Decentralized Identity Management: Prerequisiteof Web3 Identity Model

SUBMISSION DATE / POSTED DATE

03-08-2022 / 09-08-2022

CITATION

Bai, Pinky; Bisht, Charupriya (2022): Decentralized Identity Management: Prerequisiteof Web3 Identity Model. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.20424633.v1

DOI

10.36227/techrxiv.20424633.v1

Decentralized Identity Management: Prerequisite of Web3 Identity Model

Pinky Bai, Charupriya Bisht

Abstract: **Web3 is the evolution of internet requisites decentralized identity management known as a new paradigm in the identity management system. Web3 conceptualizes decentralization and based upon that needs an identity model that fulfills the requirement of any business/technology model in the new trusted third-party free era. This article presents Web3, Web3 architecture, and technologies expansion for secure and scalable services. Further, the decentralized identity management model is presented with its components (DID), reusable verifiable credentials (VC), issuer, verifier, and user centricity in perspective with the Web3 identity model.**

Keyword: **Web3, Decentralized Identity management, DID, VC.**

I. INTRODUCTION

Web3 marks a fundamental shift in standards as a new computing technology arises to solve real-world problems. Web3 is the next frontier of the internet revolution and promises an open source, permission-less decentralized computation, data storage, and peer-to-peer transactions. Web3 promises to remove third-party dependencies and ensure owners control their data and assets, providing a trustless environment among participants. The exponential growth of Decentralized Finance, Decentralized Applications, and Metaverse applications are signs of Web3 [1].

In this era of Web3 transformation, an individual's personal, professional, and consumer life are inter-mapped in a digital structure like a fabric. The identity of any physical entity is a unique secret that maps physical identity and digital realms. However, this secret is not so secret due to emerging data-based services and organizations those gain profit from breaching personal data[1,2].

According to a study by the "Mine" startup, around 350 different organizations hold users' personal data without users' knowledge. All these organizations are not so trustworthy, and users also do not provide consent to store their personal data. The biggest shortcoming of web2 is the uncertainty of users' data security and privacy. Web3 developed the problem's solution by detangling the customer and service provider relationship from the real-world identity. Web3 services allow a user to login into the system by connecting the cryptocurrency wallet without any Gmail or phone number unless it is essential. We cannot say that the web3 login system or identity system is perfect. There are phishing scams examples present in Web3 [3].

The rest of the article is organized as follows. The second section discusses Web3, its evolution, its architecture, and the technology case of web3. Web3 identity management, Identity Architecture, and the working flow of architecture, including identification and authentication, are discussed in the third section. Further, section 4 presents the successful identity models that are the sign of Web3 existence. The last section concludes the article.

II. What is Web3?

Web3 is simply an architecture of the world wide web that supports the internet and comes after two successful iterations, Web1 and Web2. Web3 came with the vision of decentralization, ownership, and user-centric; web3 focuses on a decentralized web where a user has control of their data, identity, and destiny. The first time, Wood proposed the concept of Web3 and defined Web3 as offering internet services to the users without trusted third parties and providing control to the user on their data. Many technologies facilitate the development of Web3. However, the backend is supported by the decentralized nature of blockchain. Blockchain helps in the development of Web3 by providing distributed data storage, distributed data access, and distributed data computation [4].

A. Evolution of Web

In 1960, the purpose of the internet invention was to serve the military rather than using the internet for virtual communication. The internet was released for public use in 1993 as Web1, a one-way communication channel between user and website owner. Web1 was unstructured and unsecured. Users can only read the content on the website in this era. Web1 presented raw information in static form without any hierarchal structure and integrated

identity. A New Yorker cartoonist published a cartoon as " When on the internet, nobody knows you are a dog " captioned image of a dog with a desktop defines the era of Web1. Web2 came up with more interactive websites where users can read an perform writing operations on the websites. Web2 was centralized and structured but not secure. Web2 was tied to identity, which means the user was identified as an entity on the internet. Google and Facebook are good examples of the websites of the Web2 era that redefined our internet experience. Centralized structure, the main characteristic of Web2, becomes the greatest flaw.

Web3 which up as a mark of the evolution of Web2 is a decentralized and secure structure. Now the websites are smart and are able to interpret user data to become more intelligent (Artificial intelligence). Web3 is decentralized and eliminates the third part everywhere. It enables trustless and peer-to-peer transactions all over the globe. The Web3 is about securely decentralizing most critical data like money, ownership, and identity and giving controls to the user, not the corporative. The evolution of the Web can be summarized that Web1 brought the revolution of information, and interactions were revolutionized in Web2 and Web3 had a vision of agreement and value revolution. Web3 promotes and supports distribution and decentralization concept to design a solution for real-world issues. [1,2].

B. Architecture of Web3

Web3 foundation proposed a 5-layer (layer 0 to layer 4) technology stack for Web3 in 2017, and the same layered stack is referred to in further research and projects [5]. Fig 1 represents the architecture of Web3.

Layer 0 is the foundation of Web3, on which other layers are built. Layer 0 provides two components: peer-to-peer network capabilities and platform-neutral computation to support the other four layers in operations. Layer 1, the second layer of Web3, enables the data distribution and interaction. Layer 1 includes data distribution protocols, zero trust interaction protocol, and data subscriber and publishing messaging protocol. The enhancement of the layer 1 protocol is included in Layer 2 of the Web3 stack.

Layer 2 enhances layer 0 and Layer 1 of the Web3 stack. Layer 2 includes scaled and secured protocol of layer1. The storage is incentivized, encrypted, messages are shared in an encrypted format, and computation is enhanced at Layer2. Layer 3 includes the human-readable language, codes, and libraries that help in development. Layer 4 comes up on the top of the technology stack. A user interacts with stack technology at layer 4.

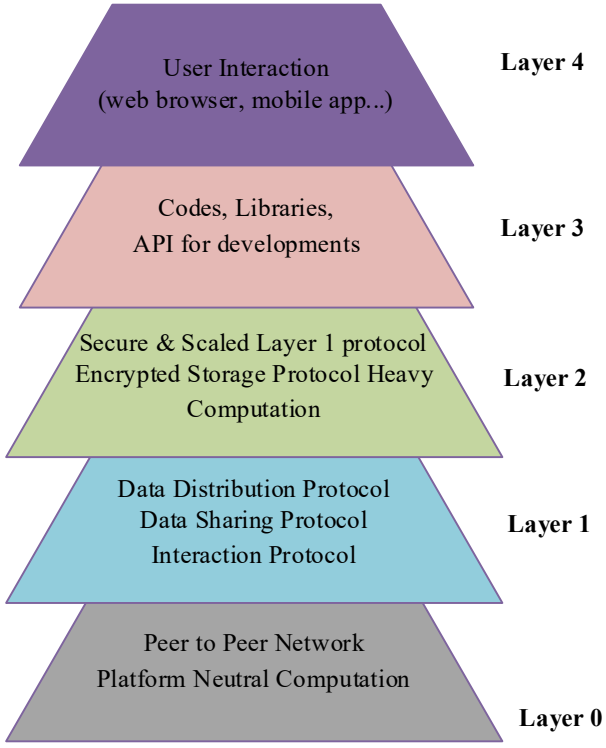

Figure1 web3 technology stack (Web3 Foundation)

C. Successfully emerged example of Web3

The generic idea of web3 is about shifting the centralized and trusted third party to a decentralized trustless structure. The quantity analysis of Web3 is complicated, so here the main, the main categories of Web3 enabled concepts are discussed:

1. Distributed Autonomous Organizations (DAO): DAO is based on peer-to-peer networks and open autonomy. Web3 is promoting the development of DAO by using the smart contract. Smart contracts improve readability and security as no competent authority can break the rules. In the DAO, all the processes starting from decision-making token distortion are on distribution channels. This configuration ensures transparency in the organization as no one can edit the rules/information available on the distributed ledger [6].

2. Decentralized Finance (Defi): If there is Web3, then Decentralized Finance cannot be avoided. The next main Web3-enabled paradigm is Defi. Defi uses smart contracts to unite borrowers

and lenders on a decentralized ledger. Defi is an advanced technological evolution in global finance after joining finance technology, regulatory technology, cryptocurrency, and digital assets. Defi uses one or more components of (1) Decentralization ; (2) Blockchain and DLT; (3) Token Economy; (4)Smart Contracts; (4) Web3, and (5) Open Banking.

The token economy, decentralized economy model, and Central Bank Digital Currency (CBDC), inspired by Bitcoin, are also fuel to Web3 [7].

3. Metaverse: Web3 is one of the enabler in Metaverse (decentralized Metaverse). Metaverse is combination of virtual reality, augmented reality and distributed ledger technology. Metaverse provide a virtual world to the user[7].

Other than the above-discussed part, decentralized Applications (dApps) that run on a peer-to-peer network and provide user-centric control to users also participate in Web3 [8]**.**

III. Web3 Identity Management

Identity management includes recognizing, validating, and allowing participants to access confidential data. The traditional/centralized schema of identity management has a trusted third party called relying party who issues the identities, manages the identity provider's credentials, and authenticates the user to access specific web services. In the decentralized identity management schema, the case is different. In decentralized schemas, the identity holders and identity verifiers agree on some protocol to exchange the identities without a third party.

Web3 is decentralized internet, decentralized computation, and has a decentralized identity model to provide the identity to each decentralized entity. With the growing demand for security and privacy, Web3 ensures security and privacy to the users. Web3 is user-centric, and the main concern is providing control to users of their assets, data, and identity. To fulfill this requirement, Web3 follows a decentralized identity model [9, 10].

A. Architecture

The architecture of the decentralized identity model can be described in figure 2. Figure 2 represents the relationships among entities and their respective tasks in the decentralized identity model. The three main actors of the identity model are the identity issuer, the identity verifier, and the user, the system's center. The user has complete control over the transaction in the identity system that is related to his asset, data, and identity. All the entities share a distributed ledger to perform their specific operations, like the user storing his public key to get the decentralized identifier (DID). The DID model working is defined in the same diagram. In distributed identity management, blockchain or any distributed verifiable registry replace the registration authority (trusted third party) in traditional identity management [11].

In the system, the identifier (DIDs) is tied with a specific user using cryptographic functions, and claims are tied with identifier. The identifier is paired with the public key on the blockchain and easily verified by the verifier by reading the blockchain. The user is the only one who directly manages the identifier claims. User stores actual identity claims offline such as identity wallets for privacy purposes.

Verifiers compare the identifiers available on the blockchain with the identifiers presented by the user in the credentials presentation to access some services. User authentication is performed with the authentication method stored on the blockchain and identifiers. The verifier accepts or rejects the user's request based on the authentication result.

In the above identification and authentication procedure, the user's personal information is not stored anywhere. Only trust between the issuer and verifier must be established before the process. The following sections will discuss the component of distributed identity model: Identification and Authentication.

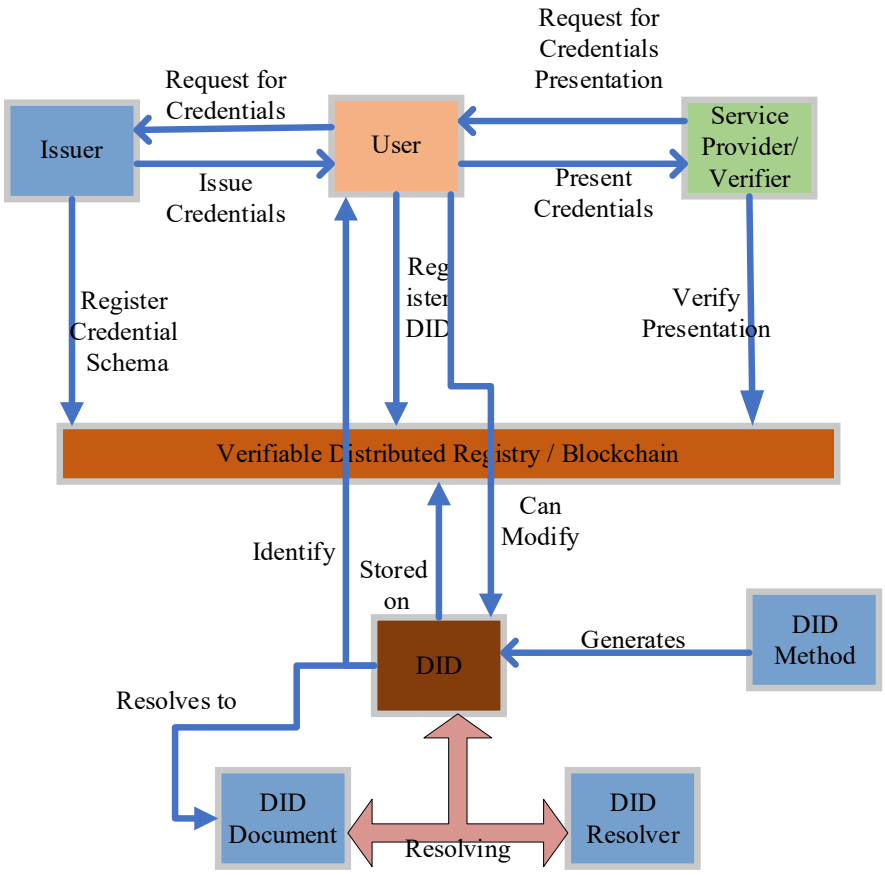

Figure 2 Identity Management in Web3 (*Ferdous et. Al, 2019, P. Bai et. al 2022*)

B. Identification

The essential requirement in any identity model is that identifiers should be securely unique. A decentralized identity model promises to generate random unique number identifiers. User share distributed identifier (DID) to the issuer to get the new Verifiable credentials (VC). The issuer issue the VCs on the request basis from the user.

To share DID, the user needs to first register for the DID. Users select the specific DID method and get the DID accordingly. DID is used as a core component in the decentralized identification model. DIDs can be defined as a unique global reference linked with a DID document and presented in the form of **did:<DID method>:< method specific identifier>**[11]. The DID method refers to a distributed network or ledger, and the method-specific identifier resolves DID to that network. Necessary components participating in identity creation are as follows:

1) **DID Documents and DID Method:** DID document has information about the identity like a public key. DID document also contains the reference to the service endpoint. Service endpoint where an issuer performs some task like storing the verifiable credentials (VC) in the VC repository. DID document has all information that require to resolve the DID.

DID methods define the generation of DID. DID method define how a DID document is written and updated. Further, DID method defines how DID is resolved into a specific document/ network/ distributed ledger [11].

2) **Verifiable Credentials**: Verifiable credentials are cryptographically secure, and privacy-protected machine-readable credentials are bound to identity through DID. DID document have the VCs. The issuer created the VC and sent it to the user, who presented the same VC to the verifier to authenticate himself. VC contains the set of claims about the user's

attributes like date of birth, name, email id, etc [12]. The issuer creates a new VC for the user, and VC includes the DID of the issuer and user and is signed with the issuer's DID.

C. Authentication

After receiving the VC, the user can create the presentation of VC (VP). VC contains multiple claims about the user; the user can select a single or multiple sets of these claims and create the VP. These VPs are presented to the verifier or service provider to authenticate the user.

D. Verification

Verifier gets the VP which contains one or more claims about the user. Verifier first resolves the DID into DID document of both issuer and user using the DID method. DID document has all the required information. After that verifier verifies the signature of the issuer and user attached with the DID document. After verifying the signature, the last step is to verify the claims to accept or reject the user communication.

IV. Identity management present in the market

Several distributed identity management models based on blockchain exist in the Web3 era. This section discussed some popular decentralized identity framework present in the real world such as Sovrin, uPort, Jolocom, and Hyperledger Indy [13].

A. Sovrin

Sovrin is an open source decentralized identity network based on a private blockchain in that only trusted participants can participate in the system. The Sovrin ledger (distributed ledger) is not publicly available. Only predefined or registered participants can access the services of the Sovrin system, which works according to the Sovrin framework. In the Sovrin, each public key has the address on the Sovrin ledger called DID, and these DID enable the universal verification of claims. Users can use different DIDs for each public and private key pair.

In the Sovrin architecture, the stewards are responsible for writing, distributing, and replicating the identity among permitted nodes. The user has complete control of identity and decides what attribute he wants to share with the service party. User has an endpoint on their phone and finds the trusted party endpoints with the help of the Sovrin ledger before sharing the information. Sovrin provides the attestation, anonymous credentials, and verifiable claims based on zero-knowledge proof. Sovrin has strong recommendations to use as an identity network based on identity recovery, unlinkability, DID, zero-knowledge proofs, web of trust approach, and Byzantine fault tolerance protocols characteristics. However, Sovrin has weak links, such as complex design architecture, no authentication services, less efficiency because of old cryptography used, and no support for smart contracts to modify the requirements.

B. uPort

uPort is also an open, decentralized framework that provides identity specific to banking and emailing. uPort uses Etherium blockchain and smart contract for the decentralized identity for the user.

The uPort framework has:

1. Mobile app or wallet for users to manage their identity
2. an uPort registry is a smart contract that links the attribute with the user ID
3. IPFS storage to store the hash of identities and DID documents

uPort provides control to the user on their data and offers minimal information disclosure. uPort has two significant weaknesses. First, the uPort registry is centralized, and authorities like the government could control the identity. Due to the uPort registry's centralization, attributes' metadata can be leaked. Thus, the relationship between the identity provider and the third party is not trustworthy and secure. A second private key stolen could breach all the user's data.

C. Jolocom

Jolocom framework is also based on Ethereum permission-less blockchain. Jolocom provides a provision to create the child DID to hide the real credentials of the user. The DIDs stored on the Ethereum blockchain along with the DID Document (DDO) that defines how to use the DID. Like uPort, Jolocom also has a wallet to store the cryptographic keys and credentials [12].

D. Hyperledger Indy

Hyperledger Indy is framework that provide decentralized identity and distributed Ledger. User get DIDs on the basis of information provided at the first interaction time like name and all. User can register, update, and revoke their DIDs any time. DDO and DID methods work accordingly.

V. Conclusion

This article presented the Web3 architecture and Web3 identity model along with some successful examples of distributed/Self Sovrin Identity models of identity management. The article concludes that

Web3 identity management aims to shift the authentication from a centralized authentication provider to a decentralized infrastructure. There is no integration of DID with the real-world identity owner, and cryptography is well established to create and prove the possession of DID. Web3 promises trust, privacy, and user control over their assets and identity.

REFERENCES

1. D. Knapp, J. C. Tate, "Blockchain 2035 The Digital DNA of Internet 3.0", 2019 ed., Andrew Blueshed LLC, SALISBURY, Maryland, 2019, pp 1- 512.
2. S. Voshmgir "Token Economy: How the Web3 reinvents the Internet", 2nd ed., 2020, pp 1-364.
3. U.W. Chohan, "Web3: The Future Architecture of the Internet?." Available at SSRN (2022).
4. G. Korpal, and D. Scott. "Decentralization and web3 technologies." (2022).
5. Web 3.0 Technology Stack, accessed via https://web3.foundation/about/ on 25th July 2022.
6. S. Wang, W. Ding, J. Li, Y. Yuan, L. Ouyang and F. -Y. Wang, "Decentralized Autonomous Organizations: Concept, Model, and Applications," in IEEE Transactions on Computational Social Systems, vol. 6, no. 5, pp. 870-878, Oct. 2019, doi: 10.1109/TCSS.2019.2938190.
7. DA. Zetzsche, DW. Arner, and RP. Buckley. "Decentralized finance." Journal of Financial Regulation 6, no. 2 (2020): 172-203.
8. J. Srupsrisopa, "Blockchain Technology: The Bridge to Web 3.0." Journal of Business, Economics and Communications 17, no. 1 (2022).
9. P. Bai, S. Kumar, G. Aggarwal, M. Mahmud, O. Kaiwartya, and J. Lloret. "Self-Sovereignty Identity Management Model for Smart Healthcare System." Sensors 22, no. 13 (2022): 4714.
10. M. S. Ferdous, F. Chowdhury and M. O. Alassafi, "In Search of Self-Sovereign Identity Leveraging Blockchain Technology," in IEEE Access, vol. 7, pp. 103059-103079, 2019, doi: 10.1109/ACCESS.2019.2931173.
11. D. Reed,, M. Sporny, D. Longley, C. Allen, R. Grant, M. Sabadello, and J. Holt. "Decentralized identifiers (dids) v1. 0." Draft Community Group Report (2020).
12. A.Sghaier Omar and O. Basir, "Decentralized Identifiers and Verifiable Credentials for Smartphone Anticounterfeiting and Decentralized IMEI Database," in Canadian Journal of Electrical and Computer Engineering, vol. 43, no. 3, pp. 174-180, Summer 2020, doi: 10.1109/CJECE.2020.2970737.
13. Š. Čučko and M. Turkanović, "Decentralized and Self-Sovereign Identity: Systematic Mapping Study," in IEEE Access, vol. 9, pp. 139009-139027, 2021, doi: 10.1109/ACCESS.2021.3117588.

Pinky Bai is a research scholar at Jawaharlal Nehru University, New Delhi. She also working as a Scientist with the Standardization Testing and Quality Certification organization under the Ministry of Electronics and IT, Government of India. Her research area includes IoT security and Privacy, Blockchain, and Smart Healthcare Security and Privacy. She completed her M. Tech from Jawaharlal Nehru University, New Delhi in 2017, and Completed her B. Tech from Rajasthan Technical University in 2015.

Charupriya Bisht is working as a Scientist with the Standardization Testing and Quality Certification organization under the Ministry of Electronics and IT, Government of India. She has more than 10 years of experience in the industry and 5 years of experience in the Security of websites, IoT, website accessibility, and Vulnerability assessment. She completed her M. Tech from Birla Institute of Technology, Pilani in 2016, and Completed her B. Tech from Banasthali University in 2011.