Security and Safety, Vol. 2, 2023009 (2023)
https://doi.org/10.1051/sands/2023009
sands.edpsciences.org

Security and Safety in the "Metaverse"

Review

Open Access

Social Governance

A review of the application of digital identity in the Metaverse

Siwen Wang[1,*] and Wei Wang[2,*]

[1] *School of Journalism and Communication, Communication University of Zhejiang, Hangzhou 310018, China*
[2] *School of Art and Design, Nanjing University of Finance and Economics, Nanjing 210000, China*

Received: 8 November 2022 / Revised: 20 March 2023 / Accepted: 30 April 2023 / Published online: 10 July 2023

Abstract The development of the internet has immensely expanded people's social scope, which has necessitated the utilization of digital identity. In regard to social networks, the utilization of anonymity or pseudonyms increases the attractiveness of the network. Nevertheless, because online payments, online transactions, and online assets are becoming prevalent features, virtualization is gradually exhibiting highly negative impacts. With respect to the Metaverse, digital identity is potentially a key factor, which can influence the balance that affects the association between anonymity and pseudonyms. To enhance the contemporary scenario and to facilitate the potential utilization of digital identity, this study considers the application of digital identity in the Metaverse, and it utilizes the "Enterprise IA" miniature model (Morey *et al.*). With regard to the current debate on digital identity, we analyzed the most prominent topic; thus, we explored the application rules pertaining to digital identity. We propose that the Metaverse is primarily characterized by its ability to digitalize the physical world. Furthermore, with respect to digital identity, the power of ownership still represents the fundamental issue. Using technologies such as blockchain and privacy filters, we can not only alter the governance logic and methods, but we can also balance the correlation between private rights and public interests. Thus, to solve the burgeoning identity trust crisis, individual competition for identity authorization rights, and privacy problems that characterize the Metaverse, we explore novel governance approaches.

Keywords Metaverse, Digital Identity, Rights, Security, Privacy

Citation Wang SW and Wang W. A review of the application of digital identity in the Metaverse. Security and Safety 2023; **2**: 2023009. https://doi.org/10.1051/sands/2023009

1 Introduction

Digital identity refers to a digital signature that can verify the identity of an individual, and it is applied to a scenario in which two or more parties exchange data via the Internet [1]. Digital identity includes all the information or data pertaining to an individual, and it entails all the data traces pertaining to individuals who utilize the internet. For individuals to enter the virtual space and participate in internet-based activities, digital identity is the most fundamental element. Nonetheless, the global understanding and management that characterizes digital identity are still mixed. Most citizens want to express themselves freely in the virtual space; however, the tendency of economic and political supervision is becoming increasingly apparent, and the phenomenon of fraudulently obtaining an individual's information and leaking it to the service provider or a non-material party is also becoming increasingly rampant [2]. Based on the statistics of Verizon (*i.e.*, an American network operator) 63% of network intrusions are associated

* Corresponding authors (email: zhechuanwsw@163.com (Siwen Wang); wangweicaida@163.com (Wei Wang))

with user password leakage [3]. Therefore, the establishment of a secure digital identity identification system, which can protect internet users and national network security, has become a pertinent issue. In regard to the user's perspective, this study not only analyzed the history and practical experience that is associated with the development of digital identity, but it also reviewed the policy supervision perspective, which entailed exploring the paths and problems pertaining to the migration of digital identity applications from the internet to the Metaverse.

2 Identity: from the traditional society to the Metaverse

2.1 Face-to-face certificate identification

In regard to traditional society, interpersonal communication is spatially restricted; thus, in most scenarios, individuals have to be physically present. Individuals are highly dependent on their feelings and memories, which enable them to identify others, interact with them, or participate in various activities. The associations among people are often closed and fixed. Once a stranger appears in a relatively stable community, people who have formed groups will unite; thus, they will verify the stranger's identity and other characteristics, which entails the utilization of various methods. Even if the stranger is introduced by acquaintances, they will inevitably be assessed and tested by other members.

During this stage, people's feelings and memories are quite strong; this characteristic enables them to interact with others in a more rigid way, and on limited occasions, and it offers limited identity information to diverse communication objects. This identity information is relatively private, and it exists in a relatively fixed community.

2.2 Paper certificate identification

The papermaking that characterized the 13th century, and the popularity of the Gutenberg printing press, which characterized the 15th century, prompted individuals to utilize documents as a memory aid. Thus, individuals became progressively dependent on notes, which facilitated the development of paper identity records.

Due to the popularity of paper, the limitation pertaining to the physical space has been transcended; thus, long-distance communication has been enhanced, and people's behavior as well as their perception have been considerably affected. Because people have gradually observed that written records are highly accurate and convenient, it is generally accepted that written records are more authoritative than memory-based records. Nevertheless, only when all stakeholders acknowledge the effectiveness of paper identity, can it be realized. The paper identification certificate includes individual rights and responsibilities. Due to the development of paper agreements, people can reduce risks, which are influenced by the gradual development of transportation tools and by the gradual expansion of the physical human interaction space.

The paper identity certificate entails the description of the observable attributes and facts pertaining to the identity subject. Owing to the augmentation of paper vouchers, authorities began registering, collecting, and categorizing personal information based on specific rules; thus, they stored information for future retrieval. Consequently, the national government has become the authorizer, verifier, and custodian of all information and data, including the individual's identity information. The paper voucher has replaced the traditional human memory; therefore, with respect to identity information, memory is no longer a crucial method.

2.3 Digital identity certificate

The impact that digital technology exerts on identity is twofold. First, digital technology has led to the emergence of a novel method for expressing and sharing identity information; second, digital technology ameliorates the security and credibility of identity authentication. With regard to the internet–Metaverse transition, the development of digital identity can be divided into two stages: the first stage entails the transformation of the real identity, whereas the second stage entails the gradual separation from reality. The first stage predominantly characterizes the internet society, and the second stage, which entails the

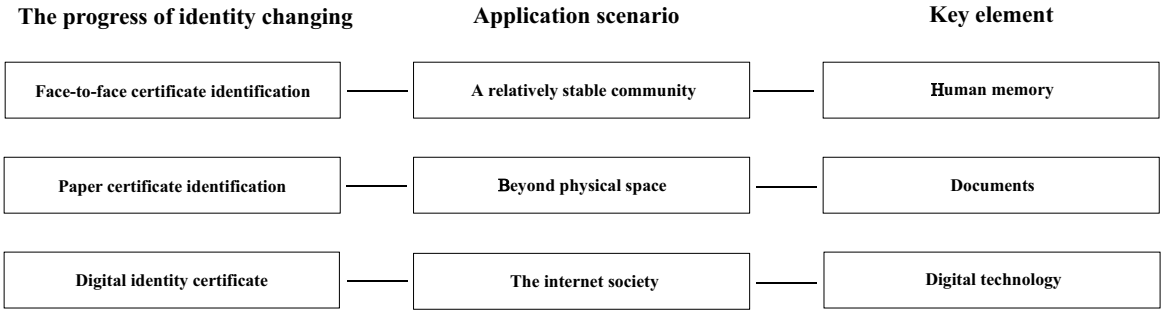

Figure 1. Flow chart of digital identity Development.

developed internet and the Metaverse, is characterized by the advent of the digital double technology (*i.e.*, avatar). In regard to the second stage, internet users possess immense choices. They can define their prospective roles. However, regardless of the role they assume, some of the traits that they exhibit are correlated with the physical reality in which they exist.

The three-stage of identity change is not linear and replaceable relationship. It is an overlapping and interwoven relationship. As shown in Figure 1.

2.3.1 Real-world–internet world identity transformation

With respect to the creation of accounts, payment of bills, banking services, and novel internet-based technologies, to prevent that characterize online transactions, users should verify their identity. Nevertheless, even in cyberspace, identity verification is still predominantly traditional. Identity verification entails the utilization of paper vouchers, which are prone to the disclosure of personal information; criminals are likely to forge this information, and the certificate that is issued by the certification authority exhibits timeliness, which may lead to personal economic losses [4].

Paper vouchers were gradually replaced by virtual cards. For users to enter virtual websites, the ID and password became the novel credentials. To authorize their identities, users primarily relied on platforms such as Google or Facebook. Nevertheless, because passwords are prone to hacking, the aforementioned method is not completely dependable [5]. To overcome these shortcomings, and to conduct secure internet-based transactions, websites began to design authentication methods that can combine the traces that individuals leave on the network into an independent digital identity. This identity is stored in the blockchain or in other distributed ledger technologies that can are robust against hacker endeavors (*e.g.*, phishing attacks). Blockchains represent a method of decentralized recordkeeping, which is popularized by cryptocurrency [6]. The distributed ledger technology (DLT) is a peer-to-peer virtual network that comprises a series of contracts, which define the rights and responsibilities of participants. These contracts facilitate peer-to-peer transformation, and they promote the synchronization and decision-making process pertaining to information without central control or third-party authorization. The distributed ledger technology does not compel users to reveal their entire identity, which enables them to independently choose the content that they require. This identity is known as a verifiable credential. However, these vouchers exhibit all the information that paper vouchers possess. Due to the design of a digital signature, the certificate is robust against forgery; therefore, the digital signature is considered to be more dependable than a physical certificate. However, the aforementioned tools all exhibit considerable shortages. For example, they still exhibit high-level energy consumption and a low-level capacity ceiling of only a few transactions per second [7]. The verifiable certificate does not affect user utility; because the certificate comprises digital and encrypted data, users can utilize it to verify their identity on the internet.

Besides the technical enhancement of the system, network users are also exploring the "self-protection pathway". Although the desire of the citizens to utilize the internet has not stopped on account of the potential leakage of personal information (*i.e.*, privacy concerns), citizens still distrust the internet. Therefore, when the users communicate, they will retain their true thoughts, and they will assume identities that can enable them to establish digital connections with others on the internet in an ambiguous and controlled manner. With respect to the internet, new entrants are constantly exploring novel methods of managing their image, such as the utilization of pseudonyms, setting avatars, sending facial expression

packets, and applying the digital double technology, which entails the separation of the real identity from the digital identity.

2.4 The digital identity–real identity separation

The advent of digital double technology has transformed the method through which real individuals utilize the internet, which has prompted individuals to rethink how they should enter the virtual world. Due to the apparent lack of restrictions that the digital double exhibits, to enhance this technology, different companies have developed dissimilar designs. Meta is attempting to design an image that immensely resembles the real individual, and because it aims to realize the virtual representation of the real world, it has equipped this image with clothing. However, some individuals think that researchers should encourage individuals to assume more roles. The digital double design should immensely consider anonymity and diversity pertaining to the virtual world; thus, the limitations of the real world, such as physical characteristics, gender, and socio-economic conditions can be overcome. With respect to the Metaverse, every designed digital double form requires a two-dimensional or three-dimensional image.

Based on the current application, the digital double technology exhibits five characteristics: first, it can enable individuals to truthfully express their feelings, and it can enable them to alter their emotions or opinions to match their roles; Second, individuals who exhibit physical disabilities can express themselves without restriction, which facilitates the mobility of the social strata; third, the digital double technology is open and diverse, and individuals can choose to experience the feelings pertaining to dissimilar nationalities, genders, and species; fourth, by providing an interactive design, the technology overcomes the restriction pertaining to the capabilities of humanlike avatars, which entail talking, dancing, and playing games; fifth, to create more experience-rich environments, designers are constantly building virtual scenes, which entails innovating virtual stories as well as visual arts and entertainment. It is worth noting that no matter the extent to which the digital double innovates, the existence of an associated intermediary between the digital double and the real individual (*i.e.*, the digital identity) is imperative.

The aforementioned discussions indicate that with respect to individuals, the pursuit of self-expression does entail the complete exposure of their identities. A digital double is just a projection of an individual's identity; it can break the stratum solidification pertaining to the real world, and it can enable the individual's real body to achieve transcendence. Simultaneously, due to the augmentation of virtual scenes, the gap between the digital double and real individuals is also expanding. For instance, Sonia Livingstone observed that to establish contact with other individuals (*e.g.*, to cheat) on youth dating websites and dating websites, and to attract them, teenagers will attempt to express diverse attitudes and to create their own digital identity, which is highly divergent from the needs of real individuals [8]. Therefore, the psychological, social, and political motivations for individuals to create digital identities are tremendously complex, and modern research should immensely consider the methods through which individuals build digital identities.

3 Application of digital identity in Metaverse

With respect to the management perspective, Morley *et al.* established a micro framework named "Five A's of Enterprise IAM" in accordance with the internet-based application of digital identity. The framework includes five crucial nodes, namely authentication, authorization, management, audit, and digital identity analytics [9], and these five nodes form a simple closed loop, which facilitates the application of the digital identity pertaining to the Metaverse. This study, which is based on the "Enterprise IAM" framework, categorizes these five nodes, and it proposes that the operation of individuals and that of enterprises are relatively similar at the authentication and authorization level; however, the management, audit, and analysis processes consider only the issues pertaining to digital identity governance, and individuals are not aware of the underlying logic. The application subjects of these three nodes principally represent the backend code writers and managers. Because the current study is limited to users' perspectives, we highly consider authentication and authorization, and we combine management with audit and analytics.

3.1 Authentication: Metaverse's "ticket"

Authentication refers to the utilization of a login name (*i.e.*, user name) and some form of private data (*i.e.*, usually a password); thus, the platform can verify or trust the identity resume. The essence of authentication is to verify that the private data that is claimed by an individual (*i.e.*, normally referred to as a password) is an identity resume proof or trust [9]. The fundamental program adds a shared key or password to the login name. For an individual to enter the virtual world, the first step entails identity authentication. Currently, there are two methods of authenticating users. The first method entails depending on virtual identity providers such as Google or Facebook to enable users to create a digital identity, which represents an integral expression between individuals and digital identity; with respect to the second, it is inferred that individuals create digital doubles in the virtual world to enable them complete virtual world activities. Digital identity is the intermediary between these two methods. The substantial difference between these two access methods is correlated with the digital identity control subject. The common following factor characterizes both methods: with regard to logging in, both methods necessitate the utilization of shared keys, such as PIN code, password, key, and dual-factor authentication.

The advent of digital double increases the complexity pertaining to the correlation between digital identity and real individuals. Digital double provides real individuals with greater autonomy and an increased expression space; however, in regard to the intermediary between real individuals and digital doubles, digital identity is still a necessity. In accordance with the preference of individuals, the association between individuals and digital doubles can be divided into three categories. The first category entails the association between temporary substitution and permanent substitution; the second states that the correlation between digital identity and real individuals is wholly independent; and the third entails the projection of digital doubles or individual ideals to compensate for the things that individuals cannot accomplish in the real world [10]. Irrespective of the correlation between real individuals and digital doubles, real individuals are required to feed the digital doubles with data, project their emotions, and process and analyze proprietary algorithms.

3.2 Authorization: the power struggle that characterizes the Metaverse

When individuals enter the network society, the next step of identity authentication is an authorization. Authentication allows individuals to perform a function, obtain permission, or fulfill certain tasks pertaining to a specific role in the system. When people log into the application or operating system, no login name or password is required. The system will regard the individual as a "visitor", and to obtain permission, another individual must ascertain their identity. This other individual may be a visitor, or they may be the VIP. Consequently, authorization is a method of granting individuals the right to implement a certain function based on authentication information; through authorization, an individual's identity and its associated account can obtain the permission through which some functions of the system can be implemented, whereas unauthorized functions cannot be executed.

Who has the power to authorize? Once the grantor of this power is confused, the existence of various digital doubles may lead to the dispersion of a singular real individual account. The "collision" between dissimilar individuals, including other problems, leads to management confusion. The following core value characterizes the Metaverse's "decentralization": more autonomy for individuals. Thus, the management modes that necessitate granting a unified identity are overcome. Digital identity has become not only an intermediary through which real individuals can enter the virtual world, but it has also become a crucial factor for the decentralization concept that characterizes the Metaverse. Nonetheless, the role of digital identity predominantly entails balancing the correlation between individual rights and interests as well as the regulatory power of managers. With regard to individual rights and interests, digital identity contains immense data, which constitutes user privacy, and it is mixed with personal interests; from the perspective of code writers or managers, providing limited rights to entrants constitutes virtual space management, and it is a crucial method of maintaining the benign operation of the virtual space.

3.3 Management: a necessary means for the sound operation of the Metaverse

There are three methods of management, which are characterized by apparent differences. Users tend to experience and observe these management methods only superficially.

Management, in a broad sense, refers to the configuration and governance control that characterize changes in authentication, authorization, and auditing. However, the authentication and authorization mechanism is decentralized, diversified, and dynamic. The narrow management perspective excludes the technical combination of authentication and authorization. Through professional technology and the identity governance process, it provides users and visitors with visibility, control, automation, and full lifecycle management services; thus, the benign operation of the Metaverse is achieved.

In regard to the internet, the problems pertaining to digital identity primarily consider the management level. The development of digital identity entails ensuring the legitimacy of network behavior. Consequently, with respect to the traditional internet environment or the future Metaverse environment, the behavior of the digitally identified virtual space subject is still shared by the initiator, creator, and controller. The characteristics pertaining to logic represent the close connection between the real world and the centralized management modes; however, these characteristics contradict Metaverse's "decentralized" value concept and "individual free choice".

3.4 Auditing: security review of digital identity

The audit process partly constitutes the digital identity management process. With regard to user access, to achieve repeatability and sustainability, the system controls the compliance of the identity-holding entity. With regard to dissimilar individuals, the dominant function pertaining to auditing is also diverse; in regard to individuals, the audit process provides a user access verification program; and with regard to the backend coders, auditing defines and implements prevention and detection strategies.

Some scholars propose that because the "Metaverse expands the temporal and spatial attributes, it promotes the holistic development of individuals, and demonstrating the life value as well as practical individuals is a crucial concern" [11]. Nevertheless, before the association between digital identity and real individuals is clarified, the developmental degree pertaining to individual "self-worth", which characterizes the Metaverse, remains to be observed. The source of this problem entails the size of the power that the real individual possesses; herein, the power chiefly refers to the individual's control over digital identity.

Some scholars propose that the Metaverse should be guaranteed by the decentralized and equitable rights-sharing mechanism and by the co-governance mechanism; thus, real individuals, digital doubles, and the real individual–digital double bonds become the internal causative factor that facilitates the Metaverse's continuous expansion. This proposition exhibits some rational robustness. When the various activities that constitute digital identity can be passively converted into machine-readable data, when the power of platform service providers is not effectively limited, and when the code writers are connected with commercial interests, the authorization of digital identity may become the main consideration of various interest groups.

Moreover, the danger pertaining to identity theft and other issues such as digital identity system security are also frequently emerging. Digital identity offers the subject a strong sense of dissociation. The solution to the security problem pertaining to digital identity depends on the security technology through which individuals employ digital identity to enter Metaverse. Although digital supervision violates Metaverse's so-called "punk" spirit, and although it is not thoroughly consistent with Metaverse's core value (*i.e.*, decentralization), centralized supervision is the most effective method of ensuring the sound operation of the Metaverse. To audit digital identity, countries have begun to adopt a variety of methods. For instance, in 2020, the European Commission proposed a secure European electronic identification scheme. The program aims to assist citizens to participate in various activities within Europe, ranging from paying taxes to renting bicycles. The EU intends to control the utilization of personal data and technology through digital identity.

3.5 Analysis: a retrospective summary of the digital identity application

Due to the development of machine learning and artificial intelligence technology, the traditional engine has immensely lagged behind artificial intelligence and other technologies, especially with regard to discovering and processing massive operational data. Simultaneously, for the Metaverse to operate optimally, obtaining concealed information and operable guidance is a prerequisite.

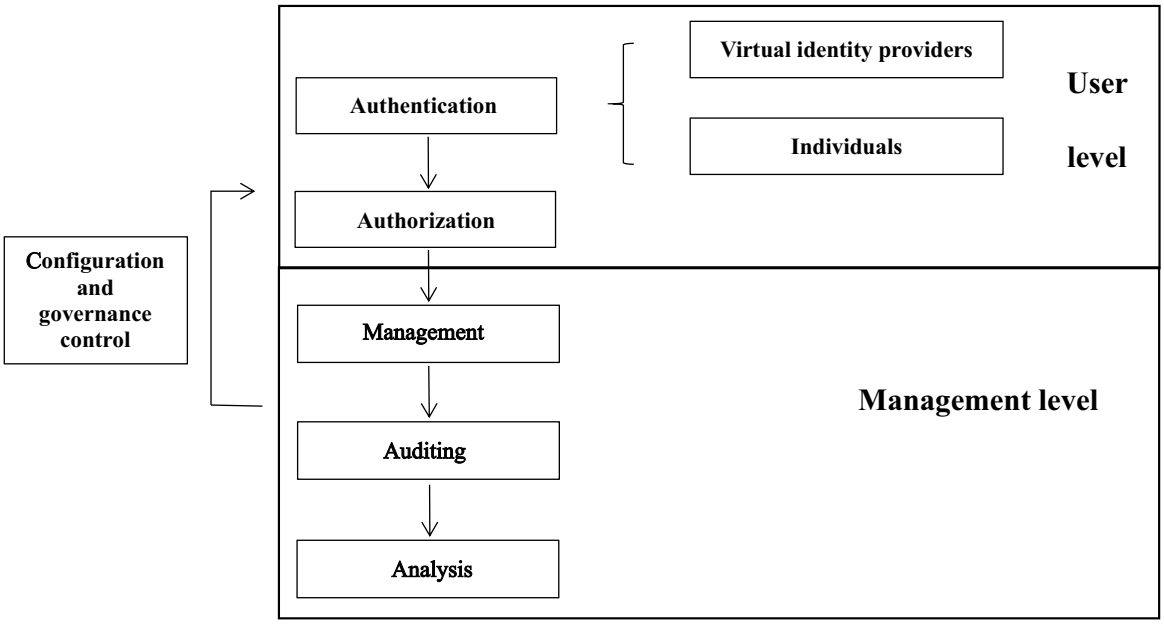

Figure 2. Application of digital identity in Metaverse.

To continuously collect and process identity-related configuration, allocation, and usage data, and to summarize all the operation digital identity processes entering the Metaverse, an analysis is performed; thus, the ability of the background to utilize data and offer users high-quality experience is ameliorated.

In regard to regulators, a comprehensive analysis of the operation of digital identity in the system is conducive; thus, with respect to the latter stage, more dependable and predictable identity governance can be affected. This data facilitates the extension of the identity audit and management functions, which enhances their dynamism and agility. Although some data can upgrade and ameliorate the system, it is likely to violate users' privacy.

With regard to users, it is akin to a multipronged approach, which can enable users to clearly understand the rules pertaining to the virtual world. The analysis enables the integration of information; using modern algorithms, it enables the information to be linked, and it provides users with highly targeted services. This notwithstanding, analysis applications are dependent on powerful data resources and on data analysis capabilities. With respect to collecting the network behaviors of users, through data analysis, these applications can achieve safe and accurate prevention and governance. Nonetheless, some fundamental data exhibit high-level privacy, which may infringe on the privacy of users in the process of data collection and integration. In regard to modern analysis applications, developers are concerned with the following question: How can applications provide users with a safe environment without compromising their personal rights?

At present, although the subject of users' application of digital identity is different from the regulatory, the closed loop of digital identity operation and supervision has been initially formed. As shown in Figure 2. However, there are still many problems to solve.

4 Proposed strategies for digital identity regulation

4.1 Transform digital identity from "personification" to "characterization"

With respect to the Metaverse, users demand the freedom to choose and control their identities independantly; through automation technology, the users want to be less controlled. This autonomy depends on the establishment of known responsibilities; therefore, it may be beneficial to balance the relationship among order management, identity automation, and autonomy, which entails the personification concept–role concept transformation.

The "role" concept can categorize users and their rights. After grouping is performed, the permission allocation is simplified with respect to common technologies or business functions. With respect to the Metaverse, a user can select one or more roles, and the system will automatically assign permissions in conformance with role groups. Simultaneously, users can independently choose their nickname, gender, and avatar, within the scope of their roles. Thus, the system ensures that there is a gap between the data (*i.e.*, the nicknames and the real identity); furthermore, the system can enable individuals to restore the public-private boundary.

With regard to the allocation of role permissions, the system shall follow the minimization principle; the permissions that are required for the account or the implementation of the specified functions are provided in the little scope, within which users can act freely and independently exercise their rights. However, a question persists. A real person can assume countless roles; thus, numerous characters will be abandoned, and an immense amount of space will be wasted.

4.2 Establish decentralized identity management modes

The blockchain, encryption algorithm, and distributed identification technologies enhance the likelihood of decentralized identity management modes. Decentralized identity management technology immensely reduces users' dependence on centralized accounts, and the centralized organization's control over user data; furthermore, it maximizes users' control over identity information. When users interact with others, it is essential for both parties to "maintain" this connection. Once one of the parties goes offline, the connection is immediately disconnected. When both parties reach a consensus, they can continue to exchange network information. Theoretically, the existence of a decentralized identity enables any person or thing to communicate with others, and it exhibits the point-to-point (P2P) interaction presentation mode. Two users can interact directly without a third-party intermediary, which fundamentally eliminates the need for centralized accounts.

Blockchain technology may immensely popularize decentralized identity management modes. First, the user uploads the public key that is utilized to verify the identity in the blockchain system; subsequently, to ensure the security of the authentication process, the user exchanges the public key through encryption as well as via private P2P connection channels. This decentralized digital identity model is similar to the functions pertaining to personal business cards, which characterize the traditional world, and it reduces the likelihood of multiple propagations, and that pertaining to the leakage of the individual's information, digital signature, and encrypted business card.

Currently, the distributed identity system has been applied to the internet. Nevertheless, the technologies that the system requires, such as verifiable credentials, trusted correlation, digital wallet, digital proxy, distributed identity, blockchain technology, and governance architecture, are still immature, and a number of areas require amelioration. For instance, the mutual trust association, which characterizes the certificate circulation process, represents the correlation network, and it is composed of the issuer, holder, and verifier. The issuer represents the source of the voucher, which crucially substantiates the voucher. Common certificate issuers include governments, universities, and banks. Theoretically, when an individual possesses a positive reputation, they can become an independent certificate issuer. A voucher holder represents the owner of a voucher, and to prove their identity, they can possess multiple vouchers. Nonetheless, with regard to the manner of identifying whether a specific individual possesses a "sufficient" reputation, no strict standard exists. Although the technology ensures credibility pertaining to the system operation to a certain extent, with respect to the practical scenario, immense loopholes exist. For instance, in 2020, hackers leaked the user registration information pertaining to domestic websites that were stored in the CSDN database; in regard to shopping websites such as Meituan and Jingdong, when users confirm the payment, the system exhibits a loophole.

4.3 Popularize the utilization of privacy filters

The privacy (*i.e.*, stealth) filter, which is a general term for user privacy protection technology, usually entails an application component, a special software, or a physical gadget that is attached to the device, and this technology shields the user's data and protects their identity. The relevant contents of the EU General Data Protection Regulation state that by employing a tool similar to the privacy filter, the user's

identity should be concealed, and that it should be collected and analyzed. Currently, privacy filters that pervade the market include technologies such as the invisibility browsing mode, screen privacy filter, and visitor shopping cart.

The stealth filter can erase some information that can be utilized by hackers; thus, it can protect the user's personality and identity. The stealth filter exhibits the following function; although the system can still mine the user's browsing traces, the user identity has been confused. Both for-profit organizations and non-profit organizations are prohibited from storing or sending data that exhibits detailed identity information. The privacy filter technology not only supports the data analysis that characterizes the system, but it also ensures that the user's privacy information is not leaked. The screen privacy filter represents a physical polarizing filter that is added to the computer screen, and this filter is principally adopted to prevent users from being monitored by others when utilizing the computer to browse privacy information. Moreover, the collection of personal items may discourage some users from utilizing the system. However, it is easy for the system to verify the identity of the user by integrating multiple items. For instance, a user who utilizes the internet to purchase related products such as baby bottles, baby clothes, baby tableware, and breastfeeding bras is probably a mother to a baby. Because code writers control the operation of privacy filters, the difficulty with which users can comprehend the privacy protection mechanism is increased; thus, a trust deficit is introduced. Therefore, the development of privacy filters that enable users to effectively choose the information that they would want to block is imperative, and it is necessary to enhance the stability of the filter.

5 Conclusion

Digital identity primarily entails identity projection; identity exposure is an indirect consequence of digital technology [12]. Although the application of digital identity entails the application of novel technology, it is immensely concerned with the competition for data resources. The secure and trusted digital identity technology is essentially a decentralized, digital identity authentication management system that aims to reestablish the sovereignty of the user's data identity and to develop a data usage method that can protect the user's privacy [13]. The development of the Metaverse has become an established trend; thus, users are likely to create more expression and self-expression mechanisms. The development of the digital identity will facilitate the establishment of social ties and the consolidation of democracy; simultaneously, various parties such as economic and political stakeholders are competing for the data that constitutes the digital identity. To liberate users, liberalize their experience, and strengthen the positive role that the Metaverse exerts on democratic values, technological advancements are imperative; moreover, scholars should rationally identify problems, and they should explore the corresponding governance approaches.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability

No data are associated with this article.

Authors' Contributions

Siwen Wang wrote most of the papers. Wei Wang revised the paper and put forward many suggestions.

Acknowledgements

Thanks to Professor Chunhui Wang for giving this review many opinions and thanks to the editors for their careful revision.

Funding

This paper is supported by the project of the Zhejiang Federation of Social Sciences (2023N065).

References

[1] Jun D, Cheng H, Personal digital identity and its ethical issues in the age of big data [J]. Res Dialectics Nat 2018; **34**: 76–81.

[2] Jean PF et al., Digital Identity: Expression and Traceability. In: Wu Y and Li H, editors, Communication University of China Press, 2021, 002.

[3] 63% of Data Breaches Result From Weak or Stolen Passwords — ID Agent, (accessed on 6 October 2021). https://www.idagent.com/blog/2017-06-16-63-data-breachesresult-weak-stolen-passwords/.
[4] Goldfarb S. Using Digital Identity to Stamp Out Credential Fraud and Fake Diplomas, 18 September 2019. https://www.evernym.com/blog/credential-fraud-fake-diplomas/.
[5] Stephen Curran, CH. Introduction to hyperledger sovereign identity blockchain solutions: Indy, aries and ursa! (accessed on 1 January 2021a). https://learnthings.online/other/2020/03/05/introduction-to-hyperledger-sovereign-identity-blockchain-solutions-indy-aries-ursa.
[6] D'Aliessi M. "How Does the Blockchain Work?" Medium, 1 June 2016, (accessed on 10 March 2023). https://medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae.
[7] Victor F, Ruppel P and Kupper A. A taxonomy for distributed ledger analytics. Computer 2021; **54**: 30.
[8] Jean PF et al., Digital Identity: Expression and Traceability. In: Wu Y and Li H, editors, Communication University of China Press, 2021, 005.
[9] Morey H and Dalan R. Identity Attack Vector (Translated by Qianxin Identity Security Laboratory). China Industry and Information Publishing Group, People's Posts and Telecommunications Press, First Edition, 2022, 9.
[10] Vincent M. The Essence of Digital Culture [M]. In: Yan Q et al. Tsinghua University Press, 2017, 158.
[11] Peng L. "Metaverse" Technology: Promoting the Free and Comprehensive Development of Human Beings [J]. Indus Econ Rev 2022; **1**: 20–27.
[12] Jean PF. Digital Identity: Expressed in Traceability. In: Wu Y and Li H, editors, Communication University of China Press, 2021, 4.
[13] Wang D, Song C, Digital identity: How to Safely Prove that You are Youself in the Digital Space. China Industry and Information Press, Electronic Industry Press, 2020, 1.

Siwen Wang is currently a lecturer at the School of Journalism and Communication, Communication University of Zhejiang. Her research interests include ethics of intelligent technology, law, and ethics of Journalistic.

Wei Wang is currently a lecturer at the Nanjing University of Finance and Economics. His research interests include cyberspace governance and the digital economy.