Decentralized and Self-Sovereign Identity in the Era of Blockchain: A Survey

Yirui Bai
School of Cyberspace Security
Hainan University
Haikou, China
21210839000001@hainanu.edu.cn

Hong Lei
School of Cyberspace Security
Hainan University
Haikou, China
SSC Holding Company Ltd.
Chengmai, China
leiluono1@163.com

Suozai Li
China Electronics Corporation Hainan Joint Innovation Research Institute Co. Ltd
Chengmai, China
lisuozai@jiri.ac.cn

Haoyu Gao
College of Data Science and Application
Inner Mongolia University of Technology
Hohhot, China
20191800498@imut.edu.cn

Jun Li
School of Cyberspace Security
Hainan University
Haikou, China
Oxford-Hainan Blockchain Research Institute
Chengmai, China
junli@hainanu.edu.cn

Leixiao Li
College of Data Science and Application
Inner Mongolia University of Technology
Hohhot, China
llxhappy@126.com

2022 IEEE International Conference on Blockchain (Blockchain) | 978-1-6654-6104-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/BLOCKCHAIN55522.2022.00077

***Abstract*—With the emergence of concepts such as Metaverse and Web 3.0, digital identity plays a very important role as one of its infrastructures. The traditional digital identity model is no longer suitable for the requirements of the digital economy to some extent at this stage. The traditional centralized identity management system has many drawbacks. For example, the owner of the digital identity does not actually control his own identity, and there is a risk of easy disclosure and theft of identity information. Blockchain technology has the characteristics of decentralization, tamper-proof, traceability, etc., which can effectively solve the problems of centralized digital identity. After analyzing and summarizing the evolution trend of digital identity from centralization to decentralization, this paper focuses on the Self-Sovereign Identity (SSI) based on blockchain. Based on the analysis and comparison of various SSI implementation schemes, the development difficulties of blockchain digital identity are summarized and the future development direction is pointed out.**

Keywords—digital identity; blockchain; decentralization; self-sovereign identity

I. INTRODUCTION

In the current era of big data, and even in the future metaverse era, people pay more and more attention to privacy protection, so the trusted interoperability of identity and related credentials has become an urgent need [1]. But as people become more involved in the network, more and more frequent and major user data security incidents inevitably make people worry about their privacy and property security. For example, in 2018, Facebook broke out a data breach [2], and the privacy of nearly 50 million user data controlled by Facebook was leaked; in 2020, the election application developed by Likud Group was misconfigured and more than 6.5 million personal information of Israeli citizens were exposed. These large-scale data leakage incidents pose a great threat to the privacy and security of users. Users' personal information is not under the control of users themselves, and the frequent occurrence of various identity problems such as the abuse of users' real identity information without authorization has exposed the importance of user digital identity management, and there is an urgent need for security protection of user identity information.

The International Organization for Standardization [3] defines identity as "the set of attributes associated with an entity" (ISO/IEC 24760-1). Digital identity is the identity we present on the internet with information and numbers. Its core is to prove "I am me" by providing and verifying identity information. The main links of digital identity management include identity owner registration identity, identity provider issuing identity, identity relying party verifying identity, and management of identity information and data. At present, the traditional centralized model is widely used in daily life, but there is a risk that identity information is easily leaked and stolen, because the user's identity is controlled by centralized organization, and the user has no control over personal identity data.

With the characteristics of decentralization, multi-party consensus, transparency, tamper-proof and traceability [4], blockchain technology provides a credible solution for the security transformation of digital identity. The decentralized identity management scheme based on blockchain technology has the characteristics of distributed data storage, point-to-point transmission, encryption security, consensus confirmation, etc., which can effectively solve the problems of identity verification and operation authorization [5]. The proposal of Self-Sovereign Identity (SSI) further emphasizes the user's control over the identity, requiring users to truly own their identities, not just let the user participate in the authentication process.

The main contributions of this paper are as follows:

- In this paper, we summarize the advantages and disadvantages of the models generated by the four stages of the evolution of digital identity from centralization to

This work was supported in part by the National Key R&D Program of China (No.2021YFB2700601); in part by the Finance Science and Technology Project of Hainan Province (No.ZDKJ2020009); in part by the National Natural Science Foundation of China (Nos.62163011).

978-1-6654-6104-7/22/$31.00 ©2022 IEEE
DOI 10.1109/Blockchain55522.2022.00077

decentralization, and analyze the existing challenges of blockchain-based digital identity.

- We combine the development history of the internet to illustrate that decentralized identity is a very important practice of Web 3.0.
- We analyze the four-layer architecture of SSI layer by layer and explain the technical implementation of each component in detail. Then we analyze a variety of decentralization and SSI implementation solutions, and finally expound the current challenges in four aspects: users, regulation, right to forget, and landing promotion, and the future development direction is prospected.

The sections of this paper are arranged as follows. Section 1 provides an overview of digital identity and blockchain-related concepts. Section 2 introduces the development of digital identity. We expound the main technologies based on blockchain digital identity in section 3. Section 4 presents the main techniques of the SSI model. Then we introduce the challenges of the development of distributed digital identity in section 5. Finally, section 6 summarizes the work of this paper.

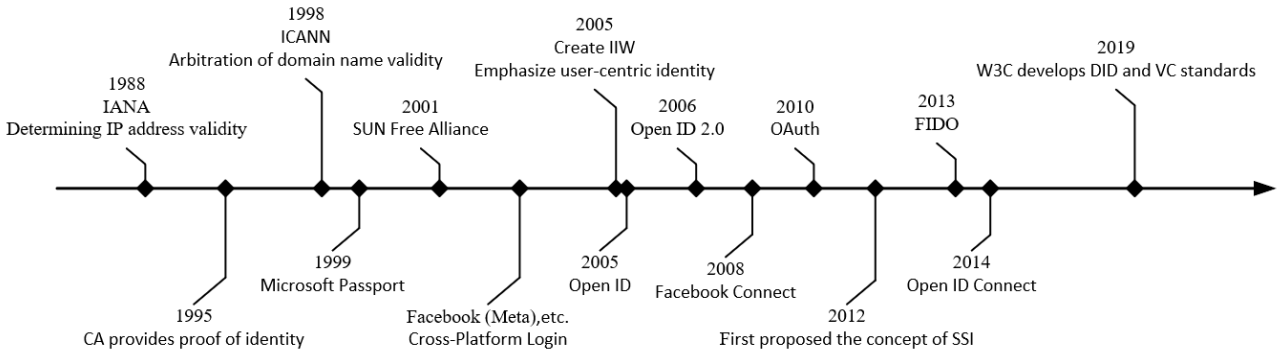

Fig. 1. The timeline of digital identity development.

II. Status and Challenges of Digital Identity

A. The Evolution of Digital Identity

The development of digital identity has gone through the stages of centralized identity, federated identity, user-centered identity and SSI, and gradually develops from a centralized to a decentralized model [6]. The hallmark of the era of centralized identity is that we use usernames and passwords to log in to all websites, and the account behind represents a real individual. The cross-platform login of Facebook (Meta), Instagram, Twitter, WeChat and Alipay is a sign of federated identity. User-centric identities give users control over their identities. In the SSI model, users can control not only their identity but also the data associated with it. Figure 1 summarizes the evolution of digital identity in time order.

1) Centralized Identity

In the early days of the internet, the government was the sole initiator and certifier of digital identities. The Internet Assigned Numbers Authority (IANA) was responsible for determining the validity of IP addresses. Later, the Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for arbitrating the validity of domain names [7]. However, as the number of websites continues to grow, centralized identities bring a lot of confusion and limitations, and users need to deal with multiple identities on dozens or even hundreds of websites with corresponding numbers. And these identities are controlled by authorities rather than users, which makes them prone to problems such as identity information leakage and high trust costs.

2) Federated Identity

The Passport program [8] launched by Microsoft in 1999 first proposed the concept and solution of "federated identity", allowing users to gain access to multiple websites through a single login. SUN organized the "Liberty Alliance" in 2001 to provide consumers with a single sign-on function for different websites. Some large social networking sites also gradually support single sign-on, such as Twitter, Facebook, WeChat and so on. Although the form of alliance helps to solve the problem of identity fragmentation to a certain extent and allows users to freely access multiple systems, each individual website is still a center, and there is no mutual recognition between large systems.

3) User-centric Identity

In 2001, the Identity Commons [9] began to integrate all work on digital identity and focus on decentralization, which also promoted the creation of the Internet Identity Working (IIW) Group in 2005. IIW emphasizes user-centric identity, putting the user front and center in the process of creating an online identity. IIW supports a number of projects that create digital identities, including OpenID (2005) [10], OpenID 2.0 (2006) [11], OpenID Connect (2014), OAuth (2010) [12], and FIDO (2013). Users store authenticators and certificates issued by different service providers in their personal devices, so users can control their data.

In the user-centric identity model, users, through authorization and permission, can decide the storage and use of identities and the sharing of identities from one service to another [13]. However, user-centric identity initiatives have not been successful. Taking OpenID as an example, users can theoretically register their own OpenID and use it independently, but due to the high technical threshold, most users prefer to register OpenID on a public and relatively reliable website to log in to other websites. Therefore, the OpenID registered by the user is at risk of being deprived by the service provider at any time, which also means that the user does not have full control of his identity data.

4) Self-Sovereign Identity

The concept of SSI was first referenced by Moxie Marlinspike in February 2012. SSI is an advanced stage of user-centric identity [14]. Both have in common that they start from the point of view that users are in full control of their identity data, but SSI goes further by decentralizing the collection, storage and use of data in an ecosystem. Also, for personal identity verification, other regular users are allowed to make statements containing the identity information of others.

For identity to be truly self-sovereign, its infrastructure needs to reside in an environment of decentralized trust, not owned or controlled by any single organization. Blockchain technology is a breakthrough to achieve this goal. The SSI based on blockchain technology allows users to truly own and control their own personal data and assets, forming a decentralized network with the features of ensuring the authenticity and validity of data. A comparison of the characteristics of the four models resulting from the four stages of digital identity development is rendered in table I [15].

TABLE I. COMPARISON OF THE CHARACTERISTICS OF FOUR MODELS.

Model name	Identifiers Generation of User	Credentials Ownership of User	Key Recovery	Optional Disclosure	Information Silo	Support Pseudonyms	Centralized Storage
Centralized Identity	×	×	√	×	×	×	√
Federated Identity	×	×	√	×	√	×	√
User-centric Identity	×	√	×	×	×	×	×
Self-Sovereign Identity	√	√	√	√	×	√	×

B. Web 3.0 and Decentralized Identity

Looking back at the development of the internet [16], the first stage of the internet, Web 1.0, was from the 1980s to the early 2000s, when internet services were built on open protocols controlled by the internet community. The second phase, Web 2.0, is from the beginning of the 21st century to the present, pushing the world from a simple static web page to an interactive experience, user-generated content, and a market economy, with Software as a Service (SaaS) built by for-profit technology companies becoming a major part of the internet [17], such as Facebook, Tencent, and other internet giant companies. Based on the unfairness and data security issues of the existing network business models mentioned above, more and more people believe that the network needs to enter the next stage of Web 3.0, and the emergence of encrypted networks makes this possible.

Web 3.0 is a term used to describe the internet-based metaverse. In other words, its virtual world will exist online and be accessible through your web browser. The core goal of Web 3.0 is to empower its users by allowing them to control their data, protect their privacy and ultimately ensure their freedom through an open, censorship-resistant web [18]. At present, there are many projects chasing related opportunities in different fields, and the open-source code of the encryption community has allowed the related technologies and infrastructure to develop rapidly in just two or three years. Decentralized identity is a very important practice throughout the Web 3.0 landscape.

The metaverse digitizes the entire world, related to energy, the environment, tangible or intangible assets, and only digital identities are truly related to "people". Without a corresponding digital identity, everything in the metaverse cannot be connected to us [19]. The development of a digital identity system is inevitable, and blockchain technology also provides a relatively credible solution to some extent.

III. BLOCKCHAIN-BASED DIGITAL IDENTITY

In the blockchain-enabled digital identity, with the help of asymmetric encryption, the private key owner uses his public key as the unique identifier of the identity, and then associates the identity attributes through smart contracts [20]. At the same time, because of the decentralized nature of the blockchain, service providers do not need to maintain user identity storage, and the method of disclosing or authorizing from the blockchain is unified. In this case, users have complete control over their data and can decide when and how to share this data with others.

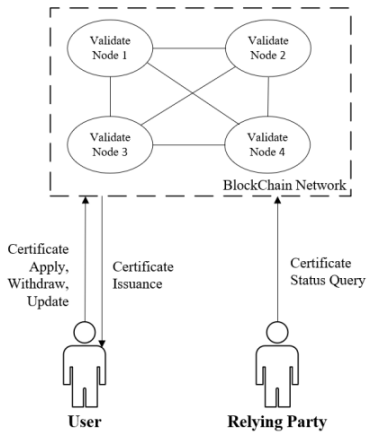

Fig. 2. Blockchain-based PKI system usage process.

A. Distributed Authentication

At present, the identity authentication system based on Public Key Infrastructure (PKI) is the most popular method. The core of the traditional PKI system is the digital certificate and the certification authority (CA).

Aiming at the problems caused by the centralized issuance of CA, such as central failure and network security, blockchain technology can realize distributed digital certificate issuance, so that the digital certificate issued by the centralized CA certification center in the past can be realized by the distributed ledger of blockchain [21]. One solution way is that the accounting and maintenance of the blockchain can be done jointly by all certificate holders in the system. The second way is to form a blockchain between CAs, so that the CAs do not have to trust each other, and the issuance and management of digital certificates are completed in a consensus manner.

As figure 2 shows, blockchain-based PKI can realize certificate application, issuance, verification and management of traditional PKI systems [22].

1) Certificate Application: The certificate user initiates a certificate application request to the blockchain network, which includes the user's digital certificate and the information required to verify the certificate.

2) Certificate Issuance: First, the verification node in the blockchain network collects the user's certificate application request, and verifies the validity of the certificate according to the information submitted by the user. Then, the verification node uses the current legal certificate information and certificate status not included in the block as records in the blockchain, and uses the consensus mechanism in the blockchain to generate a new block. Finally, the verifying node publishes the new block to the blockchain network and synchronizes it to other nodes.

3) Certificate Revocation: The user submits a certificate revocation request, which includes the user's certificate and information that can prove the user's identity. After the verification certificate revocation request is passed, the verification node will upload the legal certificate information and certificate status that are not included in the block.

4) Certificate Update: The user needs to generate a digital certificate with the same Distinguished Name (DN) item as the original certificate. The verification node will verify the chain.

5) Certificate Usage: After receiving the certificate, the relying party needs to initiate a certificate query request to the blockchain network to check the validity of the certificate. Finally, the node in the blockchain feeds back the query result to the relying party, and the query result contains the latest status information of the certificate to be checked.

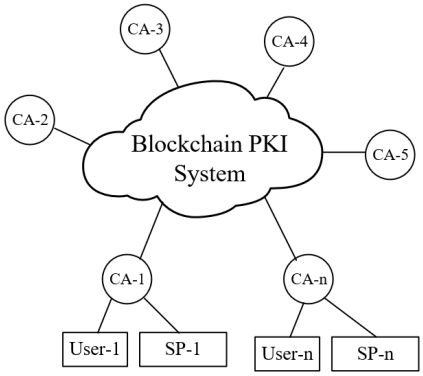

Fig. 3. Schematic diagram of multi-CA mutual trust scheme.

Suppose the verification node is limited to a specific CA. In that case, that is, in the form of a consortium blockchain [23], the CA will complete the verification of the user certificate through consensus. The consensus certificates will be recorded in the blockchain, and then these certificates will be considered as trusted certificates by all CAs in the blockchain. The role relationship of the multi-CA scheme is shown in figure 3.

B. Cross-agency Security Identity Authorization

At present, digital identity data is scattered and difficult to share, and traditional identity authorization methods are not secure enough. Under the background that unified identity cannot be quickly realized and mature, the distributed ledger of blockchain can be used to make identity sharing and authorization more secure [24]. The core idea is to identify and recognize each other's login requests and authorize access to the corresponding user data through the form of consortium blockchain, forming a trusted and secure identity information interoperability system.

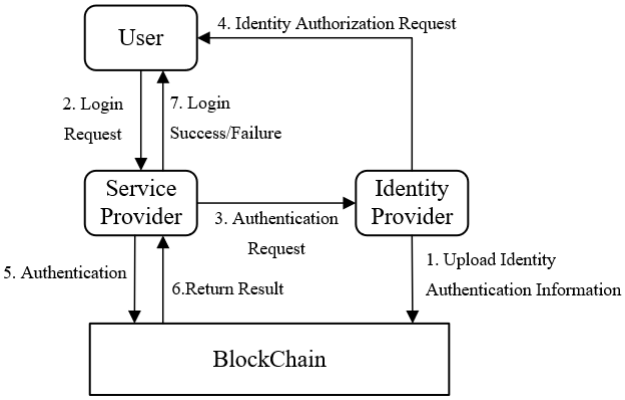

Fig. 4. Cross-institution blockchain identity authorization process.

The cross-agency security identity authorization is shown in figure 4. The specific process is as follows:

1) The Identity Provider (IdP) with user data encrypts the user information to generate a private key and a public key, where the public key generates the digital signature of the IdP, uploads the public key and digital signature to the chain, and the private key is stored locally, such as a SIM card.

2) When a user logs in to Service Provider (SP) in the blockchain, the SP will initiate a request to the IdP with the user's identity information. After receiving the request, the IdP sends an authorization application to the user and waits for the user's consent.

3) After the SP obtains the user's authorization, it matches the user's identity on the chain. After the matching is successful, it means that the user's identity is recognized and can be logged in.

In this way, the SP mainly relies on the credit of the IdP, and can complete the authentication without obtaining user information, which protects the user's privacy. The SP itself can also be used as an IdP to provide user identity authorization for other applications to form a distributed trusted identity network.

IV. SELF-SOVEREIGN IDENTITY

Blockchain provides a distributed trust environment and is a necessary technology for realizing SSI. The SSI model differs from the centralized and federated identity models in that it does not require the IdP and SP to manage credentials and authenticators on behalf of the user. The role of the IdP is limited

to the identity issuer, that is, it only issues identities and does not manage identities on behalf of users.

A. SSI Architecture

The core technology of SSI is distributed ledgers and cryptography, which can be combined with distributed digital identity identifiers and verifiable credentials to create non-repudiation and tamper-resistant identity records [25]. Figure 5 shows the four-layer architecture of SSI.

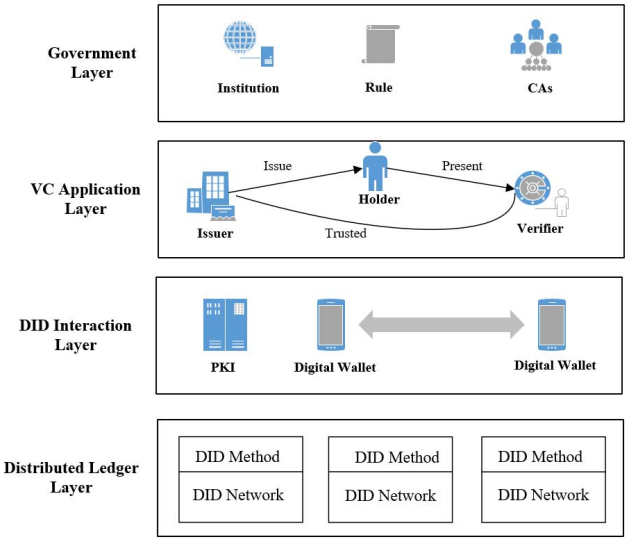

Fig. 5. The architecture of the SSI.

The first layer of the SSI architecture is the distributed ledger, which is used as a registry of distributed digital identity identifiers, so that no third party can have access to the identifier as long as it ensures that the identity owner maintains control of his or her private key. The characteristic of non-tamping of the distributed ledger makes it suitable for both the publication and maintenance of distributed digital identity data and for verifier verification of credential authenticity. The second layer is the combination of the PKI system based on distributed ledger and digital wallet to realize end-to-end interaction between users and perform activities such as certificate application, issuance, update and revocation. As a personal repository, digital wallets can realize user identity information and VC off-chain storage, so that the control of the identity truly returns to the user's hands. The third layer is the VC application layer, which implements the VC interaction of the three entity roles of the issuer, holder and verifier. In the SSI model, users are the central administrators of their identities, and they have far more control over their own data and information than anyone else owns, knows about, or shares. The fourth layer is the governance layer, where business and legal protocols need to be established to build human trust in a distributed network. In current implementations of digital identity solutions, the governance model establishes principles, policies, terminology, standards, and responsibilities that define who is a certificate authority and where to find a list of trusted.

The two key technical concepts of SSI are two new standards developed by the World Wide Web Consortium (W3C) in 2019, namely Decentralized Identifier (DID) [26] and Verifiable Claim (VC) [27], figure 6 shows a schematic diagram of the DID standard. DID provides a way for everyone to generate their own unique identifier to interact in the digital world. A VC is a digital credential owned by an individual that contains information or attributes about them such as name, date of birth, place of residence, etc.

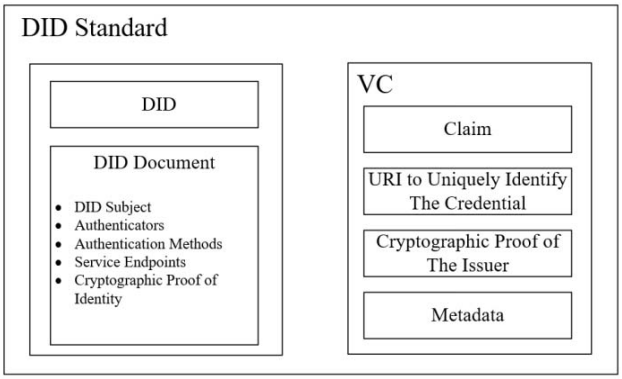

Fig. 6. DID standard composition.

The overall vision of the SSI storage approach is based on a personal portable device, where the user uses a personal repository to store and manage credentials, and it is up to the user to decide what information they want to publicly disclose. These repositories are usually digital wallets [28], which must allow users to minimize or selectively disclose information to other institutions, while preventing any third party from inferring the identities of entities in the semantics of the real world or other scenarios. In addition, digital wallets must guarantee a key recovery mechanism in case the digital wallet is lost or stolen. If a primary key is compromised, the secondary key can be used to revoke it or retrieve control of the identity. There are two types of key management systems available for key recovery: centralized and decentralized. Centralized Key Management Systems (CKMS) enable users to use a centralized key repository to store backups of their private keys and credentials so that they can be retrieved if the originals are lost or stolen, such as cloud storage [29]. In addition to cloud storage, offline backup is also an option, in which case digital wallets must be able to provide users with a secure mechanism for exporting keys to hardware. Decentralized Key Management Systems (DKMS) rely on multiple entities, individuals or nodes to store an individual's private key or private key seed. The algorithm commonly utilized by this approach is the Shamir secret sharing (SSS) [30] protocol.

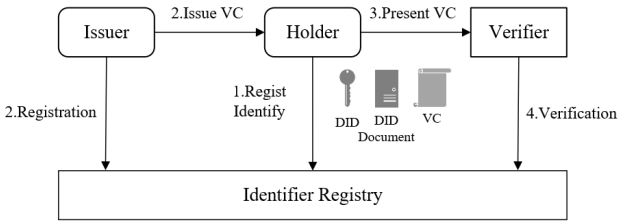

Fig. 7. SSI role relationship.

In 2018, Alexander et al. [31] proposed the relationship between different components of the VC application layer in a typical SSI architecture. Figure 7 shows the relationship between different participants in the SSI model. Issuer is an entity that owns user data and can issue VCs. Unlike IdP, the issuer does not manage certificates for users. Verifier is the SP that needs to verify the user's identity. The holder is generally a user or the user's identity agent, an entity that can request, receive, and hold a VC from the Issuer. The holder puts the issued VC in his personal repository for future use. The Identifier Registry is mainly used to maintain the database of DIDs, such as a certain blockchain and distributed ledgers.

B. Comparison of SSI project with Other Projects

In 2016, Christopher Allen [32] formulated 10 principles of SSI, including control, transparency, portability, consent, existence, access, minimalization, interoperation, persistence and protection, which have become a reference standard in the field. SSI models tend to focus on three elements [33]: user consent, interoperability, and the data is completely controlled by the user. Consent means that statements made by non-identity holders must be agreed to by the user in order to be valid. Interoperability means that digital identities should be as widely usable as possible. Control means that users must fully control their identities, relying on security algorithms to ensure the continued validity and readability of identities and their related claims.

Although SSI has been around for a short time, projects have already been launched. Table Ⅱ compares the SSI project with other representative distributed identity management projects, which helps us better understand the technical nature of the SSI model and its future direction. The comparative research objects selected in this study are ShoCard, WeIdentity, Microsoft DID, Cambridge Blockchain, uPort, and Sovrin, which are representative projects with a certain time span, differences in program characteristics, and different scenarios.

ShoCard [34] is a blockchain-based decentralized identity storage digital identity management project, and uses SSI as a gateway to achieve its applications and functions. ShoCard network implements three functions: identity verification, exchange of proof of authorization audit, and exchange of proof of personal certificates. As an early solution, ShoCard is lacking in the scope of application and privacy protection. Its user digital identity is created by the identity provider and can only be used within the corresponding ecosystem.

WeIdentity [35] is an entity identity identification and trusted data exchange solution based on consortium blockchain identity launched by WeBank in 2019. Relying on authorities to provide Know Your Customer (KYC) services, and using the consortium blockchain as a connection center for each user role and a depository center for information, promote credible data exchange.

In 2019, Microsoft released its DID implementation scheme [36]. The scheme can be disassembled into three parts: Sidetree, Identity Overlay Network (ION), and DID. ION is a Bitcoin-based two-layer network that accesses the Bitcoin network through the Sidetree protocol, which avoids the performance problems of the Bitcoin network and can support even tens of thousands of data throughput per second.

Cambridge Blockchain [37] is a company that makes digital identity software that simplifies the storage, sharing, and verification of personal data by using the most advanced privacy-preserving technologies and secure systems, providing an effective solution for businesses. The goal is to help financial institutions meet the toughest new data privacy rules (such as GDPR), eliminate redundant identity compliance checks, and proactively cater to regulation while reducing costs.

uPort [38] is a distributed digital identity management service based on Ethereum, which allows users to perform authentication, no password login, digital signature and interact with other applications on Ethereum. However, since the uPort identity relies on the Ethereum blockchain and does not provide the certificate service in the traditional management system, it is necessary to cooperate with various Issuers to help users obtain more VCs [39], which is a huge problem for the uPort project.

Sovrin [40] is a public chain project dedicated to realizing SSI, which can provide blockchain-based digital identity. The goal of the network is that anyone can issue a certificate containing a digital signature that others can verify [41]. The Sovrin project has made a lot of progress in the field of identity authentication, but in terms of the accuracy, coverage and ecological construction of on-chain information [42], Sovrin still has many technical problems to solve.

TABLE II. COMPARISON OF SSI WITH OTHER DISTRIBUTED IDENTITY SCHEMES.

Project	DLT	Storage	DID Method	Interoperability	Selective Disclosure	Auth
ShoCard [34]	Blockchain	Off-Chain	W3C compliant	Yes	No	Yes
WeIdentity [35]	FISCO-BCOS	On/Off-Chain	W3C compliant	No	No	No
Microsoft DID [36]	Multi-chain ledger based on Azure cloud service	-	DID: ion-test DID: test	No	-	Yes
Cambridge Blockchain [37]	Privacy blockchain	Off-Chain	Unknown	No	No	Unknown
uPort [38,39]	Ethereum	Off-Chain	W3C compliant	Yes	Yes	No
Sovrin [40,41,42]	Sorvin Ledger	On/Off-Chain	W3C compliant	Yes	Yes	Yes

V. Discussion and Future Directions

Although the SSI model solves the problem of user control, in the era of further intensified data interconnection in the future, it is conducive to improving the authenticity of data, protecting the privacy of user data, and can effectively reduce the negative impact of external factors [43], For example, network disconnection, network partition, etc.

A. Challenge

Some of the challenges in building a viable and effective SSI architecture are explained below.

1) User Experience: High threshold for private key management and use of identifiers

The aforementioned DID sacrifices human-readable properties in order to ensure distribution and security, and the text of the identifier is usually complicated and difficult to remember. At the same time, if the user uses multiple DIDs in order to further improve privacy and security, then each identity information (such as ID card, phone, driver's license, etc.) corresponds to a DID. So that it will be doubly difficult to manage DIDs and less acceptable to users.

In the same way as the private key, it is also a long string that is difficult to remember, and the private key is kept by the user. If the user wants to completely control his own data, the private key is theoretically known only to the user. Once the private key is lost, the corresponding data will be lost. Higher barriers to use can lead to lower acceptance of this approach.

2) Regulation

In order to safeguard the protection of people's data and information, regulations on data privacy and protection are also required, as well as regulations on electronic signatures, transactions, certificates, timestamps, etc. The promotion of SSI depends on the recognition of the legal value of elements such as blockchain network, DID, VC and digital wallet [44]. But at present, there are many countries that do not have regulations on electronic signatures and transactions, and even some countries do not have regulations on data protection and privacy.

On the other hand, although SSI has made a significant breakthrough in protecting users' personal privacy [45], it also raises the difficulty for regulation. More and more criminal organizations are using encrypted information to complete illegal transactions, and since blockchain only guarantees that data information cannot be tampered after it is uploaded, but it cannot guarantee the authenticity and timeliness of information before it is uploaded. The SSI model cannot meet the requirements of regulators when they ask blockchain to provide encrypted information or tamper with related non-compliant transaction records.

3) Right to be Forgotten

The right to forget has been challenging to implement in previous digital identity management systems, as it means having to know exactly where the data is, and also be able to identify yourself to those who own it so they can ask them to delete it, and there is no personal data in an immutable and decentralized registry. SSI achieves the first two goals more easily than other digital identity models, but the third goal is relatively difficult to achieve [46]. Additionally, digital wallets should provide easy ways to track where and for what purpose a person's identifiers are used, allowing requests for deletion.

4) Commercial Landing Promotion: the realistic conflict between user data privacy and enterprise data realization

In distributed digital identities including SSI models, due to the tendency to protect user data privacy, information disclosure is minimized [47], and only authentication results are shared. However, at present, a large number of internet companies implement business models based on user big data analysis, such as advertising business, financial business, e-commerce business, etc. These businesses need to be carried out based on the user's identity information. There are real conflicts in conservation that are difficult to reconcile. Companies with data as their core business model have no incentive to participate in such a decentralized digital identity system, so many current SSI applications have not been very successful. For the promotion of SSI, on the one hand, it is necessary to rely on the privacy awareness of users themselves, and on the other hand, the government needs to provide policy support or launch official standards for such digital identities to protect user privacy, so as to promote enterprises to change their business models.

B. Future Directions

With the integration of new standards and protocols, further development of complete SSI solutions, both public and private, in the three areas of regulation, technology, and trust frameworks can be achieved. The development of decentralized identity models will also evolve as laws, regulations and social systems evolve. In the next decade, with the continuous improvement of legal infrastructure, SSI may emerge in line with its own development of standardization, legal norms and other related supporting facilities to play its best role. The world will unify the standard of DID, and DID in the benefits and fairness to find a balance point. The regulator to verify the person or storage institutions to access the DID system, strengthen supervision at the same time to ensure the privacy of users, to achieve data truly in the hands of the user.

VI. Conclusion

This paper focuses on the field of SSI models, an emerging concept where users have absolute control over personal data information, which makes it more desirable than the current way data is stored in the metaverse. SSI has the potential to solve data security and privacy concerns because it does not require storing personal information in a central database, but instead gives individuals control over the information they store and share. This level of proven and decentralized trust is essential to bring data elements together for a unified and open metaverse.

The SSI model has the characteristics of supporting interoperability between different solutions, data portability, pseudonymization, traceability, scalability, etc., and introduces innovative solutions for managing personal digital identities. It is important to note that when developing a complete SSI solution, attention must be paid to international standards and protocols to ensure scalability and interoperability. The implementation of the SSI model is still in the early stages, but the pace of development is very fast, and the number of solutions around the SSI model is growing rapidly, which is very exciting.

REFERENCES

[1] Chen Jidong, Legal Imagination Beyond the Metaverse: Digital Identity, NFT and Multiple Regulations [J/OL], Research on the Rule of Law, 2022(5), pp. 1-12.

[2] Jin Yuanpu, Investigation and analysis report on personal privacy data leakage in the era of big data [J], Journal of Tsinghua University (Philosophy and Social Sciences Edition), 2021, 36(01), pp. 191-206.

[3] "IT Security and Privacy, A framework for identity management - Part 1: Terminology and concepts", International Organization for Standardization. (2019), (ISO/IEC Standard No. 24760-1), Available: https://www.iso.org/standard/77582.html

[4] Zhang Liang, Liu Baixiang, Zhang Ruyi, Jiang Binxin and Liu Yijiang, Overview of Blockchain Technology [J], Computer Engineering, 2019, 45(05), pp. 1-12.

[5] Zhang Tao, Li Rui and Wei Lei, et al., Research and Verification of Decentralized Digital Identity Based on Blockchain [J], Communication Technology, 2021, 54(10), pp. 2398-2402.

[6] Lennart Ante and Constantin Fischer, A bibliometric review of research on digital identity: Research streams, Journal of Manufacturing Systems, 2022, vol. 62, pp. 523-538.

[7] "A brief history of digital identity in time from 1995 to 2018", Available: http://www.lianmenhu.com/blockchain-6328-1.

[8] Microsoft and Oracle create open standard for Covid 'passports'[J], Biometric Technology Today, 2021, vol. 2.

[9] "Comparison and Research of Four Distributed Digital Identity Architectures", China Banknote Blockchain Research Institute.

[10] Lung Hsing Kuo, Fong Ching Su and Hung Jen Yang, Identifying the Efficiency of OpenID by Simulation Design[J], International Journal of Computers, 2018(12).

[11] D. Recordon and D. Reed, "OpenID 2.0: a platform for user-centric identity management," in Proceedings of the second ACM Workshop on Digital Identity Management, Virginia, USA, 2006, pp. 11–16.

[12] Sharif Amir, Carbone Roberto, Sciarretta Giada and Ranise Silvio. Best current practices for OAuth/OIDC Native Apps: A study of their adoption in popular providers and top-ranked Android clients[J]. Journal of Information Security and Applications, 2022, pp. 65.

[13] Cui Jiuqiang, Lv Yao and Wang Hu, The development status of digital identity based on blockchain [J], Cyberspace Security, 2020, 11(06).

[14] A. Preukschat and D. Reed, Self-sovereign identity: decentralized digital identity and verifiable credentials, Shelter Island: Manning, 2021.

[15] Marcos Allende López, "The Future of Identity: Self-Sovereignty, Digital Wallets, and Blockchain", LACChain Global Alliance digital identity working group.

[16] Chen Xi. Web3.0 Era: Everything you create online belongs to you [N]. Science and Technology Daily, 2022 (04).

[17] "Decentralized Identity (DID) Research Report: Important Practices of Web3.0 Development", Available: https://www.ccvalue.cn/article.html.

[18] "A series of reports on the application of infrastructure industry in the digital economy era", Fire Chain Technology Research Institute.

[19] Wolf, Alan, What To Know About The Chip-Card Conversion[J], TWICE, 2015, 30(19).

[20] Y. Jing, X. You, D. Bi and H. Li, "The Decentralized Identity and Its Application for Industrial Internet," 2021 3rd International Academic Exchange Conference on Science and Technology Innovation (IAECST), Guangzhou, China, 2021, pp. 671-674.

[21] Boyen Xavier, Herath Udyani, McKague Matthew and Stebila Douglas, Associative Blockchain for Decentralized PKI Transparency[J], Cryptography, 2021, 5(2).

[22] Maurizio Talamo, Franco Arcieri, Andrea Dimitri, Christian H and Schunck. A, Blockchain based PKI Validation System based on Rare Events Management [J], Future Internet, 2020, 12(2).

[23] Huang Yixiang, Wang Yawei, Chen Wenxuan and Zhang Zijiao, PKI cross-domain authentication model based on alliance chain[J], Computer Engineering and Design, 2021, 42(11), pp. 3043-3051.

[24] Zhang Yabing, Cross-domain authentication scheme based on blockchain [J], Computer Application Research, 2021, 38(06), pp. 1637-1641.

[25] E. Bandara, X. Liang, P. Foytik, S. Shetty and K. D. Zoysa, "A Blockchain and Self-Sovereign Identity Empowered Digital Identity Platform," 2021 International Conference on Computer.

[26] W3C. Decentralized Identifiers (DIDs) v1.0[EB/OL].[2020-04-08]. Available: https://w3c-ccg.github.io/did-spec/.

[27] W3C. Verifiable Credentials Data Model 1.0[EB/OL].[2020-01-15]. Available: https://w3c.github.io/vc-data-model/.

[28] N. Naik and P. Jenkins, "A secure mobile cloud identity: Criteria for effective identity and access management standards," in 2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud 2016), IEEE, 2016.

[29] I. Drago et al., "Inside Dropbox: Understanding personal cloud storage services," in Proc, ACM Conf., Nov. 2012, pp. 481–494.

[30] Abdel Hakeem Shima and Kim HyungWon, Centralized Threshold Key Generation Protocol Based on Shamir Secret Sharing and HMAC Authentication[J], Sensors, 2022, 22(1).

[31] Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya and Christoph Meinel. A survey on essential components of a self-sovereign identity, Computer Science Review, vol. 30, 2018, pp. 80-86.

[32] C. Allen, The path to self-sovereign identity, 2016, Accessed: 31/1/2018. [Online], Available: http://www.lifewithalacrity.com/2016/04/the-path-toself-soverereign- identity.html.

[33] Y. Jing, J. Li, Y. Wang and H. Li, "The Introduction of Digital Identity Evolution and the Industry of Decentralized Identity," 2021 3rd International Academic Exchange Conference on Science and Technology Innovation (IAECST), Guangzhou, China, 2021, pp. 504-508.

[34] Travel Identity of the Future - White Paper, SITA, ShoCard, 2016(3).

[35] "Blockchain-based distributed identity solution compliant with W3C DID and Verifiable Credential specifications", Available: https://github.com/WeBankBlockchain/WeIdentity.

[36] Stokkink, Quinten and Pouwelse, J.A, "Deployment of a Blockchain-Based Self-Sovereign Identity". 2018, pp. 2-230.

[37] Cambridge Blockchain Society, Available: https://cambridgeblockchain.org/?utm_source=cypherhunter.

[38] N. Naik and P. Jenkins, "uPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain," 2020 IEEE International Symposium on Systems Engineering (ISSE), Vienna, Austria, 2020, pp. 1-7.

[39] C.Lundkvist, R.Heck, J.Torstensson, Z.Mitton and M.Sena, "uPort: A Platform for Self-Sovereign Identity". 2017, vol. 2.

[40] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity", The Sovrin Foundation, 2016.

[41] D. Reed, J. Law and D. Hardman, (2016) The technical foundations of Sovrin. [Online]. Available: https://sovrin.org/wp-content/uploads/2018/03/The-Technical-Foundations-of-Sovrin.pdf.

[42] N. Naik and P. Jenkins, "Sovrin Network for Decentralized Digital Identity: Analysing a Self-Sovereign Identity System Based on Distributed Ledger Technology," 2021 IEEE International Symposium on Systems Engineering (ISSE), Vienna, Austria, 2021, pp. 1-7.

[43] B. N. Eddine, A. Ouaddah and A. Mezrioui, "Exploring blockchain-based Self Sovereign Identity Systems: challenges and comparative analysis," 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), France, 2021, pp. 21-22.

[44] Stokkink, Quinten, Pouwelse and J.A, "Deployment of a Blockchain-BasedSelf-Sovereignldentity, 2018, pp. 2-230.

[45] K. Gilani, E. Bertin, J. Hatin and N. Crespi, "A Survey on Blockchain-based Identity Management and Decentralized Privacy for Personal Data," 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), France, 2020, pp. 97-101.

[46] J. Kaneriya and H. Patel, "A Comparative Survey on Blockchain Based Self Sovereign Identity System," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), India, 2020, pp. 1150-1155.

[47] N. Naik and P. Jenkins, "Governing principles of self-sovereign identity applied to blockchain-enabled privacy-preserving identity management systems," in 2020 IEEE International Symposium on Systems Engineering (ISSE). IEEE, 2020.