Current Application Scenarios and Use Cases of Web3 Identity System

Fenbushi Capital | 分布式资本

Follow

--

Listen

Share

A while ago, the ENS airdrop attracted much attention to decentralized domain names. It is true that decentralized domain names can be used as a Web3 identity. However, no matter in the real world or in Web2 or Web3 world, an identity system also includes identity verification and management. For example, in the real world, identity credentials such as a person's ID card, driver's license, or student ID must all be processed and issued by a centralized agency (attester). When this person wants to enter a bar for a drink, the guard at the door (verifier) will check their ID to verify their identity. People usually keep physical credentials in their wallets or purses. During this period, people still do their own identity management.

(This article was originally created by Fenbushi Capital and written by Cryptojade.)

When entering the Web2 world, the rules of identity verification and management are quite different. The World Wide Web was born 30 years ago with no digital identity design in its underlying protocol, thus anonymity became the norm. Our digital identities are mainly created through the traditional internet account model. The created IDs and passwords are managed by the service providers, and all users' online behaviors are also completely monitored by them. The problem that arises is that internet service providers are familiar with their users' online behaviors and carry out targeted marketing and advertising. They even sell their users' personal information for profit.

Due to the ever-increasing severity of identity leaks and privacy infringement, different industries have explored the 3rd generation of digital identities such as DID (decentralized identifier) and SSI (self-sovereign identity). As a result, blockchain and zero-knowledge proof technology have become the best solutions. Since entering the era of blockchain, wallet addresses have become new identities for users, and their safekeeping of the keys means their full control of on-chain identities.

But this still seems not to be perfect. First, it is unreadable; and secondly, it cannot be associated with Web2 identities and physical world identities. At present, most blockchain projects are aimed at solving the above problems. Otherwise, with the development of DeFi, NFT, and DAO, building an identity system on the blockchain will effectively regulate the industry. The built identity system will also derive different use cases on blockchain. For example:

1. One-click login

. The login method of Web3 will enable users to keep their own accounts and keys, which will overturn the traditional identity management by internet servers.Spruce ID

recently launched "Sign-in with Ethereum" in collaboration with ENS and the Ethereum Foundation. Users can sign in to internet applications such as Google and Twitter with their domain names and private keys. Since ENS is likely to be mass adopted, it is possible to innovate the Web2 identity system.

Recently, Ontology has also launched their identity login component "ONT Login". Users can use an address or DID for one-click login while quickly authorizing information, which simplifies the process of login.

2) NFTs and artists verification

. At present, many non-fungible token (NFT) platforms create a link between art works and creators' Web2 identities, which are shown as social media accounts, websites, and other platforms. However, Web2 identities cannot be displayed effectively in the long term. For now, NFT artists need to register DIDs to verify their Web2 identities. Currently, SertoID

has already demonstrated a real use case in this regard. The DIDs created by the NFT artists (one DID can correspond to several social accounts) can be displayed on the NFT works and will last forever regardless of whether the platform remained online.

In addition to a DID related to social and other virtual identities, NFT artists also need to perform real-name authentication.Ontology

has already implemented such cases. Ontology is currently cooperating with ROCKI, a decentralized music platform, to verify the identity of artists. Artists on ROCKI first need to complete the initial steps of the KYC/AML process to verify their identity. When the verification is successful, they receive a verifiable digital certificate that can be saved and managed by themselves. By applying the ONT ID registration management SDK, ROCKI can prevent perpetrators from impersonating

artists and prevent users from buying pirated music NFTs.

3) Member selection for DAO.

DAO members are recognized as a group of people with good on-chain reputations and devotion spirits within communities. With DID, it is possible to select members based on their on-chain behaviors, while also matching their contributions with corresponding incentives. A well-regulated DAO also requires a “one person, one vote” mechanism in terms of governance and voting.

BrightID

can prove that users only have one account, and any fake accounts or robot operations will be identified. Currently, BrightID has been applied to many dapps, such as Rabblehole, 1Hive and Gitcoin.

4) DeFi’s niche solution

. DID will improve the user’s credit system and open up corresponding use cases for DeFi. This reputation system is similar to Alipay’s Sesame Credit. Ontology’s OScore

has begun to build a credit system on blockchain. OScore will calculate your on-chain credit score based on your on-chain behavior and asset statistics. This score will also affect the interest rate and the mortgage rate for participating DeFi projects.

As one of Mina’s ecosystem projects, Teller Finance

can verify whether a user’s credit score is above a certain threshold to determine whether to lend to the user. The user logs in to the website that provides a credit score query, generates a zero-knowledge certificate locally, proves that their credit score is higher than a certain threshold, and puts this certificate on the blockchain. In this process, users do not reveal any private information such as their credit scores or social security numbers.

MetaFinance

is also playing its role in the identity system ecosystem. MetaFinance will use on-chain data records to define the profile of the identity (borrowing and repayment records, transfer records, etc.) , and use it to blaze a trail for more niche applications and use cases.

5) On-chain verifiable credentials

. Currently, as the underlying infrastructure, the Polkadot ecosystem project Kilt

, Ontology

, SpruceID

, etc. are all building their own verifiable credentials to replace physical ones. For example, Kilt introduces many real-world roles such as claimer, attester/trust entity, and verifier, so that there is no need for a centralized organization for the verification.

For example, suppose you want to register an application in order to verify your residency. Under the current system, you need to prove your right of abode by providing your passport or other official documents. In this way, the service provider can access not only your place of residence, but also any other information contained in these files. And all this information is kept on the attester’s server. However, kilt protocol will enable you to prove your residency without revealing any other personal information. The claimer will not share their entire passport, but only the so-called credentials, which can represent any verifiable information or attributes about the claimer. The credentials will be saved on the claimer’s device.

The above are just use cases when DID is applied to the blockchain. When DID is combined with trusted hardware and real-world oracle machines, it can also open up more offline application scenarios. DID is not necessarily a person’s identity, but can also be a machine or vehicle’s identity to record their usage. If DID is committed to the application of the IOTs and there will be a huge space for imagination and development. Industry leaders Ontology and IoTex have real use cases in this regard.

Back to the beginning, decentralized domain names such as ENS makes our wallet addresses readable, which is a big step forward for the Web3 identity system. How to expand on-chain identity into a profile, how to derive more use cases based on the identity, and how to associate Web3 identity with Web2 identity and physical world information, these are the things the industry is exploring and working hard towards. All in all, as people’s mindsets are changing day by day, the saying has transitioned from “mastering the private key means mastering property” to “mastering the private key means mastering identity.” Privacy protection will become the consensus of Web3, and this consensus will not only promote the integration of on-chain and off-chain identity systems, but also lead to the explosion of DeFi, DAO and NFT projects in the next phase.