The Basics of Decentralized Identity (DID) and Self-Sovereign Identity (SSI)

The Basics of Decentralized Identity (DID) and Self-Sovereign Identity (SSI)

The layman's guide to understanding decentralized identity (DID),

self-sovereign identity (SSI) and web3 blockchain identity.

By Memdeklaro | May 15, 2026

Introduction

Decentralized identity (DID) is an emerging technology which aims to give people control over their personal data, choosing what they disclose and to whom they disclose it.

Under the umbrella of digital identity, self-sovereign identity and web3 identity, decentralized identity focuses on private and secure ways to store, manage and verify attestations and credentials in a digital manner.

In general, decentralized identity is a move away from centralized databases, information silos and single points of failure. Many DID implementations aim to be robust, interoperable and universal across many domains such as education, employment, health and finance.

The Basics: Public Key Cryptography

The foundation of many DID/SSI implementations is public key cryptography, sometimes called a keyring or wallet.

In public key cryptography, the user generates a very large random number which serves as their private key, and from that number, computes a public key. The private key remains secret like a password, and the public key can be shared with others like a username.

After the user generates their keypair, they can sign and encrypt messages. Signatures provide unforgeable proof of ownership or provenance, and encryption provides unbeatable privacy. The secret private key is used to decrypt messages and generate signatures, while the shareable public key is used to encrypt messages and verify

signatures.

The same technology is used in encrypted messengers, federated social networks and cryptocurrency wallets, where it is often known as web3 identity or blockchain identity.

The Use Case: Decentralized Credentials and Logins

After the user generates their cryptographic keypair, they can now associate attestations and credentials to their public key and store these attestations in their wallet, for example, their name or birth date, college degree or association membership. Users can choose which information they wish to link, and some implementations support pseudonymity.

Some DID frameworks may use a blockchain which provides a tamperproof public record, while other frameworks may store the attestations privately on the user's device, use decentralized storage such as IPFS, or use a web API.

Additionally, some implementations incorporate zero-knowledge proofs, which increases privacy by allowing a claim to be verified without sharing personal information. An example would be proving that you are over 18 without disclosing your exact birth date or photograph.

Attestations can be issued and signed by the private key of a trusted authority (such as a diploma or employee badge) or self-asserted and signed by the user themselves (such as a name or bio). These are known as verifiable credentials. For example, a college issues a digital degree or a library issues a digital library card. An example of a self-asserted credential, also known as a self-issued credential, is the Memdeklaro self-declaration of identity.

The signatures of these credentials can then be verified using the issuer's public key, proving that the credential is legitimate. This provides a secure way to verify credentials without requiring

paperwork, phone calls or proprietary APIs.

Physical documents, such as a diploma, membership card or NFC badge, continue to be valid and widely used. Decentralized identity is simply an optional alternative which can reduce paperwork, save time, and in the case of zero-knowledge proofs, improve privacy.

DID protocols can also be used to login to a service without needing a separate username and password, for example, using a web3 wallet to send and receive cryptocurrencies, using a certificate from your employer to login to the company network, or using a digital identity wallet to access your health records or schedule an appointment.

Instead of entering a password, you generate a signature using your private key, and the service verifies the signature using your public key. This can be more secure than password authentication, because the private key never leaves your device and is not shared with any third parties.

A Danger: Monopolies on Credential Issuance

However, decentralized identity can be vulnerable to the problem of centralized issuers, namely a monopoly on trusted authorities who issue and sign verifiable credentials.

For a university, employer or membership, this is generally not a problem due to the plurality of issuers: There are competing educational institutions to study at, a variety of companies to work for, and many clubs or associations to join.

The primary concern is a monopoly over the root identity or base layer - the name, birth date and birth place that the credentials are bound to.

If a DID implementation strictly requires government ID as the base layer, such as a passport, birth certificate or national ID card, this

creates a monopoly which perpetuates the exclusion currently caused by traditional identity systems.

In the legacy system, the root identity is usually generated when parents register their child's birth and the state issues a birth certificate. On reaching adulthood, the person uses their birth certificate to apply for a national ID card or passport, and then uses these documents to apply for a job, open a bank account and rent an apartment.

However, this system can become a single point of failure with devastating consequences: There are cases where parents are unable to or refuse to register their child, or where the birth country does not permit the registration (such as if the parents are undocumented or unmarried), meaning that the root identity never gets issued.

As an adult, the individual has no route to register their birth independently of their birth parents, culture, religion or state bureaucracy, leaving them with no way to enter the system.

Likewise, in the case of fleeing abuse, violence or war, an individual may not have access to a birth certificate or passport and be unable to apply for a new one.

Lack of government ID currently excludes millions of people worldwide from employment, housing, healthcare, banking, contracts and more daily necessities.

If DID implementations view government documentation as the sole trusted authority for verifying a name or birth date, the decentralized aspect would be lost and the exclusion would continue.

Memdeklaro: A Solid Foundation for Self-Sovereign Identity

In comparison, the Memdeklaro project gives people the opportunity to self-declare their own base layer or root identity.

With Memdeklaro, the user can define their own name, birth date and personal ties, independently of birth parents or the country of birth - no government ID required. After generating a Memdeklaro self-declaration, the user can independently link it to their education, work experience, memberships, finances and references.

Example Self-Asserted Credential

```
{
    "@context": [
      "https://www.w3.org/ns/credentials/v2"
    ],
    "type": ["VerifiableCredential", "IDCard"],
    "issuer": {
      "id": "did:web:memdeklaro.org"
    },
    "identifier": "120777000",
    "name": "Memdeklaro ID",
    "description": "Self-Declaration of Identity",
    "validFrom": "2024-01-31T00:00:00Z",
    "validUntil": "2029-01-31T00:00:00Z",
    "credentialSubject": {
      "type": ["Person"],
      "givenName": "Paulo",
      "familyName": "Espero",
      "birthDate": "1995-01-31",
      "note": "Conscientious Objector"
    }
}
```

Memdeklaro self-asserted credentials aim to give everyone a fair foundation to build up their life, creating a world where personal beliefs and efforts are more important than arbitrary circumstances of birth, and keeping decentralized identity truly decentralized.

Note: Memdeklaro does not implement a blockchain or act as a trusted authority - rather, the user uses the public domain template to generate and assert their own self-declaration of identity, following the philosophy of freedom of identity.

If the user wishes to use Memdeklaro with a web3 wallet or DID framework, they should sign the self-declaration with their own private key as a self-signed certificate.

In addition, the Memdeklaro platform serves only to self-declare your personal identity, and does not incorporate or verify third party credentials such as education, employment, finances, contracts or references.

Conclusion

To summarize, decentralized identity (also known as self-sovereign identity) can help users to manage their credentials efficiently, speeding up authentication via cryptographic signatures and providing privacy through zero-knowledge proofs.

However, the benefits of decentralization are lost if there is a monopoly on trusted authorities, such as requiring government-issued ID as the sole method to verify a name or birth date.

Self-declarations like Memdeklaro can help to avoid lockout by providing an accessible root identity, while verifiable credentials can help to prove education, employment, memberships and more.

As development continues, DID/SSI may become a useful tool to manage accounts and credentials, while avoiding silos and improving privacy.

Tags: decentralized identity, self-sovereign identity, web3 identity, verifiable credentials, self-attested verifiable credentials, self-issued verifiable credentials, self-attested credential, self-issued credential, self-attestation

---

See also: Ultimate Guide to Non-Government ID: Memdeklaro vs. Digitalcourage vs. World Passport