Hindawi
Mobile Information Systems
Volume 2024, Article ID 6651273, 10 pages
https://doi.org/10.1155/2024/6651273

Review Article

The Review and Comparison between Centralized and Decentralized Digital Identity Systems

Haihua Li,[1] Yue Jing ,[2] and Zhenyu Guan [1]

[1]*Beihang University, Beijing, China*
[2]*China Academy of Information and Communications Technology, Beijing, China*

Correspondence should be addressed to Zhenyu Guan; guanzhenyu@buaa.edu.cn

Received 27 August 2023; Revised 1 February 2024; Accepted 13 February 2024; Published 26 February 2024

Academic Editor: Floriano Scioscia

The growing capability of the digital world empowers physical objects to possess much more digital assets than they ever had, and the concepts of the Internet of Things and the Industrial Internet are coming out continually. Digital identity, a unique mark of two-way mapping, dynamic interaction between physical and virtual objects, is one of the fundamental elements among these novel concepts because it is the only way to distinguish each other from hundreds of millions of digital objects. In order to create a world with everything connected on the Internet, plenty of digital identity-orientated systems were raised, and new frameworks are emerging iteratively. To the best of our knowledge, this review lists some of the most applicable digital identity-based solutions by giving mechanism, digital identity solution, feature, and comparison between these models.

1. Introduction

The advent of the Internet has connected people across the world with efficiency, reliability, and consistency that was previously thought to be impossible. Through the power of personal machines such as laptops and smartphones, people can stay constantly online, receiving messages from friends and emails from websites and blogs. Generally, people define this period as the "consumer-oriented Internet" [1] where the service subject of the consumption Internet is mainly people. However, due to the rapid growth of millions of online services, the service subject of the Internet extends to machines, devices, and digital objects. Thus, the era of Industrial Internet, along with the concept of the Internet of Things, is coming. To realize the interconnection between enormous subjects, digital identity plays an indispensable role in this new era.

From the 1980s, the Domain Name System (DNS) provides digital name service for the primitive Internet which is called DAPRA Internet, and it is one of the largest name services in operation today [2]. During the same period, the Object Identifier (OID) architecture came out with the purpose of naming any object, concept, or thing with a globally unambiguous persistent name [3]. In ten years, Bob Kahn, well known as "The father of the Internet," proposed the Handle System, which is a distributed information system designed to provide an efficient, extensible, and secured global name service for the networks [4, 5]. These infrastructures all made great impacts on the development of the Industrial Internet, but they rely on a single centralized authority which may cause insecure authenticity and limited scalability issues. Thus, a more robust, persistent, distributed, self-controlled identifier which is known as the decentralized identifier (DID) is put forward (Figure 1) around in 2016 [6].

2. Digital Identity Systems

2.1. Domain Name System (DNS). Generally, the DNS could be understood by two parts: domain name and domain name system resolution (DNS resolution). The domain name is the basic identifier resource of the Internet. It is composed by strings, such as "Google.com" and "Facebook.com," and is used to identify digital objects through the Internet, for example, websites, email services, and Internet Protocol (IP) addresses. The domain name facilitates the

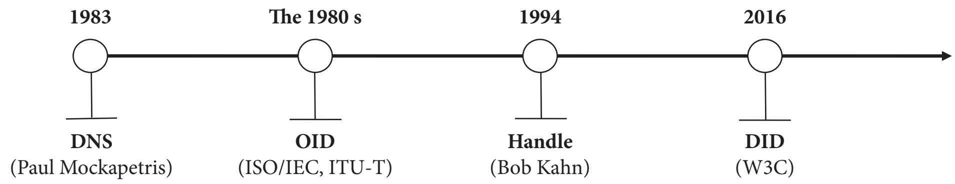

Figure 1: Some of the milestones in the internet digital identity evolution path.

user with easy access to service providers without memorizing the complex IP address. On the other hand, DNS resolution is a translation process between the domain name and the IP addresses, and it is a distributed database that records the mapping between the domain name and IP address.

2.1.1. Domain Name. The domain name is a variable-depth tree structure, which consists of a root domain, top-level domain, and the following second-level and third-level, etc., [2, 7]. Usually, the far right string is a top-level domain name, and its left-adjacent string is a second-level domain (Figure 2) name and so on.

The root domain is located at the top of the entire domain name system, represented by ".," which is usually omitted. According to the type of operating organization, the top-level domains can be divided into (1) generic top-level domains (gTLD) and (2) country code top-level domain (ccTLD). The gTLDs can be commonly seen in daily Internet activities, such as ".com," ".net," and ".org". The ccTLDs, however, have implied national attributes, for example, ".CN" stands for "China" and ".UK" stands for "United Kingdom" [8]. Take "apple.com.cn" for example, this domain contains a root domain, which is a "." behind the "cn," but is omitted, "cn," which is a top-level domain, "com," which is a second-level domain, and "apple," which is a third-level domain [8].

2.1.2. DNS Resolution. The DNS resolution is completed by the DNS resolution server. The server is the database, which stores the mapping between the domain name and IP address. It realizes the conversion between the two, and it is the gate that the user can access directly to the Internet. The resolution process can be abstract as follow, see Figure 3.

The root servers store the records of top-level domains, and they provide global top-level resolution. The top-level servers store the records of second-level domains registered under the top-level domain. At the same time, the second-level servers store the records of subsequent-level domains. The recursive servers store the caching data collected after the recursive process, and they can give user the final resolution results (note: the "records" means the mapping between a domain name and IP address).

2.1.3. DNS Resolution Process. The end user enters the domain name of the website into the browser, for example, https://example.com. The browser will send a query to the recursive server, and the recursive server will first send this query to the root server, then the top-level server, and finally the second or third-level server to search the records, see Figure 4 [9].

2.2. Object Identifier (OID). The Object Identifier (OID) is an identification system promoted by ISO/IEC and ITU. The purpose of OID is to give every single digital object a globally unambiguous persistent name. An object identifier is a tree of nodes where each node is simply a sequence of digits [10], see Figure 5.

The OID root server is divided into three different branches (also known as "arc"): ITU (0) arc, ISO (1) arc, and ITU joint ISO (2) arc. There are some designated nodes, which can be called registration authorities (RAs), and RA is responsible for the sub-RA assignment and registration. To be more specific, in the top-level, there are three RAs, and each of them has the right to assign a new sub-RA in the second-level, and the sub-RA also has the right to assign a new sub-RA in the third-level, and the rest can be done in the same manner. Therefore, the RAs can be categorized into various institutions, such as national government departments, industry associations, and standardization organizations, and based on the various RA, OID can be applied in different industries, such as health care, food traceability, finance, education, and digital credential. In another word, each digit of the node stands for a RA or a specific sort of object.

2.3. Handle System. The handle system is a distributed information system designed to provide an efficient, extensible, and secured global name service for use on networks such as the Internet [5]. In the handle system, the "handle," which means a unique persistent digital identifier, is used to identify a digital object on the Internet. The invention of the handle not only realized the identification management of digital objects on the Internet, but also meets the need for identification services in the development of the Internet of Things. A brief illustration of the handle system can be seen as follow, see Figure 6.

A handle consists of prefix and suffix, separated by periods ("/"), representing a hierarchy of naming authorities. The prefix is issued by the DONA foundation, and it is administrated by the multiprimary administrator (MPA), in which there are a total of 10 MPAs around the world [11, 12]. MPA's information is stored in the global handle registry (GHR), which also stores information of different prefixes. In a word, the GHR is a database for MPAs and prefixes that MPAs possessed. Under the prefix is the subprefix. The subprefix is issued by MPA, and every qualified entity (both

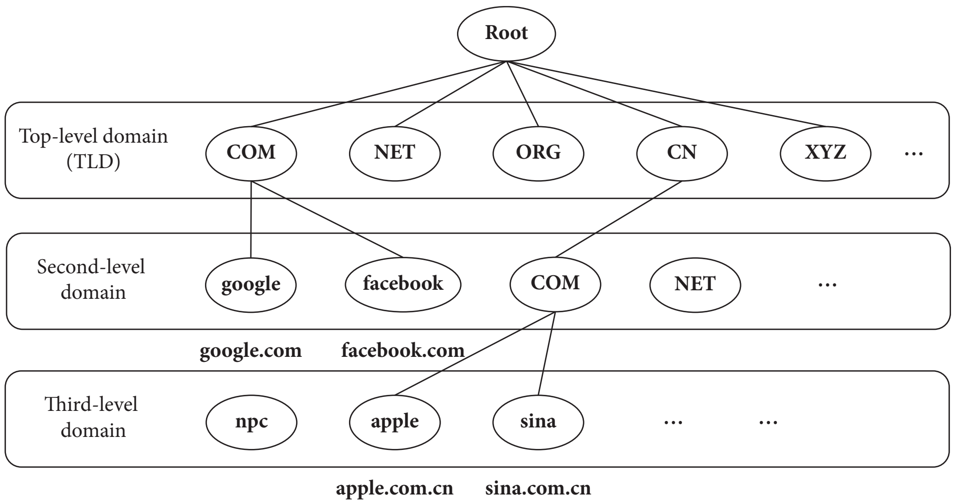

Figure 2: An illustration of the variable-depth tree structure of the domain name.

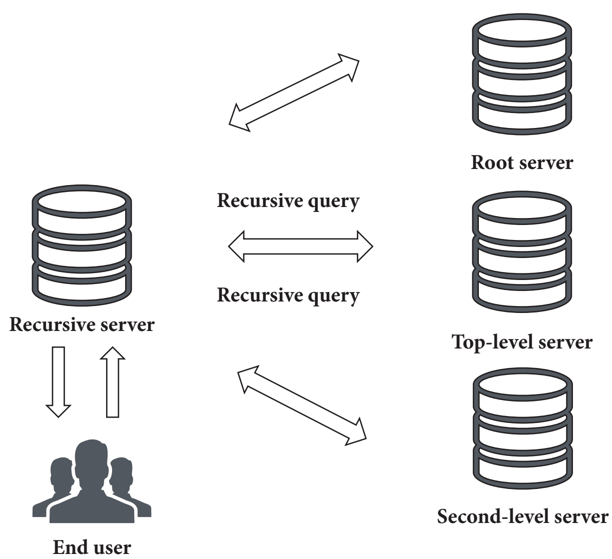

Figure 3: Classification of DNS servers.

organization or individual) can apply to be an LHS provider with the permission of MPA. The LHS provider can allocate the integral handle identifier (both prefix and suffix) with their purpose.

Take Digital Object Identifier (DOI) as an example. DOIs are widely used in academic, such as journal articles, research reports, and official publications, and they are based on handle system. "doi: 10.1000/182" is a handle, which stands for the DOI handbook. The prefix is "10.1000," and the suffix is "182." The "10" of the prefix distinguishes this handle from other handles, and the "1000" indicates the registrant. The "182" identifies the digital object, which in this case is the DOI handbook [13].

2.4. Decentralized Identity. The concept of decentralized identity has come up with the stimulation of blockchain and distributed ledger technologies, and it was also known as self-sovereign identity (SSI). It describes the digital world where users can take greater control over their digital identities instead of their identities being composed of accounts or identifiers that are borrowed from providers. This makes the Internet not only a more reliable tool but a more robust platform for creating fruitful digital experiences. The key element in decentralized identity is the decentralized identifier (DID) and verifiable credentials (VC) [14, 15].

2.4.1. The Decentralized Identifier (DID). The DID is a new type of globally unique digital identifier associated with a subject and a DID document [14]. The subject, which is normally called "DID subject," refers to the entity that this DID identifies. The DID subject could be anything, such as people, organization, thing or digital information, so it satisfies the need for industrial Internet and IoT requirements. The DID document is a set of data describing the DID subject, including the DIDs, the public keys, and the services endpoints relevant to the subject. The DID points to the DID document, and the DID document contains the information of the DID subject, see Figure 7 [14].

Unlike the other digital identity systems, which have distinct hierarchy frameworks, the DID builds a direct relationship between subjects and blockchains. Initially, anyone or anything with the proper software can generate a DID, and begin using it immediately without requiring the authorization or involvement of any centralized registration authority. This is the same process used to create public addresses on the Bitcoin or Ethereum or other popular blockchains. Meanwhile, the DID document records the way how this DID is created and its only controller. Finally, both DID and DID document are stored in the blockchain, which makes the DID self-controlled and Figures 8 and 9 decentralized.

Basically, the DID is a string, and it is randomly generated according to encryption algorithm and software, not dependent on the issuance and authorization of authority. The DID is pretty much similar to a bitcoin address, but it has more properties as follows [16]:

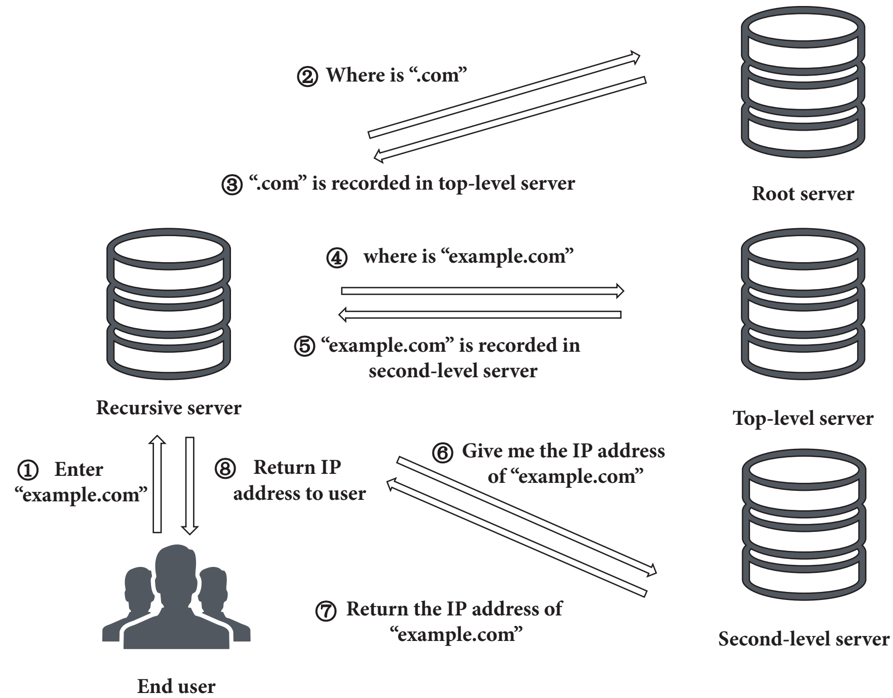

Figure 4: DNS resolution process.

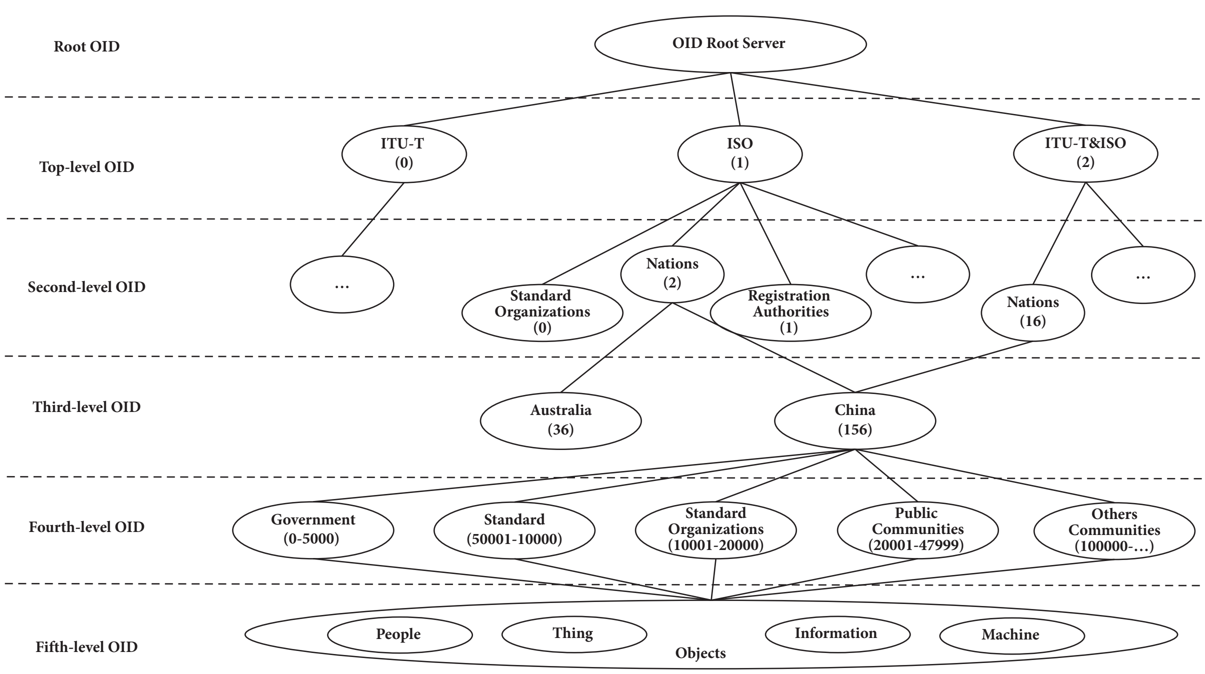

Figure 5: The tree of nodes where each node is a digit.

(i) Permanent. Once the DID is created, it can never be changed, since it is recorded in the blockchain or other distributed ledgers.

(ii) Resolvable. Since the DID is pairwise with a DID document, which contains the metadata of the subject, everyone could look it up to discover the metadata of the DID.

(iii) Verifiable. A DID is associated with one public/private key pair, the controller of the private key can prove that they are the only owner of the DID. On the contrary, anyone could verify this DID to ensure it belongs to the real controller.

(iv) Decentralized. The cryptography mechanism eliminates the need for centralized registration

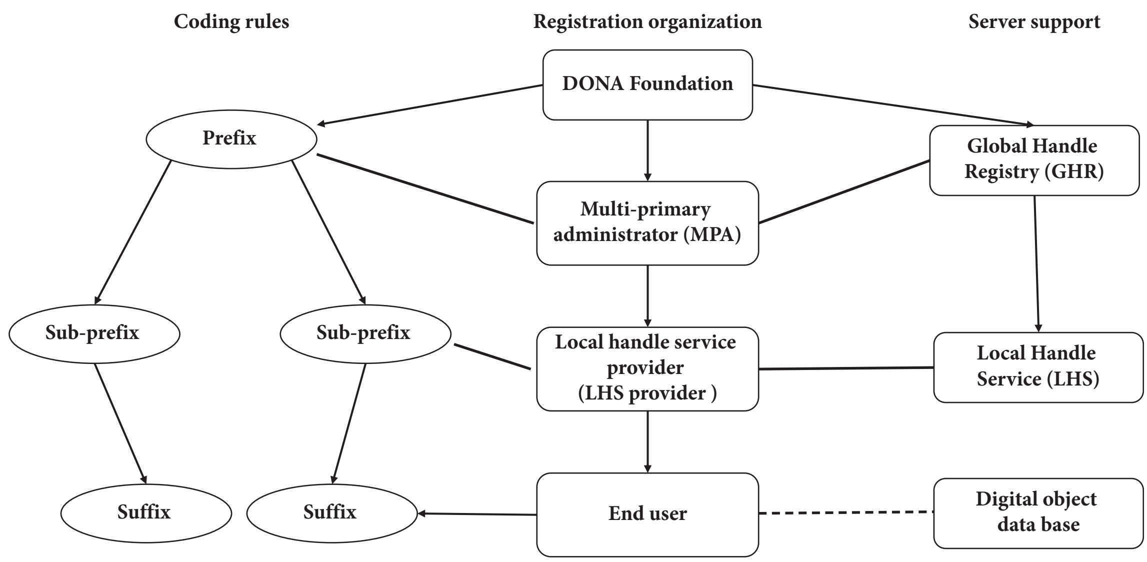

Figure 6: Overview of handle system.

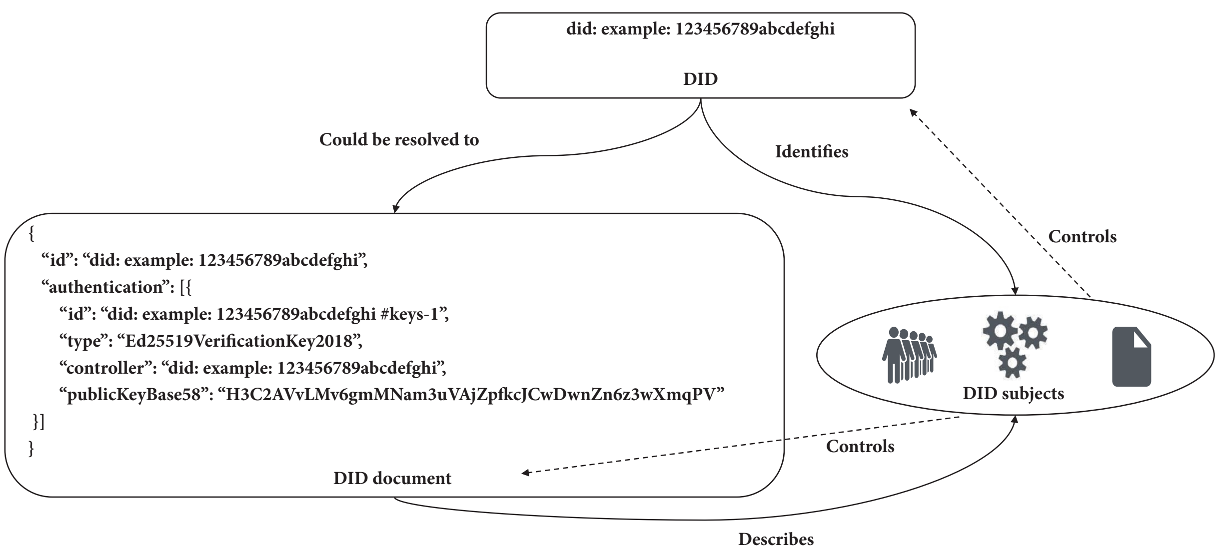

Figure 7: The relations between DID, DID subject, and DID document.

authorities, the kind of system needed for almost every other global identifier systems we use. DID and DID document could be store in blockchain, which play the role as the trust anchor, and it exactly realizes the decentralized feature of this new type identifier.

2.4.2. Verifiable Credentials (VC). The verifiable credentials (VC) are one of the most important elements of SSI, and it is the manifestation of DID. The W3C verifiable credential data model v1.1 illustrates that "Credentials are a part of our daily lives; driver's licenses are used to assert that we are capable of operating a motor vehicle, university degrees can be used to assert our level of education, and government-issued passports enable us to travel between countries" [17], while verifiable credentials are digital credentials that are closely related to DID and provide authentication for a decentralized identity. Verifiable Credentials contain 3 main components [17, 18]:

(i) Metadata: Issued with the issuer's cryptographic signature. "describe attributes of the credential, such as the issuer, the expiration date and time, a representative image, a public key to use for verification purposes, the revocation method, and so on" [17].

(ii) Claims: A declaration that is made on a topic. For instance, the statement that "Alice's date of birth is January 1, 1990."

(iii) Proofs: A proof is data about yourself that enables other people to verify the source of the data, check that the data belongs to you, that the data has not been tampered with, and finally, that the data has not been revoked by the issuer. A proof is also known as an identity document or an identity credential.

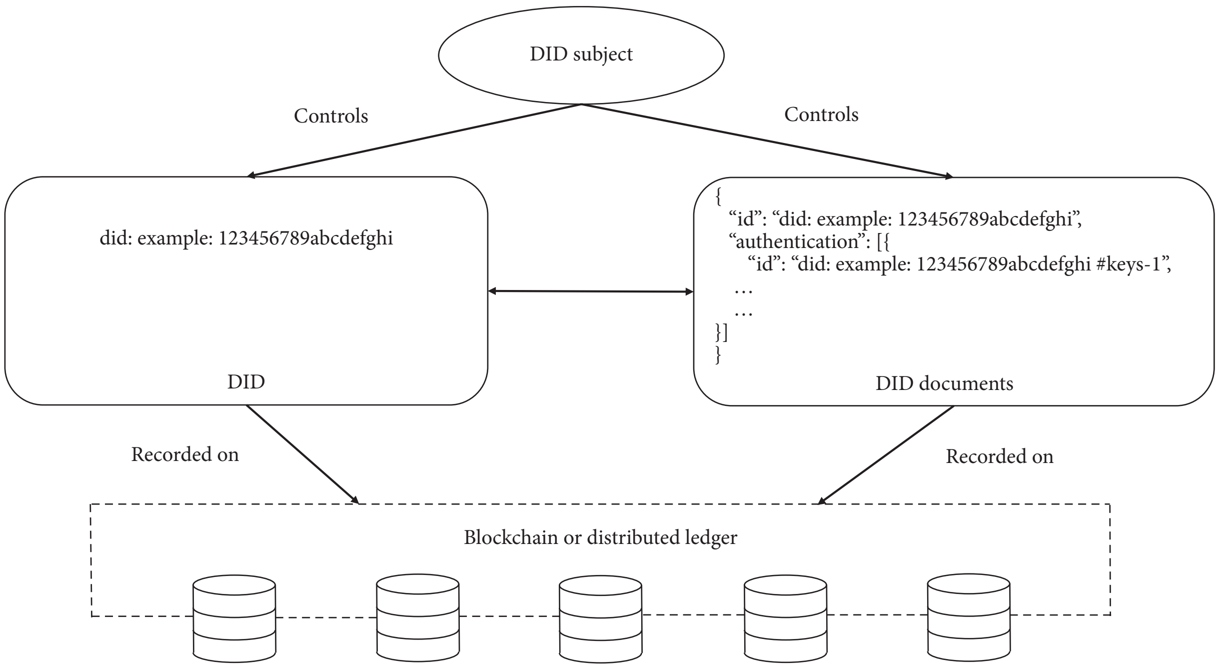

Figure 8: The DID subject, DID, DID document, and blockchain.

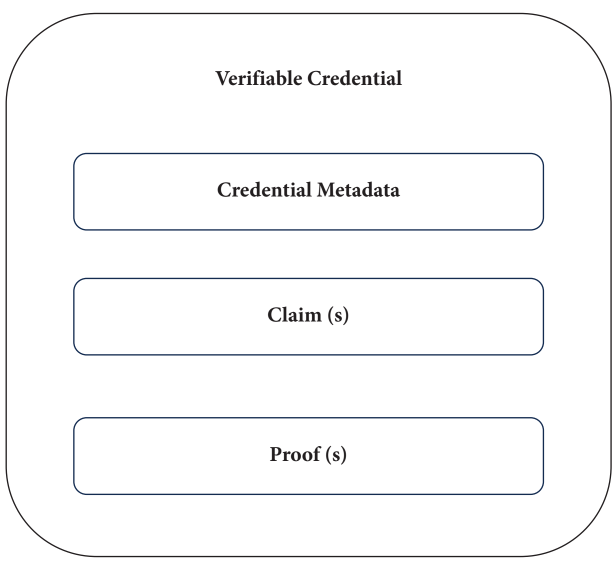

Figure 9: Components of a verifiable credential [17].

2.4.3. Movement. Start from 2016, the decentralized identity has become a key area of focus in the United States, Europe, Canada, and other Asia countries. From government, enterprise to communities, they are exploring plans that might have a huge impact on future industrial development and economic.

(1) To begin with, governmental support for DID has increased significantly.

(i) The United State government regards decentralized identity as important innovation by setting up national strategy and supporting funding to enterprises. The US government announced the implementation of the National Strategy or Trusted Identities in Cyberspace (NSTIC) in April 2011 [19]. Moreover, since 2018, the U.S. Department of Homeland Security (DHS) has signed phased project contracts with eight leading enterprises with total $3.77 million funding.

(ii) The European Union Commission has announced the EU digital identity wallet initiative, which is also called as eIDAS 2.0 (electronic IDentification, Authentication and trust Services) in which EU member states will agree on standard specifications for digital identity wallets and government-issued identity credentials that will work all across the EU [20].

(iii) The Canadian provinces of Ontario, British Columbia, and Quebec are similarly collaborating on open standard, open source digital identity wallets and verifiable credentials that will be issued by each province to its citizens [21, 22].

(2) Secondly, commercial adoptions of verifiable credentials are beginning to ramp up.

(i) Apple and Google have both announced that their digital wallets integrated into iOS and Android, respectively, will begin supporting digital driver's license credentials [23].

(ii) Microsoft is adding support for verifiable credentials to its security and Azure Active Directory products [24].

(iii) The International Air Transport Association (IATA) Travel Pass is now being used by over a dozen airlines to provide a combination of identity, itinerary, and COVID-19 health credentials to over 10,000 airline passengers per month [25].

(3) Thirdly, standard works on DID are progressing quickly.

(i) After 3 years of working, the World Wide Web Consortium (W3C) Decentralized Identifiers (DID) 1.0 specification was finally approved by the W3C DID Working Group and it is an official recommendation [14]. Meanwhile, the W3C Verifiable Credentials Working Group is finalizing the charter for the second generation of its Verifiable Credentials specification [26].

(ii) The Trust Over IP (ToIP) Foundation has published its first official specifications for decentralized governance frameworks [27].

2.4.4. Influence. From a technical perspective, DID is a technology that integrates existing cryptography, distributed storage, and various Internet protocols, TCP/IP for example, and it does not involve too many technical difficulties. However, SSI is trying to build an ecosystem based on the existing Internet that eliminates monopoly and ensures independent data control with trusted interaction. From a practical perspective, SSI reshapes the way people access Internet services. Specifically, users who want to access services on the Internet must first provide personal data to the provider to register an account. After obtaining the account, they can access various Internet services. For example, we need to log in with Google account before visiting Google service. Using DID, users can directly choose whether to use DID to access various Internet services, instead of entrusting suppliers to create accounts for themselves. That is, DID hands over the ownership of digital identities such as accounts to the users themselves. It is the "key" in the hands of the user, which can open the door to various Internet services, without the need for a supplier to manage the "key" on behalf of the user.

Also, enabling technologies such as IoT, blockchain, and digital twins can collectively contribute to creating more powerful SSI solutions with various advantages. In the IoT fields, the benefits could be summarized as follows [28]:

(i) Decentralized Data Processing. With the help of SSI solutions, IoT devices can process and share data directly without relying on a central server, and this improvement could reduce latency and enhance the scalability of the system.

(ii) Redundancy and resilience. SSI solution ensures that if one IoT node fails, the network can still function, enhancing the overall reliability and resilience of the IoT ecosystem.

(iii) Data Privacy and Security. By decentralized data storage and process, IoT devices can contribute to better data privacy. Personal information can be stored locally on devices, reducing the risk of a single point of failure and potential data breaches.

Table 1: Comparison between four systems.

System	DNS	OID	Handle	DID
Readability	High	Low	Low	Low
Security	Middle	Middle	Middle	High
Authority	High	Middle	Middle	Middle
Hierarchy	High	High	Middle	Low
Expansibility	Low	Low	Middle	High

The blockchain can benefit SSI solutions in [28]:

(i) Decentralized Trust. Blockchain eliminates the need for a central authority by providing a decentralized ledger that is transparent, secure, and tamper-resistant. This ensures trust among SSI participants without the need for intermediaries.

(ii) Smart contracts. Automated, self-executing smart contracts on the blockchain facilitate decentralized agreements and transactions. This reduces the need for intermediaries, and increases the speed of generating the DID methods.

(iii) Immutable record keeping. The decentralized and distributed nature of blockchain ensures that once data is recorded, it cannot be altered or deleted. This feature enhances the integrity of data, which is crucial for various SSI applications such as supply chain management and healthcare.

In the digital twins fields, the benefits are as follows [29]:

(i) Decentralized Simulation. Digital twins can benefit from decentralized simulation environments. This allows for more realistic and accurate modeling by distributing the computational load across various nodes.

(ii) Collaborative Decision-Making. Decentralized digital twins enable collaborative decision-making by allowing multiple stakeholders to access and contribute to the digital representation of a physical entity. This can be valuable in industries such as manufacturing and urban planning.

(iii) Real-time Monitoring and Control. The decentralized nature of digital twins allows for real-time monitoring and control of physical entities. Changes and updates in one part of the system can be reflected across the entire decentralized network, ensuring synchronization.

Moreover, DID is the most important basic resource in the Web3.0 concept. The EU believes that "Web3.0 is a new decentralized network model where users can own and control their data, while DID provides a decentralized authentication method that allows everyone to control their digital identity information" [30]. At present, various applications of Web3, such as decentralized finance (DeFi), Metaverse, and decentralized applications, all regard DID as an important means of implementation. Therefore, DID and Web3.0 are closely connected. One provides decentralized identity management, and the other provides a framework for user participation and data ownership. The two are combined to achieve an important component of Web3.0.

3. Conclusions

3.1. Features. The above paragraphs list the purpose, solution, structure, movement of the DNS, OID, Handle system, and DID four types of digital identity systems. Here we give personal viewpoints for these systems.

3.1.1. DNS. For DNS, there are 5.15 billion Internet users worldwide, which is 64.4 percent of the global population. This tremendous number indicates people's indispensable dependence on the DNS. First of all, DNS makes it easier for user to use the Internet without remembering IP address, and the distributed implementation of root server offers high speed connections for individuals [31]. Secondly, after years of improvement, DNS is a relevant secure system for user. For example, the DNSSEC adds two important features to DNS, which are data origin authentication and data integrity protection. These two approaches are used to verify that the requests for a DNS record comes from its authoritative name server and was not spoofed or manipulated in the request process [32, 33]. However, as the registry control of DNS is under ICANN [34], which means that no other organization will be able to control them, it is undeniable that the DNS is a highly centralized system, with the risks of server breakdown and man-made damage.

3.1.2. OID. The OID system provides digital identities with features of globally unambiguous persistent digital identifier, distributed management of each layer. Firstly, the OIDs identify and locate objects in various of types, so that all kinds of objects, sorted by industry and application scenarios, can be connected to the Internet, and further integrated the physical and digital world. Secondly, the OIDs are strictly managed by RAs according to the use purpose, so the entire system is well standardized, which facilitate the registration and application process. However, it is also clear that the OID is complex. For example, "1.2.156" and "1.2.36" are two arcs, and the digit behind "156" and "36" can be quite different [10]. Even the identifiers under the same arc could be different, saying "1.2.156.1000" and "1.2.156.10000," without professional knowledge it is impossible to distinguish them. Thus, the long arc implies the process of seeking the digital object should be time-consuming. When dealing with larger amounts of data, the computing process should start from the top to the bottom of the arc, and the computing power is limited by the RAs, which might vary from each other.

3.1.3. Handle. The handle system has been deployed for more than 20 years, and there are billions of identifiers that have been registered. The early applications of the handle system were mainly focused on digital content-related fields, but with the deepening of industrial digital transformation and the development of the industrial Internet, the handle system has been expanded into manufacturing fields such as railways and construction. However, the handle system is running by DONA and MPAs, so the centralized authority is still existing. Moreover, the MPAs are running by local companies or organizations, which cause the charge of the handle being not cheap, and it might be one of the reasons why it is hard to be applied in IoT scenarios, where the quantity of things is giant [35].

3.1.4. DID. Fundamentally, instead of identities being composed of accounts or identifiers that are "borrowed" from providers, DID gives the controller the right to possess digital identities. As DIDs are more broadly adopted across the web, they give rise to a more resilient Internet, where digital identity is not borrowed from a provider, the way domain names and social media accounts are, but rather controlled by a controller and thus the basis of a new kind of verifiable digital trust. This makes the Internet not only a more reliable tool but a more robust platform for creating richer digital experiences [36]. Nevertheless, DID has been a hot topic in worldwide, just like the concept of blockchain, and there are remarkable implementations, pilots in different industrial areas, but whether it will bring revolutions both in social and economic remain to be seen.

3.2. Comparison. We abstract these four systems from the perspectives of "readability," "security," "authority," "hierarchy," and "expansibility." Initially, "readability" means whether this identifier could be easily recognized by human. The domain name can be easily memorized by people, while others are machine-readable only. The complex coding schemes of OID, Handle, and DID are beneficial to industrial Internet use case, since more naming spaces provide more options, or rooms, for a huge number of industrial objects. Secondly, "security" ensures that the digital identity cannot be easily stolen or tampered. The DID are naturally generated by encryption algorithm, which is not man-made rule or method, so it increase the impossibility to crack it. Thirdly, "authority" means whether this system is well adopted by society, and well used economical production. Since DNS has been operating for over 40 years, it is the most mature system comparing with others, especially DID, which is a new concept. Fourthly, "hierarchy" obviously means whether this system is root-based or centralized. DNS and OID have root server embedded in their system architecture, which can be seen from the structure. Handle weakens the notion of centralized root, and instead, it endows different characters (MPAs) to operate the separated roots. Unlike them, decentralized identity is a totally decentralized system, with no relying parties to control digital identifier, and no root server ever exists. Finally, "expansibility" means whether this digital identity can be adapted into different systems. To be more specific, DNS are mainly used in Internet, and OID and Handle are mainly used in electronic medical records and literature publication. DID, however, as it does not rely on heavy system, it can be applied in any scenarios (Table 1).

3.3. Future Directions. Strategic technologies that can play a transformative role usually go through a process from conception to technology testing, from technology pilot to large-scale application, and it probably takes 10 years or more for each generation to develop. We have to admit that all systems play pivotal roles in today's Internet and Industrial Internet or IoT activities. While with more and more privacy and security issues coming up, previous systems are suffering regeneration and iteration. The DID depicts a new user-controlled digital world with new technology and concept. It is estimated that the potential of decentralized identity market is $0.55 trillion. Although decentralized identity is more like an infant compared with other, together with of concept of Web3, Metaverse, and NFT, we believe that the "decentralized" idea will continue to hatch, and decentralized identity will definitely make great impact on the transformation for today's Internet and Industrial Internet [37].

Data Availability

The data used to support the findings of this study have been deposited in the repositories such as https://datatracker.ietf.org/doc/rfc3650/, https://www.dona.net/mpas, https://www.w3.org/TR/did-core/, and https://www.w3.org/groups/wg/vc/charters.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by "National Key R&D Program of China" (2022YFE0139900).

References

[1] Gu-Shanshan, "The path to study and solve the internet era entertainment industry development dilemma," in *Proceedings of the 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation*, pp. 1238–1241, Nanchang, China, June, 2015.

[2] P. Mockapetris and K. J. Dunlap, "Development of the domain name system," in *Proceedings of the Symposium proceedings on Communications ar-chitectures and protocols*, Austin, TX, USA, August, 1988.

[3] R. Wieringa and W. de Jonge, "Object identifiers, keys, and surrogates: object identifiers revisited," *Theory and Practice of Object Systems*, vol. 1, no. 2, pp. 101–114, 1995.

[4] B. M. Leiner, V. G. Cerf, D. D. Clark et al., "A brief history of the internet," *ACM SIGCOMM- Computer Communication Review*, vol. 39, no. 5, pp. 22–31, 2009.

[5] L. Lannom, L. C. B. P. Boesch, and S. Sun, *Handle System Overview (Request for Comments RFC 3650)*, Internet Engineering Task Force, Marina del Rey, CA, USA, 2003.

[6] O. Avellaneda, A. Bachmann, A. Barbir et al., "Decentralized identity: where did it come from and where is it going?" *IEEE Communications Standards Magazine*, vol. 3, no. 4, pp. 10–13, 2019.

[7] A. Khormali, J. Park, H. Alasmary, A. Anwar, M. Saad, and D. Mohaisen, "Domain name system security and privacy: a contemporary survey," *Computer Networks*, vol. 185, Article ID 107699, 2021.

[8] W. Qin and N. An, "Establish a simulation platform of DNS root server in campus network laboratory," in *Proceedings of the 2020 IEEE 3rd International Conference on Information Systems and Computer Aided Education (ICISCAE)*, pp. 470–474, Dalian, China, September, 2020.

[9] Y. Jin, M. Tomoishi, and S. Matsuura, "Detection of hijacked authoritative DNS servers by name resolution traffic classification," in *Proceedings of the 2019 IEEE International Conference on Big Data (Big Data)*, pp. 6084-6085, Los Angeles, CA, USA, December, 2019.

[10] M. H. Mealling, *A Urn Namespace of Object Identifiers*, Internet Engineering Task Force, Fremont, CA, USA, 2001.

[11] Dona Foundation, "Credentialed mpas," https://www.dona.net/mpas.

[12] S. Sun, L. Lannom, and B. Boesch, *Handle System Overview (No. Rfc3650)*, RFC Editior, Marina del Rey, CA, USA, 2003.

[13] J. Wang, "Digital object identifiers and their use in libraries," *Serials Review*, vol. 33, no. 3, pp. 161–164, 2007.

[14] B. Alzahrani, "An information-centric networking based registry for decentralized identifiers and verifiable credentials," *IEEE Access*, vol. 8, pp. 137198–137208, 2020.

[15] Y. Jing, J. Li, Y. Wang, and H. Li, "The introduction of digital identity evolution and the industry of decentralized identity," in *Proceedings of the 2021 3rd International Academic Exchange Conference on Science and Technology Innovation (IAECST)*, pp. 504–508, Guangzhou, China, December, 2021.

[16] Z. A. Lux, D. Thatmann, S. Zickau, and F. Beierle, "Distributed-Ledger-based authentication with decentralized identifiers and verifiable credentials," in *Proceedings of the 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Ser-vices (BRAINS)*, pp. 71–78, Paris, France, September, 2020.

[17] Wc, "Verifiable credentials data model v1.1," 2023, https://www.w3.org/TR/vc-data-model/.

[18] N. Parashar, "What is verifiable credentials? Medium," 2021, https://medium.com/@niitwork0921/what-is-verifiable-credentials-1f0b9d2c7adc.

[19] Nist, "Get involved in the national strategy for trusted identities in Cyberspace (NSTIC)," https://www.nist.gov/blogs/cybersecurity-insights/get-involved-national-strategy-trusted-identities-cyberspace-nstic.

[20] European Commission, "Commission proposes a trusted and secure Digital Identity," European Commission, Brussels, Belgium, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663.

[21] Ontario.ca, "Ontario's Digital ID: technology and standards, ontario.ca," 2023, http://www.ontario.ca/page/ontarios-digital-id-technology-and-standards.

[22] Ibm, "Building a digital trust ecosystem for mining in British Columbia IBM supply chain and blockchain blog," 2021, https://www.ibm.com/blogs/blockchain/2021/11/building-a-digital-trust-ecosystem-for-mining-in-british-columbia/.

[23] Washington post, "Digital driver's license: here's what you should know- the Washington Post," 2021, https://www.washingtonpost.com/technology/2021/10/11/digital-drivers-license-mdl/.

[24] Microsoft Security, "Microsoft entra verified ID, Microsoft security," 2023, https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-verified-id.

[25] Iata, "IATA- travel pass initiative," 2023, https://www.iata.org/en/programs/passenger/travel-pass/.
[26] S. Lim, M.-H. Rhie, D. Hwang, and K.-H. Kim, "A subject-centric credential management method based on the verifiable credentials," in *Proceedings of the 2021 International Conference on Information Networking (ICOIN)*, pp. 508–510, Jeju Island, Korea (South), January, 2021.
[27] M. Davie, D. Gisolfi, D. Hardman, J. Jordan, D. O'Donnell, and D. Reed, "The trust over IP stack," *IEEE Communications Standards Magazine*, vol. 3, no. 4, pp. 46–51, 2019.
[28] G. Fedrecheski, J. M. Rabaey, L. C. P. Costa, P. C. Calcina Ccori, W. T. Pereira, and M. K. Zuffo, "Self-sovereign identity for IoT environments: a perspective," in *Proceedings of the 2020 Global Internet of Things Summit (GIoTS)*, pp. 1–6, Dublin, Ireland, June, 2020.
[29] U. Cali, M. S. Ferdous, E. Karaarslan, S. N. G. Gourisetti, and M. Mylrea, "SSI meets Metaverse for industry 4.0 and beyond," in *Proceedings of the 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGET-blockchain)*, pp. 1–6, Irvine, CA, USA, November, 2022.
[30] Ebsi, "EBSI a new trust paradigm for Web3," https://ec.europa.eu/digital-buildingblocks/sites/display/EBSI/EBSI+a+new+trust+paradigm+for+Web3.
[31] N. Shibata, Y. Musashi, D. A. L. Romana, S. Kubota, and K. Sugitani, "Trends in host search attack in DNS query request packet traffic," in *Proceedings of the 2012 Fifth International Conference on Intelligent Networks and Intelligent Systems*, pp. 126–129, Tianjin, China, November, 2012.
[32] K. Kakoi, Y. Jin, N. Yamai, N. Kitagawa, and M. Tomoishi, "Design and implementation of a client based DNSSEC validation and alert system," in *Proceedings of the 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, pp. 8–13, Atlanta, GA, USA, June, 2016.
[33] Y. Jin, M. Tomoishi, and S. Matsuura, "A detection method against DNS cache poisoning attacks using machine learning techniques: work in progress," in *Proceedings of the 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA)*, pp. 1–3, Cambridge, MA, USA, September, 2019.
[34] S. Rose and A. Nakassis, "Minimizing information leakage in the DNS," *IEEE Network*, vol. 22, no. 2, pp. 22–25, 2008.
[35] Y. Chen, Z. Zheng, S. Luo, and S. Li, "Research on application of handle system in the industrial internet," in *Proceedings of the 2021 4th International Conference on Intelligent Robotics and Control Engineering (IRCE)*, pp. 124–128, Lanzhou, China, September, 2021.
[36] N. Naik and P. Jenkins, "Sovrin network for decentralized digital identity: analysing a self-sovereign identity system based on distributed ledger technology," in *Proceedings of the 2021 IEEE International Symposium on Systems Engineering (ISSE)*, pp. 1–7, Vienna, Austria, October, 2021.
[37] N. Naik and P. Jenkins, "Your identity is yours: take back control of your identity using GDPR compatible self-sovereign identity," in *Proceedings of the 2020 7th International Conference on Behavioural and Social Computing (BESC)*, pp. 1–6, Bournemouth, UK, November, 2020.