of the development of the Sega VR headset [33]. In 1992, Cruz-Neira et al. used the technology available at the time to build a virtual reality environment CAVE, which would feedback correct perspective and stereoscopic projection as the audience moves within a limited range [34]. In 1995, Nintendo launched a stereoscopic video game console called "Virtual Boy" [35]. At the end of the 20th century, virtual reality technology gradually began to be exploratory applications in other fields, and the application range expanded from the military, and entertainment to the medical field. In 1999, researchers such as Rothbaum et al. proposed to use virtual reality technology for Vietnam veterans. Create war zone scenarios to help them with post-traumatic stress disorder (PTSD) exposure therapy [36].

3) The industrialization stage of the metaverse

At the beginning of the 21st century, the Metaverse gradually began to industrialize. In 2012, Google launched the virtual reality glasses device "Google Glass" and Oculus released the virtual reality head-mounted display "Oculus Rift". The two companies competed in the field of virtual reality, setting off a new wave of virtual reality technology. In 2014, the Internet giant FaceBook acquired Oculus as a whole for $2 billion. CEO Zuckerberg believed that Oculus would become a future metaverse platform and predicted that virtual reality technology would change the personal network experience [37]. Internet companies began to get involved in the field of virtual reality. In the same year, Samsung's Gear VR and Google's Google Cardboard came out successively. From then on, in 2016, High Tech Computer (HTC) began to sell HTC Vive, and Sony launched Play Station VR. In 2018, Walmart began to experiment with virtual reality technology for employee training, selecting ten pilot stores and investing in 17,000 Oculus headsets in the future to make virtual reality training the standard for all units [38]. Walmart is one of the largest retail chains in the United States, and this decision will take virtual reality technology to new heights. The application field of virtual reality technology continues to expand, and the social and economic value is deeply excavated. In 2020,

NVIDIA's "real-time simulation and collaboration platform" (Omniverse) was successfully built, and the public beta was officially launched in December of the same year.

2021 is also seen as a critical year for the industrialization of the metaverse. In June 2021, Facebook CEO Mark Zuckerberg released an epoch-making plan to his employees to transform Facebook into a "Metaverse" company, making what is now an ordinary social platform where users can live in it. immersive platform. Later, at the Facebook Connect conference in October of the same year, Zuckerberg officially announced that the company would strive to complete the transformation in the next five years or so. The Seoul Metropolitan Government of South Korea released the "Metaverse Seoul Five-Year Plan", starting in 2022, to build a "Metaverse" administrative service ecosystem in various business areas in three phases. In the "14th Five-Year Plan for National Economic and Social Development of the People's Republic of China and the Outline of Vision 2035" issued by my country in March 2021, there are also "accelerating the construction of digital economy, digital society, digital government, and digital transformation. The overall drive to change the way of production, way of life and governance".

4 Metaverse Security

The virtual world of the metaverse not only runs parallel to the real world, but also provides users with twin mirrors and immersive experiences similar to the real world. There will be new issues of technological integration and order reconstruction, as well as old problems projected into the real world. In the process of the development of the metaverse, if governance measures are not in place, the following risks may arise: 1) The risk of elevating sovereign authority and endangering network data security. 2) The risk of endangering users' physical and mental health and social order. 3) The risk of infringing on personal rights, affecting ecology and energy security.

4.1 Social Risk

The metaverse is a subversion and reshaping of the way of human existence, and it reconstructs people's view of time and space. In the dimension of time, the new digital survival mode opened by the metaverse has changed human perception of time. What the metaverse creates is a new space-time experience that connects reality and virtuality, providing humans with a place to live in a higher dimension of freedom. However, the change in the concept of time and space will inevitably bring about changes in human cognitive form and way of life in the virtual digital space. If we are too addicted to the virtual experience and separated from real-time and space, it will cause the degradation of individual abilities and the shrinking of real society. Science fiction writer Liu Cixin, in the novel "Festivals That Can't Coexist" (2016), used the characters of the novel to attack the squeeze of virtual reality on the exploration of the universe with slightly emotional words: "Intelligent civilization is nurtured in it, and in reality growing up in the middle of the sky, fly into space, but go out in virtual reality, like a firefly in a lotus pond, flickering and disappearing in the night. Look at the starry sky, there is silence, you know why." Therefore, human needs constantly seek and adjust the balance and order between virtual and real-time space to avoid alienation and opposition from reality.

In the metaverse, human form and function will be reshaped and expanded. Thus, human beings experience the evolution from the traditional "natural person" to the virtual "semi robot", which involves many ethical and moral issues. For example, human-computer interaction, virtual marriage and family, false identity and information, intellectual property, etc. Perhaps in the future, research institutions will develop ethical and ethical digital protocols as underlying technologies to support the operation of the metaverse. The concept of the metaverse constructs a highly free and

tolerant "utopian" world. How to construct an ethical and moral consensus in the metaverse within a decentralized framework and be accepted by the real society requires in-depth research from multiple perspectives. Firstly, it is necessary to formulate and improve relevant laws and regulations. Secondly, it is necessary to vigorously promote and urge relevant departments to implement it.

4.2 Crime Risk

The construction of laws and regulations in the metaverse also needs to be studied simultaneously. In the real world, laws, and regulations are used to constrain the normal social order, and the metaverse is still in the initial stage of exploration. Whether to continue to use the laws of the real world or rely on group consensus to constrain people's behavior and social governance in the metaverse requires further research. In fact, due to the lack of regulation, the metaverse world in full swing is already filled with a considerable degree of criminal risk. As shown in Fig. 4, the criminal risks of the metaverse mainly include endangering national security, endangering citizens' personal information and privacy, online gambling, pornography and money laundering, and fraud. Faced with the above-mentioned criminal risk points, on the one hand, public security organs should increase publicity and dissuasion from the social level. On the other hand, actively seeking technological breakthroughs and increasing efforts to crack down on illegal crimes.

Figure 4: The criminal risk of the metaverse

4.3 Metaverse Governance

At present, the underlying technologies in many segmented fields such as chip manufacturing, network communication, big data, and cloud computing cannot fully support the current vision of the future panorama of the metaverse. The development of the metaverse is still in its early stages and

has uncertainty. Therefore, for the governance of the metaverse, an inclusive and cautious attitude should be maintained as a whole, and specific risks that have already emerged should be dealt with in a timely manner.

On the one hand, for the current stage, promoting development is the theme, and the governance of the metaverse should mainly be regulated and guided. In terms of policies, it is necessary to provide more sufficient development space for cutting-edge enterprises and institutions in relevant fields. On the premise of fully stimulating the driving force of innovation in the relevant fields of the metaverse, we should play the decisive role of the market in resource allocation, better leverage the role of the government, and guide the rational and orderly entry of factors such as technology, capital, and human resources.

On the other hand, for the chaos caused by the metaverse boom, timely intervention and governance are needed. For example, the emergence of the metaverse has provided a broader investment and trading space for new types of digital assets such as NFTs (non homogeneous tokens) and virtual currencies, as well as channels for new forms of illegal criminal activities such as money laundering, illegal fundraising, fraud, pyramid schemes, and some capital chaos.

4.4 The Necessity of Metaverse Forensics

Thus, metaverse forensics is an extremely important but unimportant need. It's important because it is the dominant form of the next-generation Internet, and it touches every aspect of people's lives. The research on metaverse forensics will be the main work and practice of public security organs and judicial organs in the future. Fortunately, the full implementation of the metaverse may take more than ten years or even twenty years, and we have relatively sufficient time to plan and research.

At present, there are about 26 metaverse concept companies, including 2 Chinese companies. There are dozens of companies in the United States that focus on blockchain forensics, such as CipherTrace, Chainalysis, BlockSeer, Elliptic, etc. However, there are no domestic companies that focus on blockchain forensics, which requires a lot of human and resource investment to do pre-research work.

5 Metaverse Forensics

From a technical point of view, the objects of metaverse forensics include blockchain, smart wearable devices, virtual reality devices, etc., which will be discussed one by one below.

5.1 Blockchain Forensics

The entire operation mechanism of Bitcoin can be briefly described as follows: first, the client initiates a transaction and sends the transaction to any node in the Bitcoin network. After receiving the transaction, the node verifies whether the transaction is correct. If the verification fails, the node will reject it. The transaction is returned to the sender and the transaction is rejected. If the verification is passed, the node will put the received transaction into its transaction pool and continue to spread it to the network. Each node will package the transaction from its transaction pool, and The calculation is performed by adding random numbers. The block packaged by the node that first calculates the required hash value is valid, that is, the node obtains the accounting right of the packaged transaction. After that, the node broadcasts the block obtained by the calculation to blockchain network, after receiving a new block, other nodes will immediately verify the correctness of the block. After the verification is successful, the new block will be connected to its chain, and at the same time, the

transaction records that have been packaged in its transaction pool will be removed; and then restart a new round of the production block process. The above process can be summarized as shown in Fig. 5.

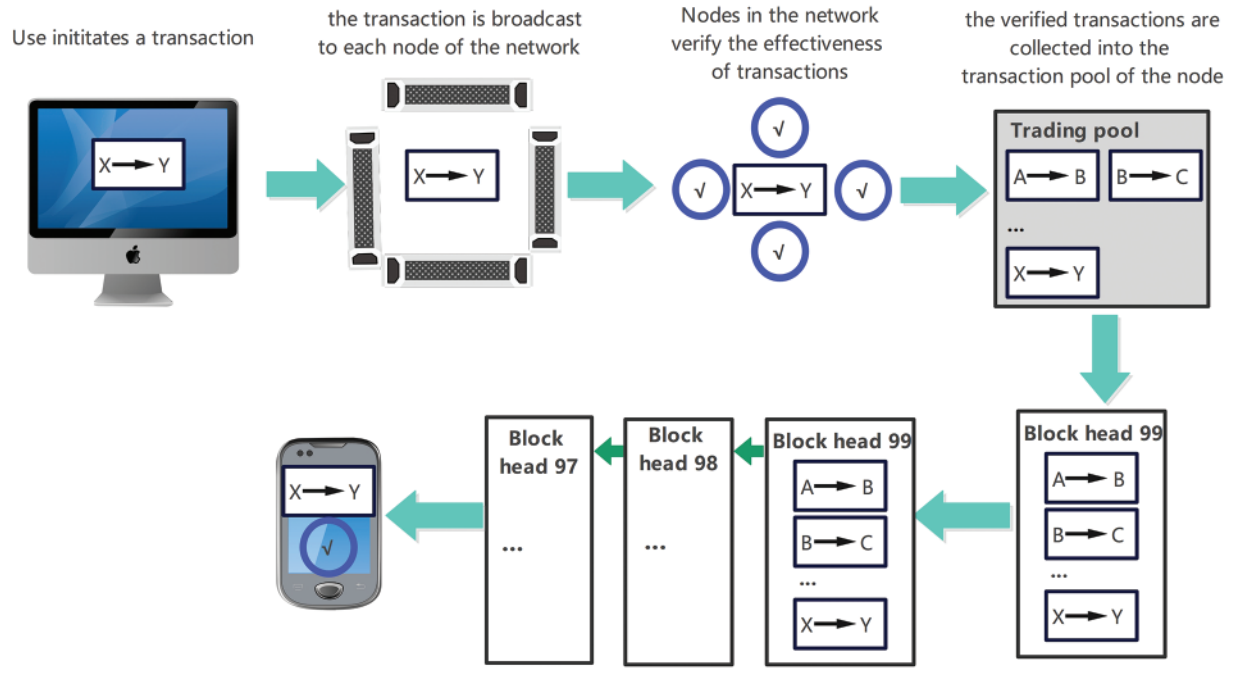

Figure 5: Blockchain operation mechanism

The above process is the following steps: the client initiates the request, each node spreads the user request in the network, the nodes participating in the record in the network verify the request data, and each node completes the user request according to the consensus algorithm and packs multiple requests to generate an area. Blocks, nodes broadcast new blocks, and non-block generating nodes verify new blocks and update the original chain. Compared with the 7-layer architecture of Transmission Control Protocol/Internet Protocol (TCP/IP), the blockchain can be divided into the application layer, contract layer, incentive layer, consensus layer, network layer, and data layer, as shown in Fig. 6.

Table 2 summarizes the functions of each layer of the blockchain architecture in Fig. 6, and summarizes the corresponding forensic data.

5.2 Forensics of Smart Wearable Devices

Smart wearable devices (also known as wearable devices, wearable smart devices, etc.) generally refer to electronic communication devices embedded in clothing, or in the form of accessories and personal wearables. Smart wearable devices combine the functions of information collection, recording, storage, display, transmission, analysis, and solutions with our daily wear and become part of our wear, such as clothes, hats, glasses, bracelets, watches, shoes, etc.

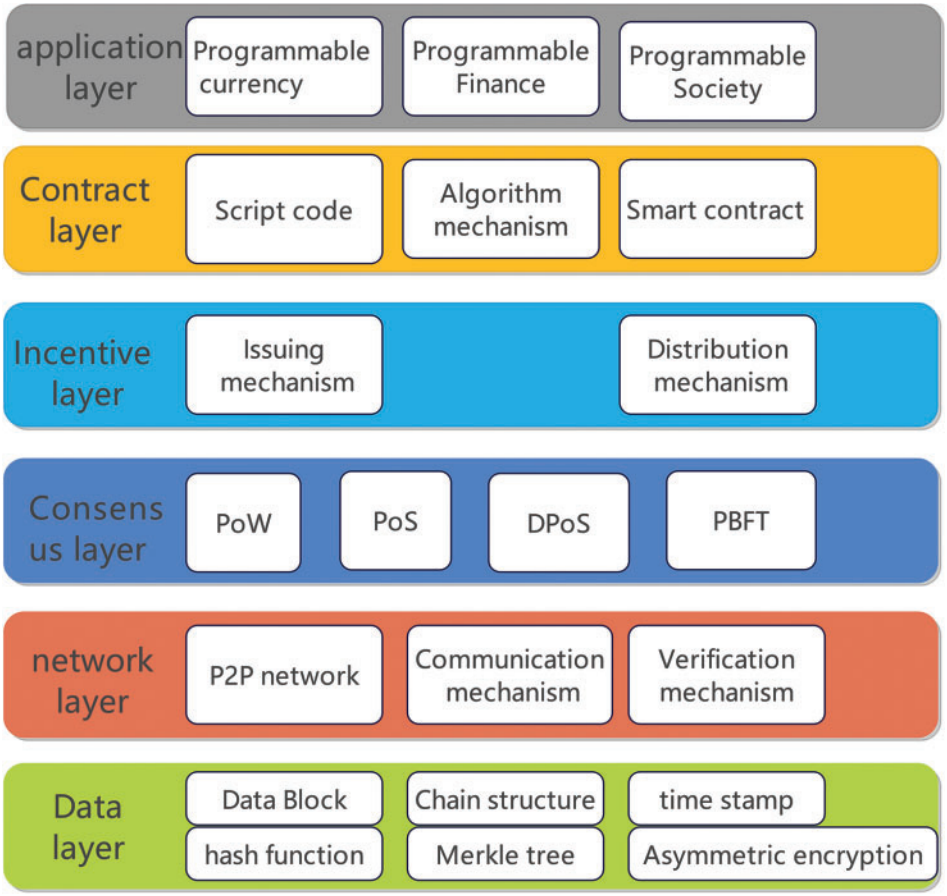

Figure 6: Blockchain infrastructure

Table 2: Blockchain forensics objects

Blockchain architecture	Function	Extractable data
Data layer	Store user transaction data.	Block header, hash value, timestamp, random value, version number, Merkle tree.
Network layer	A node network through data transmission to ensure decentralization.	Node transmission protocol and data verification technology.
Consensus layer	Nodes reach a consensus on blockchain data.	Consensus algorithm and incentive mechanism.
Smart contract layer	Expand the scope of application and programmable.	Development and data transfer of smart contract.
Application layer	Establish interaction with the application field.	User information and service information.

A smart wearable device is a hardware terminal with computing, storage, or transmission functions. It innovatively embeds technologies such as multimedia, sensors, and wireless communication into people's clothing or makes it more portable, and creates subversive applications and interactive experiences. There are many types of smart wearable devices, and although the amount of data is not large, it has very important forensic value. "Data doesn't lie!" Because people's physiological indicators are difficult to control, as a smart wearable device that is in close contact with the human body, can be prepared to reproduce, evaluate the status of relevant personnel such as victims and suspects, and thus provide clues for handling cases.

Institute of Management Studies (IMS) Research, an internationally renowned market research company, divides smart wearable devices into four major areas from application areas: fitness and health, medical and health care, industry and military, and infotainment. At present, the difficulty of obtaining evidence for smart wearable devices is that many products are too niche and the data interface is not open. This paper further summarizes the data characteristics of different types of devices, as shown in Table 3.

Table 3: Forensics objects of smart wearable devices

Field of application	Product category	Function	Retrievable data
Fitness and health	Sports monitors; fitness and heart rate monitors; smart sports glasses; smart clothing; sleep sensors; mood measuring instruments.	Fitness step counting, sleep monitoring, information viewing, event reminders, phone answering, precise positioning, etc.	Call records, chat data, voice, pictures, positioning information, trajectory, body indicators, etc.
Medical and healthcare	Continuous blood glucose monitor; ECG monitor; pulse oximeter; blood pressure monitor; hearing aid; rehabilitation system; virtual imaging device.	Vital sign detection, including blood sugar, blood pressure, blood oxygen, electrocardiogram, etc.; auxiliary and health care functions, such as hearing aid, rehabilitation, etc.	Vital sign parameters, voice, pictures, changes in body indicators, etc.
Industry and military	Hand-worn terminal equipment; smart clothing; augmented reality headset; human-computer interaction virtual training system.	Virtual simulation and control of industrial systems; military personnel training, weapon development, testing, etc.	Manipulate, interact with data; training logs; test logs, etc.

(Continued)

Table 3 (continued)

Field of application	Product category	Function	Retrievable data
Infotainment	Smart watches; smart glasses; augmented reality headsets; wearable imaging devices; immersive gaming systems.	Virtual reality, augmented reality; real-time camera, map navigation; human-computer interaction, control, etc.	Operation log, voice, picture, video, navigation information, etc.

5.3 Virtual Reality Device Forensics

Virtual reality technology is one of the important components of metaverse architecture. It takes computer technology as the core and combines related science and technology to generate a digital environment that is highly similar to real visual, auditory, and tactile sensations. Users need to use the necessary equipment to interact with objects in the digital environment, resulting in a sense and experience of being in the real world. At present, it seems that virtual reality equipment will explode in the metaverse era, which is mainly reflected in the variety of equipment, complex interfaces, and huge amounts of data. Therefore, the forensics of virtual reality equipment will be difficult. This paper discusses the forensics of virtual reality systems from another perspective, to try to bypass the complicated types of virtual devices, and then give a summary of forensics idea.

The virtual reality system is mainly composed of five parts, including professional graphics processing computer, input and output equipment, application software system, database, and virtual reality development platform. The product categories, functions, and forensic data of the components of the virtual reality system are shown in Table 4.

Table 4: Forensic objects of virtual reality system

System composition	Product category	Function	Retrievable data
Professional graphics computer	All kinds of high-performance computers, servers, etc.	Convolution operations, image processing, video rendering, etc.	Pictures, videos, etc.
Input and output devices	Stereoscopic displays, human motion capture devices, hand gesture input devices, speakers, etc.	Human-computer interaction, control, etc.	Operation log, voice, gesture, motion gesture, etc.
Application software system	3D animation design system, modeling system, behavior analysis system, etc.	Build 3D scenes, network scenes, realize control of scene objects, etc.	Various models, operation logs, control logs, etc.

(Continued)

Table 4 (continued)

System composition	Product category	Function	Retrievable data
Database	Mysql, oracle, sqlserver, sqlite, etc.	Storage, interception, security, backup, etc.	Original database information, including personnel information, database operation and management logs, etc.
Virtual reality development platform	Vizard, Virtools, Edge Of Network (EON), Quest3D, etc.	Responsible for the development, calculation, generation, connection and coordination.	Platform development, operation and maintenance information, etc.

6 Metaverse Forensics Experiment—Take Smart Wearable Device as an Example

Metaverse forensics involves a three-layer architecture of cloud-network-terminal, which corresponds to server forensics, network forensics, and terminal device forensics. Therefore, the IoT forensics scheme based on a three-layer architecture is also applicable to the metaverse. In the future metaverse scenario, smart wearable devices are a representative type of forensic device, and smart bracelets are typical of such devices. This paper conducts experimental research on smart bracelet forensics.

According to commercial statistics, China's wearable market will ship nearly 140 million units in 2021. In 2022, China's wearable market shipments are expected to exceed 160 million units, and the market size is already considerable. With the increasing popularity of smart wearable devices, it also brings severe challenges to the protection of personal information. IoT devices such as portable fitness monitoring products and wearables are inherently vulnerable to hacking due to their connection to the Internet. From attacking devices with Distributed Denial of Service (DDOS) to violating personal privacy, malicious attacks from third parties can wreak havoc on unsuspecting personal data products in some ways. Therefore, the safety of smart wearable devices represented by smart bracelets is self-evident. For example, when smart bracelets are paired with mobile phones via Bluetooth, users are required to register before using these devices. This involves the user's age, height, weight, gender, and other information. In particular, user login requires a mobile phone number or email address. After pairing, the smart bracelet will synchronize the collected exercise steps, mileage, calorie consumption, heart rate, sleep data, etc., with the APP, including your uploaded profile picture.

Supervisory Control and Data Acquisition (SCADA) systems are widely used in industrial applications. There are also various Intrusion Detection Systems (IDS) in the Metaverse [39,40]. The rest of the research in this lab is based on data sniffing. The data sniffing process of the smart bracelet is shown in Fig. 7. Research in this area is still in the exploratory stage, so some Machine Learning (ML) indicators are not given. The following is the specific experimental process:

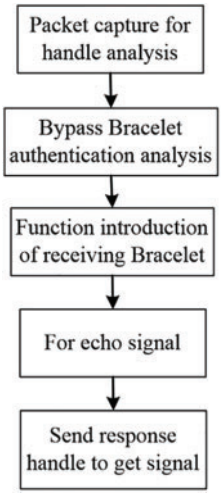

Figure 7: Bracelet data sniffing

6.1 Analysis of the Packet Capture Handle Structure

It is clear that the handle structure is the basis for Bluetooth packet capture communication, and the signal can be returned according to its handle format. When capturing packets, we should pay attention to keeping the Bluetooth device disconnected. Otherwise, it may not be able to capture its signal. It is very convenient to install ubertooth packages in Linux. We use ubertooth with Wireshark to obtain packages which are shown in Fig. 8. Pay attention to distinguish the types of packages. Damaged packages will not carry valuable data.

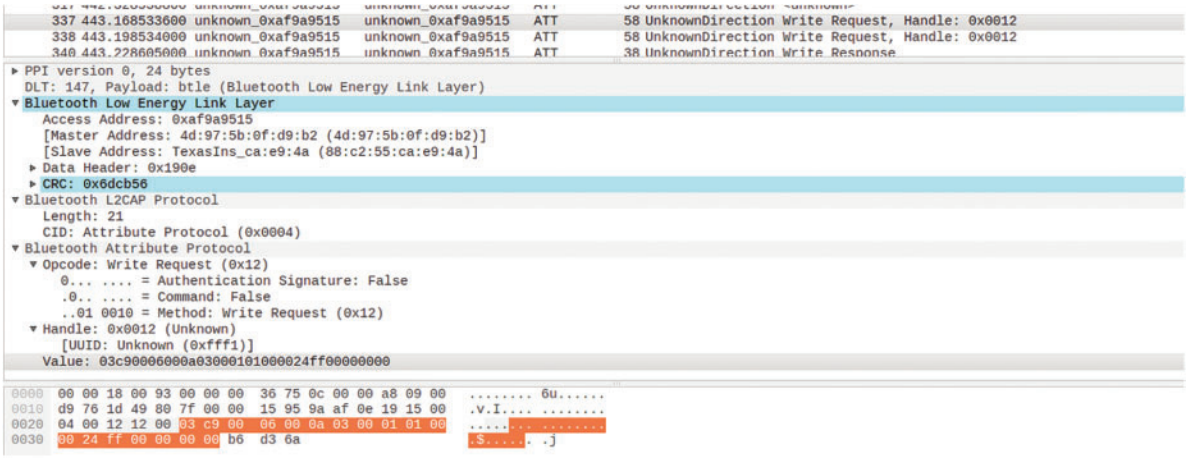

Figure 8: Packages are obtained with Wireshark

As shown in Fig. 9, the handle structure is analyzed. 03-00 is its head, the middle 00 field represents the light bulb switch, and the 00-FF field represents the ratio of RGB three colors. Knowing the distribution structure of the handle signal, you can send back the handle to control the switch and color of the Bluetooth bulb.

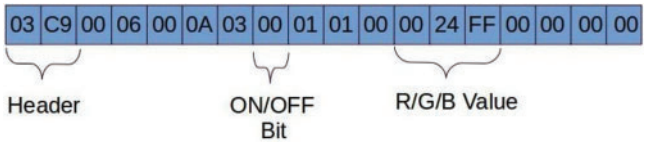

Figure 9: Analysis of the handle of the captured bluetooth light bulb

6.2 Using the Raspberry Pi's Own Bluetooth Module

Generally speaking, Bluetooth devices from legitimate manufacturers set strict authentication mechanisms when connecting. This makes it difficult to simulate and bypass the authentication environment without understanding the authentication mechanism. However, the authentication mechanism is based on the handle sending and receiving mechanism. As long as the corresponding special value is responded to, the connection can be made.

The LT716 bracelet is used in the experiment, and it does not have a very strict bypass mechanism, so there is not too much difficulty in connecting to the Raspberry Pi.

Input command: Sudo Hcitool Lescan scan for Bluetooth signal which is shown in Fig. 10.

```
pi@raspberrypi:~ $ sudo hcitool lescan
LE Scan ...
CB:28:08:D0:DC:29 (unknown)
44:70:C1:AE:21:2D (unknown)
44:70:C1:AE:21:2D (unknown)
45:62:EA:7D:F4:36 (unknown)
69:7A:76:F3:C0:31 (unknown)
69:7A:76:F3:C0:31 (unknown)
77:E6:E7:19:99:67 (unknown)
31:AC:0D:A1:A4:60 (unknown)
6E:9C:A4:80:58:81 (unknown)
74:F0:2D:6B:9E:08 (unknown)
74:F0:2D:6B:9E:08 (unknown)
57:C5:D7:EC:68:C8 (unknown)
57:C5:D7:EC:68:C8 (unknown)
39:DC:45:F5:16:C3 (unknown)
25:A4:B7:18:9C:4C (unknown)
C1:04:18:0C:28:1C (unknown)
C1:04:18:0C:28:1C Mi Smart Band 6
48:F2:3B:35:9A:43 (unknown)
48:F2:3B:35:9A:43 (unknown)
11:CA:35:17:49:75 (unknown)
60:F4:3A:E4:1D:DC (unknown)
60:F4:3A:E4:1D:DC EDIFIER Lolli Pods Plus
C7:C4:16:6D:C6:C2 (unknown)
4C:87:5D:82:2A:D7 (unknown)
4C:87:5D:82:2A:D7 LE-TTC
A4:C1:38:C5:DF:98 LT716
A4:C1:38:C5:DF:98 LT716
```

Figure 10: Bluetooth signal scan

Target lock bracelet: LT716.

As shown in Fig. 11, we use the Gatttool command in the Bluez function to try to connect: Gatttool-I connects A4:C1:38:C5:DF:98. When the mac address turns blue, the connection is successful.

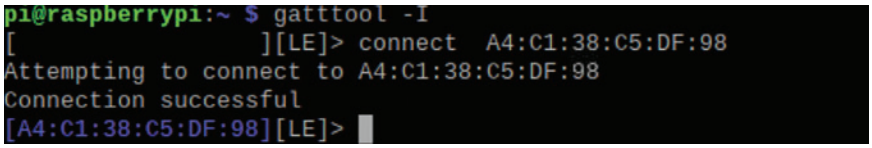

Figure 11: Bluetooth connection is successful

6.3 Data Interaction with Bracelet

This part mainly deals with the interaction, and analyzes and responds to the handle sent by the bracelet. There are many different functions on the bracelet, so key fields such as its head and functional end can be established which is shown in Fig. 12.

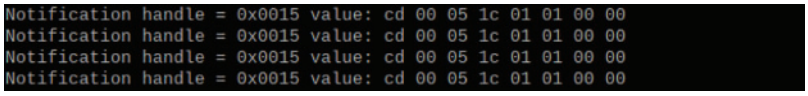

Figure 12: Corresponding handle transmission of the bracelet

Capture the corresponding handle transmission of the bracelet:

Call the host function: 4 times to call the host, close and open are the same handle. After the bracelet sends this function handle, it enters the waiting state, and if it can receive a return request during this period, it will automatically turn off this function. If the return request cannot be received, the waiting time will be extended, and it will be automatically closed.

For the camera function of the wristband, the wristband terminal presses the camera button to send the 03 handle. The mobile terminal has a reply after executing the function, and the wristband terminal receives the reply and sends the 04 handle which is shown in Fig. 13.

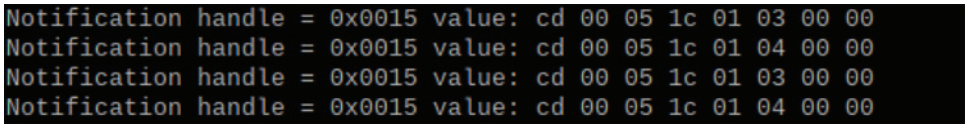

Figure 13: The bracelet terminal sends the handle after receiving the reply

From the above two functions, it can be concluded that the designer did not do much deployment on simple functions. The initial determination bit of the head is cd-00, and the effect bit is only the bit of 01/03/04 (that is, the penultimate bit, three). Only the action bits need to be changed when the handle is written.

However, this lab does not further explore write permissions, some functions require special permissions to be changed.

The next three heart rate measurements correspond to the photos of the bracelet. When measuring heart rate, no handle is sent. After the measurement, the handle is sent to the terminal immediately, to perform data encryption analysis which is shown in Fig. 14.

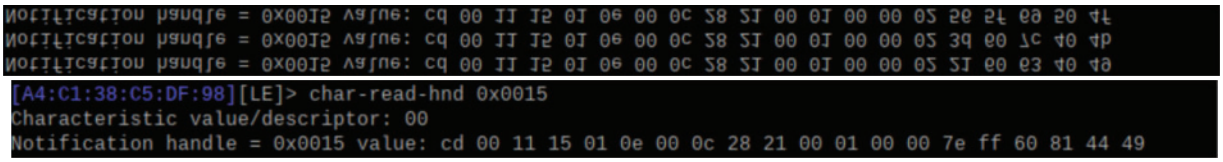

Figure 14: After the measurement of the bracelet is completed, the handle is sent to the terminal

It can be seen that the data has changed in the last 5 bits. Combining the above two functions, it is found that the header should be cd-00, and the data transmission bit should be the last 5 bits. The type and process of encryption is unclear which are shown in Fig. 15.

Figure 15: The bracelet data was modified in the experiment

The forensic analysis process of the smart bracelet is just an example of metaverse forensics. Because the data type and amount of the smart bracelet are not large, the difficulty lies in the analysis of Bluetooth packet capture and privilege escalation, and the workload of data analysis is not large. For future metaverse forensics, there will be problems such as extraction and analysis of massive data, various heterogeneous interfaces, and volatile data. In the future, there will be more and more forensics targeting blockchain and other related technologies, as well as virtual devices.

6.4 Comparative Analysis of Experimental Results

This section compares and analyzes three forensics schemes for smart bracelets, as shown in Table 5.

Table 5: Comparative analysis of experimental results

No.	Scheme	Characteristic	Tool	Advantage	Disadvantage
1	Analysis of the Packet Capture Handle Structure	Bluetooth packet capture communication, Capture Handle Structure	Ubertooth, Wireshark	Basic way, strong flexibility	Lost packets cannot get data

(Continued)

Table 5 (continued)

No.	Scheme	Characteristic	Tool	Advantage	Disadvantage
2	Using the Raspberry Pi's Own Bluetooth Module	Raspberry Pi integrated Bluetooth module to capture packets, Bypass authentication mechanisms	Raspberry Pi	High concentration, easy to operate	It is difficult to simulate and bypass the authentication environment without knowing the authentication mechanism
3	Data Interaction with Bracelet	deals with the interaction, and analyzes and responds to the handle sent by the bracelet	Self-built environment	Highest flexibility, not dependent on specific tools	Experiments with different equipment have no reference and need to be tried repeatedly

7 Future Research and Challenges of Metaverse Forensics

2021 is called the first year of the metaverse, and many technology companies at home and abroad (for example, Facebook, Nvidia, ByteDance, etc.) begin to lay out the metaverse, and the metaverse era has quietly arrived, and has been applied to real estate, clothing, entertainment, conferences, education and other application scenarios. However, the governance of the metaverse, which takes metaverse forensics as an important starting point, is full of complexities and faces many challenges. The metaverse is a vast system, and forensic evidence in the metaverse involves all aspects of this vast digital system. The research on evidence collection in the metaverse has a long way to go.

7.1 Laws and Regulations in Metaverse Forensics

Whether the metaverse can be accepted by society requires a long process. A series of ethical and moral issues that may arise during this process, such as human-machine coexistence, virtual marriage and family, false identity and information, intellectual property, etc. How to build a highly free and tolerant metaverse world within a decentralized framework. This requires forming an ethical and moral consensus and being accepted by the real society. The construction of laws and regulations in the metaverse also needs to be studied simultaneously. In addition, the legal validity and boundary issues of metaverse forensics are also worth in-depth research. Scholars believe that an international legal framework should be established to promote cooperation between countries and thus facilitate the investigation of metaverse crimes. By discussing legal issues related to the identity of metaverse users, further research is conducted on possible crimes that may occur in events in existing virtual worlds [41–43].

7.2 Security and Privacy in Metaverse Forensics

The development of the metaverse will bring many security and privacy issues. It may even affect the security of critical national infrastructure. The study of evidence collection in the metaverse is urgent. As an emerging digital ecosystem, the metaverse is inevitably subject to various forms

of cyber attacks. Network attacks may target users and their device terminals in the metaverse, as well as operators or key service providers in the metaverse. In addition, due to the explosive development mode of the metaverse, there are many design flaws and vulnerabilities in the products of the metaverse. Privacy and security have become urgent issues. References [44–49] systematically studied the fundamentals, security, and privacy issues of the metaverse. A series of key challenges and questions about the security and privacy of the metaverse is raised. Reference [50] considered the privacy protection problem of metaverse applied to the health domain. Reference [51] addressed the implications of zero-trust security for the metaverse. References [52,53] studied the problems of data security in virtual reality and digital twin technology.

7.3 Personal Identification in Metaverse Forensics

Metaverse creates a digital space that combines reality and virtuality. People have a high sense of immersion in the metaverse, which also makes it a parallel space like the real world. Therefore, living in the metaverse brings a new dimension to the digital identity that people have. In real society, personal identity is the credential for people to carry out and obtain interest attributes in various social activities. At the same time, according to different life scenarios, personal identities also have many different attributes, such as citizenship, family membership, relatives, etc. These are also closely related to our life interests. As the metaverse is a virtual digital world, how to legally identify the interests of digital identities and establish relevant protection mechanisms has become a key issue.

On the one hand, the metaverse makes it easier to be recognized by law by endowing digital identities with personality attributes. Many violations of identity and personality that are applicable in reality can also be applied to the Internet. This provides a basis for the definition of illegal acts at the judicial level and the protection of personal identity. On the other hand, metaverse uses encryption verification, digital signature, and other mechanisms to establish authentic, credible, and highly private digital identities for users. Under normal circumstances, users can freely carry out various activities on the Internet under these identities. If there are some illegal acts, the judiciary and regulatory agencies can also use this authentic information to determine the real identity of the user. In this way, the corresponding punishment is given to maintain order and stability in the metaverse. Reference [54] studied the problem of digital identity on the Metaverse and explored tools for identity conversion between self-identity and role identity. References [55–58] researched digital identity recognition in the metaverse, designed a series of algorithms based on machine learning, and achieved exploratory results.

7.4 Non-Fungible Tokens (NFTs) in Metaverse Forensics

The Metaverse is a world filled with digital works of all kinds. How to guarantee the ownership and usage rights of these massive digital works is a very important research field. NFTs are currently the best solution. One of the fastest growing areas of the Metaverse, NFTs are digital assets that represent physical objects, such as art, music, in-game merchandise, and videos. Cryptocurrencies are often used to buy and starship of anything, especially digital assets. Therefore, NFTs will play a key role in the metaverse economy online and are often coded using the same underlying software as most cryptocurrencies. The combination of NFT and blockchain technology can effectively guarantee the online verification of owner. References [59,60] discussed the application of NFT in the metaverse from an economic point of view, and pointed out the importance of metaverse forensics. References [61,62] studied the possibility of using machine learning for metaverse forensics from a technical perspective.

7.5 XR (VR|AR|MR) in Metaverse Forensics

Entry into the metaverse mainly relies on highly immersive XR (VR/AR/MR) devices, but the current virtual realization technology is difficult to miniaturize, portable and cost-effective for users to enter the metaverse anytime, anywhere, and wearing XR devices for extended periods can be uncomfortable. With the help of the extension of XR technology, the metaverse can generate a lot of new application fields. References [63–67] focused on the field of healthcare, removing the barriers between healthcare providers and recipients through metaverse holistic solutions. References [68–72] discussed the application of metaverse in the field of games, and gave some possible angles of metaverse forensics.

7.6 Blockchain in Metaverse Forensics

The combination of blockchain and Metaverse is natural and mutually promotes development. There have been many theoretical and practical results in the research of blockchain, but the research on the combination of blockchain and Metaverse is still in its infancy. References [73–75] summarized the blockchain-based metaverse application scenarios and systematically pointed out all aspects of the metaverse architecture. In particular, blockchain's impact on key enabling technologies in the Metaverse, including the Internet of Things, digital twins, multisensory and immersive applications, artificial intelligence, and big data. References [76–80] discussed the latest achievements of artificial intelligence technology combined with blockchain for the metaverse, especially how to use AI technology and how to integrate blockchain to better serve the needs of metaverse security and forensics.

7.7 Wearable Device in Metaverse Forensics

The metaverse will make extensive use of future technologies such as artificial intelligence. Using technologies such as computer vision, intelligent speech, and natural language processing, it can generate a realistic vision, hearing, and other sensations, helping to realize social and economic activities that go beyond the limitations of the real world. However, few existing forensic methods and tools are available for these emerging high-tech devices. Forensic researchers must closely follow the technical foreword and conduct intensive research on the parameters, operating mechanisms, data storage formats, etc. of these metaverse devices. The time cost and manpower investment are extremely huge because the emerging metaverse devices are not very efficient. It is possible to develop its interface. For the security and forensics research of smart wearable devices in the Metaverse, reference [81] has done exploratory work.

8 Conclusions

After experiencing the "explosion", the Metaverse entered a relatively pragmatic stage in 2022. From the perspective of industrial chain layout, ecology has been initially established in China. In terms of technology, the Metaverse is a "master" of existing information technology, and terminal entrances and interactive generation systems connected to the virtual world are being actively deployed. In terms of policies, relevant national and local support policies are also accelerating follow-up. Since the beginning of this year, metaverse industry-specific policies and drafts for comments have been issued intensively, and relevant policies in various regions have gradually been refined. Among them, some implementation plans have made detailed regulations on matters such as the introduction and cultivation of metaverse industries.

As we move toward that ultimate goal, what "possibles" will come first? At least at the moment, there are a thousand metaverses in the minds of a thousand people. The metaverse may become a new form of human society development, which will promote the connection and integration of the real world and the virtual world, and fundamentally change people's way of life. This article first outlines the background of the birth of the metaverse, the development process, the concept and connotation of the metaverse, and tries to make the readers understand the metaverse as soon as possible. Then, from a sociological perspective, study metaverse security, crime risk, and the need for forensics. Finally, three aspects of metaverse forensics are discussed from the technical point of view, and the specific experimental process is given. At present, the explosion of the concept of "metaverse", its development speed, final form, and even its impact on philosophy, culture, society and social governance, and human beings are still unknown. In short, no matter what trend we are in, we must have a clear understanding, make rational decisions, and steadily explore the metaverse!

Acknowledgement: Special thanks to colleagues and classmates from the Network Security Department of Jiangsu Police Officer Institute for their support.

Funding Statement: The work is supported by 2021 Jiangsu Police Institute Scientific Research Project (2021SJYZK01), High-Level Introduction of Talent Scientific Research Start-Up Fund of Jiangsu Police Institute (JSPI19GKZL407), Jiangsu Provincial Department of Public Security Science and Technology Project (2021KX012), Open Project of Criminal Inspection Laboratory in Key Laboratories of Sichuan Provincial Universities (2023YB03), Major Project of Basic Science (Natural Science) Research in Higher Education Institutions in Jiangsu Province (2020232001), 2023 'Jiangsu Science and Technology Think Tank Youth Talent Plan'.

Author Contributions: Jianfang Xin and Guangjun Liang conceived and designed the experiments; Qun Wang and Xueli Ni performed the experiments; Xiangmin Guo and Pu Chen analyzed the data; Guangjun Liang wrote the paper. All authors have read and agreed to the published version of the manuscript.

Availability of Data and Materials: Please contact us via email for relevant experimental data and materials.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. D. N. Dionisio 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.

[2] F. Y. Wang, R. Qin and X. Wang, "Metasocieties in metaverse: Metaeconomics and metamanagement for metaenterprises and metacities," *IEEE Transactions on Computational Social Systems*, vol. 9, no. 1, pp. 2–7, 2022.

[3] S. M. Chacko and V. Kapila, "Augmented reality as a medium for human-robot collaborative tasks," in *Proc. of the 28th IEEE Int. Conf. on Robot and Human Interactive Communication (RO-MAN)*, New Delhi, India, pp. 1–8, 2019.

[4] M. Dianatfar, J. Latokartano and M. Lanz, "Review on existing VR/AR solutions in human-robot collaboration," *Procedia CIRP*, vol. 97, no. 1, pp. 407–411, 2021.

[5] J. J. LaViola, E. Kruijff, R. P. McMahan, D. Bowman and I. P. Poupyrev, "3D user interfaces: Theory and practice," in *Presence Teleoperators & Virtual Environments*, 1st ed., London, Addison-Wesley Professional, pp. 23–28, 2017.
[6] J. S. Pierce, B. C. Stearns and R. Pausch, "Voodoo dolls: Seamless interaction at multiple scales in virtual environments," in *Proc. of the 1999 Symp. on Interactive 3D Graphics*, Atlanta, USA, pp. 141–145, 1999.
[7] Q. Yang, Y. Zhao and H. Huang, "Fusing blockchain and AI with metaverse: A survey," *IEEE Open Journal of the Computer Society*, vol. 3, no. 1, pp. 122–136, 2022.
[8] H. Jeon, H. Youn and S. Ko, "Blockchain and AI meet in the metaverse," in *Advances in the Convergence of Blockchain and Artificial Intelligence*, 1st ed., London, Intech Open Book Series, pp. 73–78, 2022.
[9] U. Majeed, L. U. Khan and I. Yaqoob, "Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges," *Journal of Network and Computer Applications*, vol. 181, no. 1, pp. 1–10, 2021.
[10] A. Dorri, F. Luo and S. Karumba, "Temporary immutability: A removable blockchain solution for prosumer-side energy trading," *Journal of Network and Computer Applications*, vol. 180, no. 1, pp. 1–9, 2021.
[11] P. Kumar, R. Kumar and G. Srivastava, "PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2326–2341, 2021.
[12] D. C. Nguyen, P. Cheng and M. Ding, "Enabling AI in future wireless networks: A data life cycle perspective," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 553–595, 2020.
[13] T. Huynh, Q. V. Pham and X. Q. Pham, "Artificial intelligence for the metaverse: A survey," *Engineering Applications of Artificial Intelligence*, vol. 117, no. 1, pp. 1–10, 2023.
[14] S. M. Park and Y. G. Kim, "A metaverse: Taxonomy, components, applications, and open challenges," *IEEE Access*, vol. 2022, no. 10, pp. 4209–4251, 2022.
[15] M. Xu, W. C. Ng and W. Y. B. Lim, "A full dive into realizing the edge-enabled metaverse: Visions, enabling technologies, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 656–700, 2022.
[16] R. Montasari, "Countering Cyberterrorism: The confluence of artificial intelligence, cyber forensics and digital policing in US and UK national cybersecurity," in *Advances in Information Security*, 1st ed., London, Springer Nature, pp. 27–51, 2023.
[17] C. Fran, K. D. Thomas, P. S. Georgios, A. Marios, G. Amrita *et al.,* "Research trends, challenges, and emerging topics in digital forensics: A review of reviews," *IEEE Access*, vol. 10, no. 2, pp. 25464–25493, 2022.
[18] Y. Akbari, S. Al-maadeed, O. Elharrouss, F. Khelifi, A. Lawgaly *et al.,* "Digital forensic analysis for source video identification: A survey," *Forensic Science International: Digital Investigation*, vol. 41, no. 6, pp. 301390–301399, 2022.
[19] M. Kim, Y. Shin, W. Jo and T. Shon, "Digital forensic analysis of intelligent and smart IoT devices," *The Journal of Supercomputing*, vol. 79, no. 1, pp. 973–997, 2023.
[20] J. Oh, S. Lee and H. Hwang, "Forensic recovery of file system metadata for digital forensic investigation," *IEEE Access*, vol. 10, no. 10, pp. 111591–111606, 2022.
[21] M. Mijwil, R. Doshi, K. K. Hiran, A. H. Al-Mistarehi and M. Gök, "Cybersecurity challenges in smart cities: An overview and future prospects," *Mesopotamian Journal of Cybersecurity*, vol. 2022, no. 1, pp. 1–4, 2022.
[22] A. A. Khan, A. A. Shaikh, A. A. Laghari, M. A. Dootio, M. M. Rind *et al.,* "Digital forensics and cyber forensics investigation: Security challenges, limitations, open issues, and future direction," *International Journal of Electronic Security and Digital Forensics*, vol. 14, no. 2, pp. 124–150, 2022.
[23] J. P. A. Yaacoub, H. N. Noura, O. Salman and A. Chehab, "Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations," *Internet of Things*, vol. 19, no. 8, pp. 100544–100550, 2022.
[24] D. Gragnaniello, C. T. Li, F. Marra and D. Riccio, "Virtual special issue on advances in digital security: Biometrics and forensics," *Pattern Recognition Letters*, vol. 159, no. 7, pp. 220–221, 2022.

[25] T. Li, H. Wang, D. He and J. Yu, "Synchronized provable data possession based on blockchain for digital twin," *IEEE Transactions on Information Forensics and Security*, vol. 17, no. 1, pp. 472–485, 2022.
[26] A. S. Abiodun and A. B. Maria, "Digital forensics AI: Evaluating, standardizing and optimizing digital evidence mining techniques," *KI-Künstliche Intelligenz*, vol. 36, no. 2, pp. 143–161, 2022.
[27] S. G. Weinbaum, "Pygmalion's spectacles," in *Classic Science Fiction*, 1st ed., London, Simon and Schuster, pp. 1–11, 2016.
[28] C. Comeau, "Headsight television system provides remote surveillance," *Electronics*, vol. 1961, no. 1, pp. 86–91, 1961.
[29] I. E. Sutherland, "A head-mounted three dimensional display," in *Fall Joint Computer Conf.*, Boston, USA, pp. 757–764, 1968.
[30] M. W. Krueger, T. Gionfriddo and K. Hinrichsen, "VIDEOPLACE-an artificial reality," in *Proc. of the SIGCHI Conf. on Human Factors in Computing Systems*, New York, USA, pp. 35–40, 1985.
[31] T. A. Furness, "The super cockpit and its human factors challenges," in *Proc. of the Human Factors Society Annual Meeting*, Los Angeles, USA, pp. 48–52, 1986.
[32] J. Lanier, "Virtual reality: The promise of the future," *Interactive Learning International*, vol. 8, no. 4, pp. 275–79, 1992.
[33] C. Y. Liao, S. K. Tai and R. C. Chen, "Using EEG and deep learning to predict motion sickness under wearing a virtual reality device," *IEEE Access*, vol. 2020, no. 8, pp. 126784–126796, 2020.
[34] C. Cruz-Neira, D. J. Sandin and T. A. DeFanti, "The CAVE: Audio visual experience automatic virtual environment," *Communications of the ACM*, vol. 35, no. 6, pp. 64–73, 1992.
[35] S. Boyer, "A virtual failure: Evaluating the success of Nintendo's virtual boy," *The Velvet Light Trap*, vol. 2009, no. 64, pp. 23–33, 2009.
[36] B. O. Rothbaum, L. Hodges and R. Alarcon, "Virtual reality exposure therapy for PTSD Vietnam veterans: A case study," *Journal of Traumatic Stress*, vol. 12, no. 2, pp. 263–271, 1999.
[37] F. Xu and W. Chu, "Sports dance movement assessment method using augment reality and mobile edge computing," *Mobile Information Systems*, vol. 2021, no. 1, pp. 1–8, 2021.
[38] N. K. K. Akhunova, "Possibilities of using virtual reality technologies in education," *Asian Journal of Multidimensional Research (AJMR)*, vol. 10, no. 3, pp. 549–555, 2021.
[39] S. Shitharth, "Enhanced optimization based algorithm for intrusion detection in SCADA network," *Computers & Security*, vol. 70, no. 9, pp. 16–26, 2017.
[40] F. Sattari, A. H. Farooqi, Z. Qadir, B. Raza, H. Nazari *et al.,* "A hybrid deep learning approach for bottleneck detection in IoT," *IEEE Access*, vol. 10, no. 7, pp. 77039–77053, 2022.
[41] H. Qin, Y. Wang and P. Hui, "Identity, crimes, and law enforcement in the metaverse," arXiv preprint arXiv:2210.06134, 2022.
[42] P. Maharg and M. Owen, "Simulations, learning and the metaverse: Changing cultures in legal education," *Journal of Information, Law, Technology*, vol. 2007, no. 1, pp. 1–28, 2007.
[43] N. Narang, "Mentor's musings on role of standards, regulations & policies in navigating through metaverse and its future avatars," *IEEE Internet Things Magazine*, vol. 6, no. 1, pp. 4–11, 2023.
[44] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu *et al.,* "A survey on metaverse: Fundamentals, security, and privacy," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 319–352, 2023.
[45] Z. Chen, J. Wu and W. Gan, "Metaverse security and privacy: An overview," *Big Data*, vol. 2022, no. 1, pp. 2950–2959, 2022.
[46] R. Zhao, Y. Zhang, Y. Zhu, R. Lan and Z. Hua, "Metaverse: Security and privacy concerns," arXiv preprint arXiv:2203.03854, 2022.
[47] R. Pietro and S. Cresci, "Metaverse: Security and privacy issues," arXiv preprint arXiv:2205.07590, 2022.
[48] J. Sun, W. Gan, H. Chao and P. Yu, "Metaverse: Survey, applications, security, and opportunities," arXiv preprint arXiv:2210.07990, 2022.
[49] M. Ali, F. Naeem, G. Kaddoum and E. Hossain, "Metaverse communications, networking, security, and applications: Research issues, state-of-the-art, and future directions," arXiv preprint arXiv:2212.13993, 2022.

[50] S. Ali, T. Armand and A. Athar, "Metaverse in healthcare integrated with explainable AI and blockchain: Enabling immersiveness, ensuring trust, and providing patient data security," *Sensors*, vol. 23, no. 2, pp. 565–577, 2023.
[51] R. Cheng, S. Chen and B. Han, "Towards zero-trust security for the metaverse," arXiv preprint arXiv:2302.08885, 2023.
[52] S. Far and A. Rad, "Applying digital twins in metaverse: User interface, security and privacy challenges," arXiv preprint arXiv:2204.11343, 2022.
[53] P. Kürtünlüoglu, B. Akdik and E. Karaarslan, "Security of virtual reality authentication methods in metaverse: An overview," arXiv preprint arXiv:2209.06447, 2022.
[54] J. Barbara and M. Haahr, "Identification and IDNs in the metaverse: Who would we like to be?" in *Proc. of the ICIDS 2022*, Santa Cruz, USA, pp. 601–615, 2022.
[55] X. Zhang, J. Wang, N. Cheng and J. Xiao, "Singer identification for metaverse with timbral and middle-level perceptual features," in *Proc. of the IJCNN 2022*, Padua, Italy, pp. 1–7, 2022.
[56] X. Zhang, J. Wang, N. Cheng and J. Xiao, "MetaSID: Singer identification with domain adaptation for metaverse," in *Proc. of the IJCNN 2022*, Padua, Italy, pp. 1–7, 2022.
[57] X. Zhang, J. Wang, N. Cheng and J. Xiao, "Tdass: Target domain adaptation speech synthesis framework for multi-speaker low-resource," in *Proc. of the IJCNN 2022*, Shanghai, China, pp. 1–6, 2022.
[58] X. Zhang, J. Wang, N. Cheng and J. Xiao, "MetaSID: Singer identification with domain adaptation for metaverse," arXiv preprint arXiv:2205.11821, 2022.
[59] Y. Hwang, "When makers meet the metaverse: Effects of creating NFT metaverse exhibition in maker education," *Compuer Education*, vol. 2023, no. 194, pp. 104693–104703, 2023.
[60] C. Wang, C. Yu and Y. Zhang, "Attention economy in metaverse: An NFT value perspective," in *Proc. of the MMSP 2022*, Shanghai, China, pp. 1–6, 2022.
[61] M. Yilmaz, T. Hacaloglu and P. Clarke, "Examining the use of non-fungible tokens (NFTs) as a trading mechanism for the metaverse," in *Proc. of the EuroSPI 2022*, Salzburg, Austria, pp. 18–28, 2022.
[62] A. Wang, Z. Gao, L. Lee, T. Braud and P. Hui, "Decentralized, not dehumanized in the metaverse: Bringing utility to NFTs through multimodal interaction," in *Proc. of the ICMI 2022*, Bengaluru, India, pp. 662–667, 2022.
[63] R. Chengoden, "Metaverse for healthcare: A survey on potential applications, challenges and future directions," *IEEE Access*, vol. 11, no. 1, pp. 12765–12795, 2023.
[64] B. Wiederhold, "Healthcare consumerism in the metaverse: Is there a benefit?" *Cyberpsychology, Behavior, and Social Networking*, vol. 26, no. 3, pp. 145–146, 2023.
[65] T. Zhang, J. Shen, C. Lai, S. Ji and Y. Ren, "Multi-server assisted data sharing supporting secure deduplication for metaverse healthcare systems," *Future General Computer System*, vol. 140, no. 1, pp. 299–310, 2023.
[66] E. Mohamed, T. Naqishbandi and G. Veronese, "Metaverse!: Possible potential opportunities and trends in e-healthcare and education," *International Journal of E-Adoption*, vol. 15, no. 2, pp. 1–21, 2023.
[67] A. Musamih, I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi *et al.,* "Metaverse in healthcare: Applications, challenges, and future directions," *IEEE Consumer Electronics Magazine*, vol. 12, no. 4, pp. 33–46, 2023.
[68] D. Shin, "The actualization of meta affordances: Conceptualizing affordance actualization in the metaverse games," *Computers in Human Behavior*, vol. 133, no. 1, pp. 107292–107299, 2022.
[69] Y. Ren, R. Xie, F. Yu, T. Huang and Y. Liu, "Quantum collective learning and many-to-many matching game in the metaverse for connected and autonomous vehicles," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 11, pp. 12128–12139, 2022.
[70] P. Babaei, R. Robinson, R. Mandryk, J. Pirker and C. Kang, "Games and the metaverse," in *CHI PLAY'22: Extended Abstracts of the 2022 Annual Symp. on Computer-Human Interaction in Play*, vol. 2022, no. 1, pp. 318–319, 2022.

[71] J. Xu, "From augmented reality location-based games to the real-world metaverse," in *CHI PLAY'22: Extended Abstracts of the 2022 Annual Symp. on Computer-Human Interaction in Play*, vol. 2022, no. 1, pp. 364–366, 2022.
[72] B. Wiederhold, "Metaverse games: Game changer for healthcare?" *Cyberpsychology, Behavior, and Social Networking*, vol. 25, no. 5, pp. 267–269, 2022.
[73] T. The, T. Gadekallu, W. Wang, G. Yenduri, P. Ranaweera *et al.,* "Blockchain for the metaverse: A review," *Future General Computer System*, vol. 143, no. 1, pp. 401–419, 2023.
[74] Y. Fu, C. Li, F. Yu, T. Luan, P. Zhao *et al.,* "A survey of blockchain and intelligent networking for the metaverse," *IEEE Internet Things Journal*, vol. 10, no. 4, pp. 3587–3610, 2023.
[75] H. Huang, X. Zeng, L. Zhao, C. Qiu, H. Wu *et al.,* "Fusion of building information modeling and blockchain for metaverse: A survey," *IEEE Open Journal Computer Social*, vol. 3, no. 1, pp. 195–207, 2022.
[76] P. Nath, J. R. Mushahary, U. Roy, M. Brahma and P. K. Singh, "AI and Blockchain-based source code vulnerability detection and prevention system for multiparty software development," *Computers and Electrical Engineering*, vol. 106, no. 3, pp. 108607–108617, 2023.
[77] O. Bouachir, M. Aloqaily, F. Karray and A. Saddik, "AI-based blockchain for the metaverse: Approaches and challenges," in *Proc. of the BCCA 2022*, San Antonio, TX, USA, pp. 231–236, 2022.
[78] J. Kang, D. Ye, J. Nie, J. Xiao, X. Deng *et al.,* "Blockchain-based federated learning for industrial metaverses: Incentive scheme with optimal AoI," *Blockchain*, vol. 2022, no. 1, pp. 71–78, 2022.
[79] V. Ahsani, A. Rahimi, M. Letafati and B. Khalaj, "Unlocking metaverse-as-a-service the three pillars to watch: Privacy and security, edge computing, and blockchain," arXiv preprint arXiv:2301.01221, 2023.
[80] Y. Lin, H. Du, D. Niyato, J. Nie, J. Zhang *et al.,* "Blockchain-aided secure semantic communication for AI-generated content in metaverse," arXiv preprint arXiv:2301.11289, 2023.
[81] S. Rostami and M. Maier, "The metaverse and beyond: Implementing advanced multiverse realms with smart wearables," *IEEE Access*, vol. 10, no. 1, pp. 110796–110806, 2022.