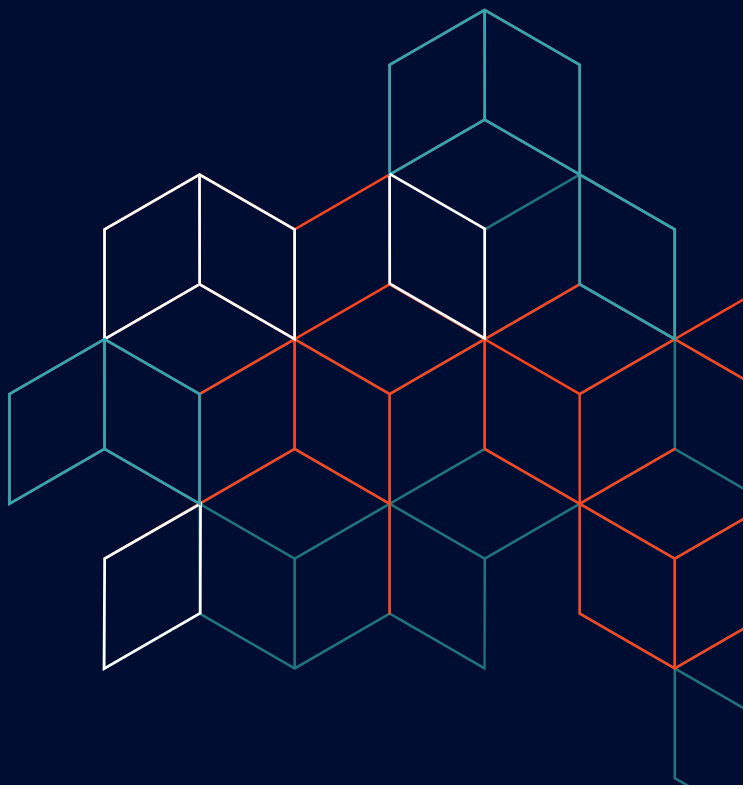
Onyx by J.P.Morgan

Digital identity – Assessing Web3's identity building blocks



Web3 is touted to be the next generation of the internet, promising a landscape where individuals not only have read and write capabilities on the internet, but also the ability to own and control their data, including digital creations, digital assets and digital identities. In this article, we dive deeper into what exactly digital identity is, what the building blocks that constitute one's digital identity are, and how digital identity can enable a new way for consumers and organizations to interact online. This is the second article in our series on digital identity. Read the article series here.

What is digital identity?

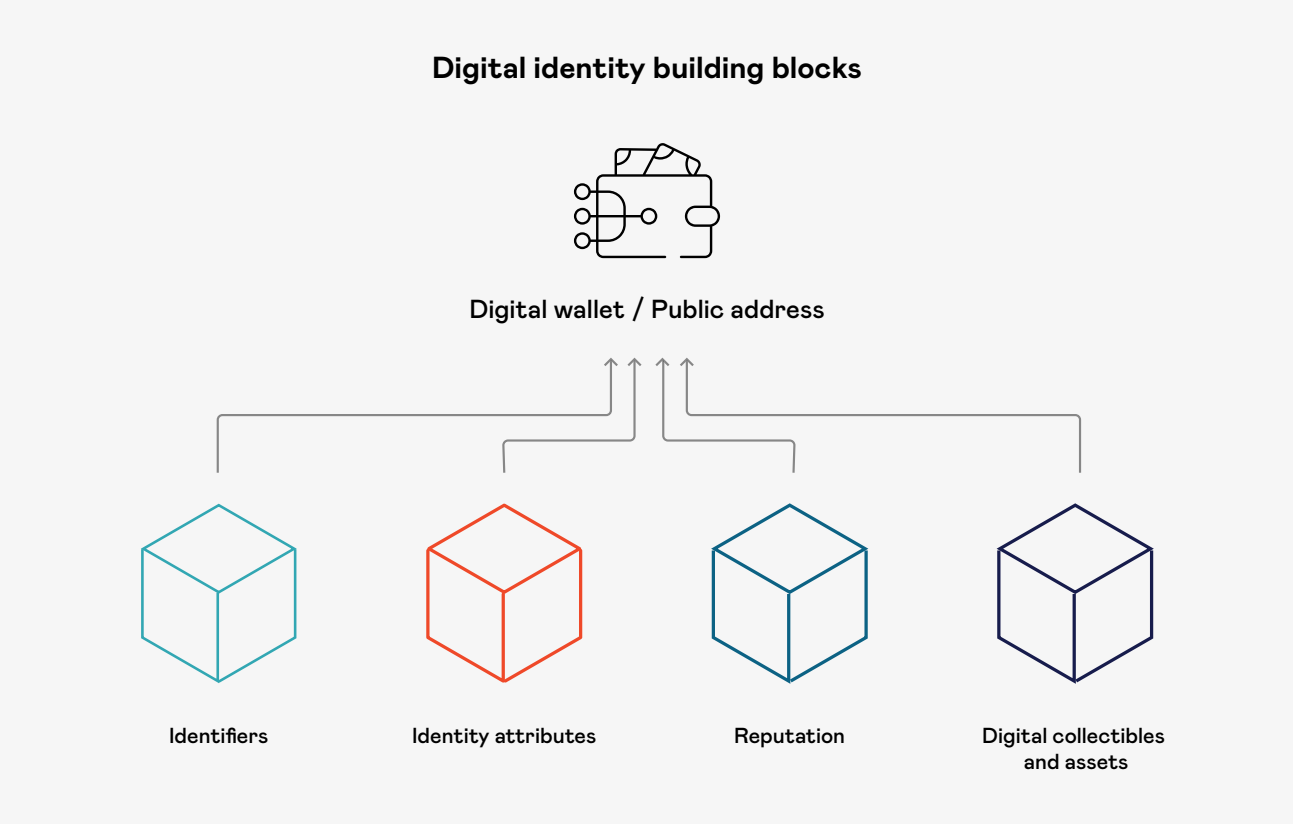
Digital identity can be defined as the way an individual or organization is identified and represented online or in the virtual world. A digital identity consists of the attributes that make up a legal identity (name, date of birth, etc.), as well as other aspects that relate to how a person or organization expresses themselves online. Currently, most data relating to our online digital identities is stored in and accessed through highly centralized or federated third-party systems. The promise of Web3 is that it allows users to retain control and access to their data and identities by leveraging decentralized networks and Web3 applications, protocols and technologies.

Digital identity could not only improve current identity ownership and verification processes, but it could also reduce fraud and enable new use cases that allow for greater self-expression and verification in Web2 and in Web3. Over the past few years, Onyx by J.P. Morgan and the wider digital identity community have been exploring Web3-compatible solutions to enable the melding of identity and ownership.

A bottom-up overview of the digital identity landscape

To better understand digital identity, it is useful to understand the aspects that make up our identity online. Digital identity is built on a foundation using various standards, frameworks, protocols and data models. The Web3 digital identity landscape can be categorized into four essential building blocks: identifiers, identity attributes, reputation and digital collectibles and assets – the combination of which form an individual's unique digital identity.

The sections below describe each of these building blocks in further detail.



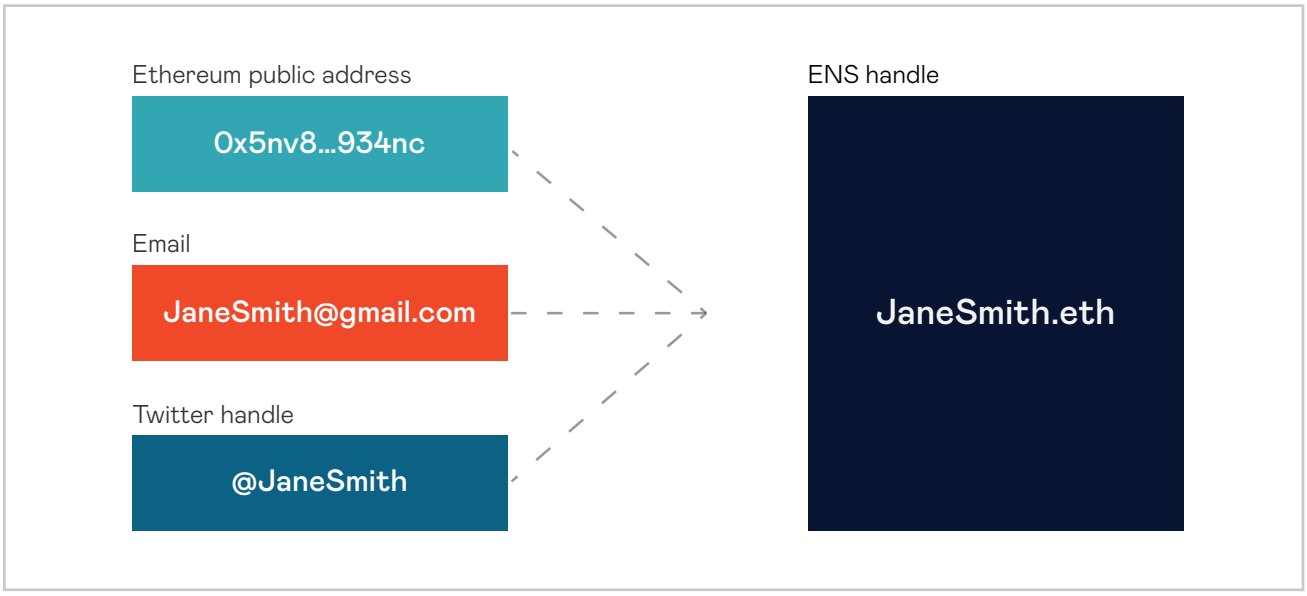
Identifiers

Identifiers are 'tags' that we use every day. Names, email addresses, account numbers, social handles are all forms of identifiers. In the context of blockchains, a person's 'public' blockchain address is their primary identifier for any blockchain-based interaction, and is typically a unique string of alphanumeric text.

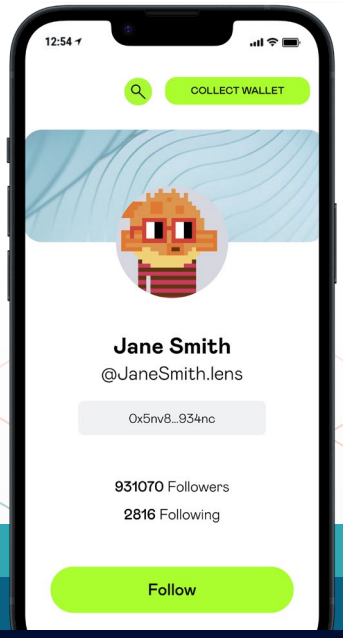
Web3 identifiers

Ethereum Naming Service (ENS), Unstoppable Domains, Lens handle, and several other naming services offer ways for users to add human-readable names to their public addresses. These services create a simplified and human-centric Web3 experience, because public addresses can be difficult to remember and share.

ENS is a naming system based on the Ethereum blockchain that enables users to represent their 42-character Ethereum public address using their ENS name. For instance, Jane Smith can create custom ENS identities to represent her personal and professional life. ENS not only encompasses Ethereum public addresses but it can also encompass addresses of several blockchains, Twitter handles, website URLs, email addresses, and Discord handles.



Lens is another system that enables the creation of identifiers in Web3. A key part of someone's Lens profile is their Lens 'handle'. A Lens profile enables a user to represent themself on the Lens social graph, and enables others to search for and discover their profile on the various Lens-based applications. Examples include Lenster, a decentralized and permissionless social media application, and Lenstube, a decentralized video sharing social media platform



Decentralized identifiers (DIDs)

DIDs are alphanumeric identifiers that represent entities, users, documents, credentials, objects or anything else that can be uniquely identified. DIDs are a recognized standard within the World Wide Web Consortium (W3C) - an international community that works together to develop web standards to ensure its long-term growth. DIDs are the fundamental buildings blocks of the self-sovereign identity (SSI) ecosystem and their utility lies in their uniqueness, their provability, and their portability.

The uniqueness of DIDs prevents confusion between subjects. Conceptually, we can compare this to a government-issued identification number. For example, there might be thousands of Jane Smiths, but each one would have their own DID. Referring to them by DID rather than by name prevents cases of mistaken identity. The portability of DIDs is one of their most powerful and important features and centers around the idea that a DID is owned and controlled by the 'subject' of the DID. This means no one can delete a person's DID, and people are free to use their DIDs across different platforms and even move their DIDs and associated data from one platform to another.

More on DIDs in a future article.

Identity attributes

Identity attributes are facts and data points about an individual and/or entity that contribute to 'who they are'. The degree you earned, the school you went to, and the company you work at are all examples of identity attributes that you may want or need to share with others to prove who you are or to prove something about you. They are attestations to a given fact or set of facts.

Proof of Humanity (PoH)

The most essential identity attribute is one that proves that you are, in fact, a person. In an increasingly online-based world, where physical in-person interaction is often non-existent, bots and scam accounts create significant risks for people and online service providers. PoH is an Ethereum-based social identity verification system that uses various protections to authenticate a person during enrolment. PoH enables users to prove that there is a live, real human linked to a specific public Ethereum address. This proof can then be used to open online accounts, to vote or to join an online community.

Following a photo upload and video verification, a person will need to be vouched for by another human that has already been registered with PoH. This provides a strong web of trust to this identity verification framework and adds to one's set of identity attributes, by enabling them to prove that they are real.

Soulbound tokens (SBT)

Proposed by Ethereum founder Vitalik Buterin, SBTs represent a person's digital identity attributes on-chain. SBTs are encompassed within the Ethereum Request for Comment (ERC) 5114, Ethereum Improvement Proposal (EIP) 4974, and several others. SBTs are a permanent, non-transferable form of a non-fungible token (NFT) that can be seen as an evolution of POAPs (see section below).

Entities and individuals, referred to as 'souls', can use their Ethereum-enabled wallets to hold and view their SBTs. The SBT could represent a fact about an individual, such as a person's degree or their professional certification. A collection of these tokens, issued by different institutions and individuals, would form a publicly-verified, on-chain identity of a user. Once a SBT is issued to the wallet of a soul, the SBT is bound to that wallet and represents an attribute linked to the soul controlling that wallet. Unlike verifiable credentials covered in the below section, SBTs are public in nature and can be viewed by anyone.

Verifiable credentials (VCs)

VCs are a W3C data model for representing identity credentials (a.k.a. attestations or claims) that can be shared at the holder's discretion. VCs are a set of claims made by one entity (the issuer) about another (the identity holder). A third party can verify these claims because the issuer has digitally signed the VC, proving its authenticity.

Claims can range from the holder's name, address and age, to qualifications they have obtained and their memberships in different organizations. It is important to note that these claims could be held in a person's off-chain wallet; therefore, unlike with SBTs, these claims do not have to be publicly viewable.

VCs are gaining traction in Europe, especially at a governmental level. European Blockchain Services Infrastructure (EBSI) is an initiative of the European commission which aims to leverage the benefits of blockchain technology for identity use cases. EBSI's VC framework proposes a trust model relying on verifiable information, and also includes specifications for expressing, exchanging, and verifying credentials.

A comparison of VCs and SBTs

VCs and SBTs aim to solve similar problem sets and use cases. We provide below a more comprehensive comparison between the two.

Characteristic	VCs	SBTs
Storage of Claims	Off-chain or on-chain	On-chain
Privacy	Yes, selective disclosure	No, anyone can view anyone else's credentials
Revocability	Yes	Yes
Technological Standardization	W3C data model v1.1	ERC-5114 and EIP-4974
Interoperability	Yes, across chains or off-chain	No, permanently linked on-chain
Governance Frameworks	Yes	No
Issuer(s)	Anyone	Anyone

Although there are various similarities and differences between VCs and SBTs, it is especially important to consider privacy, control and scalability when determining whether to use VCs or SBTs to capture identity attributes.

Privacy & Control: VCs allow for greater privacy because claims are stored off-chain, keeping personal data private. VC holders can also choose the claim (or part of a claim) they wish to present to another party. Conversely, SBTs are visible on a public blockchain, making information about holders readily available at all times, with the holder having no control over what they share with others. With VCs, a person or organization wishing to receive a VC is in control of doing so – they

can request for a VC to be issued to them. Conversely, anyone can 'issue' a SBT to anyone else, making it possible to spam a person's wallet with SBTs that they don't want or don't want associated with them. The choice between the two involves a trade-off between privacy/control and simplicity.

Scalability: Whereas SBTs are stored on a blockchain, VCs do not have to be blockchain-based. It is possible to hold credential information off-chain under the W3C standard. Further, VCs are technology and chain agnostic, meaning a VC could be used across Web2 domains or across different blockchains. SBTs are naturally blockchain focused and thus would be issued on a specific chain. Whilst a given SBT could technically be issued on many blockchains, doing so creates challenges around data consistency across platforms. There are also costs associated with minting and updating those SBTs.

SBTs and VCs both enable users to add identity attributes to their digital identity. Each have their own benefits and may be more applicable to some use cases over others.

Reputation

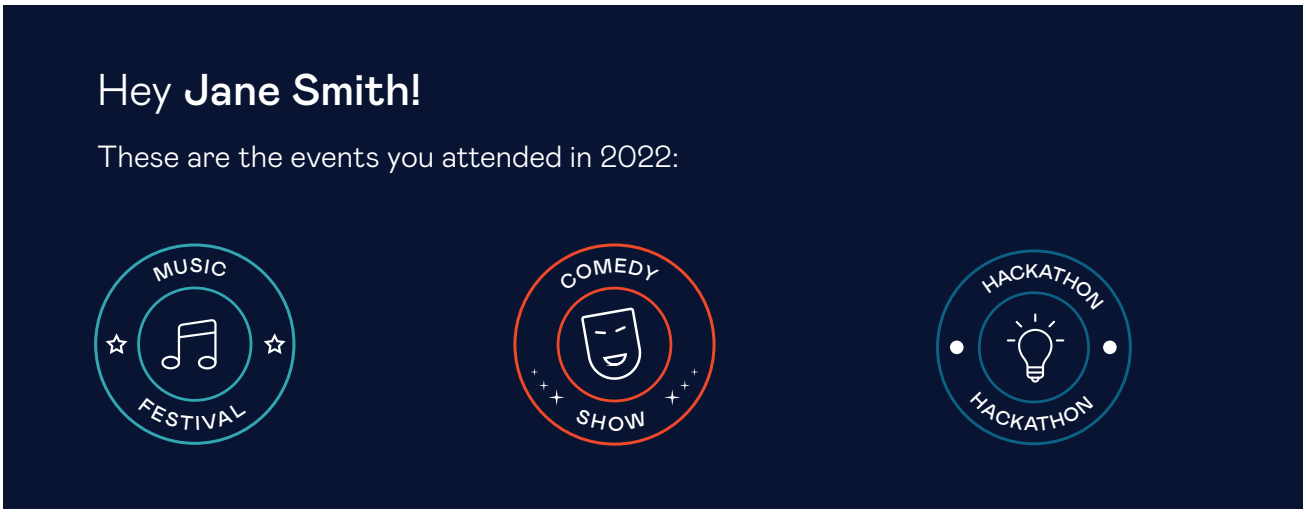
Another key factor in what makes us who we are is our standing in the world. A person's online persona, the number of Twitter followers they have - the conferences they have attended, the fact that they were early adopters of some trend - all contribute to a person's reputation and digital identity.

Proof of Attendance Protocol (POAP)

The POAP is one protocol that is commonly used within the Ethereum ecosystem to build an online reputation. It is specifically focused on creating a historical record of a person's contributions to projects or attendance at events by enabling people to capture their virtual and in-person experiences in the form of NFTs, known as POAPs.

POAPs are popular at many conferences, with POAP stations activated throughout for users to 'mint' and receive a POAP badge to commemorate their experience, akin to collecting used ticket stubs. POAPs can also be awarded to attendees in digital spaces for attending a Twitter space talk, being a Discord member, contributing to a DAO (Decentralized Autonomous Organization), attending a Metaverse concert and more. The amalgamation of these 'certificates' contribute to a person's reputation and standing in their community.

POAPs are built using the ERC-721 NFT standard, which means they are portable, immutable and transferable in nature. Some may argue that the transferability of a POAP may result in it losing its essence, as it may be sold to the highest bidder. Nevertheless, POAPs are a powerful tool for individuals to collect memorabilia in their wallet and further showcase aspects of their digital identity.

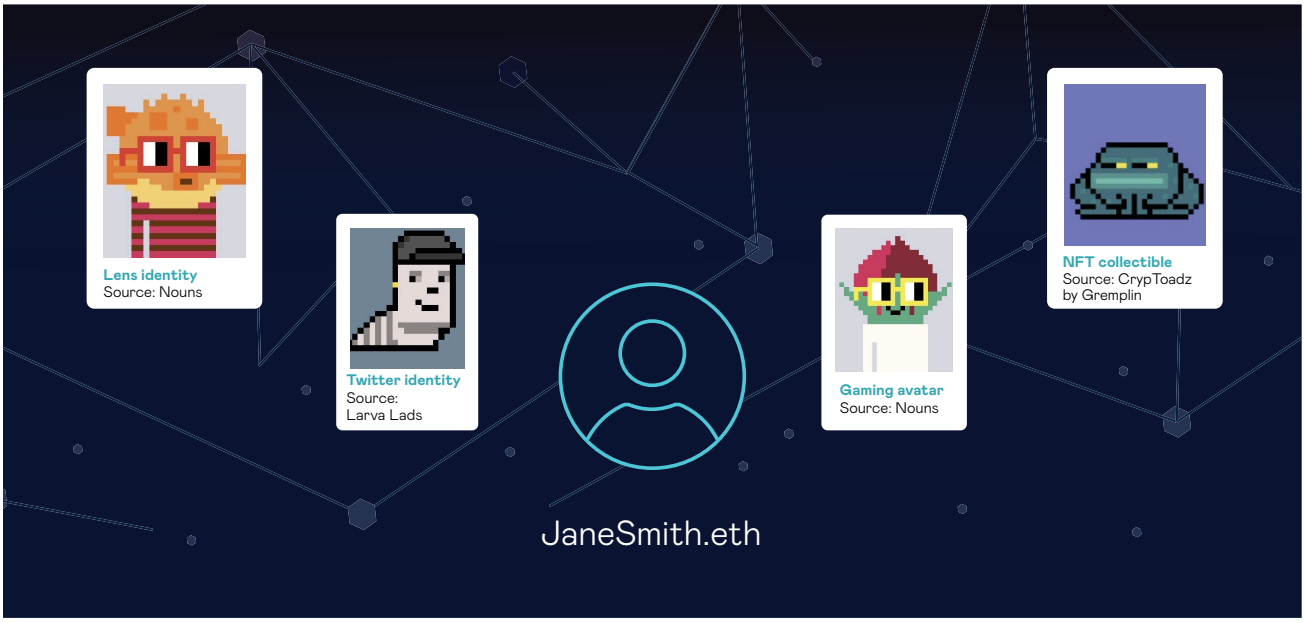


Digital collectibles and assets

Traditionally, people express who they are through the brands they wear, the cars they own, and associations they are part of.

In an increasingly digital world, people can express who they are through their digital collectibles – the items they collect and own online. NFTs are types of digital collectibles that are unique in nature and can represent digital or real-world items.

In the Ethereum ecosystem, NFTs are built using the ERC-721 and ERC-1155 standards and can be owned and viewed in an individual's wallet. Owning NFTs is a reflection of the individual's interests, and contributes to their unique digital identity. For instance, JaneSmith.eth may hold a variety of NFTs in her wallet, including digital art, in-game items, membership NFTs and PFPs (profile pictures). The types of NFTs Jane has in her wallet may serve as representations of her interests and passions and therefore portray part of her digital identity.



Digital identity wallets – bringing it all together

Each of the digital identity building blocks discussed above has its individual strengths and challenges. There is no one-size-fits-all. Instead, these building blocks work best in conjunction with one another to form a holistic identity. However, a common enabler for all four building blocks is the digital identity wallet. These wallets are the 'portal' where one can link their ENS to their public address, hold their digital collectibles, and view their POAPs, SBTs and VCs.

Some digital identity wallets also enable the creation and registration of one's DID, enabling users to also claim and share their VCs from their wallet. Wallets are the access point that enable users to start building their digital identity. In order to gain scale and adoption, it is critical that digital identity wallets are easy to use and have low barriers to entry.

Innovations such as Account Abstraction (ERC-4337) may help mitigate some of the challenges experienced when setting up a wallet. Additionally, identity applications such as disco.xyz, creds.xyz or mintkudos.xyz help make it easier for users to manage and view their VCs and SBTs in their wallets.

How Onyx has experimented with decentralized digital identity

Over the past few years, we have seen tremendous growth in the digital identity space. The above digital identity building blocks will contribute to the shift from centralized systems and honeypots of data to an era of self-expression and autonomous ownership of our own data and digital identities.

Since the beginning of our exploration into the decentralized identity space in 2017, Onyx has built concept solutions for a number of use cases that benefit from the ideas of digital identity. These range from Supplier Onboarding, VCs for document signing, issuance of verifiable legal entity identifiers (VLEIs) and most recently, Project Guardian.

As part of Project Guardian Phase 1 – a joint initiative between the Monetary Authority of Singapore, Onyx by J.P. Morgan, DBS, and SBI Digital Asset Holdings (SBI) – we explored how digital identity can be used to enable financial institutions to safely gain access to DeFi protocols on public blockchain networks. In the project, Onyx created a VC-based digital identity solution and institutional wallet that enabled traders from J.P. Morgan and SBI to execute trades on the AAVE protocol in a way that allowed them to prove aspects of their identities whilst still preserving privacy. A trader's identity attributes, represented using VCs, were 'attached' to trade instructions at the time of placing a trade. The identity attributes were then verified in real-time, on-chain, and used to determine whether the trader was actually authorized to trade on behalf of their institution or not. We showed how utilizing systems with real-time identification verification, without the reliance on large honeypots of personal data, could reduce the risk of fraud, and simplify the process of identification across applications.

While Onyx has experimented primarily with VC and DID technology, we remain open to exploring other methodologies should they be the best fit for a given use case. The digital identity space is rapidly evolving, and individuals and companies are invited to collaborate, join the community and work together towards the greater good.

This article is part of a series on digital identity.

VISIT US AT JPMORGAN.COM/DIGITALIDENTITY →

By Tyrone Lobban, Head of Blockchain Launch and Onyx Digital Assets, Onyx by J.P. Morgan and George Kassis, Vice President, Digital Identity Lead, Blockchain Launch, Onyx by J.P. Morgan

1 European Digital Identity. Retrieved April 3, 2023, from https://commission.europa.eu/strategyandpolicy/priorities20192024/europefitdigitalage/europeandigitalidentity_en