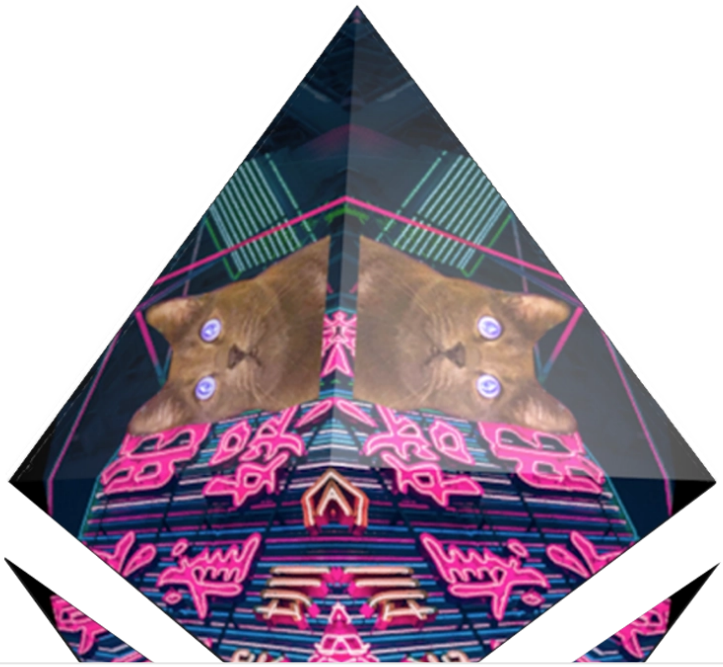

Decentralized identity

- Traditional identity systems have centralized the issuance, maintenance and control of your
- Thanks to crypto, users now have the tools to issue, hold and control their own identifiers and attestations once again.

On this page

Identity underpins virtually every aspect of your life today. Using online services, opening a bank account, voting in elections, buying property, securing employment—all of these things require proving your identity.

However, traditional identity management systems have long relied on centralized intermediaries who issue, hold, and control your identifiers and attestations. This means you cannot control your identity-related information or decide who has access to personally identifiable information (PII) and how much access these parties have.

To solve these problems, we have decentralized identity systems built on public blockchains like Ethereum. Decentralized identity allows individuals to manage their identity-related information. With decentralized identity solutions, *you* can create identifiers and claim and hold your attestations without relying on central authorities, like service providers or governments.

What is identity?

Identity means an individual's sense of self, defined by unique characteristics. Identity refers to being an *individual*, i.e., a distinct human entity. Identity could also refer to other non-human entities, such as an organization or authority.

≡ Ethereum use cases

Common identifiers include:

- Name
- Social security number/tax ID number
- Mobile number
- Date and place of birth
- Digital identification credentials, e.g., email addresses, usernames, avatars

These traditional examples of identifiers are issued, held and controlled by central entities. You need permission from your government to change your name or from a social media platform to change your handle.

What are attestations?

An attestation is a claim made by one entity about another entity. If you live in the United States, the driver's license issued to you by the Department of Motor Vehicles (one entity) attests that you (another entity) are legally allowed to drive a car.

Attestations are different from identifiers. An attestation *contains* identifiers to reference a particular identity, and makes a claim about an attribute related to this identity. So, your driver's license has identifiers (name, date of birth, address) but is also the attestation about your legal right to drive.

What are decentralized identifiers?

Traditional identifiers like your legal name or email address rely on third parties—governments and email providers. Decentralized identifiers (DIDs) are different—they aren't issued, managed, or controlled by any central entity.

Decentralized identifiers are issued, held, and controlled by individuals. An Ethereum account is an example of a decentralized identifier. You can create as many accounts as you want without permission from anyone and without the need to store them in a central registry.

Decentralized identifiers are stored on distributed ledgers (blockchains) or peer-to-peer networks. This makes DIDs globally unique, resolvable with high availability, and cryptographically verifiable ↗ . A decentralized identifier can be associated with different entities, including people, organizations, or government institutions.

What makes decentralized identifiers possible?

1. Public Key Infrastructure (PKI)

Public-key infrastructure (PKI) is an information security measure that generates a public key and private key for an entity. Public-key cryptography is used in blockchain networks to authenticate user identities and prove ownership of digital assets.

Some decentralized identifiers, such as an Ethereum account, have public and private keys. The public key identifies the account's controller, while the private keys can sign and decrypt messages for this account. PKI provides proofs needed to authenticate entities and prevent impersonation and use of fake identities, using cryptographic signatures ↗ to verify all claims.

2. Decentralized datastores

A blockchain serves as a verifiable data registry: an open, trustless, and decentralized repository of information. The existence of public blockchains eliminates the need to store identifiers in centralized registries.

If anyone needs to confirm the validity of a decentralized identifier, they can look up the associated public key on the blockchain. This is different from traditional identifiers that require third parties to authenticate.

How do decentralized identifiers and attestations enable decentralized identity?

Decentralized identity is the idea that identity-related information should be self-controlled, private, and portable, with decentralized identifiers and attestations being the primary building blocks.

In the context of decentralized identity, attestations (also known as Verifiable Credentials ↗) are tamper-proof, cryptographically verifiable claims made by the issuer. Every attestation or Verifiable Credential an entity (e.g., an organization) issues is associated with their DID.

Because DIDs are stored on the blockchain, anyone can verify the validity of an attestation by cross-checking the issuer's DID on Ethereum. Essentially, the Ethereum blockchain acts like a

global directory that enables the verification of DIDs associated with certain entities.

Decentralized identifiers are the reason attestations are self-controlled and verifiable. Even if the issuer doesn't exist anymore, the holder always has proof of the attestation's provenance and validity.

Decentralized identifiers are also crucial to protecting the privacy of personal information through decentralized identity. For instance, if an individual submits proof of an attestation (a driver's license), the verifying party doesn't need to check the validity of information in the proof. Instead, the verifier only needs cryptographic guarantees of the attestation's authenticity and the identity of the issuing organization to determine if the proof is valid.

Types of attestations in decentralized identity

How attestation information is stored and retrieved in an Ethereum-based identity ecosystem is different from traditional identity management. Here is an overview of the various approaches to issuing, storing, and verifying attestations in decentralized identity systems:

Off-chain attestations

One concern with storing attestations on-chain is that they might contain information individuals want to keep private. The public nature of the Ethereum blockchain makes it unattractive to store such attestations.

The solution is to issue attestations, held by users off-chain in digital wallets, but signed with the issuer's DID stored on-chain. These attestations are encoded as JSON Web Tokens↗ and contain the issuer's digital signature—which allows for easy verification of off-chain claims.

Here's an hypothetical scenario to explain off-chain attestations:

1. A university (the issuer) generates an attestation (a digital academic certificate), signs with its keys, and issues it to Bob (the identity owner).

2. Bob applies for a job and wants to prove his academic qualifications to an employer, so he shares the attestation from his mobile wallet. The company (the verifier) can then confirm the validity of the attestation by checking the issuer's DID (i.e., its public key on Ethereum).

Off-chain attestations with persistent access

Under this arrangement attestations are transformed into JSON files and stored off-chain (ideally on a decentralized cloud storage platform, such as IPFS or Swarm). However, a hash of the JSON file is stored on-chain and linked to a DID via an on-chain registry. The associated DID could either be that of the issuer of the attestation or the recipient.

This approach enables attestations to gain blockchain-based persistence, while keeping claims information encrypted and verifiable. It also allows for selective disclosure since the holder of the private key can decrypt the information.

On-chain attestations

On-chain attestations are held in smart contracts on the Ethereum blockchain. The smart contract (acting as a registry) will map an attestation to a corresponding on-chain decentralized identifier (a public key).

Here's an example to show how on-chain attestations might work in practice:

1. A company (XYZ Corp) plans to sell ownership shares using a smart contract but only wants buyers that have completed a background check.

2. XYZ Corp can have the company performing background checks to issue on-chain attestations on Ethereum. This attestation certifies that an individual has passed the background check without exposing any personal information.

3. The smart contract selling shares can check the registry contract for the identities of screened buyers, making it possible for the smart contract to determine who is permitted to buy shares or not.

Soulbound tokens and identity

Soulbound tokens↗ (non-transferable NFTs) could be used to collect information unique to a specific wallet. This effectively creates a unique on-chain identity bound to a particular Ethereum address that could include tokens representing achievements (e.g. finishing some specific online course or passing a threshold score in a game) or community participation.

Benefits of decentralized identity

1. Decentralized identity increases individual control of identifying information. Decentralized identifiers and attestations can be verified without relying on centralized authorities and third-party services.

2. Decentralized identity solutions facilitates a trustless, seamless, and privacy-protecting method for verifying and managing user identity.

3. Decentralized identity harnesses blockchain technology, which creates trust between different parties and provides cryptographic guarantees to prove the validity of attestations.

4. Decentralized identity makes identity data portable. Users store attestations and identifiers in mobile wallet and can share with any party of their choice. Decentralized identifiers and attestations are not locked into the database of the issuing organization.

5. Decentralized identity should work well with emerging zero-knowledge technologies that will enable individuals to prove they own or have done something without revealing what that thing is. This could become a powerful way to combine trust and privacy for applications such as voting.

6. Decentralized identity enables anti-Sybil mechanisms to identify when one individual human is pretending to be multiple humans to game or spam some system.

Decentralized identity use-cases

Decentralized identity has many potential use-cases:

1. Universal logins

Decentralized identity can help replace password-based logins with decentralized authentication↗ . Service providers can issue attestations to users, which can be stored in an Ethereum wallet. An example attestation would be an NFT granting the holder access to an online community.

A Sign-In with Ethereum↗ function would then enable servers to confirm the user's Ethereum account and fetch the required attestation from their account address. This means users can access platforms and websites without having to memorize long passwords and improves the online experience for users.

2. KYC authentication

Using many online services requires individuals to provide attestations and credentials, such as a driving license or national passport. But this approach is problematic because private user information can be compromised and service providers cannot verify the authenticity of the attestation.

Decentralized identity allows companies to skip on conventional Know-Your-Customer (KYC)↗ processes and authenticate user identities via Verifiable Credentials. This reduces the cost of identity management and prevents the use of fake documentation.

3. Voting and online communities

Online voting and social media are two novel applications for decentralized identity. Online voting schemes are susceptible to manipulation, especially if malicious actors create false identities to vote. Asking individuals to present on-chain attestations can improve the integrity of online voting processes.

Decentralized identity can help create online communities that are free of fake accounts. For example, each user might have to authenticate their identity using an on-chain identity system, like the Ethereum Name Service, reducing the possibility of bots.

4. Anti-Sybil protection

Sybil attacks refer to individual humans tricking a system into thinking they are multiple people to increase their influence. Grant-giving applications↗ that use quadratic voting↗ are vulnerable to these Sybil attacks because the value of a grant is increased when more individuals vote for it, incentivizing users to split their contributions across many identities. Decentralized identities help to prevent this by raising the burden on each participant to prove that they are really human, although often without having to reveal specific private information.

Use decentralized identity

There are many ambitious projects using Ethereum as a foundation for decentralized identity solutions:

- **Ethereum Name Service (ENS)↗** *- A decentralized naming system for on-chain, machine-readable identifiers, like, Ethereum wallet addresses, content hashes, and metadata.*
- **SpruceID↗** *- A decentralized identity project which allows users to control digital identity with Ethereum accounts and ENS profiles instead of relying on third-party services.*
- **Proof of Humanity↗** *- Proof of Humanity (or PoH) is a social identity verification system built on Ethereum.*

- **BrightID** - *A decentralized, open-source social identity network seeking to reform identity verification through the creation and analysis of a social graph.*
- **Proof-of-personhood Passport** - *A decentralized digital identity aggregator.*

Further reading

Articles

- Blockchain Use Cases: Blockchain in Digital Identity — *ConsenSys*
- What is Ethereum ERC725? Self-Sovereign Identity Management on the Blockchain — *Sam Town*
- How Blockchain Could Solve the Problem of Digital Identity — *Andrew R. Chow*
- What Is Decentralized Identity And Why Should You Care? — *Emmanuel Awosika*

Videos

- Decentralized Identity (Bonus Livestream Session) — *A great explainer video on decentralized identity by Andreas Antonopolous*
- Sign In with Ethereum and Decentralized Identity with Ceramic, IDX, React, and 3ID Connect — *YouTube tutorial on building out an identity management system for creating, reading, and updating a user's profile using their Ethereum wallet by Nader Dabit*
- BrightID - Decentralized Identity on Ethereum — *Bankless podcast episode discussing BrightID, a decentralized identity solution for Ethereum*
- The Off Chain Internet: Decentralized Identity & Verifiable Credentials — EthDenver 2022 presentation by Evin McMullen

Communities

- ERC-725 Alliance on GitHub ↗ — *Supporters of the ERC725 standard for managing identity on the Ethereum blockchain*
- SpruceID Discord server ↗ — *Community for enthusiasts and developers working on Sign-in with Ethereum*
- Veramo Labs ↗ — *A community of developers contributing to building a framework for verifiable data for applications*

Was this page helpful?

Yes No

Website last updated: March 11, 2023

Use Ethereum

Find wallet

Get ETH

Decentralized applications (dapps)

Layer 2

Run a node

Stablecoins

Stake ETH

Learn

What is Ethereum?

What is ether (ETH)?

Ethereum wallets

Community guides and resources

History of Ethereum

Ethereum Whitepaper

Ethereum roadmap

Ethereum security and scam prevention

Ethereum glossary

Ethereum governance

Blockchain bridges

Zero-knowledge proofs

Ethereum energy consumption

What is Web3?

Ethereum Improvement Proposals

Developers

Get started

Documentation

Tutorials

Learn by coding

Set up local environment

Ecosystem

Community hub

Ethereum Foundation

Ethereum Foundation Blog ↗

Ecosystem Support Program ↗

Ethereum bug bounty program

Ecosystem Grant Programs

Ethereum brand assets

Devcon ↗

Enterprise

Mainnet Ethereum

Private Ethereum

Enterprise

About ethereum.org

About us

Jobs

Contributing

Language support

Privacy policy

Terms of use

Cookie policy

Contact ↗