# Enabling Digital Business with Decentralized Identity

Create seamless, accessible, and verifiable ecosystems with decentralized identity solutions

Whitepaper

# Abstract

Digital Identity is critical in enabling businesses and organizations to interact with the billions of users who are increasingly active in our massively expanding digital climate. Individuals, who have multiple and layered digital identities and passwords across uncountable governmental agencies, banks, and online platforms, need a solution to simplify and streamline their Digital Identity. Businesses need higher efficiency and security, as well as an accurate, time-saving, and secure method of user authentication.

Current identity management systems are rife with problematic issues. The foremost being the vast network of fragmented systems with its bits and pieces of identities scattered amongst multiple sources of truth that run as silos owned by providers. The user's data and information is thus controlled by entities with traditionally weak usernames and passwords that could potentially attract honeypot systems that mine identity data.

Traditional identity systems are costly by their very nature, increasingly redundant and security-deprived, hindering the user experience and the ability for businesses or agencies to service them safely and effectively. Other blockchain-based digital identity platforms may already be using blockchain on the server-side, but the actual identity information is stored on each user's phone and not on the blockchain which makes it susceptible to data extraction by third parties using traditional methodologies and tools.

"Decentralized identity" puts consumers back in control of their personal information while businesses gain trust that consumer information shared with them is accurate and pertains to the person they are transacting with, thus decreasing fraud. Decentralized identity solutions help users, amongst other things, to control their digital identity without the input of intermediaries. As well as the individual user benefits, decentralized identity solutions have the potential to create seamless, accessible, and verifiable ecosystems. Decentralized identity holds the potential to solve many issues across the DeFi sphere and more.

The current identity environment prohibits a holistic view of a user's identity as credentials and takes away the control of their own digital identity. One user alone may have twenty or more identities, digital and non-digital, from their driver's license and insurance card, to multiple social media profiles and online retail and government accounts. None of these digital identities are fully owned and controlled by the user. The myriad of so-called user handles (or user IDs) that can be bound to a single user's identity have grown exponentially to the point that mass insecurity and an overwhelming level of inconvenience are standard.

> "Imagine a world where you are in direct control of your personal information; a world where you can limit and control how much information you share while retaining the ability to transact in the world. This is self-sovereign identity, and it is already here. Blockchain is the underlying technology paving the path to self-sovereign identity through decentralized networks. It ensures privacy and trust, where transactions are secure, authenticated and verifiable and endorsed by relevant, permissioned participants."
>
> **Source:** Techcrunch

## What is Decentralized Identity

Decentralized identity, often used interchangeably with "self-sovereign identity" (SSI), is a new approach where a user is in control of their own identity.

Decentralized identity is an approach to identity and access management (IAM) that seeks ways to allow individuals to manage their own personally identifiable information (PII) instead of using a central authority. Privacy and Security are key to a decentralized identity and are fundamental components of the architecture.

A user is able to generate and create their own digital identity without depending on a specific service provider. Central to the concept of a "Decentralized Identity" is a "Digital Identity Wallet". With this digital version of a traditional wallet,  a user can store their digital identity credentials in their digital identity wallet and produce proof of identity or share PII to a third party from this identity wallet. The wallet helps users give and revoke access to identity information from a single source, making it easier.

## How it Works

Decentralized identity requires a distributed ledger that provides the framework for identities to be managed. The setup of decentralized identity with the ledger typically consists of the following elements:

### Identity Wallet

Central to the solution is an Identity Vault. The vault contains all the user digital identity footprint. The identity data captured in the vault is then issued to 3rd party companies.

### Level of Assurance

Having a central identity vault does not solve the complex challenge of verifying a user. In a decentralized network trusting the user identity and ensuring that a right level of assurance is available is key. To ensure that the right level of assurance is present, our solution captures the NIST Level of Assurance and this in fact is central to the Identity Vault.

#### Subject

A user who creates their decentralized identity using the identity wallet.

#### Issuer/Verifier

The person who issues and verifies the identity information. They sign the transaction with their private key.

#### Service Providers

Applications that accept the authentication using the decentralized identity and access blockchain/distributed ledger to look for the DID that user shared.

#### Blockchain/Distributed Ledger

A decentralized and distributed ledger that provides the mechanism and features for DIDs and functioning.

#### DID (Decentralized Identifier)

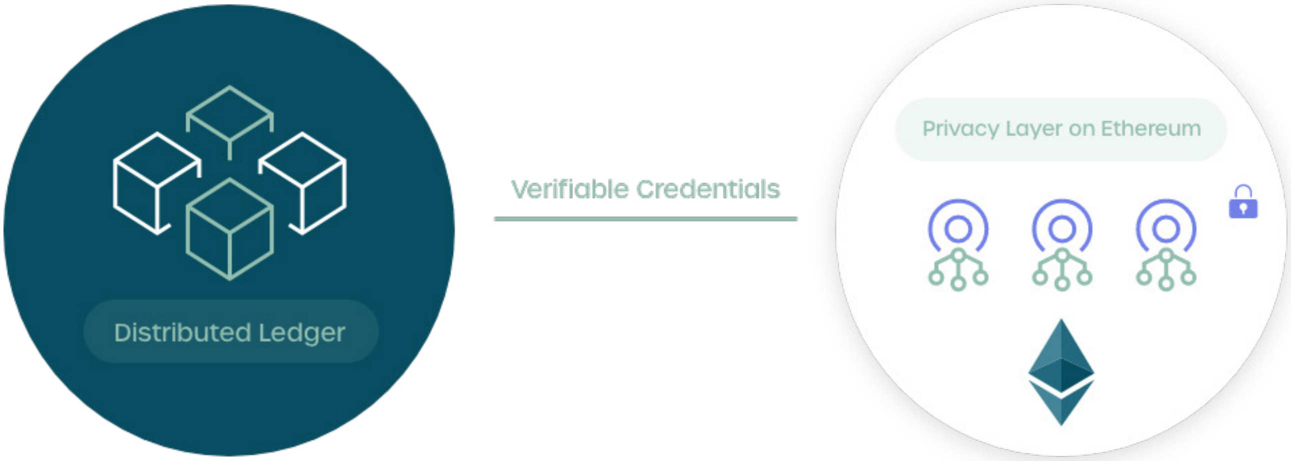
A globally unique identifier that contains details such as the public key, verification information, and service endpoints.

**The process for identity verification starts with the user being able to scan their government/institution-issued identity that is scanned by the user which is then verified and validated by third party services. In the 1Kosmos platform, a user is allowed to scan their government-issued identity which is then verified and validated with the user's biometrics and third-party sources like AAMVA.**

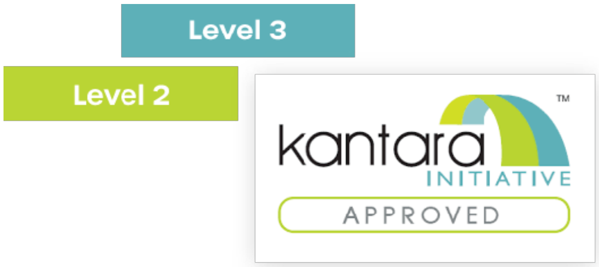
The Key to any identity data that needs to be captured is the proofing and verification of that identity. Having a central identity vault does not solve the complex challenge of verifying a user. In a decentralized network trusting the user identity and ensuring that a right level of assurance is available is key.

In a decentralized identity architecture, an application allows users to create their own digital identity where public-private key pairs are generated. In the 1Kosmos, implementation of decentralized identity, the private key is generated and stored on the secure enclave of the user's device i.e. smartphone or laptop. The digital identity wallet submits a registration payload with a public key to the blockchain, which generates a unique identifier against your wallet. The private key remains with the user's device/identity wallet and is used during the authentication and validation.

Similarly, issuers such as the government, universities, and finance institutions verify the respective identity information and add to the digital identity data in a process that is like issuing certificates. The processes, for example, verifying user identity and issuing new credentials, require issuers to sign using their private keys.



To ensure that the right level of assurance is present, our solution captures the NIST 800-63-3 Level of Assurance and this in fact is central to the Identity Vault. 1Kosmos is in fact certified by NIST to provide the right level of assurance for every identity that is proofed and verified.



## How to Authenticate Using Decentralized Identity

One additional advantage of a decentralized identity is that it removes the friction of credentials and uses biometrics for authentication. The authentication model, in this case, is to use biometrics instead of the standard username and password. These are the steps of authentication using decentralized identity and blockchain.

- The identity wallet holds verified identity details of the user such as name, age, address, education, employment details, and financial information. This information helps establish trust and makes the user eligible to perform authentication.
- The decentralized identity mechanism takes the public key associated with the private key and publishes it onto a distributed ledger such as blockchain.
- As the decentralized system provides the public key to the distributed ledger, the identity wallet receives a decentralized identifier (DID). DID is a unique identifier representing the user across the internet.
- The user shares this DID with the service provider for authentication.
- The service provider looks for the shared DID in the distributed ledger. If found, distributed ledger sends matching data to the application.
- The user signs this transaction with the private key to complete the authentication.
- The service provider application confirms the authentication success and lets the user perform the actions.

The benefits of having a user verify their documents using biometrics is that these biometrics can then also be used to authenticate the user across a variety of different services. A user can be verified while registering for access and this verification can be done based on the NIST 800-63-3 standard for identity verification. This allows an identity assurance level to be assigned to a user which adds more context behind the identity of a user and every authentication event.

This capability fundamentally changes authentication. Because now, a user can prove who they are and, as a result, will no longer need a username and password to try to prove identity.

Instead, users will provide their biometrics, which is kept in the distributed identity wallet, to login in to the service. By providing an authentication method in this manner, organizations will have a high assurance of who is on the other side of the digital connection and an immutable audit trail if needed. For more details on how this authentication works, please refer to our Zero Trust Whitepaper available here.

## About the 1Kosmos Approach to Decentralized Authentication and Identity Management

At 1Kosmos we believe that secure, private blockchain technology is critical to users' modern authentication and self-sovereign identities. Our identity management removes the central repositories and databases that attract so many hackers while giving identity control back to the owners of those identities—all without sacrificing usability or effectiveness.

1Kosmos brings decentralized identity to modern authentication with a core set of features, including the following:

### Private Blockchain

1Kosmos protects personally identifiable information (PII) in a private blockchain for an identity management approach and encrypts digital identities in secure enclaves only accessible through advanced biometric verification. Our ledger is immutable, secure, and private, so there are no databases to breach or honeypots for hackers to target.

### Identity Proofing

1Kosmos is certified to provide Identity Assurance Level 2 (NIST 800-63A IAL2), detects fraudulent or duplicate identities, and establishes or reestablishes credential verification.

### Integration with Secure MFA

1Kosmos and its distributed ledger readily integrate with a standard-based API to operating systems, applications, and MFA infrastructure and is FIDO2 certified at AAL2, protecting against attacks that attempt to circumvent multi-factor authentication.

### Streamlined User Experience

The distributed ledger makes it easier for users to onboard digital IDs. It's as simple as installing the app, providing biometric information and any required proofing documents, and entering any information required under ID creation. The blockchain allows users more control over their digital ID while making authentication more straightforward.

**About 1Kosmos**
1Kosmos enables remote identity verification and passwordless multi-factor authentication for workers, customers and residents to securely transact with digital services. By unifying identity proofing, credential verification and strong authentication, the 1Kosmos platform prevents identity impersonation, account takeover and fraud while delivering frictionless user experiences and preserving the privacy of users' personal information. 1Kosmos performs millions of authentications daily for government agencies and some of the largest banks, telecommunications, higher education, and healthcare organizations in the world.

1KOSMOS